Anonymous Digital Identity in e-Government

DISSERTATION
DER WIRTSCHAFTSWISSENSCHAFTLICHEN
FAKULTÄT
DER UNIVERSITÄT ZÜRICH

zur Erlangung der Würde
eines Doktors der Informatik

vorgelegt von
NIKLAS AUERBACH
aus
Deutschland

genehmigt auf Antrag von

Prof. Dr. Lutz Richter
Prof. Dr. Gerhard Schwabe

Juni 2004

Die Wirtschaftswissenschaftliche Fakultät der Universität Zürich, Lehrbereich Informatik, gestattet hierdurch die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 23. Juni 2004*

Der Lehrbereichsvorsteher: Prof. Dr. Martin Glinz

**Datum der Promotionsfeier*

Abstract

The ongoing implementation of e-government has brought many governments to consider issuing digital identity cards. This thesis focuses on the impact of digital identity cards on the citizen's privacy. Potential privacy threats are discussed and countermeasures that pertain to enhancing privacy are proposed. We advocate that digital identity should not solely be based on elements that disclose a citizens identity. Instead this thesis proposes a concept for digital identity cards that includes an anonymous component. This proposed approach is different from the approach taken by the current projects for digital identity cards. We propose a concept that comprises pseudonymous credentials as part of the citizen's digital identity. We discuss current implementations of pseudonymous credential systems and consider problems resulting from the implementation in resource-restricted smart card environments. We discuss requirements for the use of credentials as part of the citizen's digital identity. We discuss conceptual issues that must be addressed for a deployment of credentials. We consider the infrastructure that is necessary to support pseudonymous credentials. We discuss conceptual issues such as the choice of credential system, devices for the secure storage of credentials, non-transferability and revocation of digital credentials. An architecture is proposed that supports the use of the extended form of digital identity. We discuss barriers that must be overcome on the way to implementation. With the ongoing migration towards digital identity cards, we expect that privacy will become an issue of growing importance. This thesis contributes to the discussion on privacy in the domain of e-government and proposes anonymous services based on pseudonymous credentials as a means to alleviate potential privacy problems related to the use of electronic identity cards.

Zusammenfassung

Im Zuge nationaler e-Government Initiativen haben einige europäische Regierungen bereits elektronische Identitätskarten ausgegeben. Diese Dissertation befasst sich mit den Auswirkungen von digitalen Identitätskarten auf die Privatsphäre des Bürgers. Potentielle Bedrohungen für die Privatheit werden aufgezeigt und Gegenmassnahmen, die zum Schutz der Privatheit beitragen, werden vorgeschlagen. Diese Arbeit schlägt vor, dass die digitale Identität des Bürgers nicht nur aus Elementen bestehen soll, welche die Identität des Bürgers preisgeben. Stattdessen stellt diese Arbeit ein Konzept für elektronische Identitätskarten vor, das eine anonyme Komponente umfasst. Der vorgeschlagene Ansatz unterscheidet sich von den Ansätzen, die von gegenwärtigen Projekten für elektronische Identitätskarten implementiert werden. Das vorgeschlagene Konzept umfasst pseudonyme Credentials als Teil der digitalen Identität des Bürgers. Verfügbare Ansätze für pseudonyme Credential Systeme werden besprochen und Probleme diskutiert, die sich aus einer Implementation in Ressourcen-beschränkten Umgebungen wie Smart Cards ergeben. Wir besprechen Anforderungen für den Einsatz von Credentials in e-Government. Infrastrukturkomponenten, die für einen Einsatz von Credentials notwendig sind, werden diskutiert. Konzeptionelle Fragen werden besprochen, wie die Wahl eines geeigneten Credential Systems, die sichere Aufbewahrung von Credentials, Methoden für die Gewährleistung der nicht-Übertragbarkeit sowie Algorithmen für die Revokation von pseudonymen Credentials. Eine Architektur zur Umsetzung der erweiterten digitalen Identität wird vorgeschlagen. Hindernisse werden diskutiert, die auf dem Weg zur Implementation überwunden werden müssen. Durch die fortwährende Migration in Richtung elektronischer Identitätskarten erwarten wir, dass das Thema Privatheit wachsende Bedeutung erlangen wird. Diese Arbeit leistet einen wissenschaftlichen Beitrag zur Diskussion um das Thema der Privatheit im Bereich von e-Government und schlägt einen anonymen Dienstzugang als eine Massnahme vor, die mögliche negative Auswirkungen von elektronischen Identitätskarten auf die Privatheit verringern kann.

Acknowledgements

This thesis was written during my time as a research assistant at the Department of Informatics (IFI) at the University of Zurich. First and foremost, I would like to express my sincere gratitude to my thesis advisor Prof. Dr. Lutz Richter for giving me the chance to work as part of his research team, for supervising my thesis and for always having confidence in my work.

I would like to thank Prof. Dr. Gerhard Schwabe for receiving me into his research team, for his support and feedback during the writing of this thesis and for acting as a co-supervisor.

I would also like to thank Dr. Reinhard Riedl for bringing me into the e-Mayor project, for supporting my research and for acting as a co-supervisor.

I would like to express my gratitude to Dr. Jan Camenisch at the IBM Zurich Research Laboratory in Rüschlikon for numerous discussions on pseudonymous credential systems and for the willingness to establish a joint study agreement. I would especially like to thank Dr. Camenisch for providing me with a prototype of the Idemix pseudonymous credential system for use in my research.

Furthermore, I would like to thank the following people who have all contributed to this work:

- Nico Maibaum at the University of Rostock for a fruitful cooperation during and after the FASME project and for providing feedback on my research.

- Prof. Dr. Clemens H. Cap for numerous discussions on the topic of credentials and for inviting me to present my work to his research group in Rostock. I would also like to thank the members of Prof. Dr. Cap's research group as they have taken time for many productive discussions.

- András Kiraly for implementing a prototypical system for the use of credentials in Web-based service delivery as part of a diploma thesis. András Kiraly also developed a Big Integer library for the Java Card that was used for parts of my research.

- Dr. Els Van Herreweghen and Roger D. Zimmermann at IBM's Zurich Research Laboratory in Rüschlikon for fruitful discussions.
- All partners that were involved in the FASME project for interesting discussions at project meetings and workshops.
- My parents Doris and Hans-Joachim Auerbach for the proof-reading the manuscript, for motivating me throughout the writing of this thesis and for always believing in me.
- My partner Petra Baumgärtner for her patience and her support during the writing of this thesis.

Part of the work underlying this thesis has been performed as part of the FASME project (Facilitating Administrative Services for Mobile Europeans). The project has been funded by the European Commission in the Information Society Technology program under contract number IST-1999-10882.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Electronic government is a term that refers to the transformation of government in the age of the information society. From the citizen's point of view it means active, modern and more customer centered administrative processes. From a conceptual view, e-government comprises a re-engineering of administrative processes. From a technological perspective, e-government is characterized by the government's shift towards the Internet as an important service delivery platform. Some governments, among them the United Kingdom, have set targets that necessitate the electronic delivery of all services that are amenable to this form of delivery.

As part of e-government initiatives, some European countries have already issued electronic identity (e-ID) cards to their citizens. Finland was the first country in Europe to issue an electronic identity card, the Fineid card. Many other European countries are currently engaging in pilot projects for e-ID cards. Digital identity cards open new possibilities for administrative service delivery and also for private sector services.

E-ID cards provide reliable identification, authentication and digital signature services in distributed network interactions. The European Union supports numerous projects to advance the use of smart cards for digital identity. For instance, the eEurope Smart Card Charter (eESC) initiative was created in order to

> '...accelerate and harmonise the development of smart cards in Europe and to establish them in all shapes and forms as the preferred mobile and secure access key to citizen and business information society services' [eEu99].

A migration towards electronic identity cards will doubtlessly enable new functionality and bring many comfortable e-services to citizens. Despite many potential advantages of e-ID cards, there is also the question how these

cards will affect our informational privacy. After all, virtually any transaction in an electronic network leaves a permanent trace and can be traced back to a user. As digital identity cards use X.509 certificates to model the citizen's digital identity, there is the danger that such cards will leave identifying traces whenever they are used. This problem is acerbated by the fact that many e-ID cards are designed to be used in applications ranging from e-government to e-health. Furthermore, all current e-ID card initiatives follow the same concept of digital identity and digitally represent the citizen with an authentication and a signature certificate.

If the smart card is to become the preferred access key to e-services, governments need to take measures that address potential privacy threats related to e-ID technology. Already now, privacy activists in Europe are opposing e-ID card schemes and warn of the potential consequences for the citizen's privacy. Especially in the United Kingdom, citizens oppose the introduction of an electronic identity card. Opposition to the government's e-ID plans are not only motivated by the fact that the UK does not currently have a mandatory ID card but is also driven by concerns about the impact of e-ID cards on privacy.

This thesis develops a concept for an extended digital identity that comprises pseudonymous credentials as part of the citizen's digital identity. We consider privacy threats originating from multi-application digital identity cards and discuss how citizen cards can be modified in order to counter some of these privacy threats. Requirements for a credential-based digital identity are considered and conceptual issues related to the use of credentials are discussed. We design a system architecture for the use of credentials on electronic identity cards and describe the components that are necessary to support this concept for an extended digital identity.

Our concept of digital identity is aimed at a use in government to citizen (G2C) e-government transactions and also for a use in private sector transactions. We therefore do not consider applications of credential technology in government to business transactions (G2B) or in transactions within government or between several governmental authorities (G2C).

Research in the domain of e-government has not specifically targeted privacy-enhancing measures for digital citizen cards yet. Even the use of privacy-enhancing technologies in as part of e-government initiatives has hardly been given attention. Even more recent projects such as the eEpoch project, which aims to create a common technological base for European e-ID cards [eEu99], do not take into account privacy issues. This thesis thus makes an original contribution to the discussion of privacy issues in e-government by proposing a privacy-enhanced concept for a digital identity card.

1.1 Research Contributions

The contributions of this thesis are in part of a conceptual nature and in part of an analytical nature. The thesis makes the following original scientific contributions:

- The topic of privacy in e-government is only gradually becoming subject to discussion. This thesis contributes to the discussion of privacy issues in e-government and focuses on threats to informational privacy posed by digital citizen cards. We deliver an analysis of privacy threats that potentially arise from the use of multi-application digital identity cards. We present a conceptual model for privacy-enhancing measures and explore design options for e-service access in the context of available technologies. We propose the introduction of anonymous and pseudonymous transactions as a measure to alleviate privacy threats related to citizen cards.

- The main contribution of this thesis is a concept for an extended digital identity. We propose that pseudonymous credentials are included on citizen cards as an anonymous means of modelling digital identity. Incorporating technology to support anonymous transactions with citizen cards has not been subject to research in the domain of e-government yet. Current digital identity card initiatives in Europe solely base the digital identity of the citizen on X.509 certificates. These certificates reveal the identity of the holder. Our approach to digital identity cards comprises privacy-enhancing technologies as an innovative element. Furthermore, we propose identity information management as a new feature of citizen cards.

  As part of the concept, we design a system for the use of pseudonymous credentials on electronic citizen cards, identify the state of the art in pseudonymous credential systems and assess the system by Camenisch and Lysyanskaya with regard to its suitability for a use in e-government as part of the citizen's digital identity. Basic requirements for the use of credentials in e-government are identified.

This thesis also discusses conceptual issues related to the use of pseudonymous credentials in e-government. We make contributions of an analytical nature in the following areas:

- Evaluation of methods for the revocation of pseudonymous credentials. We present an analysis of algorithms with regard to the suitability for deployment in e-government solutions.

- Assessment of current devices and alternative options for the storage of pseudonymous credentials, ranging from a network-based storage to the Java iButton.
- We present measures to improve the usability of credential systems and give design guidelines for the use in e-government settings.
- We assess methods to ensure the non-transferability of credentials with regard to the use in e-government, consider options for the design of a credential namespace and propose a Credential Information Base (CIB) to heighten the usability of pseudonymous credentials for end-users.

A system architecture for credential-based service delivery is also part of the thesis. The system architecture is based on the Java 2 Enterprise Edition platform and uses Web services for the communication related to credential protocols. The architecture was prototypically implemented to demonstrate that pseudonymous credentials can be seamlessly integrated into Web-based service delivery [Kir03a].

1.2 Structure of the Thesis

As a guideline to the reader, we briefly outline the structure of the thesis. The thesis comprises 9 chapters of which four have an introductory character. They serve to introduce the reader to the concepts of digital identity and e-government and provide information concerning technical issues that are necessary for the understanding of subsequent chapters. Then follow five chapters that contain the scientific contributions of the thesis. The chapters are structured as follows:

- **Chapter 1** is the introductory chapter of the thesis. It provides an overview of the scientific and research contributions and presents the structure of the thesis.
- **Chapter 2** explores key concepts related to digital identity. The terms identity, anonymity and pseudonymity are introduced. We attempt a definition of digital identity and explore the concept of the 'digital persona'. Furthermore, methods for the authentication of digital identities are discussed.
- **Chapter 3** introduces the concept of e-government. A definition e-government is given and the nature of e-service delivery in the governmental domain is explored. As this thesis often adopts a European

perspective, the current state of public e-service delivery in Europe is considered.

- **Chapter 4** details the technical state of the art. The focus of the chapter lies on digital credentials and digital identity cards. The state of the art in pseudonymous credential systems is described and current European projects for digital identity cards are presented. Further technologies, such as group signatures and public key certificates, are briefly introduced in order to facilitate the reading of later chapters.

- **Chapter 5** discusses privacy threats that may arise from e-government and in particular from the introduction of digital identity cards. An analysis of privacy threats and a conceptual model for enhancing privacy is presented. We motivate the use of anonymous transactions in e-government. Choices that can be taken with regard to identification and authentication in electronic service access are illustrated.

- **Chapter 6** of the thesis proposes a concept for an extended digital identity. The concept comprises pseudonymous credentials as a privacy-enhancing technology. We present an architecture design and discuss the infrastructure that is necessary to support the use of pseudonymous credentials on digital citizen cards. Conceptual issues related to the extended digital identity are explored.

- **Chapter 7** presents the architecture and design for a prototypical implementation. Architecture components and rationale behind the design are discussed. The design of server-side components is based on the Java 2 platform, Enterprise Edition.

- **Chapter 8** critically discusses the concept for an extended digital identity with regard to its implementation in the public and private sector. We name technical and non-technical barriers that need to be overcome on the way to implementation.

- **Chapter 9** summarises the results of the thesis and gives proposals for further research in the domain of privacy and e-government.

Although the first four chapters serve as an introduction to the thesis, it is not recommended that the reader skips these sections, as they establish terminology that is used throughout this thesis.

Chapter 2

Digital Identity and Anonymity

This section introduces the concepts and terminology that are necessary for the discussion of various levels of identification in electronic services. The terms identity, anonymity and pseudonymity are explained. Based on these definitions, the concept of digital identity is explored. Various methods of authentication of digital identities are considered. In addition, related concepts such as identity escrow are introduced. This chapter is of an introductory character and aims at introducing terms and concepts that will be used throughout this thesis.

2.1 Identity, Anonymity and Pseudonymity

During the past forty years, there has been a wealth of writings, both scientific and non-scientific, concerning the question of 'identity' and what it means to be an individual in today's society. The term identity is used by several scientific communities, all of which attribute a different meaning to the term. Human identity is considered from a psychological and social perspective. The terms anonymity and pseudonymity are set forth and defined with regard to information systems.

2.1.1 Human Identity

The Oxford English dictionary defines identity as 'the sameness of a person or thing at all times or in all circumstances' [SW89]. In the Oxford Encyclopedia it is defined as 'the quality or condition of being a specified person'. Related concepts are individuality and personality. The term identity originates from the Latin word 'identitas' which means sameness.

In psychology, identity is related to self-awareness and to the question of

what one represents in relation to others. In 1890, William James introduced numerous concepts related to the self into psychology and distinguished between an internal and external perspective of identity. The phenomenal self (the self as perceived by others) was distinguished from the inner self (the self as perceived by oneself). An individual must therefore find a balance between these two perspectives [Jam90]. Psychologists argue that identity is dynamic rather than static and evolves with time. It is perceived as 'a dynamic organisation of drive, ability, beliefs and individual history' [Mar80]. Giddens observes that 'self-identity, then, is not a set of traits or observable characteristics. It is a person's own reflexive understanding of their biography. Self-identity has continuity, that is, it cannot easily be changed completely at will - but that continuity is only a product of the person's reflexive beliefs about their own biography' [Gid91].

For sociologists, identity is 'socially bestowed, socially maintained and socially transformed' [Ber00]. According to the social identity theory by Tajfel, identity comprises categorisation, identification and social comparison [Taj81]. Categorisation means that people tend to categorise objects in order to understand them and that they do the same thing with individuals (with attributes such as age, gender, religion and ethnic origin) to facilitate the understanding of our social environment. Identification means that individuals perceive themselves as belonging to one or more social groups. This leads to a concept of identity that consists of both social and individual identity.

2.1.2 Human Identification

Identification is the process of establishing the identity of a person [SW89]. This is achieved by means of a set of characteristics that describe a person. After all, the essential and unique characteristics of an individual are what identify it. The distinction between identity and characteristics is not always straightforward. Suitable characteristics may include immutable attributes (such as the date of birth) and physical traits. When using characteristics or attributes to identify a person, the problem arises that the identifying characteristics of a person may change with time. As an example, a set of attributes describing the identity of a person could include the ability to drive a car, which may change with time. Also, some physical characteristics such as height or hair colour may alter.

In the 17^{th} century, the police used sight recognition by having officers with a good visual memory try to remember a criminal's face [Cam98]. After the 1840s, photography was used for identification and record keeping. After 1890, dactylography was introduced and fingerprints as a biometric

measurement became the preferred way to identify criminals. Today, photography complemented by fingerprints is still in use although the analysis of DNA (Deoxyribose Nucleic Acid) samples is increasingly used in criminal investigations.

The concept of identity and the process of identifying a person occur in many situations in daily life. When paying for groceries by credit card, for example, the card number serves as an identifier and ties the transaction to a customer of the card-issuing company. Also, most transactions with government (such as registering a change of address) require an identification of the person. There is currently a trend to include biometric information about citizens in identity documents. Germany, for instance, is planning to include a machine-readable representation of the fingerprint in the new passport.

In administrative settings, people are usually either identified by a combination of characteristics or by a single identifier (such as a social security number) and often through a combination of both. An identifying set of characteristics in an administrative setting can be the name of the person combined with the date and place of birth and the name of the parents. The first administrative record created for a person is usually the entry in the registry of births and deaths. The birth certificate is a prerequisite for obtaining further identifying documents such as a passport.

2.1.3 Anonymity

Anonymity is defined as 'the state of not being known, not named or the state of being nameless' [SW89]. In the domain of information systems, anonymity can be defined with regard to a set of subjects, with regard to communicating parties or with regard to the evidence resulting from a transaction.

A general definition of the term with regard to a set of subjects is given by Pfitzmann and Köhntopp [PK01]. Anonymity is defined as 'the state of being not identifiable within a set of subjects, the anonymity set'. The anonymity set is the set of all subjects who might cause an action, e.g. the set of all users of a system. The larger this anonymity set is, the stronger the anonymity.

Reiter and Rubin consider anonymity with regard to communication systems. They define the notion of sender and recipient anonymity as follows: Sender anonymity means that an observer cannot link a particular message to a sender (while the receiver may be known). Recipient anonymity means that an observer cannot link a particular message to a recipient (while the sender may be known). The content of the messages may or may not be

known. If both sender and recipient of messages are not identifiable, then messages become unlinkable [RR98].

We consider anonymity with regard to a transaction between at least two participating parties. A transaction is usually documented by an electronic record. An anonymous transaction is one that cannot be attributed to a particular individual. A record documenting a transaction is anonymous if it cannot be associated with the subject of the transaction.

With regard to electronic transactions, it can be said that sender anonymity is necessary but not sufficient to achieve anonymity. The message itself must not contain data that allows linking the evidence of the transaction to an existing citizen. Therefore, the user must remain anonymous with regard to communication and the resulting records of the transaction.

2.1.4 Anonymity in Computer Supported Cooperative Work

Anonymity has also been a topic of research in the domain of computer supported cooperative work (CSCW). According to Wilson, CSCW is 'a generic term which combines the understanding of the way people work in groups with the enabling technologies of computer networking, and associated hardware, software, services and techniques' [Wil91]. In the context of CSCW, research has been undertaken to learn more about the effects that anonymity can have in computer supported cooperation (see e.g. [HTJ89], [Grä01]).

In the context of CSCW, two forms of anonymity are distinguished [GK02]:

- **Contribution anonymity:** an information system that supports the cooperation of several users can suppress the authorship of contributions when displaying them to the participants. Such systems provide a form of anonymity called contribution anonymity. In a system providing contribution anonymity, contributions are displayed without disclosing the identity of the author and are standardised with regard to their appearance. However, if users cooperate in the same place and at the same time, they may still gain context information by watching the activities of other users.

  Optionally, a system that offers contribution anonymity can make use of pseudonyms, see also section 2.1.5. Pseudonyms enable users to link together several contributions by one and the same author. Still, the real identity of the author remains hidden.

- **Process anonymity:** in settings where users cooperate asynchronously and (respectively or) in different places, the ability of the individual

> user to collect context information about other users is greatly reduced. Such settings provide a form of anonymity that is referred to as process anonymity. The strongest form of process anonymity is reached in a setup where users have no knowledge regarding the set of participants that are involved in the system. In such a case, a user is not aware of other users who remain passive and merely act as observers.

We will briefly discuss whether these two forms of anonymity can be distinguished in a system with credential-based service delivery. In a credential system, a user interacts with credential issuers to obtain pseudonyms and credentials. These credentials can then be shown to service providers in so as to anonymously gain access to electronic services. A credential-based system typically comprises a multitude of credential issuers and relying parties (see section 4.2).

The first form of anonymity that was mentioned above, namely contribution anonymity, is a form of anonymity that can hardly be applied in the context of credential-based systems. Credentials serve the purpose of establishing trust. When a user shows a credential to a relying party, a transaction record is created. However, this record serves auditing purposes and other users are normally not given access to this record. Such a transaction record cannot be considered as equivalent to a contribution made in a CSCW system. Thus, it does not make sense to apply the concept of contribution anonymity to credential-based transaction systems.

With regard to process anonymity, it can be maintained that process anonymity is achieved in a system where credentials are used in network-based transactions. A user who obtains a given credential does usually not have any knowledge about other credential holders and is not even aware of the total number of users who hold a given type of credentials. Also, a user has no way of telling which other credential holders have indeed accessed services with the help of their credentials. Under normal circumstances, not even the credential issuer can find out which credential holders have made use of their credentials and which have not. Such a knowledge can only be gained if the transaction records of all service providers are gathered and the anonymity of all users is revoked.

We conclude that pseudonymous credential systems typically offer process anonymity. A user has no way of learning about the activities of other users. In contrast, the concept of contribution anonymity is not applicable, as the transaction records created by showing a credential do not constitute a contribution that is made available to other users.

2.1.5 Pseudonymity

A pseudonym is a false or fictitious name chosen by a subject [SW89]. The use of pseudonyms is particularly common among artists. The musician Moby for instance is widely known under his pseudonym but not under his real name, Richard Hall. In the context of information systems, pseudonymity is defined as 'the use of pseudonyms as identifiers' [PK01]. In a digital world, a person may have many pseudonyms that stand alongside each other. Subjects may use a distinct pseudonym for access to every system they use on a regular basis, thereby preventing the linking of transactional data accumulated in each system.

A pseudonymous transaction is one that can only be linked to a pseudonym but not to a particular individual. The difference between anonymity and pseudonymity is that a pseudonym enables a service provider to link all transactions that involve the same pseudonym. Pseudonyms therefore enable an individual to establish a reputation under a pseudonym. Examples for this are Web-based auctions (e.g. on the Ebay platform, http://www.ebay.com) where bidders and sellers make use of pseudonyms. Both participants in a transaction can rate their respective counterpart, thus enabling pseudonymous users to build a reputation. The identity of the individual behind the pseudonym is only disclosed to bidder and seller upon concluding a deal.

Pseudonyms can be classified with regard to the way in which they are created and their relation to the pseudonym user's identity [Dat97]. This classification is shown in Table 2.1 along with some examples.

In the context of anonymity and pseudonymity, a distinction can be made between linkable and unlinkable transactions: Unlinkability with regard to the use of a resource means that a subject may use the same resource repeatedly without a third party being able to link these uses together. The use of pseudonyms leads to linkable transactions that are nevertheless anonymous. In contrast, anonymous identifiers lead to unlinkable anonymous transactions.

2.1.6 Revocable Anonymity

In anonymous and pseudonymous transactions, a subject does not disclose an identity to other parties. This may be unwanted because an anonymous individual cannot be held accountable for his or her actions. Sometimes, additional safeguards are desirable in anonymous and pseudonymous settings. In these cases, a system can be devised in which, under normal circumstances, a subject's identity remains hidden from communication partners but is disclosed under exceptional circumstances. Such a setting can be accomplished

Pseudonym Type	**Explanation**	**Example**
Self-generated Pseudonym	Generated by the owner. Only the owner can translate the pseudonym into a real-world identity	Pseudonym in an online chat
Reference Pseudonym	A pseudonym that can be translated into a real-world identity with the help of a reference list that is typically kept by a trusted third party	Social security numbers, telephone numbers
Cryptographic Pseudonym	Generated by applying a cryptographic function to identifying data. The function may be a one-way function, which leads to a one-way pseudonym	Context-dependant identifier used in the Bürgerkarte project [PKK+02]

Table 2.1: A classification of pseudonyms

by introducing a third party that can unveil a subject's identity under well-specified conditions. This leads to the notion of revocable anonymity.

The concept that enables revocable anonymity and pseudonymity is called identity escrow. Identity escrow is the application of key-escrow ideas to the problem of authentication [KP98]. A system with revocable anonymity requires a set-up phase: before accessing any services, users and service providers must agree upon a third party that is mutually trusted. This party can later disclose the identity of a user when need arises. Service providers have the responsibility to clearly define the circumstances that lead to a disclosure of identity.

This approach can be illustrated with an example: a user A would like to use services offered by a party B in an anonymous way. In a system with escrowed identity, the user A first agrees with B on a mutually trusted party E and obtains E's public key. After this initial set-up step, A can access resources offered by a party B without disclosing his or her identity. Instead of disclosing an identity, A provides information that allows the trusted third party E to determine A's identity if necessary. When accessing a service, A encrypts a certain value into the transaction record that can be traced back to A's identity if decrypted by the trusted party E. As a safeguard, A must usually prove to B that the value has indeed been encrypted. This amounts to a guarantee that E can indeed determine A's identity. Thereby, anonymity is preserved under normal circumstances. Under exceptional circumstances (e.g. if a crime has been committed) an identity may be discovered by ex-

amining the evidence (audit trail) of a transaction. Revocable anonymity permits anonymous transactions while maintaining accountability.

An important feature of identity escrow is separability. The third party E that can revoke anonymity is not involved in any communication between A and B. The third party is only called upon when the anonymity of a user needs to be revoked [KP98].

2.2 Digital Identity

The term digital identity is as difficult to define concisely as is the concept of human identity. In literature, there is no commonly agreed upon definition of the term. On a very general level, a digital identity can be defined as a machine-readable representation of a human identity that is used in electronic systems for interactions with local or remote machines or people. The purpose of a digital identity is to enable access control functionality and to tie a particular transaction or a set of data in an information system to an identifiable individual. With the help of a digital identity, a user can be identified, authenticated and authorised to access a given resource or service. The security of an information system relies to a large extent on the ability to identify and authenticate users [Pfl96]. Today's individuals tend to own a growing number of digital identities, as individuals conduct more and more transactions over the Internet [SWR97].

The narrowest definition of the term digital identity is to define it as an informational pattern by which the user is known to the system. A digital identity may be authenticated or unauthenticated. Typically, a digital identity is associated with a secret password or value for the purpose of authentication [Pfl96]. For example, a simple form of an authenticated digital identity is a user name and an associated secret password. Some transactions require a far more robust digital identity than others, since the degree of trust required can vary significantly and depends on the type of the transaction.

An individual may possess many different digital identities. This reflects the fact that in today's information age people use a multitude of digital services. These services are often provided by organisationally separate entities, which implies distinct digital identities for every single service. The difficulty of administering numerous identities has prompted a trend towards multi-service digital identities such as Microsoft's .NET Passport technology [Mic03] or the Liberty Alliance [Lib03]. These solutions are also described as identity management solutions and the resulting identities are called federated identities. These digital identities can be used for accessing a multitude of Web-based services offered by different providers. The benefit

for users is that they only have to sign in once to their federated identity service provider and not repeatedly for every service they use. Some federated identities not only comprise authentication functionality but also encompass an associated set of personal data that is used in Web-based transactions.

With regard to digital identities, we differentiate between open and closed settings. Table 2.2 gives examples for digital identities in open and closed systems. In a closed setting, a digital identity is issued by an organisation for use within that organisation's information systems. All users within the organisation are of course well known. Typically, such identities are user names and also public key certificates that are issued with the help of an internal public key infrastructure (see section 4.3.1).

Environment	**Typical Examples for Digital Identities**
Closed System	Locally valid identities: *user names, public key certificates issued by internal public key infrastructure*
Open System	Digital credentials: *public key certificates, attribute certificates, digitally signed documents and anonymous or pseudonymous credentials*; Federated identities: *Microsoft .NET Passport*

Table 2.2: Examples for digital identities in closed and open settings

In contrast, in an open distributed setting, many entities communicate with each other, often without having met before. A service provider may receive a request from a hitherto unknown user. The user presents digital credentials that certify the user's identity or other properties such as accreditations or authorisations. Credentials are statements about subjects which are issued and signed by third parties. The service provider examines these credentials and decides what access rights to attribute to this user. This process is called trust establishment (see section 2.2.1). Digital credentials will be considered in more detail in section 4.1.

In a broader perspective, digital identity can be considered to be the set of all data in information systems that relates to a given individual [Cla93], [Köh00]. This comprises all personal data that describe a user, such as credit card numbers, digital documents, certificates and other data that can be related to the user.When summing up all the data items that describe a person in different information systems, one obtains a set of data that can be described as the 'digital persona'. The term was first used by Roger Clarke who defines the digital persona as a 'model of the individual established through the collection, storage and analysis of data about that person' [Cla93]. Figure 2.1 illustrates the concept of the 'digital persona' as the aggregation of all data that is kept about a person in information systems.

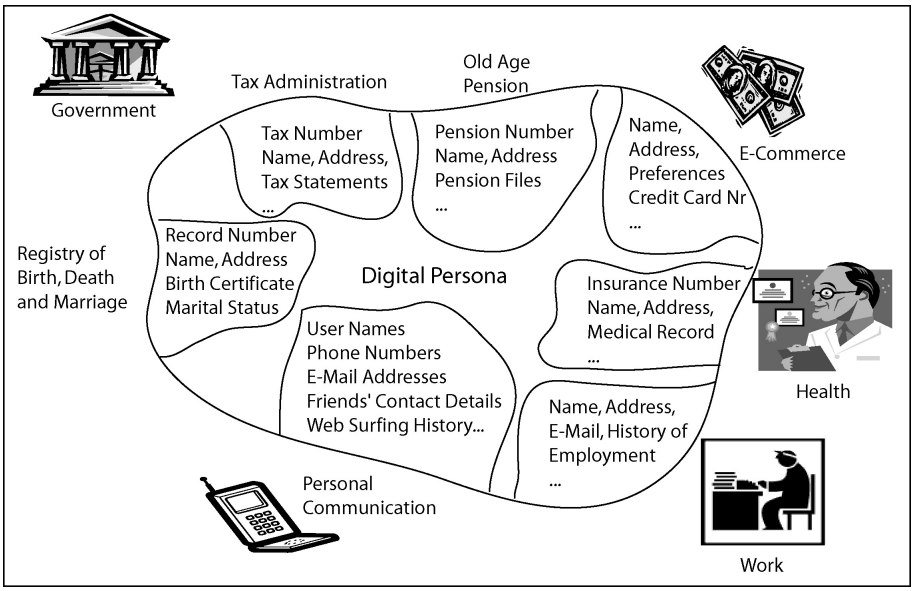

Figure 2.1: An aggregation of user-related data from several information systems leads to the 'digital persona' as a digital image of the user

This wider perspective implies that users have some control over the data that constitute the digital identity as they can choose what amount of personal data they disclose to a service provider. This is comparable to non-electronic interactions where individuals actively decide on the amount of information they communicate to another person or organisation. In daily life, users interact with a multitude of organisations and information systems which may all store a different set of data concerning one and the same user.

A digital identity can be anonymous, pseudonymous, identifying or a group identity. An identity with full identification allows a service provider to link a transaction back to an individual. Usually, this implies that an identifying set of data (e.g. the name and possibly more data) about the user can be established. Pseudonymous and anonymous identities are different. A pseudonymous transaction can be linked by a service provider to a pseudonym but not to an identifiable individual. A transaction involving an anonymous identity cannot be linked to an identifier at all. Of course, in the case of anonymous and pseudonymous identities it is possible to make use of identity escrow (see section 2.1.6) and appoint a third party that can reveal the identity behind the pseudonymous or anonymous transaction.

Several forms of digital identity can be distinguished with regard to the link between the informational pattern and an individual. Table 2.3 gives an overview on different forms of digital identity.

Digital Identity	Link between Individual and Digital Identity
Anonymous Identity	No link possible
Pseudonymous Identity	No link possible
Full Identification	One to one
Group Identity	Many to one

Table 2.3: Different forms of digital identity with regard to link between digital identity and individual

The rare case of a group identity exists in e-government. In Italy, families are treated as a group during the process of citizen registration. One family member can declare himself or herself head of the family. The latter receives a family card and may perform administrative transactions with regard to registration services for other members of the family.

2.2.1 Digital Identity in Electronic Service Access

A digital identity (in the narrow sense) is an informational pattern by which the user is known to a system. Digital identities are necessary to identify users and to authorise them to access resources (or services) within a system. In the context of e-government, such resources are for instance citizen or business services. This section shortly introduces terms related to access control. For a more detailed discussion, the reader is referred to the literature cited in this section.

Before a user with a digital identity is granted access to a service, several processing steps have to be performed. The first step is to obtain a form of digital identity. This may be a user name and password, a digital certificate or an anonymous credential. As mentioned in section 2.2, a user typically has several digital identities created by distinct issuers. Before any form of digital identity is issued to a person, the issuer performs a process called registration. In a registration process the issuer checks whether the digital form of identity is issued to the right person and whether the person meets all prerequisites and is entitled to the given form of digital identity.

In centralised, closed systems where users are known a priori, the traditional process of access control is used. In a centralised system, users are identified, authenticated and finally authorised. Figure 2.2 illustrates the steps from registration to service access. The process of access control usually comprises the following steps [Pfl96]:

- **Identification:** the user claims an identity, e.g. by supplying a user name.
- **Authentication:** the claim of identity is verified. Authentication is discussed more detail in section 2.2.2.
- **Authorization:** the system determines the actual rights of the subject. This usually entails looking up the rights of the (by now) identified and authenticated user in an access control list (ACL).

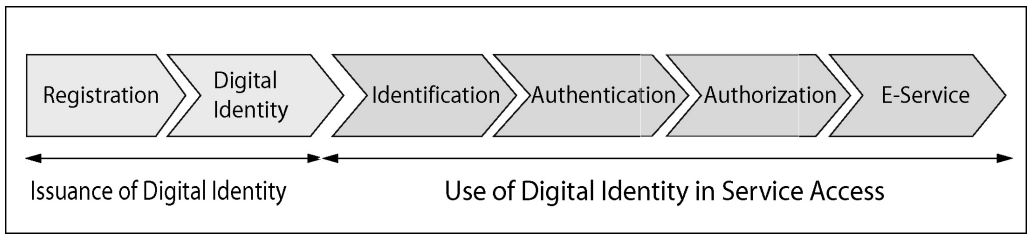

Figure 2.2: Digital identity in electronic service access

In open, distributed settings, the traditional approach to access control is inadequate. In a large-scale system such as the Internet, the set of users is not known a priori. Furthermore, subjects and resources often belong to different security domains administered by different organisations. In decentralised settings, the traditional approach to access control is replaced by the process of trust establishment (or trust management) [BFK99]. This approach bases authorisation decisions on digital credentials. Digital credentials are signed statements about subjects that are issued by third parties.

In trust establishment, service providers specify their access policy in a trust policy file. For every protected resource, this file states a set of credentials that a user must hold in order to be granted access. This trust policy file is processed by a trust engine. When requesting access to a protected resource, users present digital credentials to a service provider. The request and the user's credentials are then passed on to the trust engine. Upon receiving a request for authorisation, the trust engine verifies the user's credentials and makes an access control decision in accordance with the trust policy. Only if the user can prove possession of the required credentials, access is granted.

Trust management relies on digital credentials, which convey attributes in a trustworthy manner. This approach to access control is also sometimes referred to as attribute-based access control (ABAC) [WL02]. In systems that only use digital certificates for access control, the term certificate-based access control (CBAC) is often used. Recently, the term credential-based

access control is used for systems that base access control on any kind of digital credential [Sam02]. Essentially, the notion of attribute-based and credential-based access control are equivalent, as credentials certify attributes about a user.

2.2.2 Authentication of Digital Identities

The terms user identification and user authentication are sometimes used interchangeably, which is incorrect as these terms address different concepts. The term 'identification' refers to the action of a user claiming an identity whereas the term 'authentication' is defined as the process of verifying that claim of identity [Pfl96]. There are three possibilities of how a claimed identity can be authenticated:

1. **Authentication by something the user owns (by token):**

   A user can be authenticated by use of a unique token that can be active or passive. Examples for such tokens are a key, an ID card, a magnetic card, a smart card or even a mobile phone. The advantages of this approach are that the token may include a processor thus enabling the addition of further security mechanisms and that the user does not have to memorise a secret. The disadvantages lie in the fact that such a token is transferable and thus at risk of being counterfeited, lost or stolen.

2. **Authentication by something the user knows (by knowledge):**

   A user can be authenticated by use of a secret that is only known to the user. Examples for such secrets are a password, a personal identification number (PIN), any form of code or the answer to a personal question. The advantages of this approach are that authentication is straightforward and can therefore be implemented at low cost and that the user does not need to carry physical objects. The drawbacks are that secrets carry the inherent risk of being transferable, may be subject to exhaustive search, compromised without the knowledge of the user or that the user may simply forget them.

3. **Authentication by a bodily characteristic of the user (by biometric):**

   A user can be authenticated by biometrics. A biometric authentication may be either based on physiological or behavioural properties [Ash00].

   (a) Physiological properties: scan of iris, retina, facial image, measurement of fingerprint or hand geometry.

   (b) Behavioural properties: the walk of a person, the dynamics of writing or signing, voiceprint, the typing rhythm on a keyboard, etc.

   The advantages of this approach are that biometric properties are non-transferable and that users do not need to carry an additional token or remember a secret. The disadvantages are the difficulty of obtaining measurements, the possibly low acceptance by users and the necessity to find a trade-off between false acceptance and false rejection rates. Furthermore, there is also the problem that only few biometrics exist that apply to 100% of the population.

Authentication may of course also be based on a combination of one or more of the means mentioned above. Knowledge of a secret is generally considered the weakest form of authentication. Secrets such as PINs and passwords are to some degree often predictable or subject to attacks of brute force. The use of authentication tokens raises the problem that the authenticity of the token must be ensured.

Biometrics are often put forward as the 'silver bullet' of authentication but in practice they come with their own set of complications. Not all users exhibit a given biometric. For example, it is difficult to measure the fingerprints of people who have suffered frequent hand damage (e.g. construction workers) [Eve92]. A further problem is that the use of biometrics necessitates finding a balance between two error rates: the false acceptance rate (FAR) denotes the rate of unauthorised users who erroneously pass the test and are accepted into the system. The false rejection rate (FRR) denotes the rate of authorised users who erroneously fail the test and are excluded from the system. The balance between those rates depends on the nature of the system. In a military setting, the goal is to minimise the false acceptance rate. In a commercial environment, it may be more important not to falsely deny access to the customers.

Another problem for the use of biometrics is user acceptance: users tend to be more stressed by the process of biometric measurements than by the process of remembering and entering a secret [Ash00]. Research on digital

citizen cards has shown that many users have concerns about the security and reliability of biometric authentication [OvdB01b].

A discussion of the advantages and drawbacks of the various forms of biometrics is outside the scope of this work. Further material and a detailed discussion of many biometrics can be found in the book on this topic by Ashbourn [Ash00].

2.3 Summary

Human identity is dynamic in nature and to some degree socially bestowed. Digital identities are used in communication with information systems and mainly serve the purpose of identification and authorisation. They are also used to tie a set of data to an identifiable individual. In the narrowest sense, a digital identity is merely an informational pattern by which an individual is known to a system. In open, distributed settings, trust is established with the help of digital credentials. Today, digital identity is often interpreted in a wider sense and includes all data that is known about a user in a system.

Authentication is the process of verifying a user's claim of identity. Authentication can be achieved by token, by knowledge or by biometrics. A digital identity can be identifying, anonymous or pseudonymous. In anonymous and pseudonymous settings, it is possible to implement a form of revocable anonymity through the use of identity escrow: a trusted party is appointed that can reveal the identity behind an anonymous or pseudonymous transaction in case of a dispute.

Chapter 3

Introduction to e-Government

This chapter provides an introduction to electronic government. Departing from a brief look at the more recent evolution of e-government research, several definitions of the concept are presented. A classification of services comprised in the field of e-government is considered and examples for services of different categories are given. Differences between public sector and private sector service provision are explored. The concepts of one-stop government and service portals are considered, as these constitute an important element of e-government initiatives in many countries around the world. As this thesis often adopts a European perspective on e-government, the progress of e-service delivery in the governmental domain in Europe is examined. The results of a benchmark study are presented that was performed as part of the e-Europe initiative. Finally, the challenges in the field of international e-government services are briefly considered.

3.1 e-Government

Electronic government is a term that refers to the transformation of government in the age of the information society. In the late nineties, the concept of electronic government became an issue of high importance for governments worldwide. Many countries have engaged in initiatives to introduce service delivery over electronic channels. Some governments have even set targets for the first decade of the new millennium to electronically deliver any service amenable to this form of delivery [Off00].

However, the use of information and communication technologies in the administrative domain is nothing new but has already been practised for several decades. Also, some basic goals of e-government have existed long before the actual term 'e-government' became popular, a term that was coined in

analogy to electronic business. In 1990 for example, Lenk and Brüggemeier published a paper on citizen information services [LB90]. This type of service is to be provided to the citizen by so-called citizen information systems. The aim of the system is to increase the amount of information readily available about governmental processes and affairs and also to increase the participation of individual citizens in the governmental process. These goals can still be found in many of today's definitions of e-government.

Research on the use of information and communication technology in the public sector was also undertaken at a European level (see e.g. [Ste97]). In the year 2000, von Lucke and Reinermann published their ‚Speyerer Definition of e-government' [vLR00]. In the following year, a collection of papers on the subject was published by Gisler and Spahni [GS01]. Today, conferences on e-government are attended by both academics and practitioners alike and are held on a regular basis.

In Europe, almost all countries engage in e-government activities and the European Commission is providing substantial funding for academic and industrial projects in this field. Research projects were even undertaken to learn more about the challenges of services that involve authorities from several countries [AM02].

3.1.1 Definition of e-Government

Quite a number of authors have attempted a definition of the concept of e-government (e.g. see [GS01]). Two popular definitions by scholars shall be cited here instead of attempting another definition.

Von Lucke and Reinermann define e-government as 'conducting business transactions related to governance and administration (government) with the aid of information and communication technology. This includes the whole public sector which comprises legislature, executive and judiciary as well as companies owned by the state' [vLR00].

Lenk defines e-government as the 'enactment of processes of public opinion forming, decision making and the provision of services in politics, the state and the administration by use of information technology'. Electronic government can thus be defined as the civil and political conduct of government by use of information and communication technology (ICT)' [Len99].

Electronic government is also referred to by some authors as 'Virtual Government' or 'Digital Government' [ME02]. E-government can thus be seen

as a vision for modernising government, as it addresses judiciary, legislature, executive and all stakeholders of government. E-government will allow the delivery of new services, open new communication channels between government and its stakeholders, and it will create new forms of democratic participation.

E-government comprises both processes within governmental bodies and processes directed towards the outside. In order to reach the full potential of e-government, a comprehensive re-engineering of administrative and political processes is imperative. Although many early publications focused solely on the interaction between administration and the citizen, this perspective is too narrow. Interactions between governmental authorities, between private and public sector companies and also with non-governmental organisations are an important part of e-government.

Commonly, three domains of electronic government are distinguished according to the party that interacts with a governmental body [Gis01]. Three categories of actors exist: citizens, businesses and government. It is important to note that the term citizen usually comprises all individuals that communicate with a governmental entity, regardless of nationality and country of residence. The three domains are:

- **Government to Citizen (G2C)** e-government comprises all interactions between individual citizens and the government. An example is the electronic filing of tax declarations by citizens.

- **Government to Business (G2B)** e-government comprises the interaction between private sector organisations and the government. The electronic procurement by public organisations is an example for this category.

- **Government to Government (G2G)** e-government comprises the interaction between different governmental institutions. The interaction may be on a national or international level. An exchange of information between administrative bodies is an example for this category.

The forms of G2B and G2C are referred to as 'external e-government' while G2G is referred to as 'internal e-government'. The use of terminology is not consistent however: some authors refer to the fields as A2A (Authority-to-Authority), A2C (Authority-to-Citizen) and A2B (Authority-to-Business) e-government. Figure 3.1 illustrates the three forms of electronic government.

In this thesis, e-government is understood in the sense of the memorandum on electronic government issued by the Gesellschaft für Informatik

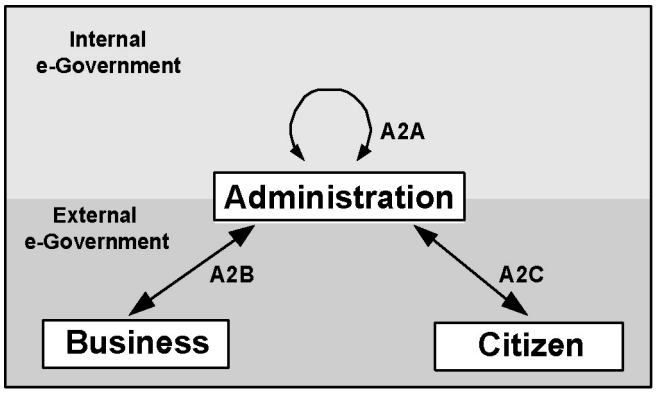

Figure 3.1: Three domains of e-government

e.V. (German Association for Computer Science), namely as a comprehensive transformation of the government in the age of the information society [Ges00]. In order to accomplish this transformation, a holistic approach to e-government should be taken. With regard to the engineering of information systems, it can be said that such an approach should be multi-disciplinary and comprise not only the viewpoint of the administration but also a social, psychological, economical and technical perspective. E-government solutions should contribute to an information society that is accessible to all citizens, not just to a small 'digital elite'.

3.1.2 Differentiation Between e-Government and e-Business

E-government is sometimes considered to be the e-business of the state. This view is inaccurate, as the concept of electronic government refers to more than the mere electronic conduct of the business of the state: it refers to the transformation of government in the information age. The use of information technology is only one aspect of this transformation. Although e-government and e-business have many points in common with regard to the technological infrastructure, there are considerable differences on a strategic and an economic level. When considering the digitalisation of governmental functions from a non-technical point of view, a certain number of differences become apparent. We can summarise these differences as shown in Table 3.1.

These differences have consequences for the design of information systems in the domain of e-government. Some important aspects are:

Organisational objectives: With the exception of non-profit organisations, private sector companies generally work profit-oriented. This is not

	Private Sector	**Public Sector**
Organisational Objectives [Gis01]	Free to choose	Prescribed by legislation
Market Position of Service Provider [BG02]	Polypoly	Monopoly
Goods and Services Offered [LT02]	Motivated by demand	Decreed by law
Reaction to Change [Gis01]	Fast	Slow
Customer Base [BG02]	Homogeneous	Heterogeneous
Process Organisation [BG02]	Flexible	Relatively static
Decision Making Principles [SB96]	Efficiency, profit	Fairness, equality

Table 3.1: A comparison of private and public sector service provision

the case with public administrative bodies. The purpose of a public sector organisation is prescribed by law and cannot freely be chosen by the management [Gis01]. Profit is usually not a goal, although there is a tendency to organise administrative entities as profit centers.

Position in the market: usually, administrative services are exclusively provided by the state. Therefore, governmental organisations have a monopoly position on their market whereas private sector companies normally face competition within their respective markets [BG02]. Also, organisations in the private sector can at any time adapt the set of products and services offered according to the demand in the market place.

Range of goods and services: the products and services offered by a governmental authority are usually decreed by law. Furthermore, some administrative services are compulsory by nature. Especially registration services are mandatory in many countries. The way a service is provided can often not be modified without an accompanying legal change [LT02]. An example is the introduction of an electronic channel for voting: in many countries, the implementation of e-voting necessitates changes in the legal framework. The strong regulation of the duties of an administrative body naturally implies slower organisational change.

Customer base: private sector companies tend to actively manage their customer base. Through the use of electronic customer relationship management (e-CRM) software they have the possibility to identify profitable customers and serve them differently from less profitable ones. Consequently, customers are not treated equally. In contrast, public administrations have no possibility of choosing or influencing their customer base [BG02]. They must serve all citizens and – more importantly - treat them equal regardless of ethnic origin, social background etc. The principle of equality is a principle that lies at the heart of democracy and that needs to be maintained at all times [SB96].

Decision making principles: Within administrative processes, there are often decisions to be made by civil servants concerning the handling of unusual cases. Especially civil registration processes comprise a substantial amount of manual exception handling [RCMA01]. This requires civil servants to take decisions based on the legal framework, their professional experience and their judgment. While in the private sector processes (and the IT systems that support them) are designed for maximum efficiency, there are different priorities in the public sector. Correctness, fairness and equal treatment are fundamental principles for the decisions within administrative procedures [SB96], [SB96]. These principles pose new challenges for systems that aim to fully automate back-office procedures.

As a consequence of these differences, experiences and know-how from e-business projects have to be reflected critically before applying them to the domain of e-government.

3.1.3 e-Government Services

A working group of the European Commission identifies four clusters of public services [Eur02a], [Cap02a]. This classification of public services is also used in a study that benchmarks the progress of electronic service delivery in European countries. The four clusters are:

1. Income generating services: services with financial flows from citizens or businesses to government. Examples for these services are VAT (Value Added Tax), income tax, social contributions etc.

2. Registration services: services that aim at recording object- or person-related data as a result of administrative obligations.

3. Return services: general public services provided to citizens and businesses as part of governmental responsibilities and in return for taxes and contributions. These services include support in seeking employment, health-related services, public facilities etc.

4. Permit and license services: documents provided by governmental bodies which give permission to drive a car, build a house etc. Examples include both personal documents and permits related to businesses (e.g. licenses to start a business).

Another, very common classification of e-government services is the one presented by Gisler that classifies services by functional area [Gis01]. Gisler distinguishes three categories of e-services:

- e-Assistance: information on commonplace situations in the daily-life of citizens and on business episodes of business customers.
- e-Administration: the support of internal and external governmental business processes.
- e-Democracy: the stimulation of democratic communication and participation. Electronic elections and the casting of votes over electronic channels are an important part of e-democracy.

Figure 3.2 illustrates this classification of services and shows examples for these service categories.

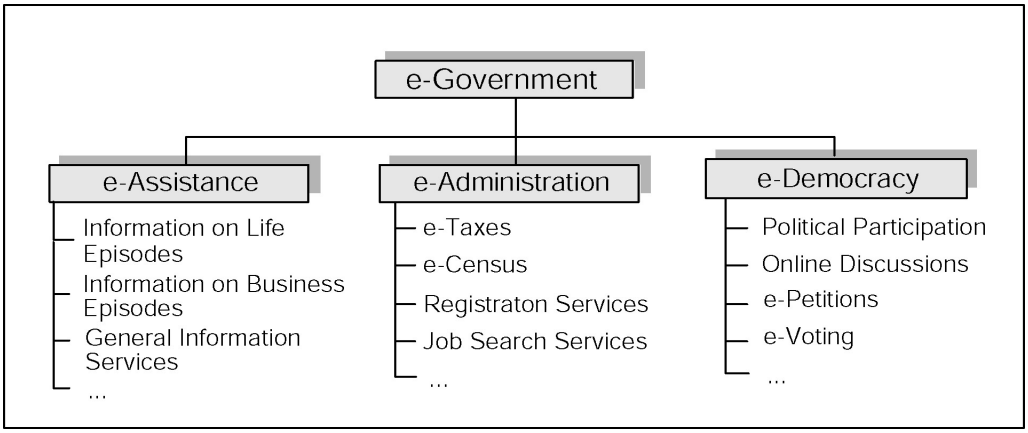

Figure 3.2: A classification of e-government services

In electronic service delivery, several evolutionary levels of interactivity can be distinguished. Gisler distinguishes three levels [Gis01]:

- Information level: services are one-way information services.
- Communication level: services may entail communication between parties.
- Transaction level: full provision of services respectively exchange of all messages necessitated by a particular transaction.

The combination of two classification criteria, namely the category of an e-service and the level of interactivity, leads to the e-government matrix [Gis01].

This matrix for the classification of services can be interpreted as a reference model for the implementation of a comprehensive e-service coverage. Starting with the provision of pure information services in the field of e-assistance, more complex services in e-administration and e-democracy may be added over time until a comprehensive set of e-government services is attained. The drawback of this approach is that precisely those services that are of highest interest to the customers (namely interactive services and transactions) are only implemented in the later stages of the model.

3.2 One-Stop e-Government and Service Portals

Electronic public services are even more convenient for the citizen if all services are accessible from a single point of entry. Today, many countries offer public services through a multitude of Web sites. This reflects the fact that a fully centralised administration is the exception rather than the rule. Public services are often provided by numerous independent administrative entities. However, the e-citizen of the future does not want to deal with a multitude of agencies but prefers a centralised self-service arena. The concept of providing a single point of entry for services provided by different governmental departments has been proposed by Lenk long before the first Web-based service portals were launched [Len92].

One-stop e-government is a concept that refers to the integration of public services from the customer's point of view [Wim02], [WT02a]. One-stop initiatives aim at creating integrated platforms for rendering all services accessible from a single point, a so-called portal. Portals are by now recognised by many governments as a key front-office vehicle to deliver citizen- and business-focused services. A customer no longer needs to know which administrative entity provides a particular service. Instead, all services can be accessed through a Web-based service portal. This requires a significant

degree of interoperability at the level of infrastructure, IT-systems and processes [Del00]. From a back-office perspective, such an integrative approach to service delivery necessitates the interconnection of logically and physically separated IT systems [WT02a]. Some countries have already implemented service portals. Table 3.2 gives examples of service portals around the world.

Country	**Portal**	**URL**
Australia	Educational Portal	http://www.education.gov.au
Austria	Government Information Portal	http://help.gv.at
Canada	Government of Canada Portal	http://www.canada.gc.ca
France	Service-Public Portal	http://www.service-public.fr
Germany	Service Portal of the Federal Government	http://www.bund.de
Hong Kong	Hong Kong Government Services	http://www.gov.hk
Netherlands	Integrated Government Portal	http://www.overheid.nl
Switzerland	Governmental Information and Links Portal	http://www.ch.ch
United Kingdom	UK Government Online	http://www.ukonline.gov.uk
United States of America	FirstGov – The U.S. Government's Official Web Portal	http://www.firstgov.gov

Table 3.2: Selected service portals in Europe and around the world

Service portals may further facilitate the access to services by providing an audience-specific presentation of content. The government of Canada delivers specific content targeted at Canadians, expatriates, resident foreigners and businesses. Australia has created an educational portal that is aimed at pupils, parents and teachers.

Portals are also drivers for a new concept in e-government, namely the structuring of services around life episodes [Wim02]. Life episodes address events that commonly happen in a citizen's life. For business customers, services are structured around business cases. As typical life episodes, marriage, moving house, or registering children for school can be mentioned. The

principle of life episodes hides the internal structures of an administration. Organising services by life episodes simplifies processes for the citizen and therefore enhances the quality of electronic service delivery. For administrations though, it creates the need to couple hitherto separated information systems – often across organisational boundaries - to provide an integrated view on services for the customers.

Currently, many portals are pure information portals and lack interactive services. They provide answers to frequently asked questions, links to authorities, on-line forms etc. It is expected that portals will evolve towards providing natural language search facilities, personalised services and finally full-fledged support for transactions, including on-line payments [Off00].

3.3 Uptake of Electronic Service Delivery in Europe

The European Commission performs a benchmark study every year to measure the progress of administrative e-service delivery in Europe. The objective of the benchmark is to enable member states to compare performance and to identify best practices. The survey covers the 15 European Union member states as well as Iceland, Norway and Switzerland. Between October 2001 and October 2003, four measurements have been effected [Cap02a], [Cap02b], [Cap03], [Cap04].

In order to measure the level of sophistication of a service, four evolutionary stages of service delivery are defined. The stages are similar to those defined by Gisler [Gis01]. Percentage values are attributed to quantify the progress towards full digital case handling, which is indicated by a score of 100%. The four stages and the associated percentage values are shown in Table 3.3.

Stage	**Online Functionality**	**Score**
Information	On-line information about a service is available	25%
Interaction	Forms are available for download	50%
Two-way interaction	Electronic processing of forms including authentication	75%
Transaction	Electronic case handling, decision making and payment	100%

Table 3.3: Four levels of online functionality and attributed percentage scores

A list of 20 common public services is used in the benchmark. Out of the twenty services, twelve address citizens and eight are aimed at businesses [Cap02a]. The benchmark focuses on online front-end public services. Table 3.4 shows the list of services that are included in the benchmark.

Citizen Services	**Business Services**
Income taxes	Social contributions for employees
Job search	Corporate tax
Social security benefits	Value Added Tax (VAT)
Personal documents	Registration of a new company
Car registration	Submission of statistical data
Application for building permits	Customs declarations
Declarations to the police	Environmental permits
Public libraries	Public procurement
Birth & marriage certificates	
Enrolment in higher education	
Announcement of moving house	
Health-related services	

Table 3.4: Citizen and business services of the pan-European e-government benchmark

The measurements between October 2001 and October 2003 show that the on-line availability of services is increasing. However, most countries are still working on the transition from informational to transactional services. With regard to individual countries, it can be said that there is a substantial spread among the countries concerning the state of e-service delivery. By October 2003, there were only six countries that on average reach the level of two-way interaction for their on-line services. These countries are Sweden, Denmark, Ireland, Austria, Finland and Norway. Among the 18 countries that participate in the benchmark study, Austria, Denmark, Belgium and Sweden have the highest growth rate with regard to on-line availability of services. Figure 3.3 shows the scores of the individual countries in the October 2003 measurement. The percentage value shown for each country is the average score achieved for the 20 services.

The survey yielded the surprising result that the implementation of business services advances much faster than that of citizen services. In all countries, business services scored on average significantly higher than citizen services. The 2003 measurement suggests that the gap between citizen and business services is still widening [Cap03].

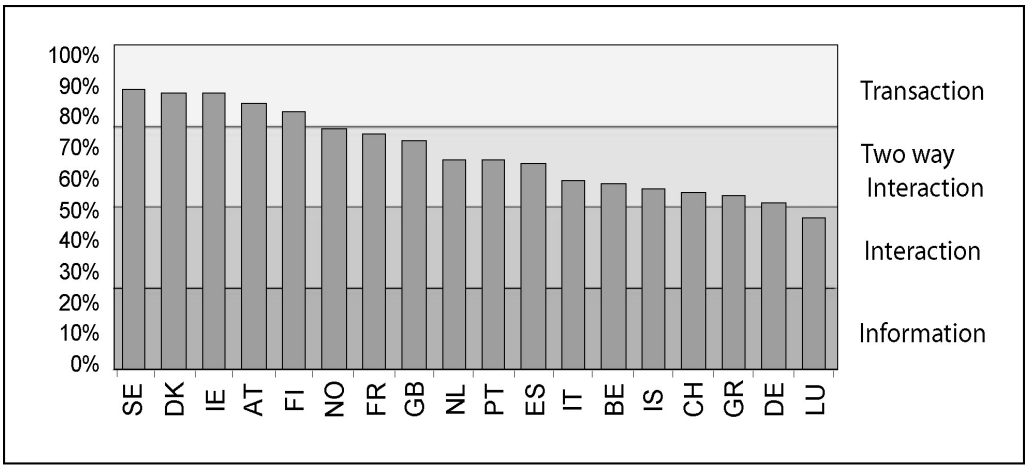

Figure 3.3: Overall scores for administrative electronic service delivery in Europe by country in October 2003

With regard to the four service clusters identified by the European Commission (see section 3.1.3), the survey shows that income generating services is the most sophisticated service cluster while permits and licenses services score lowest. Figure 3.4 shows the overall score of the four service clusters in the October 2001, 2002 and 2003 measurements. The permits and licenses cluster is the only cluster in which services do not reach the level of two-way interaction on average.

From this survey, some factors can be identified that positively affect the migration towards e-service delivery: centralised service provision, simple respectively re-engineered administrative procedures and a high degree of coordination in case of dispersed service provision [Cap02b]. Straightforward services with a coordinated service provision reached on the average the highest scores (e.g. VAT, social contributions). Countries with a high share of centrally provided services scored much better in the survey than countries with a highly federated administrative culture. Factors that have a negative impact are mainly complex administrative procedures and a decentralised administration. Electronic implementation of services that are provided in a dispersed manner typically only made progress when considerable efforts on back-office re-organisation were made and e-portal solutions were introduced.

Although the study suggests that European countries are quickly advancing towards fully transactional e-government services, it can be expected that this process will be slower than the figures suggest. For one thing, some countries have taken the advantage of 'quick wins' and have first brought those services on-line that are centrally provided and thus easy to imple-

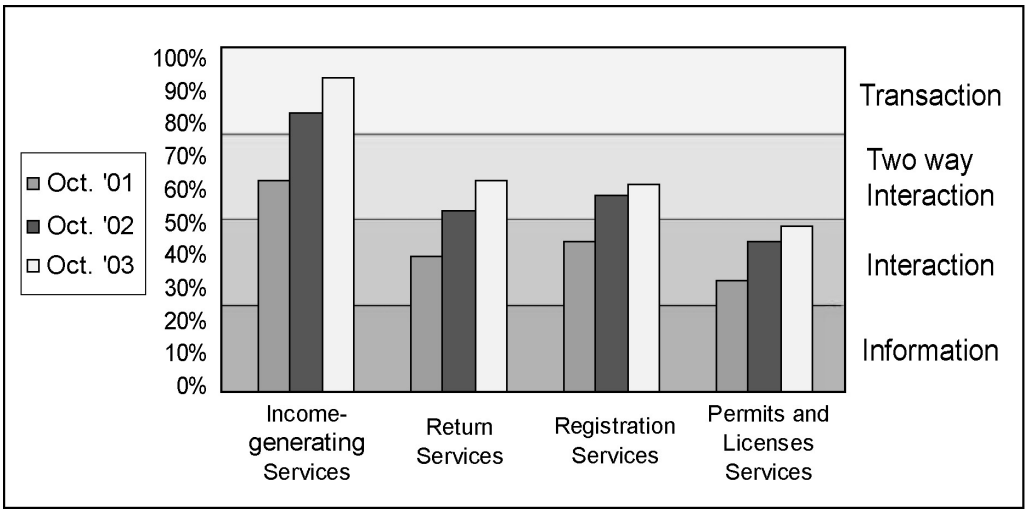

Figure 3.4: Overall percentage scores for the four service clusters from October 2001 to October 2003

ment. However, many administrative services must be re-engineered before bringing them on-line. Furthermore, some on-line transactions require digital signatures in order to become legally binding. Digital signatures are not available yet to citizens of many European countries.

Another point that has to be noted is that the study ignores the issue of service quality. The quality of e-services as perceived by the customer is important for the acceptance and thus the uptake of e-services. Citizens or business customers will not use e-services that are more complicated than their traditional counterparts. Sacrificing quality to implementation speed will not serve the government's interests.

As a medium term goal, many governments have set targets that aim at delivering all administrative services electronically wherever feasible. An example is the Bund Online 2005 campaign by the federal government of Germany [Bun03]. The campaign identifies 400 administrative services that are targeted to be delivered electronically by 2005. Another example is the 'Modernising Government' initiative in Great Britain [Off00]. It is intended to provide all services electronically that are amenable to this form of delivery. By 2005, local administrations are expected to have completed the implementation phase and serve a substantial share of their customers through Web-based interaction. In 2006, the budgets for local administrations will be cut considerably. The central government is thus effectively forcing local administration to implement the initiative on time and to achieve cost savings through e-service delivery.

3.4 Challenges of International e-Government Services

The European Union has brought a single market to Europe and with it the free movement of goods, services and labour within Europe. As a consequence, more and more people live outside their home country and become migrants within Europe. In 1996, 5.5 million EU nationals lived outside their home country. The increasing mobility of Europeans will create a demand for electronic cross-border services. Also, development and infrastructure cost of citizen card projects may motivate European countries to create infrastructure and software that can be used in more than one country. While most European countries engage in e-government activities, the question of how to inter-network these local solutions has not been taken up yet. There is hardly interoperability beyond a national level yet.

A white paper by the European Commission identifies four categories of cross-border services with a pan-European dimension [Hol02]:

1. Services for cross-border users: examples for these services are public e-procurement and e-interactions of expatriates with their national administrations.

2. Exchange of information between European public administrations: a general example is a transaction that necessitates access to databases in other countries.

3. Life episodes and business episodes at a European level: an example for a life episode at a European level is to study abroad. Examples for business episodes are the commencement of business or the employment of workers from abroad.

4. Services by Organizations at a European level: an example are the services rendered by EMEA, the European Agency for the Evaluation of Medical Products

The issue of cross-border services is only being taken up slowly. So far, it is mostly the issue of data standardisation that is considered by practitioners. A first workshop was held on the topic of pan-European data formats for administrative data [ITU03]. In the area of digital citizen cards, the IST project eEpoch aims at creating a digital citizen card that may be used by cities across Europe (see section 4.7.2.6).

International services necessitate interoperability at three levels, namely at the level of processes, information systems and data. Delivering international services is especially difficult because European countries are highly

heterogeneous with regard to administrative cultures, legal framework and procedures. The issue of international e-government services also raises the question of an electronic identity at the European level, which is so far unanswered [RR02].

The trend towards comprehensive service coverage implies that even services with special requirements will have to be delivered electronically. As a consequence, requirements for electronic solutions will become even more complex. High value service and service comprising the entry of sensitive data will be delivered through digital channels. When taking a pan-European perspective, this means that governments will have to come up with flexible digital solutions for many national particularities, such as an electronic implementation of the Italian family card. This in turn implies that digital citizen cards as bearer of the citizen's electronic identity will have to become ever more flexible.

3.5 Summary

Electronic government is a term that refers to the transformation of government in the age of the information society. It comprises the use of information and communication technology for service provision and addresses judiciary, legislature and executive. E-government services range from the support of daily life situations of citizen and business customers to the stimulation of democratic participation. The implementation of e-services by governments in Europe advances steadily, although most services have not reached a transactional level yet. Many governments have turned towards service portals that organise services around life and business episodes. Portals aim at one-stop e-government solutions that provide all services through a single point of entry. The ongoing European integration will lead to a demand for the provision of cross-border services. However, such services will need to overcome the many legal and cultural differences between European member states and will require considerable standardisation efforts among member states.

Chapter 4

Technical State of the Art

This chapter presents the technical state of the art. We start out by describing the concept of digital credentials and provide examples for such credentials. We explain the concept of anonymous and pseudonymous credential systems and detail the state of the art regarding these systems. Two other widely used forms of digital credentials, namely public key certificates and attribute certificates, are presented and the X.509 standard is briefly described. We also briefly introduce public key infrastructures (PKI), which support the use of public key cryptography. As this thesis proposes an extended form of digital identity for the domain of e-government, we present current electronic identity card projects in Europe. We also discuss the notion of group signatures and techniques for anonymous communications in computer networks.

4.1 Digital Credentials

The concept of credentials has been in use long before the invention of electronic data processing. In the Collins English Dictionary, the term credential is defined as 'a letter or other written proof of a person's position, professional capabilities, trustworthiness etc.' [Cam98]. A credential is thus a statement about properties of a subject. With the help of such a written statement, a subject can demonstrate the existence of some quality or truthfulness of a statement towards another party - provided this other party trusts the issuer of the statement.

The concept of credentials is thus not limited to the digital world. Physical tokens that prove certain privileges are in widespread use today. Examples for physical credentials are prescriptions, credit cards, a driver's license, passports, membership cards, stamps or a ticket for a movie theater. All

these tokens make a statement about the holder of the credential and are shown to some organisation when the need arises to prove a given property.

Similarly, digital credentials are signed statements concerning attributes of a subject. A digital credential serves the purpose of communicating a statement made by a third party about a subject in a trustworthy manner. As such, credentials constitute a form of digital identity and can be used in distributed settings to establish trust.

According to the definition by Herzberg and Mass, a digital credential is a statement by an issuer on some properties of the subject of a credential, that is digitally signed by the issuer and that is presented by the subject to relying parties [HM01]. In a digital setting, the party that issues a credential is called the credential issuer. The party that accepts a credential is called the relying party (or verifier).

A great variety of credential types exist in the digital world. Examples for digital credentials include:

- **Public-key certificates:** public-key certificates bind a public key to a subject. They make the public-key of an entity available to other parties in a trustworthy manner. Public key certificates contain (in the least) a public key, the name of a subject, a serial number and the signature by an issuer over that data [MvOS96]. A well-accepted standard for the format of public-key certificates is the ITU-T X.509 standard (see section 4.3).

- **Attribute certificates:** attribute certificates bind arbitrary attributes to a subject. Attribute certificates contain (in the least) attributes, a reference to a subject and a signature by the issuer over that data. The reference to a subject is established by including the serial number of the subject's public key certificate. Attribute certificates are intended to communicate information other than public keys in a trustworthy manner. The X.509 standard also addresses the format of attribute certificates (see section 4.3).

- **Digital documents:** digitally signed or otherwise authenticated documents can be used to express statements about an individual. Examples for such documents are a digital vaccination card or a digital driver's license. Individuals can be authorised to access e-services on the basis of such digital documents. Often, database records are represented by XML and are digitally signed in order to provide trustworthy information about an individual.

- **Anonymous and pseudonymous credentials:** an anonymous or pseudonymous credential serves the purpose of conveying attributes

related to a subject without disclosing an identity. A pseudonymous credential binds attributes to a pseudonymous identity while an anonymous credential conveys attributes only. Credentials can contain arbitrary attributes and constitute an anonymous form of digital identity (see section 4.2).

Two categories of digital credentials shall be examined more closely, namely anonymous and pseudonymous credentials and X.509 certificates.

4.1.1 Characteristics of Digital Credentials

Digital credentials come in many different forms that all can exhibit different qualities. Credential characteristics are chosen with regard to the requirements of a given application. Cap and Maibaum present a list of qualities that a credential can exhibit [CM01]:

Transferability: credentials can be transferable (i.e. the owner can pass the credential along to another person) or non-transferable.

Level of identification: credentials can be identifying (i.e. they contain a link to the owner's identity) or they can be anonymous or pseudonymous.

Divisibility: credentials can be atomic (indivisible) or divisible. An example for a divisible credential is an e-coin, which can be split into coins with smaller denominations.

Consumption: credentials can be shown an unlimited number of times (multi-show credentials), a limited number of times (n-show credentials) or only once (one-show credentials). An example for a one-show credential is an electronic coin, which can be spent only once.

One criterion can be added to this classification with regard to anonymous credentials:

Revocability of anonymity: an anonymous credential can either offer revocable anonymity or non-revocable anonymity. In case of revocable anonymity. a designated third party can discover the identity behind a credential-based transaction. Alternatively, anonymity can be non-revocable, i.e. a credential cannot be related to an individual under any circumstances.

With regard to these qualities, a public-key certificate is an identifying, non-transferable, atomic multi-show credential. An e-coin is an anonymous, divisible one-show credential that can be transferable or non-transferable, depending on the actual implementation of the e-cash system. An e-coin can feature revocable anonymity, i.e. the owner's identity can be discovered in case of double spending.

4.2 Anonymous and Pseudonymous Credential Systems

David Chaum introduced pseudonymous credentials in 1985 as a building block for an electronic transaction system in which users can conduct anonymous, unlinkable transactions [Cha85]. The system aims to preserve an individual's privacy while maintaining security for service providers. Credentials and pseudonyms are the basic elements of the system.

In the proposed system, users are known to organisations not under their real name but under pseudonyms. Users establish a different pseudonym with every organisation they have business with. In a transaction, users do not disclose their identity but merely a pseudonym. As users communicate with every organisation under a different pseudonym, business partners cannot trace a user across organisational boundaries. In order to maintain security, users can be held accountable for abuses committed under a pseudonym. This can be achieved by implementing a form of revocable anonymity with the help of identity escrow techniques (see section 2.1.6).

After users have established a pseudonym with an organisation, they can obtain credentials from that organisation. Credentials are statements about an individual that are signed by the issuer and can be shown to other organisations. They are used to prove statements about the holder and thus serve the purpose of establishing trust (see section 2.2.1). A credential from an organisation can be shown to other organisations (to which the user is known under a different pseudonym) without revealing the pseudonym under which the credential was originally established. Essentially, any credential can be used under any pseudonym. Credentials can contain several statements and users can choose which statements in a credential to divulge. When showing a credential, the holder can therefore disclose the exact attributes that are relevant for a given transaction.

Chaum's paper did not specify components or protocols of the system. At a general level, it can be said that such a system comprises users and organisations. In the least, it must have protocols to establish pseudonyms,

issue credentials and show credentials to organisations. For quite a number of years, Chaum's proposal could not be implemented fully but remained a vision. In the next section, we discuss two implementations of pseudonymous credential systems.

4.2.1 Implementations of Credential Systems

This section discusses implementations of pseudonymous credential systems. A first realisation of the concept was presented by Chaum and Evertse [CE87]. It is unsuitable for practical implementations however as it relies upon the existence of a semi-trusted third party that has to participate in all communications. We present two implementations of anonymous credential systems that have gained widespread attention in the privacy community. The approach by Camenisch and Lysyanskaya can be considered to be the most advanced implementation to date.

4.2.1.1 Brands' Approach to Pseudonymous Credentials

Stefan Brands proposed a credential system that implements many of the properties of Chaum's original concept. The system proposed by Brands can be regarded as a privacy-enhanced certificate system. Brands system allows an issuer to encode an arbitrary number of attributes into a credential. It allows a user to prove statements on attributes without disclosing the value of the attributes. In contrast to Chaum's proposal, the system does not distinguish between credentials and pseudonyms. However, a pseudonym may be encoded into a credential as an attribute. A formal description of the protocols can be found in [Bra00].

Brands system comprises two entities and two protocols:

- **Organisations**: organisations issue credentials to users. Organisations also accept credentials from users (in the role of verifiers respectively relying parties).
- **Users**: users obtain credentials from organisations. They show these to organisations in order to obtain access to services. Users do not establish pseudonyms with organisations. However, a credential may contain a pseudonym as an attribute.

The two protocols are:

- **Issue**: a protocol between an organisation (credential issuer) and a user that lets the user obtain a credential.

- **Show**: a protocol between a user and an organisation to show a credential. The user can select which attributes in the credential to disclose and also what statements to prove about the attributes.

In Brands' system, a credential is a triple consisting of a secret key, a public key, and the issuer's signature over the public key. The issuing organisation can encode an arbitrary number of attributes into a credential. The attributes are encoded into the secret key. The secret key consists of several big integer numbers. The public key is then calculated from the secret key. This results in a public key that is a single big integer number. Showing a credential works as follows: the user presents the public key and the issuer's signature to the verifier. The verifier asks the user to demonstrate certain statements about attributes that are encoded in the credential in order to establish facts about the user. With the help of the secret key, the user proves rightful possession of the credentials and proves statements about attributes. Brands' system allows a user to demonstrate any satisfiable proposition from proposition logic over the encoded attributes. Boolean formulas involving 'and', 'or' and 'not' can be proved. As an example, a user could prove that he is over 20 years of age and does not have Norwegian nationality.

While these features may sound compelling, the system nevertheless has drawbacks that in the opinion of the author seriously limit its suitability for practical implementations. Due to the construction of Brands' credentials, every credential is unique: every public key is unique and signed by the credential issuer. Credentials can thus be showed just once; otherwise transactions by the same user could be linked. In order to achieve unlinkable transactions, batches of credentials would have to be issued to users or a recertification protocol would have to be executed with the credential issuer after showing a credential.

Another point of criticism centers on the ability to encode a large number of attributes into a single credential and to disclose them selectively. This feature is, however, hardly of relevance in practical applications. There are presumably only few situations in which an issuer would like to encode a multitude of attributes into one and the same credential. Brands provides the example of a demographic credential that certifies nationality, income, age, current place of residence and marital status [Bra00]. However, all these attributes are currently administered by separate administrative entities, rendering such a credential impossible in most countries.

Instead of encoding n attributes into a single credential, the user could just as well hold n credentials. Handling a single credential with n attributes and deciding which attributes to show is hardly easier than handling n single credentials. The approach of encoding a large number of attributes into a

single credential furthermore poses certain difficulties regarding the expiry of the attributes. Frequent recertification of such a credential would be necessary, unless all attributes have exactly the same period of validity.

With regard to the credential qualities defined in section 4.1.1, the system proposed by Brands implements anonymous, atomic credentials. The system can be extended to provide multi-show credentials (by introducing recertification or batch issuing), anonymity revocation and non-transferability. Although Brands' system can be considered an interesting technical solution, we have come to the conclusion that the system has major drawbacks that make it unsuitable for many applications. The system implements requirements that the author judges as rather artificial and of lesser importance in many application scenarios.

4.2.1.2 Camenisch and Lysyanskaya's Approach to Pseudonymous Credentials

The credentials system proposed by Camenisch and Lysyanskaya can be regarded as the most advanced implementation of Chaum's concept to date. The system builds on earlier work by Lysyanskaya, Rivest, Sahai and Wolf [LRSW99]. The system also introduces features that were not proposed in Chaum's original paper. The new elements are local and global anonymity revocation managers as well as a root pseudonym authority [CL01]. Users must first register with the root pseudonym authority before participating in the credential system. This entity identifies the user and issues a root pseudonym. This mechanism ensures that users cannot build up several parallel identities and that users can be traced in case of fraud.

Users can establish a pseudonym with an organisation and obtain credentials from that organisation. Users are limited to one pseudonym per organisation. In the system, a credential carries a single attribute only and an expiry date. Users can choose what statement to demonstrate about that attribute, e.g. they can demonstrate that the attribute 'age' has a value bigger than eighteen.

The system features two types of anonymity revocation: pseudonymity revocation refers to the possibility to discover the pseudonym of a user. Anonymity revocation is the possibility of revealing the users identity. Camenisch and Lysyanskaya refer to these two features as local and global anonymity revocation. Before showing a credential, users can negotiate with a service provider whether any form of revocation is to be used. Furthermore, users can choose which anonymity revocation manager to appoint.

The system is built on statistical zero-knowledge proofs. In a zero-

knowledge proof, a party who possesses a secret proves knowledge of the secret to a verifier without disclosing the secret. The verifier does not gain any knowledge concerning the secret itself [GMR89]. When users engage in the credential show protocol, the credential itself is actually never shown to the verifier. Instead, the holder proves possession of a signature (by the issuer) over an attribute value. The attribute value is thereby not disclosed, neither is the signature of the issuer. The verifier does not learn anything about the credential, except that it is valid. Consequently, a credential can be shown as many times as desired without risking that transactions become linkable.

With regard to the properties presented in section 4.1.1, the credential system by Camenisch and Lysyanskaya provides anonymous and pseudonymous, non-transferable, atomic credentials that can be one-show or multi-show credentials. For one-show credentials, the system also provides double-spending detection. Users who show such a credential twice automatically disclose their pseudonym. The system can thus also be used to build an anonymous electronic cash system. The remainder of this section will describe the entities and protocols of the credential system.

The system comprises credentials and two types of pseudonyms:

- **Root pseudonym:** every user possesses exactly one root pseudonym. Users have to disclose their identity in order to establish this pseudonym. It guarantees that the identity of a citizen can be traced in case of misuse and that citizens cannot build up several parallel identities.
- **Pseudonyms**: a pseudonym is a name under which a user is known to an organisation. A user establishes a pseudonym with every organisation from which he respectively she would like to obtain credentials.
- **Credentials**: organisations issue credentials to users who have previously established a pseudonym. Credentials are issued with regard to a pseudonym but can be shown without disclosing the pseudonym.

The following entities participate in the credential system:

- **Root Pseudonym Authority:** an organisation that identifies the citizen and issues the root pseudonym to users.
- **Organisations:** an organisation establishes pseudonyms with users and issues credentials to users. Organisations also offer services that users can access with the help of credentials.

- **User:** a user obtains pseudonyms and credentials from organisations and shows them to organisations in order to obtain access to resources.
- **Pseudonymity and anonymity revocation managers:** an organisation that can examine a transaction record and assist in revealing the pseudonym respectively identity of a user. Camenisch and Lysyanskaya refer to these entities as local and global anonymity managers.

The credential system comprises the following protocols:

- **Establish root pseudonym:** a user contacts the root CA and is issued the root pseudonym.
- **Establish pseudonym:** a user contacts a credential-issuing organisation and establishes a pseudonym with the organisation.
- **Issue credential:** a protocol between a credential issuing organisation and a user. The organisation issues a credential to a user. The credential is linked to the pseudonym under which the user is known to the organisation.
- **Show credential**: a protocol between a user and an organisation that accepts credentials (relying party). The user contacts the organisation and shows a credential to this organisation. The disclosure of the user's pseudonym is optional.
- **Show credential with regard to a pseudonym:** a protocol between a user and an organisation that accepts credentials (relying party). When a user shows more than one credential, then this protocol is used to demonstrate that all credentials actually belong to the same party. Optionally, the user can disclose the pseudonym under which the relying party knows him or her.
- **Demonstrate possession of pseudonym:** a protocol between a user and an organisation (either credential issuer or relying party). The user divulges the pseudonym he has established with that organisation and proves rightful possession of this pseudonym. This protocol is a subprotocol of the two credential show protocols.
- **Anonymity and pseudonymity revocation:** a protocol between a relying party (credential-accepting organisation) and an anonymity revocation manager respectively pseudonymity revocation manager. The relying party contacts the manager and presents a transcript of a credential show. The manager outputs a value that enables the issuer

of the credential to discover the identity of the user respectively the pseudonym under which the credential was established.

While the system is clearly the most comprehensive credential implementation to date, it has to be mentioned that due to the construction based on zero knowledge proofs, the system is difficult to deploy in resource-restricted environments. The suitability of this approach with regard to the use in e-government will be discussed in section 6.7.

4.3 Public-Key Certificates and Public-Key Infrastructure

Both public-key and attribute certificates are a form of credential that is in widespread use today. This section provides a brief overview on the X.509 standard, which is a well-accepted standard for such certificates. Also, the infrastructure to support the use of public-key certificates is briefly discussed.

Public-key cryptography (or asymmetric cryptography) was proposed by Diffie and Hellman in their seminal paper 'New directions in cryptography' [DH76]. Before the introduction of public-key cryptography, only symmetric algorithms were used for data encryption. Symmetrical algorithms require two communicating partners to agree on a shared key before engaging in a confidential communication. In contrast, public-key systems use *two* keys: a public key, which can be published in a directory, and a private key, which must be kept secret. These keys are complementary: if a message is encrypted with a public key, it can only be decrypted with the corresponding private key, and vice versa. Examples for public key algorithms are the RSA algorithm [RSA78] or the El Gamal algorithm [EG85]. A thorough introduction to symmetric and asymmetric algorithms can be found in [MvOS96].

Public-key cryptography supports three generic security goals that are especially valuable in distributed settings. It provides

- confidentiality of data by encryption, without the need of establishing shared keys
- robust authentication of communicating parties by use of challenge-response protocols
- non-repudiation, as public key cryptography can be used to create digital signatures

First, the X.509 standard for public-key and attribute certificates will be discussed, followed by a brief overview on public key infrastructure.

4.3.1 Public-Key Infrastructure

The use of public-key cryptography must be supported by an infrastructure, a so-called public-key infrastructure (PKI). A PKI is not a physical object or software process; it is a set of useful services provided by a collection of interconnected components. A PKI consists of the following components [MvOS96]:

- **End-entity:** an end-entity is any entity that can be the subject of a certificate. Both individuals and machines (server, routers) can be the subject of a certificate.

- **Registration Authority (RA):** users who wish to obtain a certificate contact this entity. During the registration process, the RA verifies a user's identity and ensures that all the conditions are met for issuing a certificate.

- **Certification Authority (CA):** the certification authority generates key pairs and issues certificates. The CA publishes certificates in a directory. Registration of end-entities is usually delegated to a RA.

- **Repositories:** Two types of repositories exist:

  - **Certificate repository**: public-key certificates need to be published in a publicly accessible directory. Each CA maintains a directory in which the issued certificates are published.
  - **Certificate revocation list (CRL) repository**: if a certificate needs to be invalidated before its scheduled expiry, the CA publishes the certificates serial number in a list. Such a list is called a certificate revocation list.

An entity that issues certificates (comprising RA, CA and repositories) is informally also called a trust center. Certification authorities usually form a hierarchy: the CA at the top of the hierarchy is called the root CA and possesses a self-signed certificate. A CA issues certificates to intermediate CAs and end-user CAs. Intermediate CAs issue certificates to other CAs but do not issue certificates to end-users. Only end-user CAs issue certificates to end-entities. In any country, several parallel hierarchies of certification authorities may exist. Figure 4.1 illustrates the concept of hierarchical CAs.

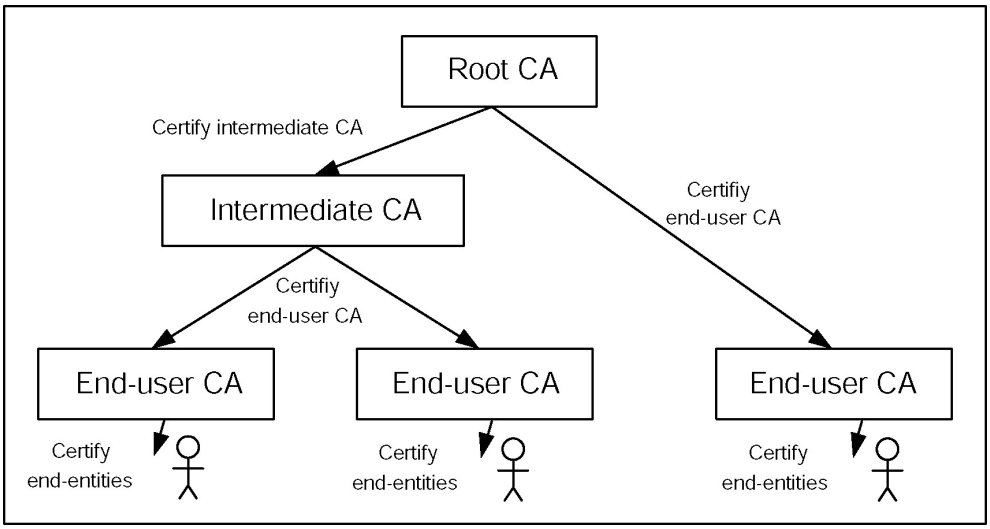

Figure 4.1: An example hierarchy consisting of root CA, intermediate CA and end-user CA

4.3.2 X.509 Public-Key and Attribute Certificates

The International Telecommunications Union (ITU) has created a standard for the format of public-key and attribute certificates in order to allow for interoperability of certificate-based applications [ITU88]. The X.509 standard is today viewed throughout the IT industry as a well-accepted standard. It was published in 1988 as part of the X.500 Directory recommendations. In 1996, X.509 Version 3 was released and introduced a mechanism to include arbitrary additional attributes (called extensions) in the certificate. The standard describes the syntax of both public-key and attribute certificates. Table 4.1 describes the fields that must (in the least) be contained in an X.509 certificate.

With regard to the certificate format, the only difference between public-key and attribute certificates is that the latter do not contain a public key (and thus lack the field 'Subject Public-key Information'). Apart from that, they comprise the same fields as a public key certificate. The link between the attributes in the certificate and an entity is achieved by including the serial number and issuer name of that entity's public-key certificate. Typically, attribute certificates are used for access control in distributed systems. Such a certificate may contain arbitrary attributes that specify e.g. group membership, a role, security clearance or other information that is associated with the certificate subject.

For the description of subject and issuer names, the X.509 standard relies on X.500 names. The X.500 standard describes directory services to

Field	Content
Version	Version of the X.509 standard
Serial Number	Unique serial number assigned by the issuer
Signature Algorithm Identifier	Signature algorithm used by the CA to sign the certificate
Issuer Name	The X.500 name of the entity that signed the certificate
Validity Period	Validity period of the certificate
Subject Name	The X.500 name of the certificate subject
Subject Public Key Information	Public key of the entity, together with an algorithm identifier and any associated key parameters.
Signature by Issuer	The signature over the data fields by the issuer

Table 4.1: Structure of an X.509 public-key certificate

manage information about objects in a worldwide scope. The objects can be organisations, people or machines. It provides the capability to look up information by name. The standard defines a hierarchical namespace that provides unique subject names across the Internet. In X.500 terminology, such a unique name is called a 'distinguished name'. A subject is described with a set of standardised attributes, e.g. with its common name (CN), the organisation it is affiliated with (O), the organisation's country (C) and the organisational unit (OU). There are many more fields that can be used to describe an entity. An example for an X.500 name is CN=Auerbach Niklas, O=University of Zurich, OU=IFI, C=Switzerland.

4.3.2.1 Revocation of X.509 Certificates

Revocation of signature and attribute certificates works as follows: X.509 certificates include a serial number in the certificate. In the case of revocation, an issuer publishes the serial number of the certificate in the certificate revocation list (CRL). This list includes the serial numbers of all revoked certificates, the exact time of revocation and usually a code that indicates the reason for the revocation. The list also indicates the time when it was published and the time when the next updated CRL will be published. The list must be signed by the issuer in order to be trustworthy.

Relying parties then consult this CRL. When presented with a certificate, the relying party checks whether the certificate's serial number is contained

in the revocation list. Also, the public key of the certificate issuer (the key that was used to sign the certificate) is checked for validity. This approach creates a need to distribute certificate revocation information to relying parties attempting to verify the validity of certificates. The need for revocation information and the intervals of updating depend on the nature of the application. Relying parties may fetch revocation lists at regular intervals, or the issuer may deliver the lists to relying parties.

An alternative approach to revocation lists is the so-called online certificate status check. When presented with a certificate, a relying party may contact the issuer of the certificate to query the validity of the certificate. Online queries eliminate the need to repeatedly communicate revocation lists. The drawback of this approach is that communication overhead (and thus latency) is added and that it only works in settings where relying parties are continuously online.

4.4 Group Signature Schemes

Group signatures are a relatively recent cryptographic concept that was first proposed by Chaum and van Heyst [CvH91]. In a group signature scheme, users form a group that is administered by a group manager. Members can issue signatures on behalf of the group with the special property that signatures are verifiable only with regard to a single group public key. Signatures remain anonymous for everyone except the group manager. Therefore, group signature schemes afford members full anonymity within a given group. Group signatures have been applied to electronic cash [Tra99] and anonymous bidding systems [NT00].

A group signature system works as follows: A group manager sets up a group and creates a group public key that is common to all group members. When a member joins, the member obtains the secret membership key along with a membership secret. If revocable anonymity is desired, an additional secret can be established for the purpose of identity escrow. The group member can now issue signatures on behalf of the group. A verifier can determine if the signer is a member of the group but cannot learn anything about the signer's identity. In exceptional cases, such as a legal dispute, the group manager can decide to open a signature and divulge the identity of a signer [CM98]. Alternatively, this functionality can also be moved to a third party, called the anonymity manager. The anonymity manager can then examine signatures and help discover the identity of the group member who has issued the signature.

The following entities participate in a group signature scheme:

- **Group manager**: the group manager is responsible for setting up the system parameters (i.e. choose group keys) and admits users into the group. When presented with a signature, this entity can determine a user's identity (unless this functionality is attributed to the anonymity manager).

- **User:** A user may join a group and issue signatures on behalf of the group.

- **Anonymity manager (optional):** the task of anonymity revocation can be assigned to an anonymity manager. This trusted party can be organisationally separated from the group manager.

- **Verifier (relying party):** an entity that accepts signed information from users. A verifier can only determine whether a signer is indeed a member of the group but cannot learn anything about the signer's identity from examining a signature.

A group signature scheme comprises the following protocols:

- **Setup**: this protocol is performed by the group manager to generate the group public and private key.

- **Join**: a protocol between a user and the group manager. This protocol is executed whenever a user joins the group.

- **Sign**: a protocol between a user and a relying party. The user issues a signature on behalf of the group.

- **Open**: a protocol between a relying party and the group manager. The group manager examines a signature by a user and reveals the identity of the user. This functionality also involves the anonymity revocation manager if revocation is to be performed by a trusted third party.

The group signature scheme presented by Ateniese, Camenisch, Joyce and Tsudik is currently the most efficient solution. A mathematical description of the protocols can be found in [ACJT00]. The modifications presented by Canard and Girault make it feasible to implement group signature schemes on smart cards [CG02].

4.5 Identity Management

We have stated that digital identity can be considered to be the set of all data in information systems that relates to a given individual (see section 2.2). Identity management departs from this concept of digital identity and intends to give users better control over the release of their personal data [KP01]. Identity management aims at giving users of electronic services the power to determine for themselves what data concerning their identity to disclose to other parties in the course of an electronic transaction. It intends to restore the power of informational self-determination to the user.

An identity manager runs on a device of the user and is involved in all communications with service providers. It keeps control over the user's data and warns the user if personal data is to be disclosed in a transaction. The identity protector as described in [Reg95] was the first proposal for an identity manager. Another early concept related to identity management was a PDA-based manager for personal reachability as presented in [GPS98]. It let a user choose when to stay anonymous respectively unreachable. A Web-based identity manager was developed by Bell Laboratories [GGMM97]. Later approaches further developed the concept of identity management to manage all transactions of a user in electronic networks [Köh00]. Identity managers were proposed on the basis of PDAs, which the user can carry along at all times. With such an approach, users conduct all electronic transactions with the help of a PDA on which the identity manager is installed [KP01], [GtMJ01], [Jen03]. There are no commercial applications yet that support identity managers.

This thesis is not addressing identity management in general but is focused on the use of pseudonymous credentials on electronic identity cards. The thesis addresses privacy issues related to the use of e-ID cards and proposes digital credentials as part of the citizen's digital identity as a measure to alleviate privacy problems.

4.6 Anonymous Communications in the Internet

Anonymous transactions in distributed systems can only be achieved if the underlying network allows for anonymous communication. In the absence of an anonymous communication channel, messages can be traced back to a specific machine (e.g. to an IP address) thereby compromising the anonymity of the user. As explained in section 2.1.3, a message is anonymous if neither the recipient of a message nor an eavesdropper can determine the sender

of the message. With regard to IP-based networks, a single IP packet is considered to be a message. As an illustrative example, one might consider anonymous Web-surfing. In the context of Web-browsing, anonymity means that neither the party that operates the Web site nor an adversary who can read all traffic on the Internet is able to determine the IP number of the user who has sent the HTTP-request.

Several proxy services exist that afford anonymous Internet communication to users and enable users to surf the Web anonymously: examples include onion routing [GMR89], Crowds [RR98] or the Java Anonymity Proxy (JAP) [BFK01]. Onion routing and JAP make use of the mix approach, while Crowds relies on a peer-to-peer approach. Mix-networks are a promising approach to anonymous communication in a computer network. While the mix technology was originally proposed by David Chaum to implement anonymous e-mail communication [Cha81], the basic approach is also suitable to achieve anonymous communication channels in packet-based networks such as the Internet.

A user achieves anonymity by routing all Internet communications through a mix cascade, which is a chain of several mix servers. The user defines the order of the mix servers before engaging in communications. A mix is a store and forward device that accepts messages from a multitude of users, reorders the messages, changes their appearance by cryptographic means and outputs them in a different order. All messages are routed through the mix cascade in an encrypted form. The last server in the cascade transfers the message to the final recipient. The order of the mixes is predefined and encrypted along with the message.

Mix networks can provide anonymous communication channels in the Internet but have the drawback that they cause a considerable overhead, as asymmetric cryptography is used to encrypt messages. Mix networks are furthermore only effective if used by a considerable number of users, as the messages of any user are effectively hidden among the messages of other users. Furthermore, users should constantly produce dummy traffic, to provide enough messages for the mixing process.

4.7 Electronic Identity and Citizen Card Initiatives in Europe

The shift from traditional, paper-based interaction with citizens to Internet-based electronic transactions requires new ways of establishing trust electronically. While pure information services do not pose the problem of reliable identification of a user, the migration towards legally binding on-line trans-

actions requires a strongly authenticated form of electronic identity. Many European countries have engaged in activities to introduce electronic identity (eID) cards and some municipalities in Europe have issued electronic citizen cards.

Before engaging in a discussion of eID card projects, we define some terms. The term optical identity card refers to an official identity document that is valid at a national level and does not carry an embedded microprocessor. Many Europeans countries, among them Switzerland, issue optical identity cards to their citizens. The term electronic identity card refers to a card with an embedded microprocessor that is valid at a national level and establishes the citizen's identity in electronic settings. Often, optical and electronic identity card are combined into a single card. Such a card carries all features of an optical card on the outside and also features an embedded microprocessor.

The term electronic citizen card refers to a card which is used to establish the citizen's identity in electronic settings but which is not valid for identification at a national level. Such cards are usually issued by local municipalities. However, both identity and citizen cards serve the purpose of identifying citizens and to enable them to issue digital signatures. Both types of cards are also referred to as 'digital' identity or citizen cards instead of as 'electronic' identity or citizen cards.

The author expects that the trend towards transactional e-government services will finally bring every European country to issue digital identity or citizen cards. Such cards will eventually become an element of daily life for many citizens in the EU. We will first present the general approach to electronic identity cards that is taken by European card projects. Following this general concept, we will present identity and citizen card projects in Europe that are currently under development or have already issued cards to citizens.

4.7.1 General Approach Taken to Electronic Identity Cards

All current eID card projects follow the same concept with regard to identification of citizens. The digital identity of the citizen is modelled by use of two key pairs and in some cases by use of an additional personal data set on the card. The cards usually provide the following functionality to a user:

- **Strong authentication in remote communications**: a citizen can be reliably identified and authenticated in remote settings. This is

e.g. accomplished by setting up an SSL connection with client-side authentication.

- **Confidential communications:** the citizen can encrypt and decrypt arbitrary data. Citizens may use this functionality to encrypt documents or send and receive encrypted email messages.

- **Digital signatures**: a citizen can issue a digital signature with the help of the card (non-repudiation).

In order to provide this functionality, the card contains two key pairs and the corresponding public-key certificates:

- **Authentication (identity) key pair and certificate**: this key pair is used for authentication purposes and also for decryption and encryption of data.

- **Digital signature key pair and certificate**: the holder exclusively uses this key pair to issue digital signatures. The EU signature directive explicitly forbids the use of this key pair for any other purpose [Eur99].

Both authentication and signature certificate are usually linked with the citizen's entry in the population register. This link is necessary to ensure that when a citizen uses an e-service, the right person's administrative records are changed. A public-key certificate usually only contains a person's name. Even if the date of birth was added, these two data items still do not allow for a reliable identification of a person.

Citizens access services either with the help of proprietary clients or with a Web browser. In the second case, additional software that extends the functionality of the Web browser needs to be installed. Such additional software e.g. provides drivers for accessing the card or a secure viewer for documents that are to be digitally signed.

In terms of an application programming interface (API) for the development of card applications, most card projects rely on the PKCS #11 standard. The PKCS #11 standard is published by RSA Data Security Inc. and describes an application programming interface between a host and a cryptographic device (e.g. a smart card) [RSA97]. The API comprises functionality for issuing digital signatures, calculating hash values and for symmetric and asymmetric encryption of data. PKCS #11 is a rather limited standard. The use of features such as storing and retrieving documents from a card is not addressed by the standard. Some projects, such as the Austrian citizen card, use a proprietary API.

4.7.2 Electronic Identity Card Projects in Europe

This section gives an overview on digital citizen and identity card initiatives in Europe. Only projects at a national level are described. Citizen card initiatives by local councils in EU member states are not discussed, with the exception of the eEpoch project. Switzerland's plans for an electronic identity card are considered as well, although it was unclear at the time of writing whether these plans will be realised in the near future. All cards presented in this section follow the approach outlined above that comprises an authentication and a signature key pair.

4.7.2.1 The Finnish FinEID Card

Finland was the first European country to issue an electronic identity card, called the FinEID card. The FinEID card serves both as electronic and optical identity card. Governmental services and also some private sector services are available for the card, e.g. on-line banking. The card costs 29 Euros and is valid for five years. Figure 4.2 depicts the front-side of the FinEID card.

Figure 4.2: The FinEID card (source: http://www.fineid.fi)

On the outside, the FinEID card carries personal data, a photograph of the card holder and a signature. The FinEID card contains an authentication and a signature key pair, along with the corresponding certificates. The cardholder's certificates contain the first and last name of the holder and a unique identity number (FINUID). No other personal data is contained on the card. The public key infrastructure for the FinEID project is run by the government. The certificates are issued by the Finnish population register (Väestörekisterikeskus).

Although the FinEID project pioneered the use of electronic identity cards and can be deemed a success on a technical level, we should mention that the cards are not used widely today. Only around 30'000 cards were issued to a population of about 7 million citizens. There still seems to be a lack of attractive on-line services that actually bring a value to the citizen.

4.7.2.2 The Austrian Bürgerkarte

The Austrian Bürgerkarte project is different from other European card projects, as it is not an actual implementation of a citizen card but much rather a specification. The Bürgerkarte project essentially specifies an interface to a cryptographic device that provides authentication and digital signature functionality to the citizen [PKK+02]. Currently, only smart cards are used as such a device.

The concept addresses the content of certificates, the issuing process of certificates and an interface between cryptographic device and applications. The first cards were rolled out by the Austrian Computer Society in 2002.

The Bürgerkarte concept comprises a key pair for authentication and one for digital signatures. Apart from the keys and certificates, no other personal data is stored on the device. The certificates are linked to an entry in the central population registry. In order to establish this link, citizens have to visit the local municipality when applying for a certificate. The certificates are issued by private sector certification authorities.

The card is intended both for e-government applications and private sector applications. In order to use the card, citizens need to install a security capsule on their computer, which acts as an interface layer between applications and the card. In the future it is planned to supply an off-card document storage space in which citizens can securely keep documents that do not fit onto the cryptographic device.

4.7.2.3 The Belgian Electronic Identity Card

In April 2003 Belgium has started the pilot phase for its electronic identity card EIC (Electronische Identiteitskaart). The government has issued 60'000 cards to inhabitants of 11 cities. The pilot will be evaluated after a trial period of at least 6 months and in case of a positive evaluation, the Belgian government expects to distribute over 10 million electronic identity cards. Both citizens and foreigners will receive an electronic identity card. These cards will eventually replace the current Belgian identity card.

The EIC serves as electronic and optical identity card. The EIC card contains an authentication and a signature key pair, along with the corresponding certificates. Apart from the certificates, the card does not contain any personal data. Local municipalities act as registration authority and also issue the cards. The national population register issues the certificates.

The EIC card is based on Sun's JavaCard technology and is capable of carrying multiple applets. It is primarily intended for accessing governmental electronic services. There are no private sector applications yet for the card.

4.7.2.4 The Estonian Electronic Identity Card

Estonia has issued an electronic identity card that also serves as an optical identity card. The card was presented in January 2002 and within one year, more than 130 000 cards were issued. Citizens apply for the card at the Estonian Citizenship and Migration Board. The card and also the certificates are issued by a private sector trust center, founded by banks and telecom companies. The card is also issued to foreigners who stay in Estonia for more than six months.

The card carries a signature and an authentication key pair. Furthermore, the card stores a data file that contains the same personal data as on the outside of the card. According to the white paper on the Estonian eID card, this file is publicly readable [Ser03]. The card is intended for the use in public and private sector applications. As an interesting feature, every cardholder gets a state-assigned email address that is also stated in the authentication and signature certificates.

Estonia and Finland plan a cross-certification with the goal to mutually accept signatures that were issued with the FinEID respectively the Estonian identity card.

4.7.2.5 The Italian Electronic Identity Card

Italy entered the pilot phase of its electronic identity card project CIE (Cartà d'Identita Elettronica) in March 2001. It is planned to roll out the card to 50 million Italians by 2005. Plans for an electronic identity card were made around the middle of the 1990s. The card serves both as an optical and electronic identity card [Gen01].

Next to the embedded microprocessor, the card also features an optical storage band on the outside of the card that can store 1.8 MB of data. The optical storage of the WORM (Write Once Read Many) type and is used to record all administrative transactions that are made with the card. The CIE is intended for access to national and local governmental services only. It is not intended for private sector applications. It can be updated securely over the network by local and national administration. In later stages of the project, it is planned to include data related to health-care services on the card.

The data set on the outside of the card is quite comprehensive. It comprises the citizen's name, data of birth, nationality, height, the current place of residence and the fiscal code. The same data set is also stored on the card. Eventually, a digital representation of the citizen's fingerprints will be stored on the optical band. The card contains two key pairs, one for authentication

and one for issuing digital signatures. Both certificates are issued by the ministry of the interior.

4.7.2.6 The eEpoch Project

eEpoch is a demonstration project funded by the European Community. The acronym eEpoch stands for 'eEurope Smart Card Charter Proof of Concept of a Holistic Solution'. It is intended as a proof of concept of the eEurope Smart Card Charter [eEu99] and aims at demonstrating the viability of a pan-European platform for digital citizen cards. The card is a multi-application card that is intended for authenticated and secure interaction with local government as well as the use in e-commerce applications.

The common technical platform comprises a smart card, a standardised card reader and client applications. The card will offer the following features:

- Standardised digital identity of the citizen through a common set of personal data
- Authentication functionality and digital signature functionality. Two different signature certificates will be used, one for the governmental domain and one for the use in e-commerce
- an electronic purse (payment service)
- a multi-application platform that allows the downloading of applications to already issued cards

The project will set up pilot sites in 6 European countries and one in Israel. A longer-term objective of the eEpoch project is to propose solutions to harmonise smart card infrastructures to support the interoperability across sectors and countries. According to the project plan, the first pilot site should go operative in early 2004.

4.7.2.7 Switzerland's Plans for a Digital Identity Card

In 2001 the Federal Department of Justice and Police carried out a study to investigate benefits and risks of a national electronic identity card [MSV01]. Based on this study, The Swiss Council authorised the Federal Department of Justice and Police to develop a concept for an electronic identity card. This concept is scheduled for publication in early 2004.

Some details on the proposed card were published in a first paper by the Department of Justice and Police [Bür03]. According to the paper, a Swiss electronic identity card will act both as an optical and electronic ID card and

replace the identity card that is in use today. It will contain an identity and a signature key pair. The card is intended for both private sector and public sector applications. It is not yet clear who will issue the certificates. The concept states that private sector issuers would be a viable alternative to a government-operated PKI.

However, some problems must be overcome before the concept can be realised. First and foremost, digital signatures do not have the same legal status as hand-written ones yet. A law on digital signatures has passed both chambers of parliament in 2003. The law will come into force in 2005.

Another problem that an ID card initiative will have to face is the lack of a centralised population register: even if citizens could be identified beyond doubt by use of an identity certificate, entries in public databases could not reliably be linked to the certificates. The government is currently working on a harmonisation of the federated population registry. As a primary driver for this harmonisation, the Swiss government states the use of data for statistical purposes. As part of the harmonisation, a federal personal identification number is to be introduced. Such a number would most probably be included in the authentication and signature certificates of the citizen.

Last but not least, a public key infrastructure will have to be built. The only company that offered certification services, Swisskey, has ceased operation in 2001. A public key infrastructure will thus have to be built either by the private sector or by the Swiss government.

4.7.2.8 Other Countries:

Germany, Denmark and Norway have currently no plans to introduce a national eID card. In Germany and Norway, local municipalities have issued citizen cards. Spain is planning to introduce a national eID card and is currently running a pilot project with civil servants. France is working on the 'Titre Fondateur' project, a visual and electronic identity card.

Table 4.2 summarises the information about electronic identity card projects in Europe. The table only comprises projects that have already issued cards to citizens.

4.8 Summary

Digital credentials are statements about a subject that are signed and used to establish trust. Both public-key and attribute certificates are a form of digital credential that is in widespread use today. Pseudonymous credentials constitute a form of anonymous respectively pseudonymous digital identity.

	FinEID	**Bürgerkarte**	**Belgian EIC**	**Estonian eID**	**Italian CIE**
Project Status (4^{th} Quarter 2003)	Productive use; approx. 30'000 cards issued	Productive; first cards issued in 2002	Pilot phase; 60'000 cards issued	Productive; approx. 130'000 cards issued	Pilot; first cards issued in 2001
Visual Identity Card	Yes	No	Yes	Yes	Yes
Key Pairs on Card	Signature, Authentication	Signature, Authentication	Signature, Authentication	Signature, Authentication	Signature, Authentication
Card Holder Authentication	PIN	PIN	PIN	PIN	PIN
Personal Data Set on Card	No	No	Yes	Yes	Yes
Personal Data Set protected by PIN	Yes	Yes	Yes	No	Yes
Capability to Carry Multiple Applets	No	Depends on device	Yes	No	No
Additional Optical Storage on Card	No	No	No	No	Yes
Storage for Digital Documents	No	Yes	No	No	No
PKI run by	Government	Private Sector CA	Government	Private Sector CA	Government

Table 4.2: An overview on digital identity card projects in Europe

Pseudonymous credentials were proposed by Chaum as a technology that can enable users to conduct anonymous transactions while maintaining security for service providers. The most advanced proposal for a pseudonymous credential system is the approach by Camenisch and Lysyanskaya. As the use of credentials makes an anonymous communication infrastructure necessary, mix networks were presented as a technology for anonymous communication channels in the Internet. Group signature systems were presented as a technology that can afford anonymous signatures within a group.

Chapter 5

From Privacy to Anonymous Transactions in e-Government

This chapter discusses potential privacy problems that may arise with the introduction of electronic service delivery in the governmental domain. First, the concept of privacy is introduced with an emphasis on informational privacy. Next, a brief overview of data protection legislation is given with a focus on the European legislation in this field.

Departing from the notion of privacy, we consider potential privacy problems of e-government systems. Some of these problems concern e-government in general, others are dangers that arise specifically from the use of digital citizen cards. Possible counter-measures to these threats to privacy are discussed. If a wide-spread acceptance of electronic services is to be achieved, these dangers must be addressed. In the light of informational privacy, anonymous and pseudonymous services are proposed to enhance the citizen's privacy. It is shown that anonymous services are a means to enforce the principles of data avoidance and data minimisation. The introduction of anonymous services opens a space of design choices for service providers with regard to identification and authentication. This range of choices is outlined and recommendations are given for the different types of services. The chapter closes with recommendations as to how the informational privacy of the citizen can be enhanced.

5.1 Privacy in e-Government

With the arrival of electronic data processing, the concept of privacy and especially that of informational privacy has been given increased attention. New information technologies have brought on the capability to store, retrieve

and distribute big quantities of data at a cost that keeps steadily decreasing. However, privacy has been an issue on people's mind long before the creation of computers.

5.1.1 The Concept of Privacy

More than 100 years ago, Warren and Brandeis wrote the landmark paper 'The Right to Privacy', published in the Harvard Law Review in 1890 [WB90]. The authors felt that 'the too enterprising press' intruded into people's privacy by taking pictures without asking for consent first. They defined privacy as 'the right to be let alone' and argued that legislation should give this right to every individual: "Political, social, and economic changes entail the recognition of new rights" [WB90].

In the twentieth century, many legal scholars and philosophers have attempted to give a definition of the concept of privacy [Gor92]. However, there can be no universally valid definition of privacy as the concept depends on social aspects, the legal framework and cultural values. The issues of privacy are "fundamentally matters of values, interests and power" [Gel98].

An implication of the nature of privacy as an interest is that it has to be balanced against other competing interests. The interest of people in their own privacy may conflict with the interests of other people or organisations [Etz99]. As an example, one can mention the interest of a bank in keeping records about their creditors for risk management purposes. Such data collections may collide with the interest that bank customers have in safeguarding their privacy.

The concept of privacy does not apply to mere information only. Privacy rights have a long tradition and are implemented in many fields [Ros92]:

- **Territorial privacy**: protects the physical surroundings of a person, i.e. in a domestic or other environment.
- **Bodily privacy**: protects the physical integrity of a person against undue interference (e.g. physical searches, DNA testing).
- **Communication privacy**: protects the personal communication of a person against monitoring by other persons or organisations.
- **Informational privacy:** the right of a person to control what data about his resp. her person can be gathered, processed and disseminated.

In the context of information systems, the consideration of privacy leads naturally to the notion of informational privacy. This restriction makes sense

as an information system usually does not affect territorial or bodily privacy (with the exception of robotics applications or some ubiquitous computing devices, which are currently outside the scope of a discussion related to e-government). The considerations will focus on informational privacy, as this category is relevant for the design of citizen-centric e-government systems. Minimal rights pertaining to informational privacy are guaranteed in many countries through data protection legislation.

Interestingly enough, the problems that haunted Warren and Brandeis a long time ago may return to threaten people's privacy yet again. With the widespread introduction of cameras in mobile phones and the increasing bandwidth in mobile telecommunication, there is again the all-present threat of photography. A picture may be taken and sent within seconds. Although the share of camera-equipped phones is still small, concerns about this new technology have been growing: in Saudi-Arabia, a government commission has forbidden camera-phones altogether and the Italian government's delegate for privacy is planning to draft a phone-specific recommendation. Time Magazine has featured an article on this new privacy threat and warned of 'a new wave of Web-voyeurism' [Gui03].

5.1.2 Informational Privacy in e-Government

A very common and well-accepted definition of informational privacy is the one given by Alan Westin in his classical work on privacy. Westin defines informational privacy as

> '...the claim of individuals, groups and institutions to determine for themselves when, how and to what extent information about them is communicated to others' [Wes67].

At the heart of the notion of informational privacy lies the understanding that some information about a person is not public but indeed private. It is not possible to give a precise definition as to which data is public and which is not. Such a notion depends on cultural understanding and personal views. Informational privacy is, just like other forms of privacy, an interest of an individual that may compete with interests of other parties. Fred Cate emphasises the subjective nature of informational privacy and illustrates the often conflicting interests with an example:

> '[Informational] Privacy is not an absolute. It is contextual and subjective. ... The privacy interests at stake in any given situation may vary from the profound to the trivial, and that valuation will depend significantly on who is making it. If, however, privacy

> permits me to avoid paying taxes ... it may be very valuable to me, but extremely costly to society as a whole. What is needed is a balance, of which privacy is a part. Determining what that part is in any specific context requires a careful evaluation of subjective, variable and competing interests.' [Cat97]

With the wide-spread use of information systems, the focus on privacy shifts towards an understanding of privacy as the right to informational self-determination. An individual should have the right to control the release and dissemination of personal data as well as the context in which the data is going to be used to the greatest possible extent. In addition to Alan Westin's definition of informational privacy, we will generally state that informational privacy and the measures to protect it should address:

- the release and dissemination of personal data
- the protection of highly sensitive data in e-government systems (see section 5.1.3)
- the latent danger of tracking and logging of users and their activities

Privacy threats may arise both from the front-office part and the back-office part of e-government transactions. The front-office part of a transaction comprises the identification and authentication of a citizen as well as the communication with the service provider. The back-office part of a transaction is concerned with the processing of data that was supplied by the citizen. Often, more than one administrative entity is involved in this stage of a transaction. Section 5.3 will explore the threats to informational privacy that may arise from the electronic service delivery in the governmental domain. We will distinguish between threats that arise from the use of smart cards and threats of a general nature that are unrelated to smart cards. Counter-measures to these threats will be proposed that have the potential to heighten the informational privacy of the citizen.

5.1.3 The Sensitive Nature of Information in e-Government

Informational privacy is an especially important issue in e-government. The data that are processed in e-government environments are often of a much more sensitive nature than the data processed in the domain of electronic business [JGAS02]. Data in governmental databases contain highly sensitive data such as social security numbers, information related to individual

taxation, data concerning religious beliefs, criminal records, demographic information and medical records. This fact may be illustrated with an example from World War II: in many European countries German occupiers could easily find Jewish citizens with the help of lists that were maintained by local administrations. Even today, many administrative systems record data about the religious affiliation.

Administrative cultures and procedures in Europe vary and so do the views on the sensitivity of data. The religious affiliation is considered a very sensitive issue in the Netherlands and in Greece, while inhabitants of Finland are very sensitive about data that relates to the gender of a person. Many other examples can be found illustrating the differences that exist with regard to the sensitivity of data.

Another important aspect that differentiates governmental data collections from private sector data collections is that administrations can force citizens to supply data. Many administrative services are compulsory in nature (e.g. citizen registration in most European countries). Administrations are thus empowered by law to collect a wide range of data.

5.1.4 IT Security Goals and Informational Privacy

The terms informational privacy and data security are sometimes wrongly used as synonyms. Data security is neither an equivalent to privacy nor does it automatically imply privacy. We therefore have to differentiate between the concepts of IT security in general, data security and safety.

IT security in general comprises measures both at a technical and an organisational level to achieve the following generic security goals [Eck01]:

- **Confidentiality**: prevention of unauthorised access to data
- **Integrity**: ensuring that data is a proper physical and semantic representation of information and that information processing resources perform correct operations. Data integrity aims at preventing unauthorised users from making modifications, and authorised users from making improper alterations, thus striving to maintain data consistency.
- **Availability**: prevention of unauthorised withholding of data or resources. Goals are timely response, fault tolerance, fair allocation and usability [Pfleeger97].
- **Accountability**: ensuring that users can be made accountable for modifications of data in the system.

- **Authenticity**: ensuring that subjects and entities are identified and that this claim of identity is verified.

Data security is one aspect of IT security. The term data security refers to the protection of data from unauthorised modification, destruction, or disclosure [Eck01]. It includes measures to prevent unauthorised use, access and disclosure of data. It also comprises means to enable the investigation of breaches in data security. Data security measures aspire to make data processing safe regardless of the legitimacy of processing.

Furthermore, a distinction between security and safety can be made: while security is concerned with the points mentioned above, safety addresses the issues of functionality and reliability. Safety requires the system to perform its functions always as expected (functionality) and to always perform them in an identical manner (dependability). Safety is especially important when considering the protection of persons against the immanent risks of an information system. The increasing number of IT systems deployed in high-risk areas such as medical information systems or public transport render this perspective increasingly significant.

Data security consequently has to be seen as a prerequisite for enforcing data protection. It is a 'conditio sine qua non' for informational privacy. Notwithstanding, issues of data security constitute only a small part of the considerations comprised in the field of informational privacy.

5.2 Data Protection Legislation

Modern data processing systems are widely perceived as a threat to informational privacy and have sparked the creation of data protection laws [OEC80]. The laws aim at regulating the collection, storage, processing and dissemination of personal data. The term 'personal data' refers to any kind of data that can be related to an identifiable individual [Eur95]. Legislation on data protection is relevant for and applicable to the design of e-government systems. Legislation varies significantly from country to country and also has an impact on economic relations between countries, as today's networked economies increasingly entail the exchange of data across borders. Information systems in the administrative domain must respect the legal framework established by data protection legislation.

5.2.1 A Brief History of Data Protection Legislation

The many dimensions of privacy make it difficult to establish detailed, operational rules about privacy protection. Instead, legislators take a constructive

approach and establish general principles, apply them to all organisations and create sanctions against non-compliance. This approach has led to the creation of data protection legislation and guidelines.

The term data protection laws is somewhat misleading as the aim of the legal frameworks is not to protect data but to protect individuals respectively their personality rights. Most data protection laws therefore address only personal information, i.e. 'any information relating to an identified or identifiable individual' [OEC80].

The interest in informational privacy increased in the 1960's and 1970's due to the widespread use of information technology. Legislative bodies began addressing the problem in the 1970's. The first modern data protection act was adopted by the German State of Hesse, the first national law by Sweden in 1974.

A very influential piece of data protection legislation is the US Privacy Act [Uni74]. The act was passed by the Congress in 1974, thereby acknowledging that the rapid development of information systems posed a threat to personal privacy.

Although the US Privacy Act was not very successful in the US, it found much attention abroad. This resulted in the fact that many elements of this policy can be found in data protection laws of other countries. The approach of a comprehensive data protection legislation was nevertheless not followed up: today, the United States prefer a sectoral approach that relies on a mix of legislation, regulation, and self regulation. As a consequence, a patchwork of laws has emerged.

The OECD recognized that the trans-border flow of personal information contributes to social and economic development but concluded at the same time that privacy and individual liberties had to be protected. The 'Guidelines on the Protection of Privacy and trans-border Flows of Information and Personal Data' were adopted by the OECD in 1980. They aim at harmonizing the different national laws and at creating a minimum standard for the protection of informational privacy in member countries.

The European Union picked up many of the principles of the OECD guidelines and in 1995 created the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data [Eur95]. This directive aims at establishing a common level of minimum data protection in EU member states.

5.2.2 Basic Data Protection Principles

The governmental advisory committee for the US Privacy Act established the notion of 'fair informational practices', a concept that turned out to

be very influential in shaping data protection legislation around the world. These practices are based on work by Alan Westin and can be described as follows [Wes67]:

Openness and transparency: there should be a general policy of openness about collections of personal data. Especially, there should be no secret data collections. Means of establishing the existence and nature of collections, the main purposes of their use as well as the identity of the data controller should be generally known.

Purpose specification principle: the purpose for which personal data are collected should be specified at the time of collection and the subsequent use limited to the purpose stated. A change of purpose must be communicated to the data subject.

Limits of collecting: there should be limits to the collection of personal data. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data quality: collections of personal data should be relevant to the purposes for which they are used. Furthermore, they should be accurate, complete and kept up-to-date.

Reasonable Ssecurity: collections of personal data should be protected by adequate organisational and technical security safeguards against risks such as the unauthorised access to data, its destruction, modification, or disclosure.

Accountability: a data controller should be accountable for complying with measures that give effect to the principles stated.

Supervision and sanctions: a supervisory authority should be created that is responsible for supervising the observance of data protection regulations. The authority should have the power to impose sanctions on controllers in case of non-compliance.

Individual participation principle: an individual should have the right to request information from a controller whether a collection contains data about the individual. Requests should be answered within reasonable time and at a reasonable charge. Furthermore, individuals should have the right to have records rectified, completed or erased where appropriate (i.e. in the case of incorrect or illegally stored data).

5.2.3 EU Data Protection Directive

The creation of a unified internal market in Europe substantially increases the need for cross-border data flows. While such an exchange of data is deemed necessary for economic progress, it creates at the same time the need to protect basic privacy rights of citizens. In order to create a uniform minimum standard of data protection, the European Commission issued a draft proposal for a directive on data protection. In 1995, the European Council passed the EU Directive 95/46/EC 'on the protection of individuals with regard to the processing of personal data and on the free movement of such data' [Eur95]. Some interesting aspects of the directive are presented in this section.

The directive applies to the processing of any data that relates to identifiable persons, where persons (data subjects) may be identified 'by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity' (Article 2(a)). The directive applies not only to electronic data processing, but also to paper-based data collections (Article 2(c)). The regulations of the directive do not apply to data collections for the purposes of public security, defence, state security and law enforcement. Data processing by natural persons for purely personal purposes is exempted from the regulations as well (Article 3).

In order to make a data collection legitimate, two basic criteria must be met: firstly, the consent of the data subject is necessary. Before expressing consent, the data subject has to be informed about the context and purpose of the data collection (Article 7 and 10). Secondly, the context of processing must be lawful. This requires the data items that are collected to be adequate in relation to the purpose of the collection (Article 6 b and c). They must also be accurate and kept up to date during their lifetime. Furthermore, data collections must be destroyed when no longer needed and the purpose of the data collection must not be changed during its lifetime (Article 6 e).

The directive defines the criteria for 'legitimate data processing', thereby enforcing the principle of necessity of data processing. Sensitive personal data revealing racial or ethnic origin, political opinions, religious beliefs, and the processing of data concerning health or sex life is generally prohibited unless specific conditions are met (Article 8). The directive also respects the individual participation principle by granting data subjects an access right to collections (Article 12) and the right to object to collections (Article 14).

While the directive incorporates the basic privacy principles described by Westin, it also exceeds these principles in some domains: member countries must create a supervisory authority to monitor the adherence of public and

commercial bodies to the directive (Article 28). A registry of data collections must be kept by this authority or by a data protection official (Article 18). Transfer of personal data for processing in countries outside the European Community is generally prohibited unless these countries provide an adequate level of protection (Article 25).

The impact of the directive is two-fold: on the one hand, the scope for processing and collecting personal data is clearly defined. Processing of personal data is generally prohibited unless the data subject expresses explicit consent and the context of the processing is lawful. For the first time in Europe, a legally binding minimum standard for the processing of personal data has been created.

On the other hand, the directive effectively forces countries doing business with EU member states to adapt their data protection legislation accordingly. Several countries have already adapted their legislation so as to provide what can be considered an 'adequate level of protection'. Prompted by the directive, the U.S. Department of Commerce developed the Safe Harbor framework in order to avoid interruptions in business dealings with the EU. Companies that self-certify adherence to a set of guidelines are deemed to provide sufficient data protection. Up to now, large companies have been slow to sign up and a report by the EU Commission revealed serious flaws in the agreement [Ped02].

On a critical note, it has to be added that data protection legislation only affords a very basic level of protection to citizens. It could be argued that data protection laws often do not deter organisations from processing data in unlawful ways. In practice, it is mainly the data subject's responsibility to detect abusive data collecting practices and to take action against controllers. Local or national data protection officers usually only take measures against a controller upon complaints by citizens. As data subjects are often unwilling to do paper work and invest time to enforce their data protection rights, organisations can often abusively process data without incurring penalties.

5.2.4 Local Implementations of the Data Protection Directive

EU directives constitute part of a legal framework that is not directly applicable in EU member states. Instead, member states have to harmonise their legislation so that it complies with a given directive and adopt new laws where necessary. The national data protection acts of the member states vary slightly with regard to the level of protection. Some countries

(e.g. Austria) offer a higher level of protection as compared to some other countries within the EU.

Although Switzerland is not an EU member state, the national data protection law complies with the EU directive. There are no major differences between the directive and Swiss legislation: the principles of quality of data, special regulations concerning the treatment of sensitive data, the principle of consent by the data subject and the principle of purpose specification can all be found in Swiss legislation. There are some slight differences though: Swiss regulations protect data on both natural persons and legal entities. Regulations encompass all manual data collections while manual collections in the EU are only covered by the directive if they are structured (i.e. they are indexed by one or more search criteria). A slight deviation exists concerning data transfers abroad: the EU directive demands an adequate level of protection in third countries while Swiss law requires a level of protection equal to the one granted locally, thus offering a higher level of protection.

5.3 Potential Threats to Privacy Posed by e-Government Systems

This section discusses problems that arise as a consequence of the digitisation of public administration. People are often concerned about privacy issues related to e-government and also increasingly about citizen cards [BBC02], [BBC03]. Although information and communication technology provides tremendous opportunities for reshaping the relationship between government and stakeholders and for creating more efficiency in bureaucratic systems, it also creates significant security and privacy challenges. General privacy problems are considered first, then problems are discussed that are particular to smart card technology.

5.3.1 General Threats To Privacy

The privacy threats mentioned in this section arise from the use of information and communication technology by governments. However, some of the threats are not particular to e-government but exist in e-commerce systems, too. Various surveys have shown that privacy is a substantial concern on the internet and particularly in e-commerce transactions [ACR99]. In the public sector, governmental bodies process high volumes of data. They are empowered by public law to collect data on citizens and can enforce their right to do so. Governments thus have the potential to accumulate large data

collections, which may create potential conflicts with the citizen's interest in informational privacy [SB96].

5.3.1.1 Unauthorised Access to Personal Data

Administrative records are created in the course of a transaction by civil servants. These records are usually in electronic form and accessible by electronic means. Governmental information systems store records concerning a high number of individuals. They contain information ranging from demographic data to data that relate to the financial situation of a citizen and sometimes even information concerning the citizen's health. There is a danger that civil servants may access these records and misuse information, e.g. by passing it on to third parties. Data may be passed on electronically or non-electronically (e.g. on paper). Unauthorised access to personal data in e-government is even more undesirable as data in administrative systems are often of a very sensitive nature. Sensitive data need a particularly high level of protection against disclosure and misuse.

5.3.1.2 Integration of Data Collections and Personal Profiles

Most countries provide administrative services to citizens through more than one administrative body. The tax administration for instance is organisationally separated from the population registry office and organisationally separated from health services. Furthermore, countries with a federated administrative culture provide many administrative services in a decentralised fashion. In decentralised administrative settings, there is often no unique identifying number for citizens across systems. Without unique identifiers, matching records from independent databases is quite difficult [BS01a], which in itself has a privacy-protecting effect: linking records from several databases in order to gain more data about a citizen becomes then much harder. Unique identifiers for citizens across databases have the potential to undermine the citizen's privacy as they make it relatively easy to exchange personal data across administrative systems. In acknowledgement of this danger, Austria has introduced the use of a context-dependent identifier for each administrative act to prevent automatic linking of citizen records [MR02].

5.3.1.3 One-Stop e-Government

A current trend in the field of e-government is the creation of portals that facilitate one-stop e-government [Wim02], [WT02b]. One-stop e-government is a term that refers to the integration of public services from the stakeholder's point of view. This may be a citizen or a corporation. This concept requires

all public services to be made accessible through a single point of access even if these services are provided by organisationally independent entities. From a back-office perspective, such an integrative approach to service delivery necessitates logically and physically separated IT systems to be interconnected [WT02a]. One-stop e-government also requires the ability to match records in IT systems run by different administrative bodies. Although administrations may not exchange data without the consent of the data subject unless a law explicitly allows them to do so, citizens fear that integrated administrative systems may give authorities more control over their lives. It must be prevented that one-stop e-government solutions automatically allow civil servants to gain insight into any administrative system that is internetworked with their own administrative entity. Exchange of personal data between authorities should only happen with the citizen's explicit consent, respectively at his or her own request, or where law provides a basis for the exchange. The trend of inter-networking administrations leads to a situation where successful attackers get access to a growing range of databases.

5.3.1.4 Identity Theft

Identity theft involves acquiring pieces of a person's identifying information with the goal of impersonating that person and act in his or her name [Cav97]. Identity theft is possible because it is often the case that identifying information is used to gain access to information and resources (not necessarily electronic ones). At the same time, a wealth of identifying information is available publicly. Addresses, phone numbers, social security numbers, credit card numbers or bank account numbers may be looked up publicly or can easily be acquired from transaction records. Acquiring identifying information of a victim may enable an attacker to commit numerous forms of fraud: to conduct credit card transactions under the victim's name, divert the victim's mail or gain unauthorised access to databases. Especially fraudulent transactions damaging the victim's credit records are very common [Ber00].

The danger of identity theft is accentuated through electronic data processing and digital networks. According to the Federal Trade Commission, the number of identity theft complaints in the US increased from about 82,000 in 2001 to 162,000 in 2002 [Gla03]. This problem is also acknowledged by some governments. A recent study undertaken in the United Kingdom by the Cabinet Office concludes that identity theft is a growing problem that has been underestimated in the past. The study warns that identity theft may open up new possibilities for organised crime [Cab03].

A good example for the dangers posed by global identifier numbers is the social security number (SSN) in the United States of America. The SSN was

incepted in the 1930s as an identifier for a government retirement program. At times, SSN numbers of citizens were available for sale on Web sites. By now, the SSN is so overused as an identifier that is has become an unreliable means of identification. In the light of these facts, the state of California is considering a law that keeps schools and universities from using the SSN as an identifier [Gla03], [Nor03].

5.3.1.5 Public Private Partnerships

The increasing number of public-private partnerships creates an increased need for electronic communications between non-governmental and governmental organisations. The interoperability and secure data exchange between partners poses additional security problems and can be regarded a potential privacy threat [JGAS02].

Many countries have begun to privatise services that used to be provided by the state. Handing service provision over to private companies also necessitates that historic transactional data are handed over to private sector companies. The record collections of the government are doubtlessly of a commercial value. Care must be taken to assure adequate protection by private service providers. The handing over of records constitutes a threat to privacy. At the same time however, it provides the opportunity to revise record collections. Outdated records should be deleted and data should be rendered anonymous where possible.

5.3.2 Threats To Privacy Posed by the Introduction of Citizen Cards

Some of the general dangers discussed above can be handled through organisational measures and measures that address the 'back office' part of an electronic transaction. Apart from these general dangers, there are also some risks that arise through the use of smart cards. These risk are acerbated by the fact that citizen cards will be used in a wide range of applications. Privacy concerns are expected to have a detrimental effect on the acceptance of e-government solutions [WGPR02]. Especially plans for the introduction of citizen cards have raised objections by privacy activists. A recent poll in the United Kingdom undertaken by the Home Office showed that a majority of citizens opposes the introduction of digital identity cards [BBC03]. In the United Kingdom, opposition to a proposed electronic identity card arises not only from privacy concerns but also from opposition to the concept of a mandatory ID card. In the United Kingdom, citizens are currently not obliged to carry any form of identifying document.

Optical ID cards are well accepted in many European Democracies. In many countries, citizens carry identity cards without being concerned too much with privacy issues. The ability to prove one's identity facilitates many administrative procedures and is helpful in many situations in daily life (e.g. when collecting registered mail at the post office). Showing an optical identity card to a human verifier does usually not leave a permanent record. Conversely, electronic identity and citizen cards are more problematic, as all electronic transactions have the potential of leaving traces. The potential threats to privacy arising from the introduction of digital citizen and identity cards are discussed in this section.

5.3.2.1 Multi-Application Identity Cards

Current smart card projects in Europe address many different applications ranging from health service cards to full digital identity cards. Identity cards embed two digital certificates on the card: one for authentication, the other for digital signatures only (see section 4.7.1). The authentication certificate will allow citizens to conduct a whole range of transactions on-line, including on-line shopping, e-banking, paying taxes or even e-voting. However, conducting transactions based on identity certificates also poses a serious threat to the cardholder's privacy.

Whenever the citizen uses the embedded authentication certificate for the setup of a secure connection or other authentication purpose, all transactions within the session can be linked to the identity of the card holder. The use of a single authentication certificate for multiple applications will enable health care institutions, shops, Web sites and governmental agencies to link records comprising a multitude of transactions by a given customer. While a data collection of a single service provider on its own may not be perceived as a threat to privacy, there is always the possibility that several providers may exchange data and compile detailed personal profiles about the cardholders.

Most internet users have come to realize that there is almost no privacy on the internet, as any electronic transaction leaves a trace. As a consequence, many citizens fear that the introduction of multi-purpose identity cards will undermine their privacy and possibly give administration more control and insight into their lives. These concerns will have to be addressed by any government that engages in a digital ID card initiative, as user acceptance is a critical success factor [WGPR02].

An increasing number of applications on citizen cards will also mean a growing number of opportunities to use the card. As pointed out already, electronic transactions leave permanent traces so that a growing number of card transactions implies a much more dense transaction trail. This is

especially privacy-invasive when cards are used to implement applications that require frequent showing of the card (this is e.g. the case in public transport applications). Smart cards that leave identifiable traces with every transaction have the potential of strongly invading the citizen's privacy.

5.3.2.2 Unintentional Disclosure of Personal Data

Citizen cards may or may not carry identifying information on the surface (e.g. the Austrian citizen card lacks these features). Some card issuers put publicly accessible (electronic) personal data onto a card. While optical information on the surface of the card is hardly problematic, publicly readable electronic information concerning a citizen's identity poses a severe privacy threat: whenever the citizen uses the card, a service provider may read identifying information from the card. Publicly readable data sets therefore pose the hazard that citizens unknowingly disclose their identity or other personal data. This poses the risk that transactions are linked and it facilitates the creation of personal profiles.

5.3.2.3 Technology-driven Creation of Identity-based Services

Citizen cards that incorporate an authentication certificate will offer a simple means for strong authentication of the citizen's identity. There is a danger that the authentication certificate on the card will lead to an increased deployment of identity-based services, i.e. services which force the citizen to disclose his or her identity. Technical features of a citizen card may be used by developers and service providers simply because they are available and convenient to use. The use of an authentication certificate tied to a identifiable individual is a very strong form of authentication. Both from a technical and a data protection perspective, such a strong authentication is not necessary in many transactions.

5.3.2.4 Card Operation without the Citizen's Consent

It is important that a citizen card should only operate under the owner's control. This implies that the owner has to be aware of all operations involving the card. This problem mainly concerns contact-less cards. Normal, contact-based cards usually only operate after authentication of the card holder (e.g. after entering a PIN) and the user is therefore aware of card operations. With contact-less cards, the issue is more difficult: care has to be taken so that card services are not used without the owners consent, as these cards may be operated without the user being aware of it. Data could for instance be read or an electronic wallet could be accessed without the

owner even noticing the card activity. Design measures at the application level must be taken to protect users against misuse. One such measure is an audit trail that records every use of the card.

With regard to smart card operation in general, it can be said that the exact nature of a card operation should always be communicated to the owner. This especially applies to a reading out of personal data from the card. Before retrieving any personal data from the card, card holders should be asked for consent.

The threats to privacy that were mentioned here need to be addressed by every government intending to introduce electronic service delivery. A combination of technical and organisational measures must be enforced in order to counter these dangers. Trust in electronic services is an important prerequisite for the uptake of card-based services in the administrative domain. The next section discusses steps that can be taken to enhance informational privacy in e-government systems.

5.4 Measures to Enhance Privacy

This section presents measures that have the potential of augmenting the citizen's privacy. First, some basic measures concerning information systems will be presented. Some of these basic measures apply to information processing in the private and the public sector. Following these, measures will be detailed that specifically address privacy threats arising from the use of citizen cards.

5.4.1 General Measures to Enhance Privacy

The measures proposed in this section are of a general nature. With the exception of the measure concerning the unbundling of administrative documents, the measures presented here apply to the information processing in general. The enactment of basic data protection legislation and measures for data security are taken as a prerequisite and are not mentioned specifically.

5.4.1.1 Privacy Policies and Machine-readable Privacy Statements

A privacy policy is a statement by an organisation that details how personal data is handled by that organisation. Such policies are especially common in countries that do not have strong data protection legislation in place. Most companies who do business on the Web have begun to include a privacy statement on their Web pages. Such a statement helps users to inform themselves

about how their personal data is processed. Based on such policies, they can make an informed choice concerning which providers to do business with or what personal data to disclose to them. A privacy policy should in the least detail the following information:

- what personal data is being collected
- what the data will be used for
- whether the data will be shared with other organisations
- whether users can access their data
- contact person for issues related to data processing
- pointers to further information concerning that organisation's data processing

Privacy policies can also be expressed in machine-readable form. The World Wide Web Consortium (W3C) has recognized the fact that many providers of Web-based services collect a wealth of personal information and that users have little control over the processing of their data. The Platform for Privacy Preferences (P3P) is a W3C standard that enables users to inform themselves about a Web site's privacy policy and automatically discover potential discrepancies with their own privacy preferences [W3C02a].

A provider of Web-based services can specify a privacy policy in XML. This machine-readable policy statement is then made available on the service provider's Web-page. Users express their own privacy preferences in a language called APPEL (A Privacy Preference Exchange Language). Figure 5.1 shows a fragment of such a privacy preferences document. When accessing a site with a P3P policy, the browser matches the policy statement against the user's own privacy preferences. A warning is issued to the user if discrepancies exist. However, while P3P provides a standard mechanism for describing privacy practices, it does not set a privacy standard which Web sites must comply with.

On a critical note, it has to be mentioned that P3P has not been very well received by the public. Only few sites carry P3P statements. With regard to user agents, popular Web browsers support P3P. However, preferences are difficult to formulate and users still must rely on external tools for this purpose.

Another concern is that users have no way of telling whether service providers really adhere to the principles stated in P3P policies. It is practically impossible for users to tell, unless sites are audited and certified with regard

```
<?xml version="1.0" ?>
 <appel:RULESET xmlns:appel="http://www.w3.org/2001/02/APPELv1"
    xmlns:p3p="http://www.w3.org/2000/12/P3Pv1">
<appel:RULE behavior="limited" description="Site may use health or medical
   information for analysis or to make decisions that may affect what
   content or ads you see, etc.">
  <p3p:POLICY>
   <p3p:STATEMENT>
    <p3p:PURPOSE appel:connective="or">
     <p3p:pseudo-analysis required="always" />
     <p3p:pseudo-decision required="always" />
     <p3p:individual-analysis required="always" />
     <p3p:individual-decision required="always" />
    </p3p:PURPOSE>
    ....
```

Figure 5.1: A fragment of a privacy preferences document expressed in APPEL

to policy implementation by independent entities on a regular basis (see section 5.4.1.3).

5.4.1.2 ERM Policies for Data Collections

Privacy policies are often augmented by electronic record management policies. An electronic record management (ERM) policy is a practice statement on how to handle the life cycle of an electronic record. An electronic record is a documentation of a transaction that has taken place. The Association of Record Managers and Administrators (ARMA) defines an electronic record as ‚recorded information regardless of medium or characteristic, made or received, that is useful in the operation of the organisation‘ [Kah02]. As such, electronic records exist in different forms (e.g. database records or electronic documents) and may have originated on paper or electronically. An ERM policy must describe which kinds of records are to be kept, which are to be destroyed and for how long records should be kept. An ERM policy complements legal frameworks such as data protection legislation or accounting legislation. The scandals at Enron and Arthur Andersen have shown that implementing and enforcing ERM policies is important for any organisation.

For a governmental administrative body, an ERM policy, where not already in place, is helpful to ensure proper handling of sensitive records. ERM policies may help raise awareness of the problems arising from the handling of sensitive personal data. Heightened awareness in turn can lead to the realization that avoiding personal data wherever possible can bring a benefit to authorities and citizens.

5.4.1.3 Certification of Data Processing Practices

Data protection legislation and published privacy policies are only effective if they are adhered to. Subjects who disclose personal information to organisations have generally no way of telling whether that organisation processes data in accordance with legal regulations and published privacy policies. In order to alleviate this problem, data protection audits can be carried out to certify compliance with data protection legislation or privacy policies. Two types of audits can be distinguished: data protection audits aim at certifying legal compliance of data processing while privacy policy audits aim at certifying compliance with a privacy policy.

A data protection audit is carried out by an independent entity and comprises an evaluation and appraisal of data protection measures. Hardware, software and processes are subject to such an audit. As part of the audit, data security measures must be reviewed as well, as data security is a prerequisite for meeting data protection exigencies. As a result of the audit, an independent entity confirms that the requirements of the data protection legislation are met. As a benefit of an audit, an organisation can communicate to users that data processing is in accordance with the legal regulations. This may help the organisation to gain an advantage over competitors whose data processing is not certified. An example for such certification is the 'GoodPrivacy' seal in Switzerland, which an organisation can obtain after being audited by an accredited security company.

The second type of audit aims at certifying that personal data is processed in compliance with a privacy policy published by that organisation. The privacy policy may be expressed in human readable or machine readable form (i.e. a P3P document). These audits serve the purpose of demonstrating to users that the principles expressed in the policy are indeed adhered to. Of course, such an audit must also take basic data security measures into account. An example for this kind of audit is the BBBOnLine Privacy Seal [Bur03].

5.4.1.4 Unbundling of Administrative Documents for Electronic Purposes

Citizens possess a multitude of documents that are issued by governmental bodies and which confirm certain statements about the holder. Examples are the birth certificate, a passport or the driver's license. As more and more services are offered on-line, there is a need to create digital counterparts of today's paper documents [Rie01].

However, the introduction of electronic documents in e-government raises

privacy concerns, as showing a document to a digital verifier is different from showing a paper document to a human verifier. Showing a document to a human verifier does not normally leave a permanent record, since most persons do not have a perfect photographic memory. In contrast, showing a document to a digital verifier gives the verifier the chance to obtain a copy of the document. After all, an electronic document is nothing more than a string of bits that may be easily copied.

This concern is even more severe, as administrative documents usually contain much more information than really needed. When showing a driver's license, the verifier is interested in obtaining proof of my ability to drive a car. Additional data such as age, nationality etc. are not of primary interest and are not correlated with my driving aptitude [CM01].

Therefore, the design of these electronic documents should be different from the paper-based form. Documents should be split into smaller data units that can be shown independently. Such a redesign can be justified with the privacy principle of data minimisation. Only the data necessary in a given situation should be divulged. Consequently, unbundling data items in digital documents has the potential of strengthening privacy and of increasing the informational self-determination of citizens.

There are many examples for data items that can be unbundled. In the administrative domain, examples include documents indicating the current place of residence or documents stating the nationality, proof of age etc. The unbundling of documents can be achieved by using smaller, digitally signed XML documents or by use of digital credentials.

The use of pseudonymous credential technology (see section 4.2) also offers the chance to implement some of these documents in an anonymous form. It is the verification of characteristics of a person that matters in many transactions, not their identity. This is for example the case when buying alcohol (where the age is of interest, not the buyer's identity). A credential could be used to prove the age without disclosing the holder's identity.

5.4.1.5 Transparency in Record Keeping

The basic data protection principles as defined by [Wes67] call for a right of participation on the part of the data subject. The principle of participation states that data subjects have the right to know what data about them is stored in a collection. Furthermore, it gives them a right to amendment in case of incorrect records. Some European countries have taken up this principle and are planning to take further steps to improve transparency in record keeping. A fair amount of transparency is reached by allowing the citizen to inspect the records in governmental IT systems. An example is

Sweden: the government is introducing measures that allow citizens to see the information that is stored about them in a given administrative system, with the exception of security relevant data.

5.4.2 Privacy-enhancing Measures for Smart Cards

Many countries in the European Union are considering issuing digital citizen and identity cards to their citizens: Austria, Belgium, Finland and Estonia have already done so (see section 4.7.2). Privacy activists perceive many citizen card initiatives as a threat to the citizen's privacy [Dav01]. Measures aiming at safeguarding the privacy of citizens must address not only back-office systems but citizen cards as well. The following measures have the potential of increasing the informational privacy of the citizens and are specific to identity and citizen cards.

5.4.2.1 Avoidance of Publicly Readable Data Sets on Citizen Cards

Digital citizen cards should not carry any data that is publicly accessible. Inserting a citizen card into a card reader must not lead to an automatic disclosure of personal data. Especially data sets including the name and the date of birth are privacy-invasive. Making such data publicly readable has the effect that every use of the card leaves traces that make transactions linkable to a specific individual. The same can be said about publicly readable card numbers. Card numbers do not directly point to an individual. Nevertheless, a transaction can be tied to a number and thus consecutive transactions involving the same card may be linked.

Instead, the card should only grant access to data fields after the owner of the card has been authenticated, for instance by entering a PIN or by use of biometrics. Even during a transaction, the citizen should be informed by a service provider when data is about to be read from the card. The owner should then have the possibility to consent to data access or to deny access. Smart cards should be made a 'safe' bearer for personal information. They should not automatically disclose information that enables the linking of transactions. Modifying cards in compliance with this exigency is a prerequisite for delivering smart card-based anonymous services.

5.4.2.2 P3P Profiles for the Access to Web-based Commercial Services

The Platform for Privacy Preferences (P3P) is a standard defined by the World Wide Web consortium (W3C) and provides a simple, automated way

for users to gain more control over the use of personal information on the Web [W3C02a]. Users can specify their own privacy preferences which will then be matched against a service provider's policy. Including such user preferences on a citizen card makes sense, as citizen cards will be increasingly used as multi-application cards and thus used in e-government and e-commerce transactions.

The citizen card can act as the bearer of the citizen's P3P privacy preferences. When using a card in an electronic transaction, the P3P profile can be transferred to the browser and matched against a Web site's P3P policy. Including P3P profiles as a data item on citizen cards ensures that the citizens always have their preferences at their disposal. Privacy-enhanced Web-transactions would thus be available to the citizen at all times and not only at the user's own machine.

5.4.2.3 Support for Anonymous and Pseudonymous Transactions

The most effective measure to improve the citizen's privacy is to introduce support for anonymous transactions. Anonymity in transactions warrants that transactional data cannot be associated with a specific individual. It therefore prevents the creation of personal data in the sense of data protection legislation. Technologies that improve informational privacy by controlling the release of personal data are often described as privacy-enhancing technologies (PET). These technologies aim at minimizing or eliminating the amount of identifiable data [Cav97].

Research has shown that in the domain of e-government, certain services in European countries will have to be delivered anonymously [Rie03]. An example for this type of services is the field of social security applications in the United Kingdom. If a comprehensive electronic coverage of administrative services is desired, support for anonymous transactions will become a requirement for citizen cards. Such requirements will constitute a driver for the integration of privacy enhancing technologies into citizen cards. Anonymous digital credentials are currently the best technical means for enabling anonymous and pseudonymous service delivery.

The privacy threats mentioned in this section have implications for the design of e-government systems. This thesis addresses measures that can be taken with regard to citizen cards and proposes the use of credentials as an important building block for the citizen's digital identity.

5.4.3 A Conceptual Model of Privacy-Enhancing Measures

The measures to enhance privacy that were presented in the preceding sections can be combined into a layered model. Threats to privacy and especially informational privacy should not be addressed by technological means alone. Instead, measures must be taken at several levels, namely at the level of society, the legal framework, organisations and the individual. Measures at lower levels provide the basis for measures at higher levels. Figure 5.2 depicts these layers of privacy protection.

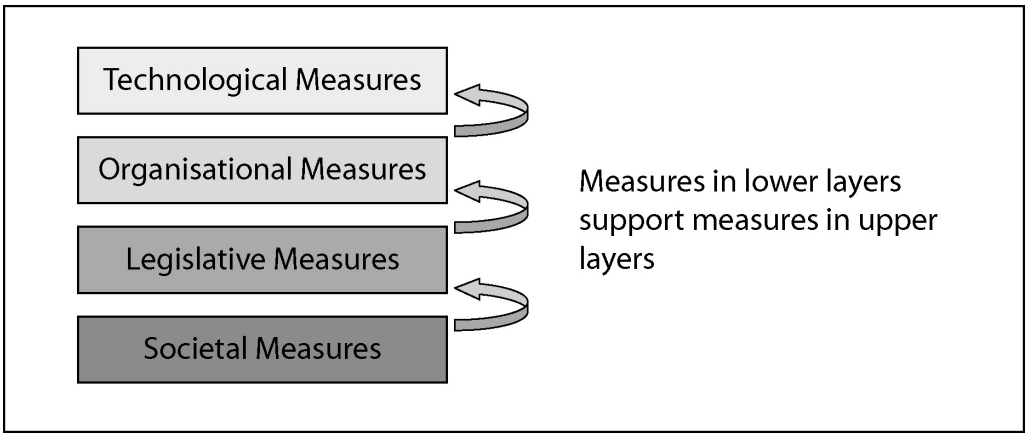

Figure 5.2: A layered model for measures aiming to enhance privacy

This high-level model comprises measures at the following layers:

Societal measures: at the level of society, awareness needs to be created for privacy issues. A public debate should be initiated about privacy issues related to e-government, the amount of protection that is desired and measures that can be taken to counter privacy threats. As a basic measure, citizens should inform themselves about informational privacy in general, the legal framework and technological measures that are at their disposal. Raising awareness will help motivating a critical mass of users to adopt privacy enhancing technologies. Last but not least, individuals should also make use of the rights that data protection legislation affords them.

Legislative measures: at the level of the legal framework, laws need to be enacted that regulate privacy protection and sanctions against organisations that process data in unlawful ways. Non-compliance with this legislation should result in penalties that are severe enough as to deter organisations from misusing personal data. Most countries have already enacted data pro-

tection laws. These laws afford a basic level of protection to the citizen with regard to informational privacy.

Organisational measures: public and private sector organisations can take several organisational measures in support of privacy protection. As a basic prerequisite, data security measures need to be taken. Service providers should describe the practices of personal data processing in privacy policies. As a further step, organisations should be audited by external entities to ensure compliance with data protection legislation. Such audits could be carried out by government, professional auditing groups or privacy groups. These audits could also comprise further policies such as electronic record management policies or P3P policies. The results of the audits should be available to users, e.g. by obtaining seals that certify compliance and that can be published by service providers on their Web pages.

Technological measures: privacy-enhancing technologies should be supported by government as well as private service providers and made available to end users, e.g. by encorporating them into citizen cards. Service providers from the private and the public sector should adapt their infrastructure in support of PETs if the use of such technology is to have any effect. Rolling out privacy enhanced technology to end-users only makes sense if services exist that can be accessed by the use of such technology.

Pressure by interest groups and by the public may motivate service providers to increasingly offer privacy-enhancing services. Most importantly, citizens should make use of privacy-enhancing technology wherever available. Service providers who support such technology should be preferred over those who do not offer privacy-enhancing services.

5.5 Anonymous and Pseudonymous Transactions in e-Government

Pseudonymous credentials are a privacy-enhancing technology that can afford anonymous transactions to citizens. In this section we discuss anonymous transactions and motivate a revocable form of anonymity. We examine the choices that can be made with regard to the level of identification and give examples for identified, pseudonymous and anonymous transactions.

5.5.1 Motivation for Anonymous and Pseudonymous Transactions

We have stated that the concept of digital identity also serves the purpose of binding a set of data to an identifiable subject (see section 2.2). Most information systems today store identifying data along with transactional data to allow for this binding. There are services however, where identifying a user is unnecessary or even undesirable. Even these services can be delivered electronically, but the system should be designed in a way that affords anonymity to the users. We will first give some examples of real-world transactions that are usually performed anonymously and discuss beneficial effects of anonymity.

Many transactions in the real world are anonymous. Examples for common transactions that do not involve the disclosure of an identity are:

- the buying of goods against cash or the trading of goods against goods
- enquiries at an information desk
- telephone conversations using a public phone or prepaid phone card
- surfing the Web from an Internet cafe
- participating in voting or public census
- some medical tests (e.g. for sexually transmitted diseases)

Many more examples of anonymous transactions can be found. Anonymity can have positive or negative effects, depending on the setting. Desirable effects of anonymity include:

- Possibility to voice one's opinions without fear of repercussion: in many settings anonymity is important to obtain reliable information (e.g. in political polls and in voting)
- Reduction of prejudice in communications: gender, ethnic origin and other characteristics can be masked and will not influence the opinion of addressees
- Possibility to obtain sensitive information: information can sometimes only be obtained by guaranteeing anonymity to the informant. This is often the case in criminal prosecution.

The arguments against anonymity mostly focus on a lack of accountability. It is argued that anonymity has negative effects as people may behave in an undesirable way if they cannot be held accountable for their actions. More specifically, it is feared that anonymity will make law enforcement more difficult. If an action cannot be traced back to a person, it is assumed that this will create an incentive for behaving in ways that were before sanctioned by the community or its executive bodies. Researchers suggest that people tend to behave differently in the relative anonymity that the Internet affords. People e.g. invent new identities for themselves when acting anonymously on the Internet [Bah97], [Dör90], [Nak98].

In the non-digital world, people have a certain degree of freedom to choose between levels of anonymity: the choice of living, for example, in a small town versus life in a big city, airplane travel versus boarding a train, paying cash versus credit card transactions, making phone calls from home instead of using a public telephone and so on [JM98]. In a digital world, this freedom of choice does not really exist. Any electronic transaction leaves a trace. Therefore, all transactions that include identifying data may be traced to an individual. It follows that including privacy-enhancing technology on citizen cards in order to allow anonymous transactions may help restore some of the freedom that is currently lacking in the digital world.

The fair informational practices as defined by Alan Westin stipulate the data protection principles of data avoidance and data minimisation. These principles can also be found in the EU directive on data protection. They stipulate that personal data should only be collected, stored and processed when truly necessary. As a consequence, the collection of personal data should be avoided, and, where it cannot be avoided, minimised. Anonymous and pseudonymous service delivery are the most effective way to avoid the creation of personal data. Correspondingly, access control decisions and data processing should be based on the smallest set of data possible in order to enforce the principle of data avoidance. This leads to the requirement of an anonymous and attribute-based access to information systems. Anonymous and pseudonymous digital credentials are the technological means of choice to allow users to access services anonymously. The requirement for privacy-enhancing technologies in e-government systems can thus be derived from basic privacy principles.

Despite possible undesirable effects of unconditional anonymity, there is a strong motivation to support anonymous transactions in the domain of e-government. As pointed out, services should be delivered anonymously wherever possible. Keeping the set of personal data as small as possible enhances the citizen's privacy. Anonymous and pseudonymous transactions are thus a measure that may encourage the citizen's trust in electronic service

delivery. The undesirable effects can be countered by introducing anonymity revocation in case of misuse, as will be explained in the next section.

5.5.2 Motivation for a Revocable Form of Anonymous Identity

Although governments around the world are adapting their legislation in order to accommodate electronic service delivery, no government has yet changed the legal framework in a way to grant citizens an absolute right to anonymity. In the Netherlands, there was recently a discussion whether citizens should have a general right to anonymity [Off01]. The Dutch government rejected this notion and argued that communications with government are subject to statutory regulations and that it is essential to trace a communication back to its originator. At the same time though, they admitted that anonymity might be desirable in some circumstances.

For the electronic delivery of services, the high importance that is attributed to traceability implies that any anonymous system in the governmental domain may have to incorporate some form of identity escrow. In case of a legal dispute, a designated body should be able to trace a credential holder's transactions back to the subject behind the credential. It is technically feasible to implement such a form of revocable anonymity in a credential system.

In the discussion on anonymity, most authors who argue against anonymity build their argumentation on the loss of accountability resulting from anonymous transactions [SWR02, JM98]. It is generally feared that anonymity will pose an incentive which can engender unlawful behaviour. While this argument holds in situations with absolute anonymity, it is clear that revocable anonymity does not have this drawback. We have seen that revocable anonymity does indeed guarantee that an individual may use a service while remaining anonymous for the service provider. At the same time, it is warranted that a third party can divulge the identity behind a transaction in case of misconduct.

Despite hiding some information from service providers, such a system affords strong trust relationships. It has been argued that traceability is a desirable property in electronic commerce systems. Trust is strengthened if all participants face the perspective that transactions may be traced to their origin [SWR97]. Traceability can be established through identity escrow (see section 2.1.6) and does effectively protect the privacy of individuals. Recovering an identity with the aid of the third party is a means of penalising those who behave in an unlawful way. It is, however, only unlawful conduct

as well as behaviour falling short of contractual obligations that will lead to an identity disclosure (anonymity revocation).

A solution incorporating revocable anonymity has therefore the potential of increasing trust in e-government systems while protecting the citizen's privacy. Many electronic service providers require users to disclose their identity 'up front'. A protocol that hides identity but nevertheless allows identification under special circumstances may constitute an acceptable and privacy-protecting substitute.

5.5.3 Anonymous Transaction Records and Data Protection Legislation

It is often desirable that anonymous transactions in electronic systems leave an audit trail. Anonymous credentials that feature identity escrow leave traces that can be used to discover the subject behind a transaction. The existence of such an audit trail raises the question whether a service provider has to treat the records of anonymous transactions as personal data in the sense of data protection legislation. If such records are to be considered personal data, then service providers have all the responsibilities of a data controller and need to take measures to safeguard the records. This in turn, would have a negative impact on the cost of anonymous service provision.

According to the article 2(a) of the EU directive on data protection, information must be considered personal data if it relates 'to an identified or identifiable natural person'. The same article also specifies that an identifiable person is one who 'can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

In a system with identity escrow, the issuer of a credential can make a link between a record and an individual with the help of a trusted third party. Since a link can be made, audit data of transactions based on anonymous credentials must be classified as personal data. Consequently, records of anonymous transactions that contain encrypted identity information are subject to data protection legislation. As such, the transaction records constitute a data collection and the controller of the records must take action to safeguard these records. Even though the records are hardly useful to anyone but the credential issuer, they must be classified as personal data and treated accordingly.

5.5.4 Design Choices for e-Government Services

A service provider has numerous choices of how to identify and authenticate users when migrating to electronic service delivery. Most importantly, it must be decided whether users stay anonymous, use a pseudonym or need to be identified in the course of the given service. The design choices can be classified with regard to three criteria: the level of identification, the strength of authentication and the level of traceability.

1. With regard to the **level of identification**, three choices exist:
   - anonymous identity: the user either does not present any form of electronic identity or provides an anonymous digital credential.
   - pseudonymous identity: the user presents a pseudonymous user name or other form of pseudonymous identity, e.g. a pseudonymous digital credential.
   - full identification: the user provides a set of identifying information or a digital credential that allows an identification of the user.
2. With regard to the **strength of authentication**, four choices are possible:
   - no authentication: the identity claimed by the user is taken at face value.
   - weak- to medium-strength authentication: the identity is authenticated by use of an associated secret, e.g. a password, a personal identification number (PIN) or a credit card number.
   - high-strength authentication: the user authenticates with an electronic credential. The credential-bearing medium is protected by a password or a PIN. An example for this category is a digital certificate on a smart card secured by a PIN.
   - very high-strength authentication: the user authenticates with an electronic credential. The credential-bearing medium is protected by biometrics. An example for this category is a digital certificate on a smart card secured by a finger print sensor.
3. As a third criterion, the **level of traceability** can be considered. This criterion only applies to anonymous and pseudonymous transactions. Traceability refers to the general ability of service providers or designated third parties to trace a transaction back to an individual. In an identified transaction, a user is traceable by definition. With regard to level of traceability, two choices are possible:

- revocable anonymity: the user may be traced by a third party in case of undesirable behaviour.
- unconditional anonymity: the user remains anonymous to all parties under all circumstances.

In the category of high-strength authentication, we only consider digital credentials (such as certificates or anonymous credentials) that are stored on a portable device and cannot be extracted from this device. Before using the device, the holder is authenticated by means of a personal identification number or by use of biometrics. The use of biometrics leads to a very strong authentication, as the device can only be used by its rightful owner.

This classification permits twelve conceptual choices for the implementation of electronic services (when excluding the criterion of traceability). This leads to a matrix as a space of design choices as depicted in Figure 5.3.

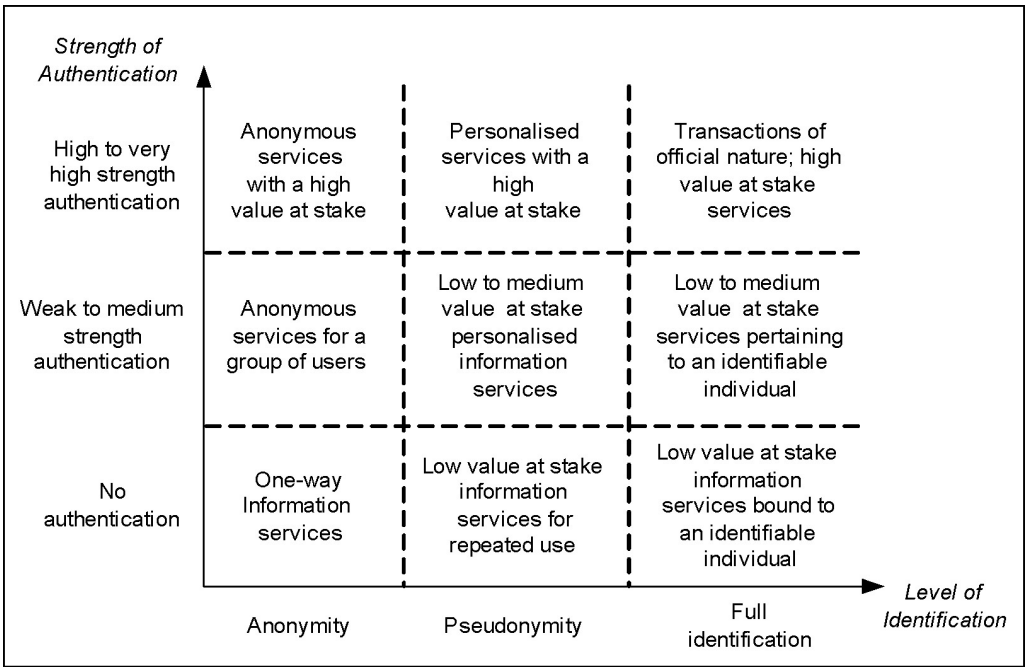

Figure 5.3: Design choices for electronic service access

In this matrix of design choices, we use the term value at stake. The level of authentication for a service should be chosen according to the value that is at stake in the transaction. The term value at stake refers to the damage that may arise from a transaction in case of the misuse of an identity. If an attacker succeeds in misusing an identity, financial loss or other kinds of

damage may occur both on the part of the service provider and on the part of the customer. Possible consequences of an identity misuse include financial loss to the service provider, financial loss to the customer, inconveniences for the customer or damage to the reputation of the service provider and customer. The value at stake thus describes the potential damage in which an identity misuse in a transaction may result.

In this illustration, the authentication levels of high-strength and very high-strength are collapsed into one class: applications where a high value is at stake are today implemented with both kinds of authentication. An example are digital signature cards: signing a document by use of a signature card requires a strong authentication of the card holder in order to prevent misuse. Nonetheless, such cards are today only secured by personal identification numbers (PINs). In most legal frameworks, securing a card by use of a PIN is deemed a strong enough authentication of the card holder, even for applications where a very high value is at stake. The application area for high-strength and very-strength authentication thus overlaps in practical implementations.

The space of design choices can be illustrated by example. These examples are not all specific to the field of e-government. Examples of weakly authenticated services apply to informational services of all kinds, including governmental ones.

Examples for the service categories of the matrix depicted above are:

Anonymity without authentication: informational services that are accessible to anybody and thus do not require any form of access control. An example is information that is publicly available to any visitor of a Web page. However, it has to be noted that users who access such information may leave identifiable traces in form of the visitor's IP address. If full anonymity is desired (e.g. when visiting a page that addresses people that belong to a social minority), an anonymising proxy (e.g. a mix network) should be used to eliminate these traces.

Pseudonymity without authentication: this category comprises informational services that may be personalised to some degree but do not require a strong authentication. The misuse of a pseudonym by another party results only in no inconvenience and no financial loss. An example is information of a general nature that is publicly available on a Web page but personalised to some degree (e.g. a personalised weather forecast).

Full identification without authentication: this category comprises transactions which require identifying information (such as a name and an

address) but which do not cause harm in case of the misuse of an identity. An example is the process of ordering governmental forms or low cost brochures in print to one's home address.

Anonymity and weak- to medium-strength authentication: this combination occurs seldom. One example for this category are anonymous on-line surveys where one wants to ensure that users do not participate more than once. This can be achieved e.g. by use of a password that cannot be used more than once. Another example are e-services to which all users are issued the same password, thus affording anonymity within a given group. Such an approach may be suitable to afford anonymous information services to a closed group of users.

Pseudonymity and weak- to medium-strength authentication: this category encompasses information services with a low to medium value at stake. The misuse of a pseudonym by another party results in no or only minor inconvenience and negligible financial loss to both the individual and the service provider. An example are medical test results that may be published on a Web page or the participation in an on-line community.

Full identification and weak- to medium-strength authentication: services that are bound to an identifiable individual and that have a low to medium value at stake. The misuse of an identity by another party results in no or only minor inconvenience and negligible financial loss to both the individual and the service provider. Such a service may be the on-line ordering of goods and services that have a low value.

Anonymity and strong authentication: anonymous services where a high value is at stake. Examples are services that entail sensitive data or anonymous transactions that are legally binding. Electronic voting is one such legally binding, anonymous application. Another example are concessions in the domain of social security, where services involve sensitive data.

Pseudonymity and strong authentication: this category comprises pseudonymous services with a high value at stake. An example for such services is accessing a database with patents. Users of such a database do not want third parties to know which patent documents they have examined. At the same time, several visits by the same user must be linkable for billing purposes.

Full identification and strong authentication: legally binding transaction and services with a high value at stake that require the identification

of the customer. A typical example from the domain of e-government is the declaration of a change of address to the municipality. Any service that comprises a signature by the citizen falls into this category.

In fact, not all of the combinations in the service access matrix occur in practice. Especially the combination of weak authentication (use of a password) and anonymity may be considered to be somewhat artificial. As a general guideline, it can be said that the level of authentication directly depends on the value that is at stake in a given electronic transaction. The higher the value at stake, the higher the level of authentication that is to be applied. An unauthenticated or weakly authenticated service access generally only makes sense for applications where a low value is at stake.

A cautionary note should also be given with regard to identity-based services: low levels of authentication in identity-based services should generally only be chosen if two conditions are met. First of all, the financial loss to the service provider should be low in the case that an identity is misused. Furthermore, the consequences and inconvenience to an individual whose identity is misused must be minimal. If these conditions are not met, higher levels of authentication should be chosen.

This matrix shows that an anonymous service delivery does indeed not imply a low level of trust. An anonymous or pseudonymous digital credential establishes a form of identity, albeit an anonymous one. High authentication levels can be reached for anonymous and pseudonymous transactions through the use of digital credentials and biometric authentication to the device that stores the digital identity of the citizen. Anonymous transactions are therefore even possible in settings where the service provider must ensure that only authorised subjects gain access to a resource.

5.5.5 Recommendations for Service Design

Introducing the possibility of pseudonymous and anonymous transactions opens up a wider range of design choices for electronic service delivery. With regard to the design of services and the concept of digital identity, the following general recommendations can be made:

1. At the design stage of an e-service, a privacy-driven view should be assumed and it should be examined whether a citizen's identity is truly relevant for a given service. As part of an e-government initiative, design-guidelines should be created to help decision-makers to choose the appropriate levels of identification and authentication for e-services.

2. Existing systems should be reviewed with regard to the need for identifying data. Data should only be linkable to an identifiable individual where truly needed. Wherever possible, pseudonymous and anonymous records should be used.

3. Public awareness of privacy problems needs to be intensified. At the same time, an increased understanding of privacy enhancing technologies ought to be created. Today, privacy-enhancing technologies (PETs) are not yet widely used, although the respective technologies are becoming available.

4. The concept of digital identity should be augmented with anonymous and pseudonymous credentials. Digital credentials can effectively support the data protection principles of data avoidance and data minimisation. Credentials also help citizens to better control the release of personal information. Digital credentials should therefore be introduced as part of the digital identity of the citizen.

5.6 Summary

The introduction of electronic service delivery in the governmental domain poses new threats to the citizen's privacy. Some of these threats are related to the introduction of digital citizen cards. Privacy has always been an issue in e-government due to the fact that the data processed in governmental administrative systems is of a rather sensitive nature and that government is among the largest data collectors. The use of digital citizen cards accentuates privacy problems even further: the use of citizen cards increases the risk that a citizen's transactions may be traced and linked, given the fact that these cards will be used to access a multitude of electronic services from different domains. Addressing privacy problems is of primary interest if the citizen's informational privacy is to be safeguarded. Addressing these problems would also pertain to building trust in e-government systems, which is of crucial importance, as trust is a major factor in the acceptance and thus for the broad uptake of electronic transactions in the governmental domain.

The fair informational practices, as defined by Alan Westin, stipulate the data protection principles of data avoidance and data minimisation, which are also found in the EU directive on data protection. They stipulate that personal data should only be collected, stored and processed when truly necessary. Anonymous and pseudonymous service delivery are the most effective way to avoid the creation of personal data. Consequently, designers of information systems should, wherever possible, include ways of allowing users

to act anonymously. Where feasible, digital identities that hitherto related to identifiable individuals should be replaced by anonymous identities. This, in turn, necessitates a new approach to digital identity: citizen cards should be modified to allow for the anonymous access to services as an additional feature. This requirement can be met by incorporating anonymous digital credentials as part of the citizen's digital identity.

Threats to privacy must be addressed by social, legal, technical and organisational measures. On a social level, a debate on privacy issues is desirable in order to raise public awareness of privacy threats and technology that is available to counter them. Basic legal measures include the creation and enactment of data protection legislation. On a technical level, privacy enhancing technologies (PETs) offer a means to better protect the citizen's privacy. On an organisational level, measures include publishing and enforcing privacy policies, the support of PETs in service access and audits of data processing practices.

From a privacy-centric perspective, it is desirable that credentials and other privacy-enhancing technologies such as P3P documents are incorporated into citizen cards. The use of credentials as part of the citizen's digital identity opens up the possibility of delivering services in an anonymous or pseudonymous modus while maintaining strong trust relationships. Digital credentials are the very technology that has the potential of strengthening privacy and of restoring to some degree the informational self-determination of the citizen. E-government and the digitisation of governmental institutions can offer the chance of improving the citizen's privacy, instead of undermining it.

Chapter 6

Concept for An Extended Digital Identity

This chapter presents the concept for an extended digital identity. As a new identity element, pseudonymous credentials are introduced. The proposed concept for a citizen card comprises privacy-enhancing technologies as part of the citizen's digital identity. We critically assess the credential system proposed by Camenisch and Lysyanskaya with regard to the suitability to implement the proposed concept for an extended digital identity. We present an architecture that supports our concept of digital identity. The architecture is based on a Web-based service delivery and on Web services. We discuss the components that need to be deployed by credential issuers, service providers, and on the client side. The architecture also comprises an off-card storage to augment the citizen card's storage capacity. We examine whether credentials can be stored by network-based brokers or whether they must be stored on a device under the citizen's control. We discuss the suitability of portable devices as storage for the citizen's digital identity. Furthermore, conceptual issues with regard to a deployment of credentials are discussed: Current methods for the revocation of pseudonymous credentials are considered, as are methods to achieve the non-transferability of credentials. We present a concept for a credential namespace. Furthermore, we discuss measures that can be taken to make the concept of credentials more usable.

6.1 A Concept for An Extended Digital Identity

Numerous European countries are engaged in projects for digital citizen cards. Today's generation of digital citizen represents information related

to the identity of the holder mostly with X.509 certificates. Section 4.7.2 has introduced some of these citizen card projects. All current cards contain two key pairs, one for the identification of a citizen and another one for issuing digital signatures. The goal of a strong identification is at the heart of this approach. In their nature, most of these cards are static and do not allow the addition and management of further information to model a citizen's identity. Once these two certificates are stored on the card, the digital identity of the citizen is fixed. The current approach is thus static in nature.

Furthermore, we have argued that the current approach to identity cards has the potential to invade the citizen's privacy. We have described potential privacy threats in section 5.3.2. Privacy dangers are acerbated by the fact that most cards are to be used in a wide range of applications. The current cards that are to be used in public and private sector services pose the danger that a cardholder's transactions can be easily linked and that transactions will increasingly necessitate an identification of the cardholder.

This thesis proposes a concept for an extended digital identity for the use in e-government. In contrast to the current approach, it introduces new elements to the digital identity of the citizen and thus provides scope for new applications of citizen cards. The major enhancement is that the concept comprises privacy-enhancing technologies. Pseudonymous credentials are introduced as part of the citizen's digital identity. Cards that comprise credentials can be used to deliver e-services anonymously or pseudonymously. From a data-driven perspective, the concept includes new data elements to model the citizen's digital identity. From a functional perspective, it proposes new functionality for digital citizen cards. Concerning the infrastructure for smart card-based solutions, this approach requires additional system components.

The extended digital identity proposed in this thesis introduces pseudonymous credentials as a new element of the citizen's digital identity. In this approach, the citizen's digital identity comprises the following elements:

- Authentication certificate
- Signature certificate
- Attribute certificates
- Privacy Preferences Profile document (P3P profile)
- Pseudonymous credentials
- Digital documents

A P3P profile does not constitute a digital identity but is nevertheless included as an additional element, as it pertains to the goal of privacy. With the exception of the Austrian Bürgerkarte project, none of the initiatives address the storage of digital documents. We consider digital documents as a part of the digital identity that will increasingly become important as administrative processes can increasingly be accessed electronically. The research project FASME sees document handling facilities as an integral part of citizen cards and provided document management capability as well as a secure document storage outside the card [MCH+01].

Most importantly, anonymous credentials are added to the digital identity as an anonymous element. Credentials enable the citizen to demonstrate attributes in an anonymous manner and to access services without disclosing their identity. By use of credential technology it also becomes possible to split identity-related information into a set of smaller statements that may be shown independently of each other. The inclusion of credentials as an anonymous element in the digital identity constitutes a form of privacy-enhancing technologies (PET) on the citizen card. There are currently no citizen cards that integrate privacy-enhancing technologies. The elements representing the digital identity will be discussed in section 6.1.1.

Introducing new elements to the citizen's identity also necessitates the introduction of new functionality to address the management of these elements. We propose the following set of functionality for a device that manages the digital identity:

- Authentication, encryption and signature capability
- Storage of P3P profiles
- Storage of digital documents
- Credential management functionality
- Identity information management functionality

Authentication, encryption and digital signature capability are standard features of today's digital citizen cards. The approach thus introduces three new management functionalities to citizen cards. The card serves as a bearer for P3P profiles that may be used in conjunction with any P3P-enabled Web-browser. The card also manages the citizen's anonymous credentials. As a third innovative element, the approach incorporates identity information management functionality on the card (see section 6.3.3). The next section will briefly discuss the elements of the extended digital identity.

6.1.1 Elements of the Extended Digital Identity

Our approach to an extended digital identity consists of several elements which are briefly outlined in this section. Two of the identity elements, signature and identity certificates, are today a regular part of all digital citizen card initiatives in Europe. These two elements each comprise a certificate and an associated key pair. A signature key pair for example consists of a private key and a public key, with the latter being embedded in a public key certificate.

6.1.1.1 Authentication Certificate

The authentication certificate belongs into the category of identity certificates. The authentication certificate binds a public key to the identity of an individual. This association is normally based on the data recorded in the registry of population (in Austria for instance, the respective data is established on the basis of the national population register). The authentication certificate and its associated private key are used in cases when citizens need to be authenticated beyond doubt. A separate key pair is necessary for authentication, as for reasons of security, the signature key is exclusively used for issuing signatures. The authentication key pair is also used to establish encrypted communication channels or to encrypt and decrypt arbitrary data (e.g. email messages). Authentication certificates are implemented as X.509 certificates [ITU88].

6.1.1.2 Signature Certificate

A single signature certificate is stored on the card. It currently does not make much sense to provide facilities to manage more than one signature certificate, although technically very well feasible. There is an ongoing debate whether citizens should be issued several key pairs to reflect the changing roles in which they act. As an example, a citizen who is allowed to sign contracts on behalf of their employer would then be issued a key pair that is exclusively used to sign for the company. This would lead to a situation where citizens possess a key pair for every role in which they issue signatures. However, there is an alternative to this approach: roles can also be modelled by signing with a single signature certificate and conveying any additional information pertaining to roles by use of XML documents or attribute certificates. This approach has the benefit that users do not need to administer several key pairs.

6.1.1.3 Attribute Certificates

Attribute certificates bind attributes to the public key of an individual. In this way, attribute certificates make it possible to model additional identity-related information about an individual. The X.509 standard also addresses the format of attribute certificates. Today, this type of certificates is not yet used in e-government. Once digital signature and digital identity cards come into widespread use, this typed of certificate may be used to model e.g. roles that a citizen plays. Also, attribute certificates may be used for the purpose of certificate-based access control (see section 2.2.1). The citizen card should therefore provide the possibility of storing any type of attribute certificate and make these certificates accessible on request.

6.1.1.4 Digital Documents

A digital document represents any kind of information in electronic form which, in its entirety, describes an object [ZS95]. The provision of seamless electronic services necessitates that administrative bodies create digital versions of documents that today are still handed to the citizen in paper form. The modern citizen has to handle a variety of official documents such as a birth certificate, driving licence, car documents, passport, building permission, and so on. We expect an increased use of digital versions of administrative documents with the migration towards electronic service delivery. A digital identity card can serve as a storage for such administrative documents. Documents that are stored on the card are always at the holder's disposal. As the storage capacity of the card is limited, documents can be moved to an off-card document storage accessible over the Internet to which the card serves as an access key.

6.1.1.5 P3P Profiles

Citizens can express their privacy preferences for Web browsing in the APPEL language and store the resulting XML document on their citizen card. This allows citizens to identify sites that engage in privacy-invasive data processing. Of course, this benefit can only be realised if service providers make their policies available as P3P statements. The smart card plays the role of the bearer of such profiles: it stores established profiles and makes them available to a P3P-enabled web browser. The advantage of this approach consists in the fact that the storage on a mobile device offers unconstrained availability of privacy preferences.

6.1.1.6 Anonymous and Pseudonymous Credentials

Anonymous and pseudonymous credentials constitute an extension of the digital identity that affords anonymous and pseudonymous transactions to citizens. A credential represents a statement concerning a subject signed by the party who issued it. Both anonymous and pseudonymous credentials should be supported:

- **Anonymous credentials** do not contain any visible reference to the identity of the owner. Accessing service with an anonymous credential leads to a situation where a service provider cannot link several transactions by one and the same citizen. A scenario for anonymous service delivery in e-government will be discussed in section 6.1.5 in order to illustrate the benefits of anonymous credentials.

- **Pseudonymous credentials** embody a pseudonym. They are used for pseudonymous service access, i.e. in situations where a citizen who accesses a service repeatedly must be recognised. Pseudonymous are useful for personalised service delivery or in services where a reputation needs to be built by the user.

  An example for a pseudonymous service is for instance on-line education for unemployed citizens. Let us assume that government offers on-line training courses for unemployed citizens. These services are to be provided in a personalised manner: a citizen should only be given access to on-line courses which are relevant to his or her profession. However, it is not necessary that the provider of such on-line training knows about the identity of the citizen. An personalised access to such services can be provided while maintaining the benefits of anonymity. By the help of a pseudonymous credential, a citizen can enjoy personalised services under a pseudonym and thus remain anonymous towards the service provider.

The citizen card plays the role of credential manager: it handles the issuing protocol, stores credentials and displays these on request. The card also assumes the task of archiving credentials that are no longer valid. The next section discusses the basic requirements for an implementation of the extended digital identity.

We have presented the elements of the extended digital identity that comprises pseudonymous credentials. In the remainder of this section, we will first discuss requirements for the use of credentials in e-government. We will then present an architecture that supports the concept of the extended

digital identity. As a further important aspect, we will revisit the pseudonymous credential system proposed by Camenisch and Lysyanskaya. We will appraise the system with regard to the suitability for the implementation of the proposed concept for an extended digital identity. We will also make suggestions what features are to be used in an actual deployment. The section will close with an application scenario that illustrates the benefits of anonymous service delivery based on credentials.

6.1.2 Basic Requirements for the Use of Credentials in e-Government

This section discusses basic requirements that must be met in order to deploy anonymous and pseudonymous credentials as part of the citizen's digital identity. This list states requirements at a high level of abstraction and is not intended as a detailed requirements specification. We state the following basic requirements [Aue03]:

- **Storage of credentials in a device under the user's control:** credentials should be stored on a device that the citizen can carry along rather than on a server that makes credentials accessible over the network (see section 6.2).

- **Smart card as a tamper-proof storage**: the digital identity of the citizen should be stored on a tamper-proof device in order to minimise the risk of identity theft and comply with legal regulations for digital signatures. Also, a tamper-proof environment is the safest way to prevent the transfer and lending of credentials. The choice of device is considered in detail in section 6.2.2.

- **Citizen card as anonymous bearer of the digital identity:** if a card is to act as an access device for anonymous services, the card itself must not leave identifiable traces upon insertion into a card terminal. Necessary modifications to citizen cards in order to fulfil this requirement are detailed in section 6.2.3.

- **Non-transferability of credentials:** citizens should not be able to transfer or lend their credentials to other citizens. The property of non-transferability is best achieved by use of a tamper-proof storage device. Different strategies to achieve non-transferability are assessed in section 6.7.2.

- **Support for anonymous and pseudonymous transactions:** both anonymous and pseudonymous credentials should be supported. In some e-government applications, it may be important to personalise services for citizens. Personalisation in anonymous settings is possible by use of pseudonyms. Examples for services that necessitate anonymous respectively pseudonymous delivery were provided in section 6.1.1.6.

- **Support for unlinkable multi-show credentials and one-show credentials:** a credential system for e-government should support both one-show and multi-show credentials. Citizens should be able to show their credentials to many different service providers without transactions becoming linkable. Multi-show credentials should also be constructed in a way so that citizens do not have to recertify them after every use. For some scenarios, one-show credentials are necessary. A one-show credential is used to model rights that can be used only once. For instance, a citizen on low income may have the right to one free consultation with a counsellor within one month. Such a right can be implemented with a one-show credential that is valid for one month. A citizen can then freely chose when to use the credential (within the one-month period) but cannot use the credential (and thus the associated right) more than once.

- **Use of credentials over the network and in local settings:** citizens should be able to use their credentials in Internet-based transactions. Notwithstanding, credentials should also be available in local settings where a citizen demonstrates possession of a credential at the point of service provision (e.g. at the local library or a sports facility).

- **Traceable anonymous transactions:** in order to embrace a service provider's need for security, credentials should implement a revocable form of anonymous identity. This requirement was motivated in section 5.5.2.

- **Anonymous communication infrastructure:** system components are interconnected by a middleware based on Web services. The middleware must allow for anonymous communication channels in order to provide anonymity at the application level (see section 6.6.2).

- **Off-line storage to augment the citizen card's capacity:** citizens may accumulate many credentials and digital documents over time. Documents that are infrequently used should be kept on a server accessible via Internet. Similarly, credentials that have expired should

be archived in a secure network-based storage space. Such a storage facility is discussed in section 6.6.1.

- **Audit trail for citizens:** any access to an element of the digital identity should be logged by the card. The citizens should be able to inform themselves what information concerning the identity was provided in a transaction. This feature also helps to discover unauthorised access to identity elements (see section 6.3.3).

- **High degree of usability:** despite the use of a rather complex technology such as pseudonymous credentials, it is an important goal that credential-based services are nevertheless easy to use. If the handling is complicated, there is the danger that users bring themselves at a disadvantage through lack of understanding of the user interface. Also, lack of usability poses the danger that users will not embrace credentials. Concepts to enhance the usability of credentials are discussed in section 6.7.4.

These requirements have a direct impact on the architecture of a credential-based system. The next section presents the architecture components that support the concept of the extended digital identity.

6.1.3 Overview of the Architecture

The concept for an extended digital identity introduces pseudonymous credentials as a privacy-enhancing technology on the citizen card. As compared to the infrastructure of current identity card projects, this approach to digital identity requires changes in the infrastructure for card-based services in order to support the use of pseudonymous credentials. The citizen card must be equipped with a credential manager that manages the life cycle of credentials. Both public and private sector organisations may act as issuers or as relying parties and thus need additional infrastructure components. This section provides an overview over the architecture for the use of credentials in e-government. Figure 6.1 illustrates the architecture components.

The architecture comprises the following components:

Identity manager on the smart card: this component is installed on the citizen card and manages functionality related to the citizen's digital identity. This includes the handling of pseudonymous credentials. This component also keeps track of how elements of the digital identity are used (identity information management). The card acts as representative for the

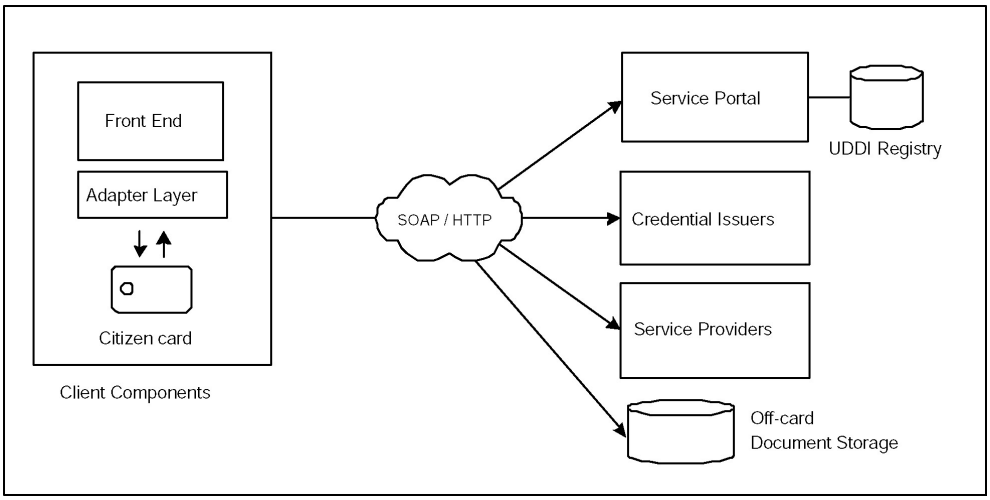

Figure 6.1: Overview of architecture components

citizen and as a manager of the life-cycle of all pseudonymous credentials that the citizen owns. The card acts as an anonymous bearer for the identity of the citizen. The card must not contain a publicly readable card number or a publicly readable data set. The card is also used as an access key to the off-card storage facility.

Off-card storage for documents, credentials and audit data: smart cards have a very limited storage capacity. Today's smart cards feature about 64 KB of memory, which may not be enough to store all administrative documents and credentials that a citizen accumulates over time. A secure off-card storage extends the memory of the card and stores identity elements that have expired or that are rarely used (archival functionality). Similarly, the log files that track identity usage can be moved to the off-card storage periodically to free precious memory space on the card.

Credential issuers: both private and public sector organisations issue credentials to citizens. Issuers of credentials must therefore add infrastructure components to handle the issuing process and keep track of issued credentials. The issuer needs to maintain a high level of security, as unauthorised users should not be able to obtain credentials. A credential issuer publishes a list that details the type of credentials that an organisation issues. The infrastructure that is maintained by a credential issuer is discussed in more detail in section 6.4. Credential issuers need to handle the registration and issuing process for credentials and administer credential revocation lists where necessary. An organisation can both act as a credential issuer and offer credential-based services.

Service providers (relying parties): both private and public sector organisations may offer services that can be accessed anonymously by use of credentials. The paradigm of credential-based service access necessitates additional software components. Service providers need to be able to establish trust based on credentials. They have to decide which credential issuers to trust and which credentials to accept. They also need to be able to establish the validity of credentials.

Middleware to interconnect components: a middleware based on Web services interconnects the components of the architecture. More specifically, the middleware supports all credential-related protocols (issuing and showing credentials) and the communication between citizen card and off-card storage. In order to preserve anonymity, anonymous service must be accessed through an anonymous communication channel.

Anonymous communication infrastructure: anonymity at the application level necessitates anonymous communication channels. Anonymity at the network level ensures that service providers cannot trace a communication back to a specific IP number of the user's machine. Such communication channels can be achieved e.g. based on mix networks.

Front-end and adapter layer: on the client side, three components are deployed: the citizen card, an adapter layer and a front-end. Citizens access services with the front-end, which can be a proprietary client application or a Web browser. An adapter layer serves as interface between client software and the citizen card. The adapter layer also provides integration with the middleware.

Service portal and service registry: we presume that a service portal exists that serves as a single point of entry for e-government services. The service portal helps citizens to discover services that are useful for them. The portal can be associated with a UDDI (Universal Description, Discovery and Integration) registry where descriptions of Web services are published. This component serves the purpose of service discovery and is not specific to credential technology.

In the next section, we will discuss whether the pseudonymous credential system proposed by Camenisch and Lysyanskaya is suitable as a basis to implement the proposed concept of an extended digital identity.

6.1.4 Assessment of the Approach by Camenisch and Lysyanskaya

In this section we revisit the features of the pseudonymous credential system proposed by Camenisch and Lysyanskaya. We critically appraise the functionality of the system and discuss whether the system is suitable to implement our concept for an extended digital identity. We discuss whether all features of the system are really needed for implementations in the context of e-government. We give recommendations how the credential system can be used in e-government and what features need to be changed. The following aspects shall be discussed:

Dependence on root pseudonym: The root pseudonym serves security purposes. It ensures that a user's identity can be discovered in case of fraud. Users establish a single root pseudonym and need to be identified when doing so. We expect that this pseudonym is established when the citizen card is issued. However, during the life-time of the card, users never obtain credentials under the root pseudonym or otherwise actively make use of this pseudonym. Users do not need to be aware of the existence of this pseudonym but much rather of the fact that they can be held liable in case of unlawful behaviour. Consequently, this pseudonym can be made fully transparent to the user. The root pseudonym thus should be hidden from the average user and only be displayed to advanced users.

Credentials and pseudonyms: the approach by Camenisch and Lysyanskaya offers all features that were originally proposed by Chaum. Users can establish pseudonyms and obtain credentials. The system thus supports both fully anonymous as well as pseudonymous service access. The system also offers one-show and multi-show credentials. It thus provides a rich set of features that covers a wide range of application scenarios. With regard to the handling of credentials and pseudonyms, the recommendations from section 6.7.4 should be implemented: we advocate that the management of pseudonyms and credentials should be automated where possible.

Choice of revocation manager: letting users choose from a set of revocation managers is a desirable feature. Users may have preferences with regard to a manager as typically not all users trust the same parties. Consumer protection organisations or data protection commissioners can make recommendations that help users choose a manager. The choice of manager should be made at the time when the credential is issued, not as part of the show protocol.

Distinction between pseudonymity and anonymity revocation: Camenisch and Lysyanskaya propose two types of revocation managers: one type can help to discover the pseudonym of a user and the other type the identity of a user (see section 4.2.1.2). This feature pertains to security and allows authorities to trace users who engage in fraudulent behaviour. However, it can be argued that having two types of revocation is of little practical value. We give two reasons why we believe that a single type of revocation is sufficient for practical implementations.

On the one hand, for purposes of fraud detection, only a user's identity is of interest. If a credential system is implemented following the proposal by Camenisch and Lysyanskaya, then the user's identity is only known to the root pseudonym authority. Pseudonyms and credentials are established anonymously and cannot be related by any organisation to an existing individual. Discovering a pseudonym behind a transaction is thus of little value for purposes of law enforcement.

On the other hand, we can argue that pseudonymity and anonymity revocation is equivalent in many situations. In many applications, pseudonyms and credentials are only issued to identified users. This argument especially applies to e-government settings. Many documents are only issued to identified citizens. E.g. a driver's license can hardly be issued without identifying the citizen. In such settings, the issuer can map a pseudonym to an existing individual. As a consequence, disclosing the user's pseudonym becomes semantically equivalent to disclosing the user's identity.

In order to reduce complexity and make the system easier to understand, we argue that only anonymity revocation should be implemented. User should not have to worry in what cases their pseudonym or their identity is disclosed and in what cases these two kinds of revocation amount to one and the same thing.

Revocation of credentials: we have discussed the revocation of pseudonymous credentials in section 6.7.3.2. We have argued that the approach to revocation of credentials proposed in [CL02] is not suitable for a deployment on citizen cards. Current approaches to revocation generally do not scale well. Thus, new algorithms for credential revocation will have to be developed. Deploying applications that rely on revocable credentials should thus be avoided.

We conclude that the credential system proposed by Camenisch and Lysyanskaya offers a rich set of features that has the potential to cover a wide range of application scenarios. We deem the basic system as suitable for a deployment in e-government applications. However, the many features

also make the system more difficult to understand for users. Care has to be taken that the system is implemented in a way that maintains usability. Consequently, not all features of the system should be used.

Measures must thus be taken to hide complexity where possible. The measures proposed with regard to usability (see section 6.7.4) should be implemented in order to achieve a better usability of the overall system. Furthermore, we argue that only anonymity revocation (i.e. identity discovery) should be used in practical e-government applications. If these recommendations are followed, the use of pseudonymous credentials is to a large degree automated and can become manageable for the average user.

The next section provides an illustrative example scenario from the domain of social security that clearly illustrates the benefits of including pseudonymous credentials as part of the digital identity.

6.1.5 A Scenario for the Use of Pseudonymous Credentials in e-Government

The following scenario stems from a meeting with members of Newcastle city council in the United Kingdom that took place in the course of the FASME project [AM02]. The scenario is specific to the United Kingdom's welfare system. However, the scenario illustrates the problems of identity-based services and the benefits of an anonymous service access. These benefits apply to other countries as well.

6.1.5.1 A Scenario from the Domain of Social Security

The United Kingdom has a welfare system that is intended to provide support for citizens in need. Supportive measures include e.g. counselling and financial support in the form of benefits. Examples for benefits provided by the welfare system are housing benefit, council tax benefit, unemployment benefit or income support for people on low income [SBLB03]. People on income support can claim exemption from health care charges, vouchers towards the cost of cultural activities, free school meals for their children and a benefit toward the cost of VAT (Value Added Tax) on their fuel bill. Income support implies further discounts at various institutions, such as the council's sports facilities, the local library or the theatre [RCMA01].

Citizens who receive any of these benefits are issued a social security booklet by the local council. The booklet contains an entry for each of these benefits and details the period over which the benefit is received. This booklet serves as proof of eligibility whenever a citizen wants to claim a discount that is available to benefit recipients. However when claiming the

discount, citizens have to prove their eligibility by presenting their social security booklet.

This system has two considerable drawbacks: on the one hand, the system is paper-based: issuing and updating the booklet is a cumbersome and expensive process. On the other hand, citizens have to carry the booklet with them at all times, which is inconvenient and often poses the danger of discrimination. The use of the booklet leaks data about the holder: producing the booklet, e.g. at the council's sports facilities, makes it obvious for the bystanders that someone receives benefits. Use of the booklet is perceived by many citizens as discriminatory. Consequently, many people do not make use of all benefits and discount's they would be entitled to. Privacy problems thus reduce the effectiveness of the welfare system.

6.1.5.2 A Solution based on Citizen Cards and Anonymous Credentials

The existing paper-based system can be re-engineered using citizen cards and anonymous credentials. A credential-based service would be more citizen friendly and better protect the citizen's privacy. With the help of pseudonymous credentials on a citizen card, citizens can prove eligibility without disclosing their identity. If this scenario was realised using traditional attribute certificates, service providers would be capable of compiling lists of benefits recipients. As data regarding a citizen's social situation can be considered as rather sensitive, leaking such data is highly undesirable. In such a scenario, anonymous credentials can offer a way to deliver services electronically in a trustworthy way while protecting a citizens privacy [Aue03].

A digital citizen card can act as a carrier for trustworthy digital credentials that state the form of benefits that a citizen receives. Such a credential would be issued by the benefits agency, stored on the card and replace the entry in the social security booklet. The credential can be shown in any situation that necessitates proof of a benefit (e.g. where a discount is tied to a benefit). The credential merely states that the holder is on income support. It does not make any statement about the holder's identity. When a credential is shown, a service provider only learns that a citizen is eligible for a given benefit. Of course, disclosing a credential must be at the cardholder's discretion - just as today use of the booklet is up to the citizen. A system based on a combination of citizen cards and digital credentials has the potential to replace the social security booklet and better protect a citizen's privacy. This scenario could be delivered with anonymous credentials. Pseudonyms are not necessary in this scenario.

A solution based on citizen cards and anonymous credentials would offer several benefits:

- Convenience: citizens can apply for benefits over the Web and thus save time
- Savings in personnel cost: an electronic solution would render the benefits booklet obsolete and thus save some of the civil servant's time
- Privacy protection: a solution based on credentials would enhance privacy in two ways:
  - Benefits can be obtained without disclosing to bystanders that a subject receives benefits
  - In contrast to an identity-based implementation, service providers cannot compile lists of benefit recipients. Citizens can claim discounts in a fully anonymous way

In this scenario, a citizen is anonymous towards service providers only and not towards the issuing authority. Pseudonymous credentials thus allow for a re-engineering of processes so that anonymity is maintained only towards certain parties or in parts of a given process.

Although an electronic implementation could also be based on attribute certificates, an implementation based on credentials has clear advantages with regard to privacy. Such an implementation would also maintain security: in case of fraud, credential holders can be traced.

6.2 Considerations Regarding the Storage of Credentials

In this section we consider options regarding the storage of pseudonymous credentials. We discuss whether such credentials can be kept on a network-based server or on a device under the citizen's direct control. We also assess several kinds of devices with regard to their suitability as manager of digital identities in e-government.

6.2.1 Brokered Approach versus Credentials on the Citizen's Device

When introducing anonymous and pseudonymous credentials as part of the digital identity, two approaches with regard to the storage of credentials are

conceivable: the first approach is to store the citizen's credentials on a device that is under the citizen's control. This device is used to execute all credential protocols such as receiving or showing a credential. An alternative approach is to manage the user's credentials centrally on a server that is accessible over the Internet. In such a scenario, the user would log into this server whenever a credential needs to be shown. The server then executes all protocols related to credentials. Both approaches have benefits and drawbacks. Both approaches are briefly discussed and a justification is given for the use of the first approach, i.e. the implementation of credentials on a citizen card instead of a network-based credential manager.

In a network-based approach to credential-management, only the authentication and signature certificates are stored on the user's smart card. Anonymous credentials are stored on a server that is accessible over the Internet. Such a server could be operated by government or by private sector service providers. When accessing a credential-based service, the user would first log in to the credential server. All credential protocols would then be carried out between client, credential server and service provider. This approach is depicted in Figure 6.2.

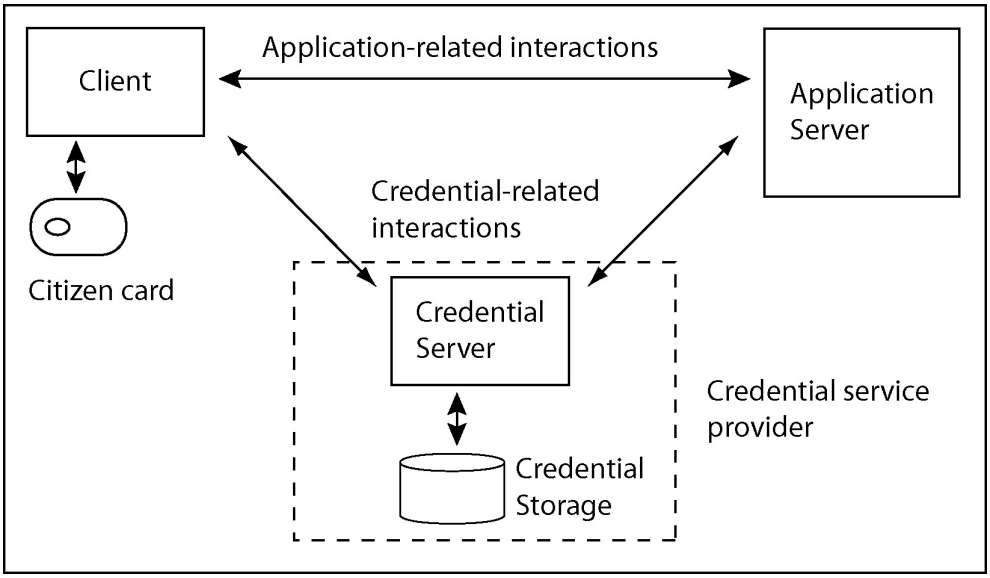

Figure 6.2: A network-based approach to credential storage

The benefits of this approach is mainly that the smart card's resource restrictions do not apply any more: mathematical complexity and storage space requirements of credential systems are no concern as the server offers a much stronger set of resources.

However, storing credentials in a location accessible by network has some drawbacks:

- **Danger of impersonation**: the secret keys of the credentials need to be stored on the server. This enables the party that provides the storage to impersonate the user. Storing secret keys on the server also makes it an attractive target for attack.
- **Privacy**: the party that stores the digital credentials has access to all credentials. It must be trusted not to divulge personal data to third parties or make use of personal data in an unlawful manner.
- **Lack of tamper-proof environment**: non-transferability of credentials becomes harder to implement (see section 6.7.2)
- **Communication overhead**: all credentials must be fetched over the network from the credential server, which adds overhead to the protocols. Furthermore, credentials can only be used in settings where access to the Internet is given.

In the card-based approach, the user's citizen card safely stores the citizen's digital identity including the credentials. When accessing a service that is based on credentials, the smart card executes the necessary protocols in conjunction with the host.

The benefits of this approach are:

- **Control**: the digital identity and the credentials are fully under the control of the user. There is no need to trust a third party with the storage of the digital identity, which contains sensitive data elements
- **Efficiency**: the digital identity is at the user's disposal without the need to fetch elements over the network
- **Support for off-line scenarios**: the digital identity and especially anonymous credentials can be used for using services in places that are not permanently connected to the Internet
- **Security**: a tamper-proof device can offer a high level of protection for the citizen's digital identity. It also can be used to achieve non-transferability of credentials

The main drawback of this approach is the resource-restrictedness of smart cards with regard to processing and memory capacity. Anonymous

and pseudonymous credential systems are harder to implement in these environments.

We have stated as a requirement that citizens should be able to use credentials not only in network-based services, but also off-line for 'local' services. An example for the local use of a credential is e.g. the proof of eligibility for a free school meal. In the UK, children of parents with a low income are eligible for free school meals. This may involve showing a credential in the school cafeteria, where no constant network connectivity is given. In order to satisfy this requirement, a network-based credential storage should not be chosen. In the future, it is conceivable that Internet access will be ubiquitous.

Still, a big hindrance to the network-based approach is that a party has to be found that can be trusted with securely storing the citizen's credentials for use over the network. It is questionable whether a party exists that the citizens would fully trust not to abuse their credentials. Commercial entities such as banks can provide secure storage but at the same time may be tempted to use the information for customer relationship management (CRM) activities. Governmental entities are undesirable as well, since affording them access to credentials will empower government to collect even more data about citizens. Even storing of credentials in an encrypted form would not alleviate the problem, since the credential would need to be decrypted when showing them.

We conclude that a use of credentials as part of the citizen's digital identity should make use of a device that is under the control of the citizen to administer the credentials. For reasons of trust and because of the resulting limitations in functionality, a brokered approach that stores credentials on a server should not be chosen.

6.2.2 Choice of Personal Device for the Management of the Digital Identity

So far, we have assumed that smart cards will be used to store information related to the citizen's digital identity. In this section, several kinds of devices are being discussed with regard to their suitability as an end user device intended for the management of the citizen's digital identity.

A device that is used to manage the digital identity of the citizen needs to satisfy a number of requirements: first of all, the device needs a sufficient memory capacity to store the digital identity. The device also needs a processor that is powerful enough to carry out cryptographic calculations within reasonable time. The device should also have a compact form factor since

users should be able to always carry the device with them. Furthermore, it should be a low-cost device as the government may have to issue such a device to all citizens. Last but not least, it must provide a secure storage for the secret part of digital identity elements.

A highly important constraint are thus the security requirements that such a device has to meet. Some elements of the digital identity contain confidential information which must be safeguarded. This is, for instance, the case with secret keys that are associated with the authentication and signature certificates. Anonymous credentials as well contain a secret component which must only be used by the holder of the digital identity. The protection of the secret information must attain a high level in order to minimise the danger of identity theft. An attacker might succeed in coming into the possession of secret information and could thus impersonate the rightful owner of the digital identity. The exigency of protection applies especially to the keys for the digital signature. The signature function is the basis of legally binding signatures and the device has consequently to comply with the specifications of the EU signature directive [Eur95].

In principle, only those devices come into consideration that can be constantly carried by their owner, and which have the capability to securely store information and perform calculations. A typical example for a device that many people always carry with them is the mobile phone. In the following, mobile phones, PDAs, smart cards and iButtons are considered with regard to their suitability as a bearer of the citizen's digital identity.

6.2.2.1 Smart Cards

The smart card is a robust plastic card that incorporates a microprocessor. Most Europeans are well acquainted with the smart card technology, as it is typically used for telephone and banking cards. Owing to its form factor, a smart card is also ideally suited as a optical identity card. The outer surface can be used for safety features such as holograms, photos or fields for signatures [RE00].

Typical smart cards are equipped with memory in the range of a few kilobyte and with relatively weak processors. Today's generation of smart cards are multi-application cards, i.e. they can carry several applications that are independent of each other. This allows several applications to exist side by side on one card, which in turn offers the possibility of installing new applications if needed. A firewall mechanism ensures that one application cannot access the memory space of other applications. Most multi-application smart cards on the market can be programmed in Java. Smart cards are generally regarded as a tamper-proof computing environment [Sch96] which means

that they are safe from replication and manipulation. Unauthorised persons can neither modify the contents of a card nor can they read out any information. This makes the smart card exceptionally well suited for the secure storage of secret information.

Nevertheless, the concept of the smart card brings also certain disadvantages. A crucial detriment is the lack of an in- and output facility. The card depends on a host system which accepts inputs for the card and shows the results of computing steps performed by the card. This host system must be absolutely reliable so as to ensure that neither input nor output are manipulated. The limited storage capacity and the weak performance of the processor are equally disadvantageous. Although most cards are equipped with cryptographic co-processors for certain standard algorithms, e.g. SHA-1 and RSA, complex algorithms deviating from the latter cannot be easily implemented on a smart card.

It is the security features, the form factor, the high acceptance and the low cost that make the smart card an appropriate device for the management of the digital identity. Smart cards are the only portable devices to comply with the requirements of the EU signature directive (except for the iButton).

6.2.2.2 Mobile Phones

Mobile Phones are today a constant companion of a considerable number of Europeans. It is estimated that in 2002 around 60% of the population of Europe owned a mobile phone [Eur02c]. The acceptance of this technology can be regarded as very high, in particular among the younger generation. Mobile phones are becoming increasingly Internet-enabled which means that they can access Internet-based services. Mobile telecommunication standards such as GPRS (General Packet Radio Service) or UMTS (Universal Mobile Telecommunications Standard) make it possible to transfer growing volumes of data. Mobile phones are increasingly being equipped with features which were formerly only found on PDAs. Modern mobile phones also offer a Java runtime environment, usually the Java 2 Micro Edition platform [Sun02a]. This allows the user to install Java applications on the phone.

A clear advantage of mobile phone is that they possess input and output facilities. The user interface to manage the identity could thus be implemented on a device that is under the control of the owner. This would reduce the necessity of relying on external devices with user interfaces such as kiosks or card terminals (equipped with display and keyboard). The input facility of mobile phones, however, is mainly limited to numbers and 'yes' or 'no' answers. Entering characters is rather cumbersome. Besides, most displays

are too small to display more detailed dialogues to the user. The inadequacy of the display is particularly disadvantageous when it comes to displaying documents that have to be digitally signed. It follows that in order to sign digital documents, a host computer with a bigger display is still necessary.

Next to the limited user interface capabilities, there are further limitations. Many of the phones comprising a Java runtime environment are equipped with processors that are relatively weak as compared to those of PDAs. On account of these weak processors, it is not possible to implement cryptographic algorithms of a more complex nature. We expect however, that hardware resources of mobile phones will become more powerful over time. A much more serious problem is the lack of basic safety features in present operating systems. Most mobile phone operating systems do not provide sufficient security features to meet the requirements for a secure management of secret keys. Users are free to install any type of software on the phone which poses the risk of installing an attacker's software as well. Mobile phones usually do not feature a tamper-resistant storage area for secret keys. This lack poses the risk that an attacker's software could gain access to secret keys.

A possible remedy might consist in the storing of the keys on a smart card which is inserted in a second card terminal inside the phone. In this case, however, all cryptographic operations would also have to be effected on the smart card in order to guarantee the secrecy of the keys. Inserting a citizen card into a mobile phone would solve the problem of a trustworthy user interface (provided no untrusted software is installed on the device). The user could then show credentials by help of the mobile phone. This solution has the advantage that dialogues are displayed on a device that is under the users control and that the user trusts. Such a solution would of course not offer total anonymity, as a mobile phone user is not anonymous towards the network operator.

Despite the considerable prevalence of mobile phones and their general acceptance, there remain certain disadvantages, with the lack of security features of the operating systems being the greatest drawback. However, mention must be made of the fact that mobile phones have already been used for e-voting in mobile government settings, for instance in Manchester in May 2003 [Loc02].

6.2.2.3 Personal Digital Assistants

A PDA (Personal Digital Assistant) is a compact, lightweight computer that is easily portable. It is used as an electronic agenda, address book and for taking notes. PDAs mostly have no keyboard but are operated by means of

a display that is sensitive to touch. The top of the range PDAs are equipped with colour displays, powerful RISC-CPUs and a storage capacity of several dozen megabytes. Their display is considerably larger than that of most mobile phones and they provide a much higher resolution. Owing to their increasing computing capacity, PDAs are suitable for more and more complex tasks. Most PDAs offer a Java runtime environment in the form of the J2ME platform.

PDAs would therefore be in principle well suited for the management of the digital identity. Dialogues with the user can be directly effected on the device which also administers all identity-related information. As is the case with mobile phones, the central problem of PDAs is the lack of security features of the current operating systems. Be it the PalmOS, the PocketPC or the Symbian operating system, none of these provide secure bootstrapping of the device. PDAs do not provide a tamper-resistant storage area for cryptographic keys. An attacker's software residing in the memory might therefore read out secret keys from the device and misuse them. Again, a smart card could be used in the PDAs card terminal, but this approach would still not overcome the smart card's resource restrictions.

As compared to smart cards that normally cost less than ten Euros, PDAs are much more expensive. An e-government that is intent on avoiding the deepening of the digital divide would have to distribute PDAs free of cost to all citizens so as not to be exposed to the reproach of discrimination. The advantage of a relatively powerful computing environment and a bigger display area is therefore set off against the drawbacks of high cost, the lack of safety features and the fact that they are not used by the greater part of the population. A survey conducted by the European Commission 2001 showed that only 3% of all Europeans own a PDA [Eur02b].

In the future, PDA and mobile phone will be increasingly combined by manufacturers into a single device. Combined devices that integrate the functionality of a PDA with a mobile phone are widely available already. Also, as part of this trend, the display size and the amount of memory available in mobile phones keeps growing.

6.2.2.4 iButton

The iButton is a button-like device which is comparable to the Java Card in terms of processing capacity [Max02]. The microprocessor is enclosed in a 16 mm steel can.The communication with the terminal is either accomplished in a contact-less way or by means of a button terminal. In contrast to the smart card, the iButton features a single button that the user can press in order to give input to the button. Moreover, iButtons are also available in a

version that features a cryptographic co-processor. The iButton has its own power supply. Today, iButtons are widely used for the implementation of electronic ticket systems (for instance in skiing resorts). Like the Java Card, the iButton can carry multiple applications and its software can be developed in Java. The iButton supports the same API as a Java Card. Figure 6.3 depicts an iButton by Dallas Semiconductor.

Owing to its own power supply, the iButton is even more tamper-proof than a smart card. The iButton becomes active on detecting signs of manipulation and can actively delete the contents of its memory. The higher tamper resistance is advantageous with regard to the storage of identity-related information. On the other hand, its form factor prevents it from being used as an optical identity card as it is practically impossible to incorporate a photo or other safety elements on the surface of the iButton. A further disadvantage is the fact that a biometric sensor for authentication cannot be directly embedded in the button.

Table 6.1 presents a comparison between various end user devices with regard to their suitability as a carrier of the digital identity. Summing up, we can say that at the present moment the smart card is the only portable end user device that can meet the high safety requirements which such a device should provide so as to ensure a secure management of the digital identity. In addition, smart cards are cheap, are already in widespread use and are equally suited to function both as digital and optical identity card.

We thus currently deem the smart card the only suitable device. But it is precisely its limited resources that constitute a challenge for the software developer in the sense of accomplishing a higher degree of functionality on the card.

Before mobile phones and PDAs can be considered appropriate for the management of the digital identity (without adding a smart card to the device), their operating systems will have to provide further security features. It is in particular the lack of tamper-resistance that prevents PDAs and multi-application phones from being used for the storage of secret keys. However, they can assume this function if a smart card is inserted in the device with the smart card taking on the management of the keys. In the future, both PDAs and mobile phones may become trustworthy computing devices if features proposed by the Trusted Computing Group (TCG) are incorporated into these devices. The trusted computing initiative is briefly introduced in the next section.

	Mobile Phone	**PDA**	**Smart Card**	**iButton**
Acceptance	Very high	Medium	High	Very low
Input Facilities	Numeric key pad	Touch screen	None	Single button
Output Facilities	Small display	Medium-size display	None	None
Tamper Resistance	Low	Very low	High	Very high
Ability to Carry Multiple Applications	Yes	Yes	Yes	Yes
Suitability for Optical Identification	Very low	Very low	Very high	Very low
Typical RAM size (4^{th} Quarter 2003)	1 - 256 MB	8 - 512 MB	16 - 128 KB	64 - 134 KB
CPU	32 Bit	32 Bit	8/32 Bit	32 Bit
Suitability to Carry Digital Identity	Medium	Low	High	Low

Table 6.1: A comparison of portable devices with regard to suitability as a managing device for digital identities

6.2.2.5 Towards Trusted Personal Computing Platforms

Smart cards provide many security features that turn them into trusted computing environments. They are generally considered to be tamper-proof. However, the same cannot be said about other computing environments such as PDAs or the smart card's host platform. In order to turn personal computers into trusted computing environments, extended functionality at the hardware and operating system level is required. Some requirements were already mentioned earlier. Today's operating systems would have to be changed fundamentally in order to become more trustworthy [ELPW03].

Computer manufacturers have recognised that future applications may benefit from enhanced security features and have founded a consortium to address the current lack of features. The Trusted Computing Platform Alliance, or TCPA, has over 170 members and was founded by Compaq, HP, IBM, Intel and Microsoft [TCP03]. Prior to this initiative, all five companies

had been individually working towards improving the trust available within computing platforms. The work of the TCPA was motivated by the common awareness that high-value business transactions require an adequate level of trust. Software security solutions are vulnerable because of the lack of OS security. In April 2003, the activities of the TCPA were taken over by a new consortium, the Trusted Computing Group (TCG). The TCG is a non-profit organisation, has an open membership policy and aims to develop an open standard for a trusted computing platform [TCG03].

The handing over of activities to the TCG was mainly motivated by public criticism. The TCPA initiative was heavily criticised by several authors. It was expected that the TCPA initiative might be misused to gain more control over the users and that it would be used to enforce stringent DRM (Digital rights management) mechanisms. It was also feared that trusted computing platform features would give PC manufacturers and operating system manufacturers control over what type of hardware and software can be run on a computer [And02]. Furthermore, the TCPA features can potentially invade the user's privacy, as the manufacturers may be able to read data concerning a computer's configuration over Internet connections.

Through the combination of software and hardware components, the TCG aims at creating a trusted computing platform. The specification addresses certain hardware components, the BIOS (Basic Input Output System) and the operating system of a computer. The basis for the approach is a hardware module called Trusted Platform Module (TPM) that provides basic cryptographic functionalities and a tamper-proof storage for security-relevant data. In terms of functionality, TCG compliant computers allow (in the least) the detection of BIOS manipulation, secure bootstrapping, authentication of code before execution, persistent storage of confident information and basic cryptographic capabilities such as secure random number generation and the handling of digital signatures. The TCG specification is designed to be both platform and OS agnostic [TCG03].

Undoubtedly, the TCG initiative will bring new security features to personal computing platforms. PDAs and mobile phones cannot be regarded as secure computing platforms before the features of the kind specified by the TCG become available. Therefore, the smart card is currently still the only portable device that can provide an adequate level of security for the handling of identity-related data. Once extended security features become available for future generations of portable devices, they latter may develop into suitable devices for the management of the citizen's digital identity.

6.2.3 Modifying Citizen Cards for the Support of Anonymous Transactions

If anonymous credentials are to be deployed on citizen cards, the cards must act as anonymous carrier for credentials. So as to achieve the goal of anonymity, the citizen card must not leave identifiable traces in the course of an anonymous transaction. Many of today's concepts for citizen cards have features that would allow an identification of the card holder in every transaction. These features would have to be modified. The two problematic features are publicly readable data sets and card numbers that are transmitted to the host computer upon insertion of a smart card into a card terminal.

A publicly readable data set is a set of data that relates to the holder of the card, is stored on the card and can be read from the card by a service provider upon inserting the card or upon unlocking it by use of a PIN. Many citizen card initiatives include plans for such data sets. Typical data items include the name of the card holder, the nationality, the date of birth, possibly a card number, and in some cases even the citizen's identity certificate. The public data set may also include special access codes that specify how user interfaces should be presented to disabled users [CEN00]. As an illustrative example, the Estonian identity card features a publicly readable data set that is quite comprehensive: a service provider can read the name and first name, the date of birth, the place of birth, the sex and the nationality of a card holder from the card [Ser03]. The data is accessible before the authentication of the card holder by personal identification number (PIN). Such publicly readable data sets ought to be protected by a PIN or removed from cards altogether so as to avoid the danger that the card leaves identifying traces right after insertion into a card terminal.

The second problematic feature of many citizen cards is a unique card number that is transmitted to the host upon activation of the card. Smart cards do not have their own power supply but are supplied with energy by the card terminal. When receiving power, the smart card responds with a so called 'answer to reset' (ATR) message [RE00]. This message contains various information concerning communication protocols and card type and is standardized by the ISO/IEC 8716-3 standard [ISO97]. The ATR message includes a field of 16 bytes called 'historical bytes' that may be used by the card issuer to carry a unique identification number. Along with the ATR message, an ATR file may be transmitted. Table 6.2 shows the content of the ATR message.

In anonymous service delivery, the ATR message is problematic as either the 16 historical bytes in the ATR message or the ATR file may contain a card identification number. Such a number would render all transactions by the

Data Element	Length in Bytes	Content
TS	1	Initial character
T0	1	Format character
TA1, TB1, ...	14	Interface characters
T1..T16	16	Historical characters
TCK	1	Checksum

Table 6.2: Structure of the 'Answer To Reset' (ATR) message

card linkable. In order to use a citizen card as a carrier for digital credentials, neither the ATR message nor the associated ATR file must contain a unique card number.

A concept for a citizen card that is intended to support anonymous transactions must avoid both publicly readable data sets and card numbers in the ATR message or the ATR file. If a unique card numbers is needed in a citizen card scheme, it must not be publicly accessible but only be disclosed after the card owner's consent. From the perspective of privacy protection, any personal data on the card should only be disclosed after informing the card owner and obtaining consent.

6.3 Client Side Components

An important part of e-government initiatives is to deliver services electronically so that citizens can access services independent of time and place. For that purpose, citizens need to have a personal computer at home, a smart card reader and some further software that serves to make the citizen card functionality available to applications. In this section, we present the concept for an adapter layer, describe the functionality of the on-card identity manager and describe identity management functionality.

6.3.1 Adapter Layer

There are two options when choosing a front end with which the citizen can access e-services: the first option is to deploy a proprietary stand-alone application written in Java or any other programming language. Citizens would have to install this front end at home. The second option is to make use of a standard Web browser, which can be expected to be already installed on most personal computers. There is a clear trend towards Web-based service delivery and it can be expected that virtually all governments will opt for Web

browsers as front ends for their e-government applications. Consequently, all card functionality, such as issuing a digital signature or showing a credential, should be accessible from Web browsers.This leads to an architecture as depicted in Figure 6.4.

A concept for the use of smart cards as manager of the digital identity must address some limitations of smart cards and of Web-browsers as a front end:

- Limitations of smart cards with regard to user interface and network connectivity: Smart cards do not have a user interface and cannot connect to a network. They rely on the host computer to handle interaction with the user and to handle communications over a network
- Standard Web browsers do not provide adequate functionality for the use of citizen cards. Web browsers only support the PKCS #11 standard for accessing smart card functionality. This standard is very narrow in focus as it only addresses the use of X.509 certificates (i.e. authentication, signature and attribute certificates).
- Web browsers do not provide application logic or user interface components to handle anonymous and pseudonymous credentials. Although all protocol steps related to credentials (such as showing a credential) are performed on the smart card, the browser must handle credential-related messages from servers and call the respective functions that are provided by the smart card.

In order to achieve a flexible architecture that allows for an integration of Web browsers and stand-alone Java applications with the smart card, our architecture comprises an adapter layer. This adapter layer is situated between the smart card and the front end, which can be a Web browser respectively a Java client. All credential-related messages are processed in this layer. The browser is only used to display dialogues and application content to the user. As the adapter layer handles all communications with servers, it effectively acts as a proxy for the Web browser.

A similar approach is taken by the Bürgerkarte project in Austria, where an adapter layer (the so-called security capsule) acts as an adapter between browser and smart card. However, the security capsule does not act as a proxy for the browser. The security capsule offers services to the Web browser (for authentication and digital signatures) and does not communicate with service providers. The functionality of the card is exposed by the capsule via an HTTP-based interface.

The proposed adapter layer serves four purposes:

- **Integration of smart card functionality:** the adapter layer makes the services of the smart card available in Web-based applications. It provides a high-level interface to the card's functionality. The adapter layer also provides connectivity to the secure off-card storage.

- **Proxy for Web browser:** the adapter layer acts as a proxy for the Web browser. The adapter layer makes enables the use of credentials in conjunction with a Web-based service delivery. Protocols related to credentials are implemented as Web services.

- **Handling of presentation logic:** as Web browsers cannot handle credentials, the adapter layer generates user dialogues related to credential protocols.

- **Interface to anonymous communication infrastructure:** a prerequisite for the anonymous use of service over the Internet is an anonymous communication channel. The adapter layer routes communications related to anonymous services through a mix network. The layer serves as interface to the mix cascade.

This layer can also facilitate an extensibility with regard to new smart cards: by adding further smart card adapters, proprietary APDU-level interfaces can be mapped to the same high-level interface. Thereby, the integration of different types of citizen cards becomes possible without changing client applications.

The adapter layer has an interface to the middleware and exchanges protocol messages related to credentials with remote servers. However, credential protocol messages themselves are not processed in the adapter layer. The layer only relays these messages between remote server and the smart card. All cryptographic protocol steps are performed on the smart card, where the credentials are stored. Thereby, it is warranted that secret keys never leave the smart card. The components of the adapter layer are discussed in the chapter that describes the system architecture.

6.3.1.1 Security Considerations

The adapter layer must be considered a security-critical component in the proposed architecture. This is the case as smart cards do not provide facilities for user input and output. The layer must thus be trusted to display all dialogues as expected and transferring user input to the smart card without manipulating it. Examples for dialogues include:

- displaying a document to the citizen before signing it (the layer must be trusted to display the right information)
- obtaining consent from the user to use an element of the digital identity, e.g. show a credential (the layer must be trusted to transfer the yes/no decision truthfully to the card)
- inspection of the card content (e.g. display all credentials that the citizens owns)

A security-critical activity is also the inspection of the card content, e.g. anonymous credentials. The layer gains information about what credentials the user possesses and must be trusted not to leak this information to third parties. The necessity to put trust in software components that handle user interaction is a problem that is inherent to all smart card-based systems [SS99]. On a positive note, it has to be mentioned that even by manipulating the adapter layer, an attacker could not gain access to any secret keys stored on the citizen card. All cryptographic operations are executed on the card and secret keys never leave the tamper-proof card environment.

In order to improve security, the code of the adapter layer should be digitally signed by the issuer. This gives citizens a means to ensure that the application code has not been manipulated. Digitally signed code is only a guarantee for the code's authenticity provided the Java runtime environment has not been manipulated. Furthermore, ensuring authenticity of code at the application level does not protect citizens from attacks on the underlying operating system or computing infrastructure such as monitoring communication between application and card reader. Better security at the application level can only be attained once additional security features of the kind proposed by the Trusted Computing Group are implemented on personal computers. Without additional security features at the level of the operating system, the goal of trustworthy client components is difficult to reach. The Trusted Computing Group initiative was discussed in section 6.2.2.5.

6.3.2 Identity Manager on the Citizen Card

A key component of the proposed approach to digital identity is the identity manager. This manager is installed on the citizen card and manages all components of the citizen's digital identity. Managing these elements with a single applet offers two important benefits: firstly, a unified interface can be presented towards client applications that make use of the smart card. A well-designed interface facilitates application development. Secondly, an

integrated approach makes it feasible to provide identity information management functionality to the citizen. This feature lets citizens track the use of their digital identity. The functionality of identity management is not a part of any current digital citizen card concept. Identity information management is described in section 6.3.3.

The identity manager addresses the whole life-cycle of the elements making up the digital identity of the citizen. It offers all functions that are found on traditional citizen and identity cards, such as computing digital signatures, authentication of the card holder by authentication certificate or the decryption of messages sent to the citizen. Furthermore, it handles anonymous and pseudonymous credentials. Another important task of this component is to manage the memory of the citizen card. The identity manager thus provides four key functionalities:

- manage the life-cycle of identity elements
- identity information management
- manage card memory
- serve as a key to the secure off-card storage

Since smart cards do not offer facilities for user input and output, the credential manager is dependant of a host system for the communication with the user. As a basic security measure, users should give consent whenever an identity element is accessed in a transaction. The credential manager thus interacts with a client software on the host. The client software must be trustworthy. It must be trusted not to manipulate user input and output that is transferred from the host to the card.

With regard to management of anonymous and pseudonymous credentials, the identity manager supports

- establishing and storing pseudonyms
- obtaining and storing credentials
- showing credentials to relying parties
- proving possession of a pseudonym to relying parties
- displaying credentials and pseudonyms to the citizen

The manager thus keeps a list of all pseudonyms, credentials and associated secret keys. All credential protocol steps are executed in the card's protected environment. This is necessary, since almost all protocol steps of a credential system involve calculations with secret keys. These keys should not leave the card environment in order to prevent identity theft and maintain non-transferability of credentials. Furthermore, storing and retrieving pseudonyms and credentials should be automated as far as possible. Users should not have to assign names to credentials manually.

In terms of management functionality, the identity manager monitors the available memory space and moves data to the off-card storage when necessary. The memory capacity of a smart card is relatively limited. An off-card storage facility which is accessible over the Internet is used to augment this capacity. The credential manager is responsible for monitoring the amount of memory that is still available on the card and to move information to the off-card storage once the available memory drops below a certain threshold. For instance, all identity elements that have expired can be encrypted and moved to the storage. Likewise, large documents can be kept in the off-card storage to save space on the card. In order to move content off the card, the identity manager again depends on the host computer. The host must query the card at regular intervals whether data should be transferred off the card. This could e.g. happen after every write operation to the card. In case of a transfer, the host must accept content from the card and send it to the storage over a network connection. A concept for a network-based card extension is described in section 6.6.1.

The identity manager that is outlined above would form the core of a digital citizen card. Alternatively, it could be envisioned to use an identity manager as an additional applet on existing digital citizen cards. Such an add-on applet would enable the handling of anonymous credentials on existing citizen cards. In such a scenario, the identity manager would be installed as an additional applet on the card and only manage anonymous credentials. Other elements of the digital identity would still have to be managed by the core applet of the existing citizen card. However, such a setting could only work if the citizen card itself does not leave identifiable traces. The card must not disclose a unique card number upon insertion into a terminal or have a publicly readable data set. If the card leaves identifying traces, anonymity cannot be achieved. As most planned citizen cards leave such traces, there will be only few occasions where a credential manager may be used as an add-on applet. Furthermore, identity management functionality could not be provided, since the credential manager as additional applet would only manage anonymous credentials.

6.3.3 Identity Information Management Functionality

Next to handling all parts of the digital identity, the identity manager provides identity information management functionality. The identity manager keeps a log file on the card that documents every use of the digital identity. Whenever a certificate, digital document or anonymous credential is shown to a service provider, the manager records this event. Based on this information, citizens can reconstruct what identity element they have used in a transaction. They can also establish what personal data they have disclosed to a given service provider in card-based transactions.

For every transaction involving an identity element, the card records the time, the IP number of the service provider, the identity element that was accessed and the operation performed with the element. Table 6.3 shows the information that is written to the log file each time an element of the digital identity is used. A log entry comprises the name of the service provider's IP number, the time of the transaction, the identity element that was used (e.g. a credential) and the operation performed with the element (e.g. "show"). So as to keep records as compact as possible, every identity element is assigned a unique identification number by which it is referred to. The identity manager assigns these numbers in consecutive order when a new element (e.g. a credential) is stored on the card. Once the log file reaches a certain size, parts of the file can be transferred to the off-card storage (secure card extension).

Data Item	**Description**
Date and Time	Date and time at which the element was shown
Identity Element	Identifier of identity element
Location	IP number of the service provider
Operation	Operation that was made with the identity element (e.g. sign, show etc.)

Table 6.3: Information that is logged by the identity manager upon use of an element of the digital identity.

The information concerning the use of identifying and anonymous elements is helpful to the citizen in order to perform an analysis concerning the use of the digital identity. This may be helpful to identify service providers that notoriously collect high amounts of personal data. Next to the goal of informing citizens, this feature also pertains to security: since the card tracks any access to the identity information stored on the card, misuse of the card can be easily detected by citizens. If a dishonest terminal software tries to access identity elements after the card has been unlocked, then such

behaviour can be detected inspecting the log file. This mechanism is thus apt to discourage misbehaviour on the part of service providers.

Identity information management functionality is an innovative feature proposed as part of the concept for an extended digital identity. It is not part of any current electronic identity card initiative. Implementation of this feature necessitates slight changes to card protocols as opposed to traditional citizen cards. On the part of the host computer, the host has the responsibility of informing the card about time and location of the terminal (respectively of the service provider's IP address in remote settings). A trust assumption must be made that this information is supplied truthfully by service providers. On the part of the citizen card, every operation involving an identity element is augmented by an update operation of the identity information log file that is kept on the card. Since the records that are written to the log are relatively small, the overhead in terms of time is negligible. Figure 6.5 illustrates the signing of a document with the added step of updating the card's log file. As the log file can be periodically transferred off the card, space is not a concern either.

The process of issuing an electronic signature is augmented by a step to update the identity information management log file

This approach to identity information management could be extended by another measure: In situations where digital documents are signed, the card could automatically send a copy of the signed document to the off-line storage facility. Such a feature would ensure that citizens can always reconstruct what information they have signed. This feature would add some overhead to the signature process but would make sense considering the fact that a digital signature is legally binding. Being able to reconstruct what one has signed can be of high importance, especially in legal disputes.

6.4 Credential Issuer Infrastructure

Individuals establish pseudonyms with an organisation and can then obtain credentials from that organisation. Any private or public sector organisation may act as issuer of credentials. A credential issuer certifies statements about a subject. Typically, these statements are directly related to the business activities of an organisation. As an example, the population register may act as issuer of an anonymous credential that certifies the age of a citizen. Such a credential would be non-revocable in nature, as it certifies a statement that does not change over time.

In order to act as a credential issuer, an organisation needs to add infrastructure components to its current information systems. These components

are needed to issue credentials and make information available that is relevant for both users and relying parties. Figure 6.6 depicts the infrastructure that is operated by a credential issuer. A credential issuer operates the following components:

- **Registration manager and credential certification:** this entity handles the registration process and issues pseudonyms and credentials
- **Anonymity revocation manager:** an entity that can examine a transaction record and discover a subject's identity from that record. An issuer may have its own revocation manager. Usually, the anonymity revocation manager is organisationally separated from the issuer's organisation.
- **Credential information base (CIB):** publishes relevant information for relying parties and individuals. The following information is published:
  - **Credential policy and practice statement:** these documents describe the semantics of the credentials and the practices adhered to in the issuing process.
  - **Credential revocation list (CRL):** in case of revocable credentials, a list is published that contains all credentials that were revoked by the issuer.
  - **Issuer public key:** the credential issuer publishes its public key. This key is necessary for relying parties so that they can determine the authenticity of credentials.
  - **Credential descriptions:** this document contains a description of the credentials that are issued by an organisation. The description comprises a label for the credential in natural language, a credential type number (which is an identification number) and furthermore information about the credential format.

These components are described in the following sections. Some of these components must provide a high level of security (registration and credential issuance) or be highly available (credential revocation list).

6.4.1 Registration Manager and Credential Certification

This entity handles the registration of citizens and issues credentials. Citizens who would like to obtain a credential contact this entity over the network.

A citizen who first contacts this entity must establish a pseudonym with the organisation. Depending on the nature of the credential, citizens must be identified when issuing the credential. During the registration process, the issuer ensures that the citizen meets all conditions in order to issue a particular credential.

We expect that for e-government applications, most credentials require an identification of the citizen before issuing them. The social benefit scenario described in section 6.1.5 would require an identification of the citizen, as the issuing organisation has to contact further organisations (e.g. the Internal Revenue Service that is in charge of income taxes) in order to determine the eligibility for benefits.

The issuing organisation keeps a database concerning pseudonyms and credentials. The database details all pseudonyms that were established. For every pseudonym, a list is maintained of the credentials that were issued to this pseudonym. For every pseudonym and credential, the transcript of the issuing protocol is kept. This is necessary to allow for anonymity revocation in case of fraud. If credentials are revocable, the issuer also keeps a list that details the revoked credentials. This list is published at regular intervals.

An organisation may issue several types of credentials. Information concerning the credentials, polices and the format of the credentials should be published in the credential information base (CIB). The CIB also contains information that is directed at the end user, such as information concerning services that can accessed with the credential.

The registration and credential certification entity basically serves the same purpose as a certification authority (including the registration manager) in a traditional public key infrastructure. A high level of security must be achieved for information system components that handle the issuance process and keep data about issued credentials. These components are critical for the overall security and trustworthiness of a credential system.

6.4.2 Credential Information Base

The credential information base (CIB) is a publication point for information related to the issuing, handling and revocation of credentials. It contains information directed at end-users and relying parties. For citizens, the CIB offers a guide that is written in a non-technical style that provides an introduction to credentials. It also details the semantics of the credentials issued by that organisation.

The CIB makes the following information available:

- **Pseudonymous credential policy (PCP):** describes credentials, formats and revocation list formats.

- **Pseudonymous credential practice statement (PCPS):** describes the practices that are followed when issuing credentials.

- **Credential revocation list (CRL)**: a list of invalidated credentials. This list is an optional component and is only published if credentials are indeed revocable.

- **Public key and credential formats**: the organisation's public key is provided in XML format. Also, a list of credential types is provided as an XML document.

- **Credential holder's guide**: a guide aimed at citizens that introduces credentials. The semantics of the organisation's credentials are also described.

6.4.3 Credential Revocation List

Publishing a credential revocation list (CRL) is only necessary if the credentials issued by the organisation are indeed revocable. A CRL is a list of credentials that are revoked, i.e. invalidated before their scheduled date of expiry. Such a list is published by the credential issuer in a publicly accessible directory and is updated at regular intervals. Relying parties download this list recurrently, as they depend on the list to determine the validity of credentials. The directory in which the list is published is thus a security-critical component and needs to be highly reliable.

However, one can argue that the revocation of anonymous credentials is still somewhat problematic. Approaches to revocation are discussed in section 6.7.3. As technology for revoking credentials is not very advanced yet, a deployment of revocable credentials should be avoided where possible until better algorithms for revocation are available. In systems where credential revocation is implemented, the directory that contains the CRL must be a highly-secured and highly-available component. CRLs must be updated at regular intervals, published in a well-known location and they must be digitally signed by the issuer. The directory service that publishes the list must be highly reliable. If the service fails, validity of credentials cannot be determined reliably anymore.

6.4.4 Credential Policy Documents

Credentials are essentially signed statements about an individual. Service providers rely on these statements in order to make access control decisions. Therefore, service providers must have a clear understanding of what attributes a credential conveys Also, service providers must decide what credential issuers they trust. Credential issuer publish two documents that describe the semantics of credentials and the practices that are observed in the issuing process. These documents help relying parties in the process of their decision making. The documents are the pseudonymous credential policy (PCP) and the pseudonymous credential practice statement (PCPS).

These documents are important for users and relying parties alike. Relying parties consult these documents in order to decide whether to trust a credential issuer (and thus accept this issuer's credentials) and how to interpret these credentials. Users may also consult these documents to inform themselves about semantic of credentials and the issuing process. Issues that (in the least) have to be addressed by policy statements are:

- the conditions that a subject has to meet in order to obtain a given credential
- the types of credentials that the organisation issues
- the attributes that the credentials certify
- whether the credentials are revocable
- the conditions that must be met in order to have a citizen's anonymity revoked
- the set of acceptable revocation managers

The two documents are:

- **Pseudonymous credential policy (PCP)**: this document describes what kind of credentials an issuer certifies and what attributes each credential contains. The CP also describes the format of a credential and the format of the credential revocation lists.
- **Pseudonymous credential practice statement (PCPS)**: this document describes the practices that a credential issuer adheres to in the issuing of credentials.

These documents are very similar to the certificate policy (CP) and the certificate practice statement (CPS) as published by certification authorities (CAs) who issue public key certificates. An important difference is however that these documents describe a technology that most users are not familiar with. Furthermore, they must address the issue of anonymity revocation. With regard to anonymity revocation, the documents should state the exact conditions under which anonymity can be revoked. The document must also detail what parties act as anonymity revocation managers.

6.4.5 Machine-readable Specification of Credentials and Public-Key Publication

In terms of technical information, the credential information base contains a machine-readable specification of the format of all credentials of that issuer. Such a description can be realised using XML (Extensible Markup Language). The credentials may contain numerical codes to represent textual information. Mapping tables that describe these mappings from numerical values to text should also be published in the CIB (Credential Information Base). Both format-descriptions and mapping-tables are security relevant as they pertain to the correct interpretation of credentials. Both kinds of information should thus be digitally signed. XML is a format that is well suited to be digitally signed [W3C02b]. This technical information is necessary as relying parties have to take access decisions based on credentials. The description of the structure of a credential should be in a format that allows the description to be integrated into an access policy language.

6.4.6 Credential Holder's Guide

Policy documents such as the pseudonymous credential policy statement (PCPS) are usually not read by the end-user. They contain a lot of technical jargon and are generally targeted at a professional audience that is already familiar with processes related to issuing of credentials. In order to provide meaningful information to citizens, a credential information base should therefore also complement policy documents by information that is intended for the end user. A CIB (Credential Information Base) must comprise documentation that describes the handling of credentials in a language that is accessible to the average computer user. Documents in the CIB must describe the semantics of the credentials and explain what statements the credential makes about its holder and what the credential can be used for. The CIB should also comprise a list of services in which this credential can be used.

The credential holder's guide describes the credentials that are issued by an organisation. It describes preconditions that must be met for obtaining the credentials. It also states under which conditions the anonymity of citizen may be revoked. The guide should also contain an introduction to credentials in general. Such an introductory text should promote the understanding of credential technology and thus contribute to the usability of such systems.

6.5 Components Operated by Service Providers

Introducing credentials as part of the citizen's digital identity has the goal to afford anonymous and pseudonymous transactions to users. The fact that services may be accessed anonymously with the help of credentials has an impact on the infrastructure of service providers. An implementation of credential-based service delivery makes it necessary to adapt access control components. In credential-based systems, the traditional approach to access control (namely to first identify and authenticate a user, followed by authorization of the user) cannot be followed in a credential-based scenario, as the traditional approach requires that users are known a priori and can be identified. This section will discuss the architecture on the side of service providers. The generic systems components for credential-based service access are discussed and their functionality will be examined.

In credential-based access control, users are not identified. Instead, attributes that describe the users are established with the help of credentials. Based on the established attributes, an access control decision is made. On a technological level, credential-based access is very similar to certificate-based access control, where attributes are established from public key and attribute certificates, see section 2.2.1. Both credential-based and certificate-based access control base authorisation decisions on attributes and are thus also described as attribute-based access control techniques [Sam02].

When introducing credential-based services, an organisation has to adapt the access control component of the system. Two changes are necessary: as a first modification, the access control component must be enabled to determine the validity of a credential. The component must thus be able two carry out the credential show protocol. Furthermore, the access control components must support the specification of credential-based access control policies (trust policies). A trust policy is a document that specifies which credentials a user must possess in order to access a credential.

Credential-based access control is very similar to certificate-based access

control. For organisations who already operate components for certificate-based access control, the transition is straightforward. The access control component must merely be enabled to support credential protocols and support the specification of credential policies.

We assume that a dedicated component is used to make access control decisions. This component may be separated from application-related servers and it is contacted by a server when an access control decision is to be made. A service access that involves credentials works as follows: when setting up an electronic service, the service provider specifies an access control policy in a policy file. The policy file contains rules that specify which credentials are needed to access a particular resource (e.g. a service). The trust policy is formulated in a trust policy language which is usually implemented on the basis of XML. The policy file is interpreted by a trust engine. Users show their credentials to this engine, which then decides whether to allow access or not. This decision is communicated to the application server, where the access control decision is enforced.

We assume that a dedicated access control component is used that comprises trust engine, a policy file and an engine to collect all certificates that are necessary to determine the validity of a credential. Figure 6.7 illustrates the architecture components.

The architecture comprises the following elements:

- **Server:** the user communicates with the server of the service provider. In the case of Web-based service delivery, this server is typically a Web server or a J2EE (Java 2 Platform, Enterprise Edition) application server. This server is typically interconnected with legacy systems and further back-end servers that contain application logic.

- **Legacy systems and further back-end servers:** typically, not all parts of a transaction are handled on one server or within one information system. Pre-existing legacy systems must be integrated. Many e-services require access to data that is kept in legacy systems or rely on legacy systems to perform part of a transaction.

The access control subsystem comprises the following components:

- **Trust policy**: the trust policy is a document that contains rules pertaining to access control. The policy states what credentials must be shown in order to gain access to a protected resource.

- **Trust policy engine**: the trust policy engine is usually part of an access control product. It interprets the trust policy and takes the

actual access control decisions. It is contacted by the application server when a user wishes to access a protected resource. The user is then informed what credentials are necessary in order to access the given service. The user then shows these credentials to the service provider. The engine decides whether to allow access or not and informs the application server about the decision. The trust policy engine must be able to evaluate credentials. It must be capable of executing all cryptographic protocols related to a given kind of credentials.

- **Certificate collector:** credentials are signed statements by an issuer. When verifying a credential, the issuer's public key and the validity of the public-key must be known. This usually entails checking a chain of certificates until the certificate of the root CA is reached. The certificate collector communicates with remote certification authorities and fetches all certificates that are necessary to judge the validity of a given credential.

An access control subsystem can be a subsystem of its own or it can be seamlessly integrated into a component-based software architecture. Today, certificate-based access control is already in widespread use. We thus expect that the migration towards credential-based access control does not cause any difficulties. From a technical perspective, the main difference in comparison to certificate-based access control is that credentials use different algorithms. With regard to policy languages, differences are small as well.

6.6 Other Infrastructure Components

This section describes further infrastructure components of the system. We describe a concept for an off-card storage for documents. We examine conceptual questions related to an anonymous communication infrastructure. The functionality of the revocation manager, which serves to trace individuals in case of misbehaviour, is also discussed.

6.6.1 Secure Card Extension to Extend the Storage Capacity of Smart Cards

In this section, we describe a concept for a secure storage facility that is accessible over the Internet and that augments the smart card's memory capacity. The concept for a secure card extension (SCE) described in this section was developed as part of the FASME project by the University of

Rostock [MCH+01]. We follow this concept and propose that next to the storage of electronic documents, also expired identity elements and identity information management log files should be stored in the secure card extension.

A typical smart card offers only around 64 KB of memory. This space is used for both applications and application data. It is to be expected that this capacity is not sufficient to hold the multitude of digital documents, credentials and other application data that a citizen accumulates over the life-time of a citizen card. An off-card storage facility that is accessible over the Internet can be used to safely augment the storage capacity of the card. All data that is moved to this storage is encrypted. The card acts as an access key to this storage. Information that is only used infrequently or that is kept for archival purposes may be moved to this storage facility. Such a storage service could be offered by private sector providers or by the government.

With regard to our concept of digital identity, the off-card storage facility can be used to hold the following data:

- **Digital documents:** administrative documents of the citizen that are not used anymore (or used infrequently) can be moved to the storage. Furthermore, some documents may be simply too large to fit onto the citizen card. The off-card storage is then used to store such documents.
- **Identity elements that have expired:** pseudonymous credentials and attribute certificates have a limited life-time. After expiry, they can be moved to the storage and be archived outside the card environment.
- **Log files of identity element usage:** the card tracks every use of a digital identity element. The log file that records this data must be periodically moved off the card to free resources. If the log grows beyond a pre-defined threshold, entries are archived in the secure storage and the log file is cleared.

In order to realise such a concept, the card manages its own memory resources and decides when to move information to the off-card storage. Connectivity to the off-card storage is achieved by use of the middleware. In our concept, the adapter layer interfaces to the off-card storage. Every time new documents or identity elements are stored on the card, the card must have the chance to transfer content from the card. The adapter layer must thus support the card by accepting content and sending it to the secure storage. This leads to an architecture as depicted in Figure 6.8.

In order to safely keep documents outside the protected card environment, all documents are stored in encrypted form. A dedicated key pair is stored

on the card for this purpose. In case the citizen loses the card, a recovery of the card storage's content should nevertheless be possible. This can e.g. be achieved by providing a trusted entity with a copy of the key pair. An ever safer way to ensure the recoverability of content is to use secret splitting: the secret key is split into several part which are given to several parties that the citizen trusts (e.g. friends, family members etc.). An unauthorised access to card content is then only possible if all parties that own a part of the secret conspire with the provider of the storage service. The provider of the storage service alone cannot access documents as they are stored in an encrypted form.

The security features of the storage are:

- **Authentication of card holder:** citizens are authenticated with the authentication key pair when connecting to the storage.
- **Encrypted communication channel:** the connection between the client and the storage is secured by SSL (Secure Sockets Layer).
- **Encrypted storage of documents:** all documents are encrypted with an asymmetric key before they leave the card environment.
- **Receipt-fullness of storage service:** the storage service provider issues a receipt for each document that was saved in the storage (see below)

Citizens are issued a receipt every time they deliver information to the storage. Citizens can thus prove that they have stored a document in the off-card storage in case of dispute. As issuing one receipt per document would potentially lead to a large amount of receipts, all receipts are accumulated into a single compact value by use of a one-way accumulator [BdM94]. Accumulators combine a set of values into one short value so that there is proof that a given value was incorporated into the accumulator. This value has a length of 1024 bit and is updated after every storage or deletion operation. The implementation of this mechanism is described in [CMH02].

A prototypical implementation of such a storage was realised as part of the FASME project. The storage is called the secure card extension (SCE) and is based on a J2EE server and a standard Java Card. Details on the implementation of the concept can be found in [MCH+01] and [CMH01]. The off-card storage is completely transparent to the user: the card actively decides where to store information and moves content where appropriate. Citizens do not have to decide where documents are kept. However, users notice a higher latency when documents are fetched from off-card storage or stored there.

The need for a secure storage of administrative digital documents is also recognised by other projects. The Bürgerkarte project in Austria states in the specification that citizens should in the long run be provided with a network-based storage for their personal documents [PKK+02]. However, neither a specification nor a detailed concept has been presented yet. In the Netherlands it is currently being debated whether a digital safe deposit should be put at the disposal of each citizen [vB01]. This digital safe-deposit would contain a copy of the information stored in the registry of population. But

also medical or financial information could be stored safely in such a digital deposit. Furthermore, banking institutions as well are planning to design services which in future will provide the secure keeping of documents [Tro00].

As we are aiming at providing an anonymous form of digital identity, the next section discusses whether such a storage has to be realised anonymously.

6.6.1.1 Identified versus Anonymous Storage Space

An important conceptual regarding an off-card storage is the decision whether such a storage needs to be operated anonymously. An anonymous storage space would imply that the provider of the storage service does not know whom a storage space belongs to. We argue that it would be difficult to provide a fully anonymous storage service, as the storage must often be used in transactions where the citizen is identified. There would be the danger that citizens unintentionally behave in a way that destroys the anonymity. Also, economic reasons indicate an implementation where the provider knows whom a storage space belongs to.

The problems related to an anonymous card extension are best illustrated by an example that demonstrates that anonymity is easily compromised: let us assume that a citizen engages in an identified transaction, obtains a document and sends it to the anonymous storage. Let us further assume that the citizen is the only active user of the storage at that point in time. If the party that provides the e-service conspires with the storage service provider, they can uncover who the owner of this particular storage space is. We conclude that anonymity cannot be guaranteed by technology alone in this scenario but that it also depends on the behaviour of the user. Anonymity would depend on a sufficient number of concurrent users. However, this condition cannot be guaranteed. Promising an anonymous storage service that is used in both anonymous and identified transactions would thus provide a false sense of security to users. This problem arises as the storage service is used in both anonymous and identified transactions.

A further argument against an anonymous storage space can be provided when assuming an economic perspective. In order to minimise infrastructure cost, it is desirable to provide the storage in a non-anonymous way: in an anonymous setting, all accesses to the storage would have to be routed through the anonymous communication infrastructure. This would create additional traffic (and thus cost) which can otherwise be avoided.

We recommend that it should not be attempted to operate an off-card storage anonymously. Although the provider of the storage service can then link a storage space to an individual, privacy is nevertheless maintained to

a large degree: since all data is encrypted, the provider of the storage can hardly learn anything about a citizen by examining the content of the storage.

The only resulting limitation of a non-anonymous approach is that the storage should not be accessed in the course of anonymous transactions. The identity of the citizen may otherwise be uncovered if the storage provider conspires with the provider of the anonymous service. It may happen that a given citizen is the only individual accessing the storage at that point of time. While this is unlikely, the case cannot be excluded. The off-cards storage thus must not be accessed in the course of an anonymous transaction. As a precaution, documents obtained in an anonymous transaction should be stored on the card for some period before moving them to the card storage. This could be achieved e.g. by setting a flag that signals that the document is not to be moved while the transaction lasts.

6.6.2 Infrastructure for Anonymous Communications

Credentials are to afford anonymous transactions to citizens. However, as services are accessed over the Internet, anonymity can only be achieved if the underlying IP network allows for the creation of anonymous communication channels. Otherwise, messages can be traced back to a specific machine (e.g. to an IP address), thereby compromising anonymity. Anonymity at the application level requires anonymity at the level of communication networks. For the use of credentials in e-government, an infrastructure must be provided to citizens that allows them to communicate anonymously over the Internet with service providers. Such an infrastructure raises questions regarding the operation, the potential of misuse and infrastructure cost.

A first consideration concerns the choice of potential providers of such an infrastructure, i.e. whether the infrastructure should be operated by government or by the private sector. Selecting mixes for a cascade is a question of trust. We propose that both the government and private sector organisations should operate mix nodes. Even religious communities may be a potential operator of a mix. This way, citizens could be given the possibility to decide for themselves whom to trust. Citizens could select nodes in the mix cascade or simply use a configuration based on recommendations by consumer protection agencies or privacy activists. In order to justify trust in the infrastructure, operators of mixes should be audited at regular intervals. Such audits help citizens to make an informed choice rather than choosing providers based on mere trust.

Another concern of such an infrastructure is the potential for misuse: anonymity makes it more difficult to pursue offenders who use the Internet to access illegal content. An anonymous communication infrastructure that

can be used for accessing arbitrary sites with encrypted connections would empower users to exchange illegal content in total privacy.

Again, a balance needs to be found between privacy and security, respectively traceability. One solution would be to build traceability features into the infrastructures. This is undesirable, as we already have traceability at the application level. A better solution might be to offer an infrastructure that provides anonymous, encrypted connections but that lets users only access a restricted set of hosts. Service providers would then have to apply to government in order to have their sites included in the list of acceptable hosts. Although undesirable because this solution requires centralised administration, it may be the only way to enable the use of credentials without providing an infrastructure that makes life for criminals easier.

The second concern is cost: due to the use of asymmetric cryptography, such an infrastructure creates a considerable overhead. In order to support a high amount of users, a large number of mix nodes is necessary. As messages are routed through several nodes, the need for bandwidth grows as well. It is to be expected that setting up a mix network that can support large-scale operation as required for e-government would constitute a significant cost factor.

The proposed architecture for an extended digital identity makes integration of anonymous communication channels straightforward: in order to obtain anonymous communications, users route all connections through a cascade of mixes. The proposed adapter layer can serve as interface to the mix cascade. The front end respectively the browser then uses the adapter layer as proxy for Internet communications. All communications related to anonymous services must be routed through the mix cascade. The Web browser (front end) must be configured to use the adapter layer as proxy before engaging in service access. This can be done automatically when starting up the adapter layer. The use of the mix network is completely transparent to users. However, users will notice an increased latency for communications through the anonymous channels. The mix cascade can be pre-configured based on recommendations or, if desired, the composition of the cascade can be chosen by the citizen.

We conclude that technologies for anonymous Internet communications are available today. However, the legal status and permissible usage of such an infrastructure have to be clearly defined. Also, such an infrastructure can be expected to cause high cost, as the overhead caused by encryption greatly increases bandwidth requirements and creates a need for strong processing capacities of the mix nodes.

6.6.3 Anonymity Revocation Manager

We have argued that the possibility of tracing participants of anonymous transactions pertains to security and trust in anonymous systems. The need of a revocable form of anonymity was discussed in section 5.5.1. Consequently, an entity must be introduced that can discover a citizen's identity in case of unlawful behaviour. This entity is the anonymity revocation manager. With regard to such managers, we will discuss two issues: we consider what parties may be chosen to act as revocation managers and also who should be involved in the definition of conditions for anonymity revocation. Also, we consider whether this entity must be a highly available component if the system.

An anonymity manager alone cannot discover a subject's identity when presented with a transaction record: divulging a subjects identity requires cooperation between relying party, anonymity manager and credential issuer: a relying party presents a transaction record to the manager who then examines the record and outputs a value which the issuer can relate to an individual. The feature of revocable anonymity is achieved through the use of identity escrow (see section 2.1.6). A revocation manager can be part of the issuing organisation or an entity independent of the credential issuer.

With regard to the choice of revocation managers it is important to realise that users, issuers and service providers alike must trust such an entity. Both public sector and private sector companies can act as revocation managers. Also, religious organisations can act as revocation managers. Suitable private sector companies are e.g. trust centers that issues public key certificates. In the public sector, the judiciary is an entity that is usually trusted by large part of the population. In countries where citizens do not trust their government, private sector organisations and religious organisations are clearly preferable over an anonymity revocation agency operated by government. There is no limitation as to how many revocation managers exist in a country. It is thus possible to give the user the choice between several different managers. Citizens can then choose a revocation manager based on individual preferences. Choosing a revocation manager should thus not pose a problem, as several managers can be appointed.

A critical issue with regard to anonymity revocation is the definition of the conditions under which anonymity can be revoked. This problem has hardly been discussed yet in literature. While it has been stated that conditions must be communicated to a user before a credential is obtained, it was hardly examined what parties should participate in the definition of these conditions. We argue that not only the credential issuer but also relying parties must have a saying in the definition of revocation conditions.

We argue that relying parties (i.e. service providers) must participate in the formulation processes. After all, it is relying parties that suffer damage if a credential holder engages in fraudulent behaviour. All relying parties are stakeholders and thus should be involved in the formulation process of revocation policies.

The revocation manager is a security-critical component in a credential system: it must perform its duties as expected by users, service providers and credential issuers. However, the entity must not be highly available. Anonymity revocation is not a process that is performed on-line: when asked to examine a transaction record and revoke the anonymity of a user, the revocation manager should first carefully deliberate the circumstance and decide whether all conditions for revocation are met. In terms of security requirements, the entity must safely guard its key pair. However, even if a key pair is lost, the damage is limited. Even if the attacker has access to transaction records, the help of the credential issuer is needed to uncover a citizen's identity. Furthermore, only citizens who have chosen this particular manager are affected.

6.7 Conceptual Issues Related to Credential Systems

6.7.1 Concept for a Credential Namespace

Citizen cards in conjunction with pseudonymous credentials enable citizens to access services anonymously. With the help of credentials and the attributes encoded therein, citizens prove statements in a trustworthy way while remaining anonymous. From the attributes, service providers infer facts about the citizen and make access control decisions. This approach necessitates that a service provider specifies which credentials (respectively attributes that are encoded in the credentials) are to be demonstrated in the course of a transaction.

Credentials therefore have to be identifiable, i.e. they have to possess a unique name. We advocate an approach where only one attribute is encoded in a credential. If a credential has a unique name, then the attribute encoded therein is also uniquely identified. The requirement that credentials respectively attributes need a unique identifier leads to the problem of a credential namespace. The development of a namespace is a process that is inherently dependent on the requirements of the community by which the namespace is to be used.

In the context of information systems, the term namespace conventionally

refers to a set of names. A namespace thus must not contain duplicate names. However, such a narrow definition of a namespace would impair the use of credentials in e-government. Attributes may be used by issuers in the public and private sector. Several issuers who certify the same attribute do not necessarily assign the same semantics to it. This is especially the case when adopting an international perspective: differing administrative cultures make a cross-border use and interpretation of attributes difficult.

6.7.1.1 Desirable Characteristics for a Credential Namespace in e-Government

A credential is essentially a statement about a subject that is signed by the issuing party. The statement takes the form of one or more attributes that describe properties of the subject. Such an attribute consists of a label (the name of the attribute) and the attribute value. An attribute has a domain which describes the possible range of values that the attribute can adopt.

The challenge when designing a credential namespace is to come up with a concept that guarantees unique attribute names within the namespace but at the same time affords issuers the freedom to decide for themselves which attributes to certify. The namespace should be open rather than closed. This means that issuers should be free in their choice of attribute names without having to consult a central coordinating entity. It should be possible for an issuer to add new attributes at any time.

In an e-government setting, issuers from the private and public sector need to be accommodated. A concept for a credential namespace has to address a multitude of issuers and achieve uniquely identifiable attributes without restricting the issuers too much. Credentials may be issued by a governmental organisation (e.g. an attribute describing the right to drive a car) or by a private sector company such as a bank (e.g. an attribute certifying that an individual is credit worthy).

The desirable properties for a credential namespace can be summarized as follows:

- Openness: issuers may add new attributes at any time and choose attribute names freely
- Uniqueness: credentials are uniquely identifiable
- Decentralised operation: issuers operate without central coordinating entity

- Differentiation of credentials with regard to credential characteristics: one and the same attribute may be certified as a multi-show and one-show credential. The namespace must allow to differentiate between these two credentials

It can be expected that private sector companies will only certify statements that they can verify reliably. A bank may want to certify the creditworthiness of an individual but not want to certify whether a citizen has ever defaulted on debt. Statements will in most cases lie within the scope of the issuing organization. Notwithstanding, there may be exceptional cases where private sector issuers certify attributes that traditionally lie within the authority of government. The next section discusses the question whether public sector organizations need a reserved namespace of their own.

6.7.1.2 Open Namespace versus Namespace with Reserved Parts

Many statements about a citizen can only be reliably certified by the government. The set of attributes that is usually certified by the government varies from country to country. General examples for such attributes are the right to travel abroad (travel passport) or the right to build a house (building permission). Only the government issues paper documents certifying these statements. Counterfeiting them is a criminal offence and counterfeiters risk severe penalties. When implementing such statements as credentials, the question arises whether some parts of the potential namespace should be reserved for use by governmental bodies. Such an approach would define a set of attributes that may not be used by private sector organizations.

Arguments can be stated against such regulations: first and foremost, we can argue that a prohibition of attribute certification cannot be enforced by technical measures but only by statutory means. As a consequence, an authority would have to check at regular intervals whether issuers adhere to the regulations. Such checks can be conducted electronically in the proposed system by examining an issuer's credential information base. Nevertheless, such checks would nevertheless entail costs.

A much stronger argument against reserved parts of a namespace is the argument that such a regulation is not strictly necessary in an electronic scenario: issuers have no real motivation to certify attributes that lie within the authority of government. The only motivation to do so may be fraudulent behaviour. Such behaviour would probably remain without consequences, as service providers are free to choose which issuers to trust and which credentials to rely on. They typically make such a choice based on the policy statements of a given issuer. A service provider can be expected not to rely

on credentials by an issuer who certifies attributes that clearly lie outside the issuer's scope of business. The credential policy documents specify the exact conditions under which a credential is issued and also describe the semantics of a credential. Based on this information, service providers can make an informed choice concerning whom they trust. No sensible relying party would accept credentials by a private sector issuer that certifies statements from the governmental domain.

Instead of applying strong regulation, it may be more promising to work with recommendations: It may be envisioned that government publishes a list of attributes that are to be used by governmental bodies only. Such a list would urge relying parties to be cautionary about the acceptance of credentials by private sector organizations that make statements concerning the listed attributes.

We conclude that it does not make sense to regulate a namespace overly. Service providers may be expected to take trust decisions carefully and to have a working knowledge of the local administrative culture. It can further be assumed that most credential issuers have no motivation to certify attributes that lie outside the scope of their organization respectively that most relying parties would choose not to trust such credentials. Therefore there is no real need for creating a reserved namespace for governmental use.

6.7.1.3 Technical Implementation

The most natural solution for implementing a namespace that is open and features unique attribute names is to create subspaces within which issuers can act autonomously. Such an approach also satisfies the property that the concept works without central coordinating entity.

Subspaces for issuers are unique provided issuer names are unique. This property can be guaranteed as every issuer possesses a public key certificate and thus a unique name based on X.500 notation. Figure 6.9 illustrates the concept of a hierarchical, federated namespace for credential systems.

Within a local subspace, unique identifiers are required for credentials. This is accomplished by assigning a unique number (called credential type)to a credential. A credential is then identified by a pair consisting of issuer name and credential type. Identifying individual credentials from the same issuer by a type instead of by attribute name yields the benefit that a given attribute can be certified in different ways. The same attribute can be certified as one-show and as multi-show credential. A credential is thus uniquely identified across the system by a pair of descriptors, namely the issuer name and the attribute name. This is a very natural approach, as the attributes contained

in a credential are always interpreted as statements of an issuing party. Trust decisions are always taken with regard to the party of the issuer.

Such an approach leads to a federated namespace. Every issuer has its own local subspace. Within this space, the issuer may certify arbitrary attributes without having to mind restrictions regarding attribute names. Issuers are free to choose which attributes they want to certify. The global namespace is then made up by the sum of these local namespaces, thus forming a federated namespace.

The precondition that issuer names are unique is easily met in a credential system: as every issuer usually has a public key certificate. The certificate contains a unique subject name which is used as identifier for the local namespace. This name is specified by means of an X.500 name (see section 4.3.2). The X.500 standard specifies the elements that are used to specify a subject's name and defines a global name space with unique subject names. Apart from a standard for unique issuer names, there is no need to further standardise the credential namespace.

6.7.2 Concepts to Achieve the Non-Transferability of Credentials

A user may hold a multitude of credentials issued by different organisations. It often occurs that a credential certifies an attribute based on which the subjects obtain access to resources to which they would not obtain access without this credential. Also, a credential may lead to benefits that have a financial value. In practice, subjects may thus be inclined to lend or pass on credentials to friends. Similarly, they may try to buy credentials from other users in order to obtain credentials from which they expect certain benefits. Credentials are after all digital information and are thus easy to replicate, unless technical measures are taken to prevent this.

As access decisions and trust decisions are made on the basis of credentials, issuers have an interest to make the transfer of credentials impossible. In a system where the transfer of credentials is possible, relying parties are unable to trust the credentials they are presented with. Transferability of credentials would make a credential system useless. A credential that was issued to a given subject should be used exactly by that subject and not by anyone else. Several approaches can be found in literature that address the non-transferability of credentials. They fall into two categories: one class of algorithms tries to dissuade a subject from passing on credentials by associating them with a valuable secret. The other approach relies on a tamper-proof device to safeguard credentials.

6.7.2.1 Non-transferability by Association with a Secret Information

Credentials that should be non-transferable are associated with a secret information (that has to be provided by the subject). If the subject passes the credential on, the associated secret value is passed on together with the credential. The secret has to be valuable to the subject, such as a credit card number or a password for a bank account. In literature, two approaches of this kind can be found: PKI-assured non-transferability and circular encryption.

- The approach of **PKI-assured non-transferability** assumes that every user has some valuable secret value that will then be associated with non-transferable credentials. This may be the signature key of the subject or an information provided by the subject such as a credit card [GPR98].
- **Circular encryption** is a concept that works in absence of a valuable secret. Instead of associating a single secret value with every credential, all credentials that are to be made non-transferable are associated with each other. This leads to a situation where passing on a single credential is equivalent to passing on all credentials. The recipient of a single credential gains the power of using all credentials that were issued to the holder of the original credential [CL01].

This kind of approach to non-transferability builds on the assumption that users understand the technology they are dealing with. It is also necessary that users are aware of the consequences of passing credentials on. This approach is thus suited only for well-educated users that have a good understanding of technological issues and that act prudently at all times.

6.7.2.2 Non-transferability by Tamper-proof Device

Lending credentials or obtaining credentials from other users necessitates that a subject can access all data that is related to a credential (publicly accessible as well as secret information). If a credential manager is implemented in a tamper-proof environment, the subject can be denied access to secret information by technical measures. To achieve this objective, only one condition must be met: the secret information associated with a credential must never leave the tamper-proof environment. Generally, a user should not even have the option to access the secret information associated with a credential. Displaying the secret part of a credential to the user requires this

information to be moved outside the safe environment. This implies that also an attacker's software may gain access to that information. Consequently, identity theft would become possible. Therefore safe-guarding secret information from the citizen's access is imperative both to protect the citizen form identity theft and also to achieve non-transferability of credentials.

In a deployment of credentials in an e-government setting, only the approach of ensuring non-transferability by tamper-proof device should be chosen. Users should not be led into the temptation to lend their credentials to others. If users have the possibility to access the secret information associated with a credential, they may be tempted to pass a credential on, notwithstanding the consequences. Associating credentials with valuable information is thus a dangerous approach, given that users may possibly yield to temptation (they are humans after all, not machines). Especially citizens in an economic hardship situation may be tempted to trade credentials for a short-term financial gain and might ignore potential long-term consequences.

Associating the user's credentials with the signature key is an especially dangerous concept, as giving this secret away may have the most severe consequences for a user. The recipient would obtain the capability to issue legally binding signatures in the name of the original credential owner. A citizen-friendly solution should exclude such possibilities by design. Thus, neither circular encryption nor PKI-assured non-transferability are an approach that is viable for e-government solutions. Instead, this goal should be met by using a tamper-proof environment for the management of credentials.

6.7.3 Revocation of Anonymous Credentials

Revocation of a credential is the process of declaring a credential as invalid before the expiry of its original lifetime. In the most literal sense, to revoke a digital credential is to declare a signed statement as invalid. A revocation is necessary once a credential is regarded as unreliable. The issuer of a credential is responsible for revoking credentials that have become untrustworthy. A revocation of a credential must promptly be communicated to parties who rely on the statement made in a credential.

There are a number of reasons why a certificate or a credential could become untrustworthy prior to its expiration, both technical and non-technical ones. Technical reasons include the situation that the credential's secret key has been compromised (i.e. an unauthorized party has gained access to that key), that the issuer's signature key has been compromised or that the issuer has ceased operation. A credential may also need to be revoked for non-technical reasons. This is typically the case when a statement made about

the credential's subject no longer applies. Also, revocation may become necessary if is detected that a subject has obtained a credential fraudulently.

6.7.3.1 Why Revocation of Anonymous Credentials Poses A Challenge

The revocation of X.509 public key and attribute certificates was discussed in section 4.3.2.1. X.509 certificates can be revoked with the help of certificate revocation lists. Revocation of anonymous, unlinkable credentials is considerably more difficult than the revocation of signature or attribute certificates. The difficulties arise from the fact that users of anonymous credentials would like to stay anonymous towards the relying party. In order to achieve anonymity, such credentials must not include any identifying information. Several anonymous, unlinkable credentials issued to different users must be indistinguishable for a relying party. The approach taken for X.509 certificates, namely to include a certificate serial number that may be published in a list of revoked certificates, cannot be taken for anonymous credentials.

6.7.3.2 Methods for the Revocation of Anonymous Credentials

Three approaches to the revocation of anonymous, unlinkable credentials can be found in literature. The following section discusses these with regard to their suitability for a practical implementation in an e-government setting.

1. Approach by Bresson and Stern

Bresson and Stern propose a mechanism for the revocation of unlinkable, anonymous group signature certificates [BS01b]. The approach builds on revocation lists. The proposed method is quite general in nature and is also applicable to anonymous credentials.

Every anonymous credential must be associated with a secret number. In credential systems that feature anonymity revocation, such a number is already present. In other systems, this number must be added. When showing a credential, the number is encrypted and becomes part of the signature. Revocation works as follows: an issuer who would like to revoke a subject's credential simply publishes the corresponding secret number in a signed revocation list. Whenever a subject shows a credential, an additional step is added to the show protocol, namely demonstrating that the subject's credential was not revoked. This is achieved by proving in a zero-knowledge way that the encrypted secret number is not equal to any plain-text number

in the revocation list. Unfortunately, this requires a proof for every value in the list.

As a consequence, the complexity of this approach is linear in the number of revoked credentials. This has a direct impact on the total time that it takes to show a credential and also on the size of the record documenting the transaction: the time required to show a credential grows linearly with the number of credentials that are revoked. Also, the record documenting the show-protocol becomes longer and grows linearly with the number of revocations. Furthermore, the zero-knowledge proof adds a number of exponentiations to the protocol, which makes it unsuitable for the implementation on low-cost smart cards.

2. Approach by Camenisch and Lysyanskaya

Camenisch and Lysyanskaya propose the use of dynamic accumulators to facilitate the revocation of anonymous credentials and group signature certificates [CL02]. One-way accumulators were first introduced by Benaloh and de Mare [BdM94]. Accumulators combine a set of values into one short value so that there is proof that a given value was incorporated into the accumulator. A dynamic accumulator is similar to a one-way accumulator but has the additional property that values may not only be added but also removed from the accumulator.

In this approach, the issuer of a credential maintains an accumulator that contains a witness of all credentials that are not revoked. Every credential is associated with a secret number e and a number u that is used in the proof of validity. These two numbers are pre-calculated by the issuer for the expected number of credentials in the system. The issuer then communicates the resulting accumulator value to the relying parties.

Showing a credential now entails an additional step: next to engaging in the showing-protocol, a subject also needs to prove that its secret value is contained in the published accumulator by using the values e and u. This proof should not leak any information about the secret value e (i.e. it must be a zero-knowledge proof). If this proof fails, the relying party knows that the credential has been revoked. The proof adds a number of exponentiations to the protocols, which makes it problematic for the use on low-cost smart cards.

When a credential is to be revoked, the issuer removes the associated secret value from the accumulator and publishes the new value to relying parties. Unfortunately, all other credential subjects need to be contacted as well so that they can update their value u with respect to the new accumulator value. If a subject does not update, the proof of accumulation will fail and the subject's credentials from that issuer will be considered as revoked.

As a consequence, users have to check for revocation (resulting in a changed accumulator value) before using their credentials. This is less problematic for users who are frequently online. Nevertheless, checking frequently for updates can be considered to be cumbersome.

3. Approach by Canard and Girault

In a paper on group signatures, Canard and Girault propose a method for the revocation of anonymous, unlinkable group signature certificates that uses revocation lists [CG02]. The method proposed is generic and can be applied to anonymous credentials as well. The approach is specific to smart cards, as it relies on the existence of a tamper-resistant environment.

As in the previous two approaches, every credential must be associated with a secret number. When an issuer revokes a credential, the secret number is published in the signed revocation list. When a subject shows a credential, the revocation list is transferred to the smart card and the card checks whether the secret number of the credential to be shown is contained in the list. If so, the credential is not shown. If it is not revoked (i.e. the number is not contained in the revocation list) then the show protocol is carried out. The show-protocol itself is not changed. In this approach, some trust must be put into the smart card: a relying party is not offered a proof that the credential is not revoked but must trust the card to execute the check for revocation properly. Such an assumption is only possible since smart cards are tamper-resistant environments.

The advantages of this method are that the size of the transaction trail is independent of the number of revoked credentials and that it is smart card friendly in the sense that it does not require complex calculations. The drawback is that the time needed to check for revocation grows with the number of revoked credentials. In the first place, the whole list has to be transmitted to the card, which is rather slow due to the limited input and output speed of smart cards. In the second place, all entries in the revocation list have to be compared to the secret number of the credential. This second drawback may be somewhat lessened: the smart card may store a pointer that keeps track of which entries have already been compared. When a revocation list is transferred to the card, only new entries are examined.

6.7.3.3 Assessment of Revocation Methods

The three methods for revocation outlined above all come with their own benefits and drawbacks. When evaluating these approaches with regard to the use in a practical implementation, the following points are of high significance:

- **Run-time of revocation check:** the time needed to check for the revocation of a credential should be constant and as small as possible.
- **Size of transaction records:** showing credentials leaves a transaction record that is necessary for auditing purposes. Its size should be constant, i.e. independent of the number of revoked credentials
- **Mathematical complexity:** an algorithm should not comprise overly complex mathematical calculations since smart cards are highly resource-restricted environments.
- **Management overhead for users:** user-friendliness is a design goal of almost any end-user application. Users should not be actively involved in or bothered by the revocation process. A system should not force users to update their credentials after a change in the user base.

A comparison of the three methods with regard to those four evaluation criteria is given in Table 6.4.

	Bresson and Stern	**Camenisch and Lysyanskaya**	**Canard and Girault**
Size of Transaction Records	Grows linearly with the number of revocations	Constant	Constant
Run-time of Revocation Check	Grows with number of revocations	Constant	Grows with number of revocations
Mathematical Complexity	High	High	Low
Management Overhead for Users	None	High	None
Suitability for a Practical Implementation	Very low	Low	Medium

Table 6.4: A comparison of revocation methods for anonymous credentials

With regard to the above-mentioned criteria we conclude that the efficient revocation of anonymous credentials is still somewhat of an open problem for researchers. There is no solution yet that satisfies all requirements. The

approach suggested by Bresson and Stern is not practicable, as the size of transaction records and the time of a revocation check grows linearly with the number of revoked credentials. Although the solution proposed by Camenisch and Lysyanskaya is quite elegant, it puts a significant burden on the shoulder of the users. The possibility of frequent updates would force users to conduct daily revocation checks. Such an approach can only work if the credentials are managed by a device that is constantly connected to a network so that credentials may be updated at any time. This would cause considerable additional cost to the operation of a credential system.

The approach by Canard and Girault is highly suitable for the use with smart cards but essentially does not scale. As the time for a revocation check depends on the number of revoked credentials, it is only suitable for applications where the number of revocations is expected to be very low. Otherwise, checks for revocation quickly become very time consuming. Furthermore, service providers have to make additional trust assumptions with regard to tamper-resistance and software on the smart card. This is not a hindrance to this approach, but nevertheless undesirable.

We conclude that revocation mechanisms still need to be improved. Credential revocation should be avoided wherever possible. Issuing credentials with a short lifetime and re-certifying them at regular intervals can in many cases replace revocation. Revocation should only be used where high-value applications are concerned and considerable damage may arise from relying on credentials that have become invalid. In cases where revocation is necessary, the approach by Canard and Girault is the only currently practicable approach. Still, the shortest possible lifetimes should be chosen to minimise the need for revocation.

6.7.4 Towards An Improved Usability of Credential Systems

If credentials are to be introduced as part of the digital identity, the usability of a credential-based system must be a prime concern. Usability is the extent to which users can access the functionality of a system with effectiveness, efficiency, and satisfaction in order to achieve specific goals. Usability thus comprises four aspects [Nie93]:

- **Learnability:** the effort needed to learn the system's functionality and memorise it.

- **Effectiveness:** the degree to which a system fulfils its intended pur-

pose and enables users to perform specified tasks accurately and completely.

- **Efficiency:** the effort expended by the user to achieving accurate and complete task performance.
- **User satisfaction:** the comfort and acceptability of the system as perceived by its users and other people affected by its use.

Usability is an important aspect if credentials are to become a feature of digital citizen cards. Two further concerns can be mentioned that motivate usability as an important design goal for credential-based systems:

- **User acceptance:** privacy-enhancing technologies such as credentials only augment privacy if they are actually used by citizens. Average citizens should be able to use credential-based services, not only highly-educated or technophile users. Usability, more specifically user satisfaction, has a direct impact on the acceptance of a system.
- **Security:** at the same time, usability is a security concern, as users are a source of error: a complex interaction design increases the danger that users take wrong decisions and put themselves at a disadvantage.

In order to achieve usability, a good interaction design is of crucial importance. With regard to credential systems, usability is mainly created at the level of interaction design. A credential system only has three types of protocols in which the user is involved. These must thus be supported in a user-friendly way. The three protocols are establishing pseudonyms, obtaining credentials and showing credentials (which may entail the disclosure of a pseudonym). As an additional feature, the user needs an easy way to view pseudonyms and credentials.

Instead of attempting to give comprehensive guidelines for the user interface and interaction design of credential-based applications, we will state three principles that in the opinion of the author pertain to the usability of credential systems:

1. **Hiding complexity:**

   The exact details of a security mechanism can often be hidden from the user in order to reduce complexity. Generally, users do not want to be bothered with security aspects. As Bruce Schneier puts it: 'People want security - but they do not want to see it working' [Sch00]. Citizens are primarily interested in obtaining services, not in managing

credentials. As a consequence, much of the complexity of credential protocols should be hidden from users. Yet, hiding details does not mean that information is kept from the user. A user interface can be designed to present several levels of detail, e.g. one for the average user and one for advanced users. Every dialogue screen can be augmented with a button that allows the user to choose between detail levels.

2. **Automated management of credentials and pseudonyms:**

   The management of pseudonyms and credentials on the user's side should be fully automated. When establishing pseudonyms or obtaining credentials, these should be stored on the smart card without forcing users to choose a storage location or to assign names to credentials manually.

   With regard to pseudonyms, this property is easy to satisfy: as only one pseudonym per organisation is created, the pseudonym can be stored under the organisations name. Using the pseudonym itself as a name is impractical, as pseudonyms are merely big numbers. Users thus do not have to enter a name for a pseudonym.

   Credentials are stored together with the pseudonym under which they were established. The unique credential type can be used as identifier. When a citizen views the credential, a credential description as specified by the issuer is displayed, not the credential type. The description can be retrieved from the issuer's credential information base (see section 6.4). Citizens thus do not have to manually assign pseudonym or credential names during the issuing protocol. Credential management can be automated to a degree where users merely have to acknowledge that they want to obtain a credential or pseudonym.

3. **Minimising decisions that need to be taken as part of the show protocol:**

   To further heighten usability, care should be taken to minimise the number of decisions that users must take when showing a credential. Users may feel under pressure when showing a credential for many reasons: e.g. time pressure or perceived pressure from dealing with a technology that is new for them. Users should not have to take decisions under pressure, respectively the number of decisions should be kept to a minimum. After all, decisions related to the show protocol potentially affect the user's security. Thus, when accessing a credential-based service, citizens should only have to decide which credential respectively what set of credentials to show.

However, credential systems can be designed to let the user take further decisions during the show protocol. Such decisions include e.g. selecting a revocation manager from a list when showing the credential. Another decision that can be taken as part of the show protocol concerns the statement that is to be proven about an attribute encoded in the credential.

From the viewpoint of usability, it is undesirable to take such choices at the time of the show protocol. Strategies can be devised to take choices earlier in time:

- **Choices with regard to revocation managers**: such choices could be taken at the time when a credential is issued: a credential issuer can agree with service providers on a list of acceptable revocation managers. This list can then be presented to citizens when they obtain a credential from this issuer. The user simply chooses a manager from the list. This preference is stored on the card together with the credential and to ensure that the chosen revocation manager is always used.
- **Choices with regard to proofs about attributes**: another design choice that is relevant to both privacy protection and usability is the encoding of attribute values into credentials. At the design-time of a credential, an issuer must decide how to encode attribute values into credentials. This choice can be illustrated with a credential that certifies that an individual is more than eighteen years old. The first approach consists of encoding a statement into a credential that is common to all individuals that hold a given credential (e.g. 'age bigger than eighteen'). The alternative approach that can be taken is to directly encode a characteristic of an individual (e.g. the date of birth) into a credential.

  In the case of the first approach (an issuer encodes a statement that is common to all holders), citizens need to take less decisions when showing a credential. Citizens only have to decide whether to show the credential or not. As a further advantage, the same statement is divulged to all verifiers the credential is shown to. This makes it easier for citizens to know what data about themselves they have communicated to a relying party. As a drawback, this approach potentially leads to a larger number of credentials and a more frequent recertification of credentials.

  In the case of the second approach (an issuer encodes a characteristic of an individual), a citizen who shows a credential must

decide whether to show the credential and also what statement to prove about that attribute. Concerning the statement, a citizen can decide to prove a statement (e.g. age bigger than 25) or to divulge the attribute value altogether.

Although the first solution may lead to a higher level of privacy protection, it remains to be seen what the citizen's preferences are with regard to the trade-off between privacy and the overhead of administering credentials. We find the solution of encoding a statement common to all credential holders easier to use, as less decisions need to be taken when showing a credential. However, usability tests will have to be conducted with actual citizens in order to find out which solution citizens prefer. Citizens may very well choose to divulge more personal data and in turn reducing the overhead for administering credentials. The usability of credential systems is clearly an important issue for further research (see sections 6.7.4 and 9.2).

An interaction design that adheres to these three recommendations leads to a token metaphor for the use of credentials: using credentials becomes as easy as using a token. Today, citizens use many paper documents that can be interpreted as tokens, e.g. cinema tickets or membership cards. If the handling of pseudonyms and credentials is fully automated and no decisions need to be taken when showing a credential, the handling of credentials becomes as easy as the handling of e.g. a cinema ticket. If showing a credential is to be as easy as showing a token, then this fact needs to be reflected by the user interface: a user should only have to decide whether the credential is to be shown or not (a simple yes/no decision). Apart from that, the citizen should not have to take any decisions during the show protocol.

Of course, a user-friendly interaction design goes far beyond the points mentioned here. It comprises e.g. aspects such as designing button graphics in a way to clearly convey the function behind a button. Employing a user-centered design process would thus be necessary when designing a credential-based system for use in e-government. A user-centered design processes emphasises the user perspective throughout design, development, and test.

6.7.5 Implementing the Concept of Credentials in Smart Card Environments

We have argued that adding credentials to the citizen's digital identity is beneficial and that smart cards should be used as carrier of the digital iden-

tity. Although smart cards offer the benefit of a portable, tamper-proof computing environment, they only offer a small memory capacity, very limited processing power and low bandwidth for input and output operations. When planning to implement the concept of credentials in a smart card environment, a number of design choices must be made, owing to the characteristics of these cards.

Today, the majority of smart cards is equipped with an embedded 8-bit microprocessor. Smart cards typically feature between 8 and 64 KB of RAM and 8 KB of ROM in which the system software is stored. Due to the limited processing capacity of smart card environments, credential systems that make high demands regarding processing power cannot be deployed in such environments. However, we will show that the mathematical complexity of credential systems can often be reduced by shifting some trust to the smart card. Indeed, it will be shown that by making certain trust assumptions, complexity can be lowered to a degree that renders cryptographic co-processors unnecessary. The drawback of such an approach is that users and relying parties have to put more trust into one of the system components, namely the smart card.

In this section, we present two concepts how the concept of credentials can be realised on smart cards. We also discuss the modifications to smart cards that would be necessary to deploy the approach by Camenisch and Lysyanskaya in a smart card environment. The first approach uses citizen cards as universal attribute storage while the second builds on the concept of group signatures (see section 4.4). These two concepts take a very different approach from the chosen by Camenisch and Lysyanskaya. We will then assess all three approaches with regard to the suitability for a deployment on citizen cards.

6.7.5.1 Smart card as Trustworthy Attribute Storage

Credentials are signed statements about a subject. The simplest approach to implementing pseudonymous credentials on smart cards is to install an attribute manager on the card that stores attributes. A pseudonym is a name under which a subject is known to an organisation and can thus be treated as an attribute as well. When a credential is to be shown, the attribute manager answers questions regarding the attributes.

The attribute manager receives signed statements from issuers about attributes and pseudonyms. Such a statement consists of one or more attributes, the life-time of the attributes, an expiry date and the issuer's signature over that data. These statements must be signed so that citizens cannot

fake attributes. The smart card then stores these attributes along with the information about the issuing party and the expiry date.

Showing a credential to a relying party is very simple: showing a credential means that a relying party wants the subject to demonstrate some property. This demonstration could for example be the question whether the subject is more than eighteen years old. The relying party sends this question to the smart card along with a list of acceptable issuers of such a statement. If the smart card finds an attribute 'age' which is greater than eighteen, it replies with 'yes', otherwise with 'no'. The card answers all questions truthfully. If a credential is to be shown with regard to a pseudonym, the card also outputs the pseudonym under which the user is known to the organisation.

Since the smart card is tamper-proof, users can neither manipulate the stored attributes nor influence the functionality of the attribute manager. Such a solution allows a card-based implementation of a pseudonymous credential system that is suitable for deployment on any 8-bit smart card. However, it has the drawback that the security of the system entirely depends on a single component. The most important part of showing a credential, namely the verification of an attribute, is entirely performed on the card. Relying parties have no way of verifying whether a card works properly - they must trust the smart card to answer all requests truthfully.

6.7.5.2 Credentials based on Group Signature Certificates

According to Pfitzmann and Koehntopp, anonymity is defined as 'the state of being not identifiable within a set of subjects, the anonymity set' [PK01]. The anonymity set is the set of all subjects who might cause an action. Departing from this definition, we map the problem of anonymity to a group membership problem. An anonymous credential essentially certifies an attribute of a subject in an anonymous way. If we interpret all subjects that have a common attribute value as a subgroup of the population, we can set up a group membership scheme that lets a citizen prove membership (i.e. possession of the quality that is common to all group members) while remaining fully anonymous within the group [Aue03]. Such groups could be the set of all people who have a driver's licence, the set of all citizens on income support or the set of all people over eighteen.

By using the approach presented by Canard and Girault, group signature schemes can be easily implemented in smart card environments [CG02]. This approach allows to implement a simple form of anonymous credentials: after all, an anonymous credential that certifies the right to drive a car makes a statement that a person belongs to the group of people who have a driver's

license (as opposed to the group of people who do not). Of course, this approach merely provides away to prove an attribute and does not address the use of pseudonyms [Aue03].

Let us consider the example of social benefit recipients: the agency that administers the benefit would first set up a group. The group public key certificate states that members of the group are on income support. Eligible citizens are issued the group public key certificate and the corresponding private key. Showing the credential corresponds to showing the group public key certificate and signing a challenge to prove membership in the group (and thus eligibility). Citizens can now show this credential as many times as desired without incurring the danger that transactions can be linked. After all, group signatures provide full anonymity within the group. All members of the group possess the same group public key certificate and by definition, signatures of group members are indistinguishable.

A group signature credential consists of a group public key certificate common to all members, an associated secret key and a user specific secret (for purposes of identity escrow). The group public key certificate contains the issuer name, an attribute value, a date of expiry, the group public key and the signature of the issuer over that data. Figure 6.10 illustrates such a credential.

With regard to identity escrow, the approach by Canard and Girault trades complexity for trust assumptions. The identity escrow step (necessary to achieve revocable anonymity) does not rely on verifiable encryption but on trusting the smart card to encrypt a user-specific value into a signature. Relying parties must therefore trust the card to indeed perform this step. Since smart cards are tamper-proof, this assumption is reasonable. The security of the scheme thus depends on the tamper-resistance of smart cards.

In this approach, the smart card serves three purposes:

- it protects the citizen from identity theft by securely storing credentials
- it ensures that anonymity is revocable
- it ensures that credentials cannot be transferred

The system has some limitations with regard to functionality. These result from the fact that attribute value and expiry date are embedded in the group public key certificate. All users must share the same attribute value. Since the date of expiry is part of the certificate, all users also share the same date of expiry. It is impossible to assign different life-times of credentials to members of the group.

6.7.5.3 Considerations Regarding the Approach by Camenisch and Lysyanskaya

The third option is to deploy the approach by Camenisch and Lysyanskaya on digital citizen cards. This approach has the advantage that a high degree of multi-lateral security is achieved. A system is said to offer multi-lateral security if it is secure for all participating parties and not just for a single party [FP97]. When implementing this approach, only minimal trust must be placed into the card: all protocol steps are secured by zero-knowledge proofs which let a party verify that the protocol is indeed adhered to. Despite the use of proofs in all protocol steps, two reasons necessitate using a tamper-proof environment to store the citizen's digital identity: on the one hand, the card must ensure non-transferability of credentials. On the other hand, the card needs to protect the citizen from identity theft.

The benefits of using the approach by Camenisch and Lysyanskaya are thus a high degree of security as well as a comprehensive set of functionality with regard to pseudonymous credentials. However, the system makes use of zero-knowledge proofs: a card must thus be capable of calculating numerous exponentiations involving big integer numbers (e.g. 1024-bit numbers) when executing a credential protocol.

Mathematical operations involving big integer numbers on today's 8-bit Java Cards are hardly feasible: as part of this thesis, a BigInteger library for the Java Card platform was implemented that provided basic functionality such as multiplication, subtraction and addition of big integer numbers. The experiments showed that even a single multiplication of two 1024-bit numbers takes in the range of several seconds [Kir03b]. These findings are in line with published results by other researchers (see e.g. [EN01]). We thus expect that additional hardware support will be needed. In order to implement the approach by Camenisch and Lysyanskaya, two changes to current Java Card architectures will in our opinion be necessary:

- **Support for big integer numbers:** the current Java Card specification does not support mathematics with big integer numbers [Sun02b]. Today, even the support for 32-bit integers is optional. The specification would have to be extended to include a 'BigInteger' data type, as it is the case in the current Java 2 Standard Edition.

- **Enhancement of processing capabilities**: today's smart cards are equipped with cryptographic co-processors that only support some commonly used algorithms (e.g. RSA, DSA, DES or ECDSA). Hardware support for a wider range of mathematical functions is desirable in order to efficiently implement credential systems.

At the time of writing, no smart card manufacturer has announced plans yet for a general-purpose cryptographic co-processor that would allow developers to implement a wider range of algorithms on smart cards. However, we expect that credential technology might be a driver for the integration of such co-processors. If there is sufficient demand on the market for credential systems, manufacturers will be motivated to adapt their products. A similar situation existed with regard to elliptic curve cryptography: once a demand became apparent for digital signatures based on elliptic curves, manufacturers reacted quickly and built support for such algorithms into their cards. Today, elliptic curve cryptography is even a part of the Java Card standard. The Austrian citizen card is an example for a project that makes use of elliptic curve cryptography for digital signatures.

6.7.5.4 Conclusion

We have presented three approaches to implementing the concept of credentials on smart cards. The three approaches vary with regard to functionality and security assumptions. The first approach, which uses the card as secure attribute storage, can provide a pseudonymous credential system as intended by Chaum. However, this approach should not be chosen for actual implementations, as security fully depends on the tamper-resistance of the smart card.

In the approach based on group signature certificates, tamper-resistance is a prerequisite as well, as it guarantees that anonymity can be revoked in case of fraud and that credentials are non-transferable. Since smart cards are indeed tamper-resistant, this security assumption is reasonable [CG02]. The advantage of this approach is that it can be implemented even on low-cost smart cards. This approach would be adequate for realising many scenarios in e-government. For instance, the social security scenario that was described in section 6.1.5 could be implemented with this technology. Scenarios that do not require pseudonyms could be implemented today with group signature certificates. This would allow governments to conduct pilot projects with low-cost smart cards.

Nevertheless, it is advantageous to use the approach by Camenisch and Lysyanskaya: it provides a wide range of functionality and only requires tamper-resistance for the prevention of identity theft and to ensure non-transferability of credentials. As implementing this system on smart cards is merely a question of hardware support, we expect that any deployment of credentials on citizen cards for productive use will rely on the approach by Camenisch and Lysyanskaya.

We conclude that currently it is not possible yet to implement the ap-

proach by Camenisch and Lysyanskaya in a smart card environment. However, if governments were signalling a need for credentials as part of the citizen's digital identity, we expect that industry would react quickly to satisfy this need. We expect that hardware support for a wider range of cryptographic algorithms will become available on future generations of smart cards. At the current point of time, group signature credentials could provide a solution for many scenarios and enable governments to make first pilots with anonymous service access.

6.8 Summary

The concept for an extended digital identity comprises pseudonymous credentials as part of the citizen's digital identity. For reasons of trust and security, the citizen's credentials should be kept on a device that is under the user's control and not in a storage on the network. Currently, the smart card is the only device that offers an adequate level of security for the storage of the digital identity and high portability at the same time. Also, as smart cards are tamper-proof computing environments, they can be used to prevent citizens from lending or transferring credentials. Other approaches, such as PKI-based non-transferability or circular encryption, should not be used in e-government for reasons of security.

The citizen card acts as anonymous carrier of the digital identity. On the citizen card, an identity manager is installed that manages the life cycle of the elements of the digital identity, including pseudonymous credentials. The identity manager also provides identity information management functionality: every access to an identity element is recorded in a log file. The citizen can inspect this log file. This functionality pertains to security as it allows citizens to track all accesses to their citizen card. The card's functionality is exposed to applications through an adapter layer. This layer serves as an interface to the middleware, provides a high-level API for application developers and allows to use normal Web browsers as front ends. In order to overcome the storage space limitations of a citizen card, an off-card storage is used to store expired elements of the digital identity and any data that does not need to be kept on the card. In order to maintain anonymity, an anonymous communication network must be used to anonymise the traffic of credential-based services.

With regard to the use of credentials in e-government, the criterion of usability is highly important. We recommend that decisions that need to be made as part of the credential show protocol should be minimised. Also, complexity shall be hidden wherever possible. Reducing decisions leads to a

token metaphor where citizens merely have to take a 'yes/no' decision when showing a credential.

The pseudonymous credential system proposed by Camenisch and Lysyanskaya is suitable for practical implementations. However we recommend that some features should be omitted respectively changed. Only anonymity revocation should be used, not pseudonymity revocation. Furthermore, the handling of pseudonyms and credentials should be automated as far as possible in order to improve usability. Revocation of anonymous credentials is still somewhat of an unsolved problem. Current approaches are either unpractical or do not scale very well. Consequently, revocable credentials should be avoided where possible.

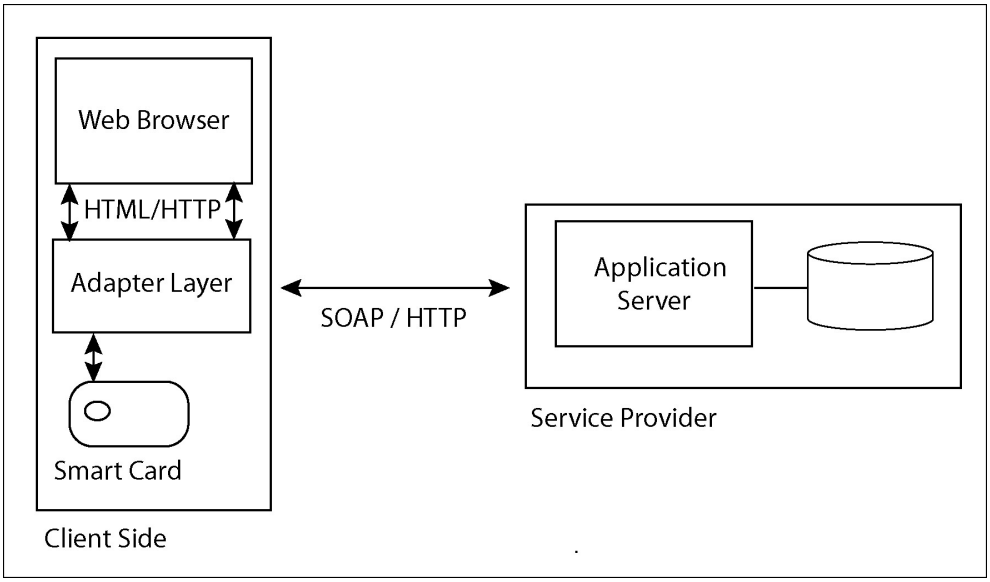

Figure 6.4: Client side architecture with an adapter layer between application and smart card

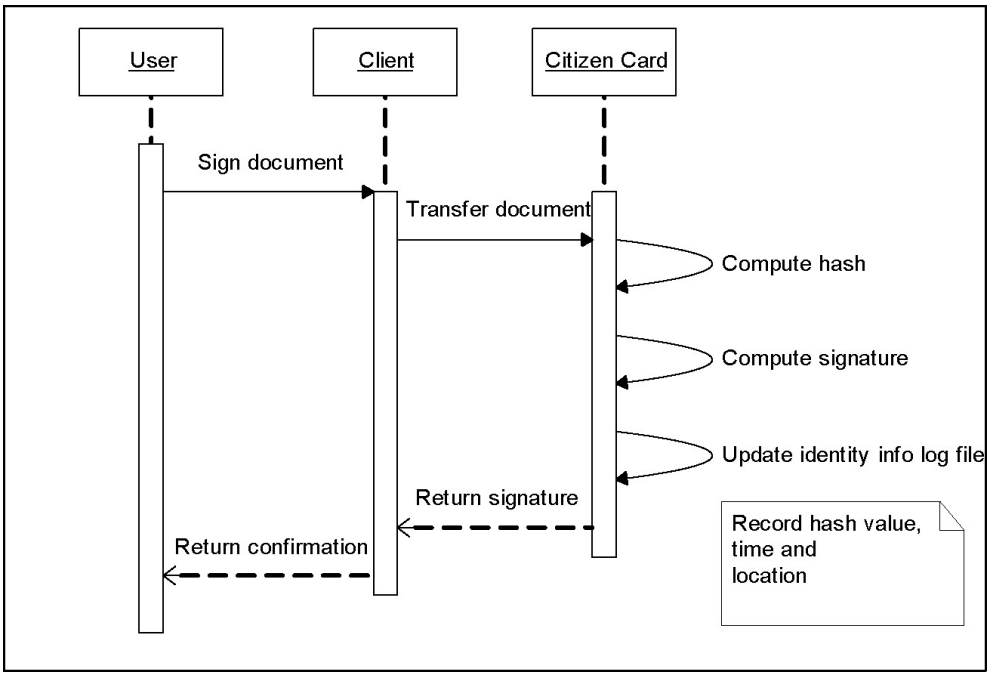

Figure 6.5: The process of issuing an electronic signature is augmented by a step to update the identity information management log file

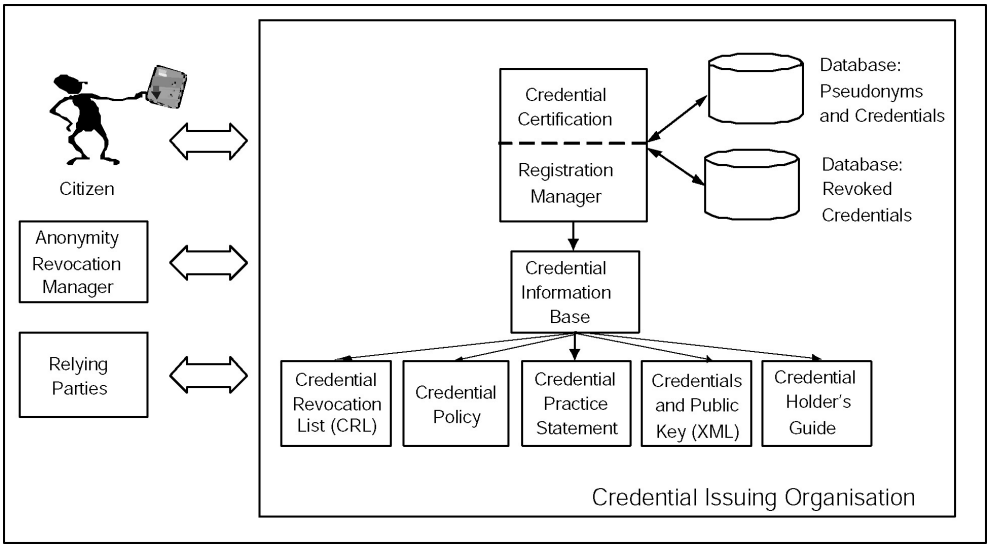

Figure 6.6: Infrastructure operated by a credential issuer

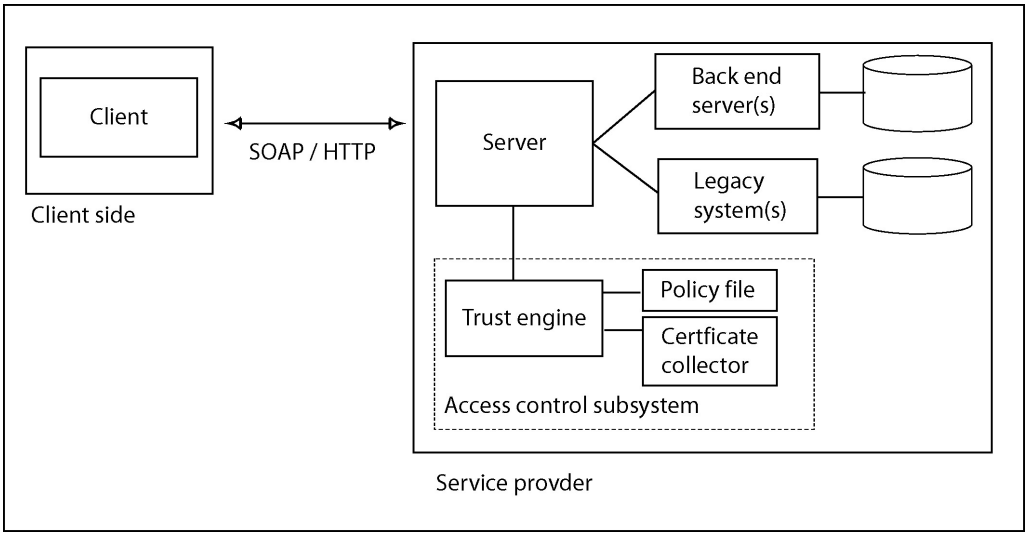

Figure 6.7: Architecture overview of components operated by service providers

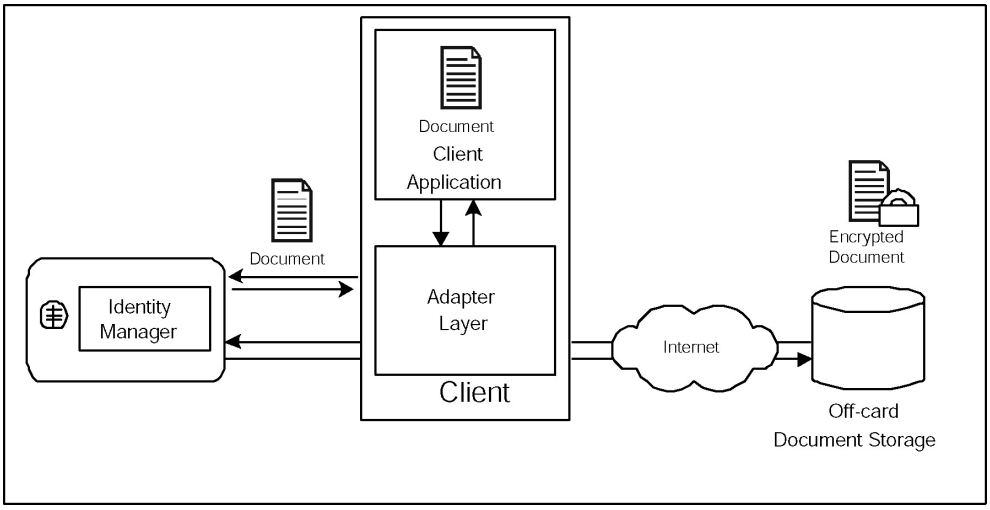

Figure 6.8: The secure off-card storage extends the smart card's storage capability (Source: [MCH+01])

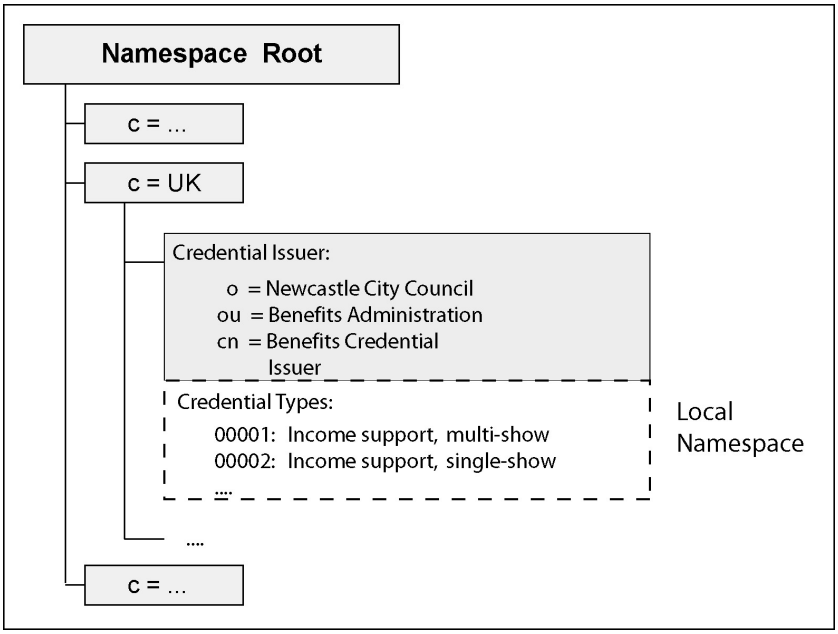

Figure 6.9: In a hierarchical, federated namespace, issuers can certify arbitrary attributes in local namespaces

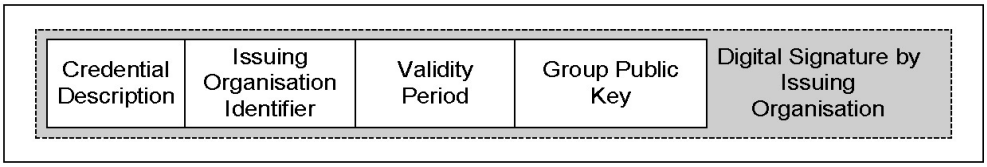

Figure 6.10: Public part of a credential based on a group signature certificate

Chapter 7

Architecture and Design

We describe the architecture and design of system components for the extended digital identity. The architecture aims at an integration of credentials into Web-based service delivery. Citizens use a standard Web browser to access credential-based services. The server side builds on the Java 2 platform, Enterprise Edition (J2EE). For the implementation of credential protocols, Web services are leveraged. We first give an overview of the architecture and explain the rationale behind key decisions. We motivate the use of the J2EE platform and of Web services. The architecture follows a four tier approach that comprises enterprise Java beans (EJB) to encapsulate application logic.

7.1 Architecture Outline

We have proposed a concept for an extended digital identity that comprises pseudonymous credentials. In this chapter, a further description of the architecture and design is presented. An architecture description usually comprises an explanation of significant design decisions, a description of the structure of the system, the components of the system and the interrelations between the components. An overview on the components of this architecture has already been given in section 6.1.3. We have also discussed the basic functionalities of the components. In this chapter, we describe how the proposed architecture can be implemented and provide further detail on the design.

The architecture design aims at a Web-based service delivery, i.e. services are represented as a series of HTML pages. Thus, service providers can keep existing infrastructure related to Web-based services such as design tools for HTML pages and Web servers. For an implementation of credential-related protocols, Web services are used. The following key decisions were made:

- **Enterprise Java beans (EJB) for server side components:** the J2EE platform defines a multitiered approach to server side application development. It also provides a standardised model for components, the so-called enterprise Java beans (EJB). The J2EE platform combines suitability for scalable information systems with the benefits of component-oriented application development. We will motivate the use of the J2EE platform in section 7.1.3.

- **HTML-based user interface:** Web browsers are used as a front end. Many citizens are already accustomed to the use of HTML-based user interfaces. A further advantage is that Web browsers are available for free and are already installed on most personal computers. Integration with the middleware and the smart card is achieved through the use of an adapter layer.

- **Light-weight client approach:** only a minimum of application logic related to presentation and component integration is kept at the client side. Business logic is kept on the server side in the EJB tier of the J2EE architecture. Only a small amount of functionality that is related to presentation, to the middleware and to the citizen card is located in the client tier (within the adapter layer). This approach leads to a relatively light-weight client.

- **Portal for service discovery:** services are discovered through a portal. The portal provides a single point of entry for all services. The portal only supplies pointers to services, thereby facilitating service discovery. Communication with service providers is not routed through the portal.

We will motivate the use of the J2EE platform for server side components and the use of Web services as a middleware in the next sections.

7.1.1 Motivation for an Architecture Based on Web Services

In the proposed architecture, Web services are used for the implementation of credential protocols. Web services can also be used for the communication between adapter layer and the off-card storage. The components that are interconnected by Web services are the front-end components used by the citizen to access services, the off-card storage, credential-issuing organisations and providers of credential-based services.

In our architecture, Web services are used for the communication between components of the client tier and service providers. We make a synchronous use of Web services. This decision was taken since Web services are used for interactions that mostly happen as part of a service access. For instance, when accessing a credential-based service, credentials are shown by use of a Web service. As the show protocol comprises three consecutive steps that must be performed in a synchronous manner, a synchronous use of Web services is a suitable choice.

In contrast, for the communication between governmental organisations, asynchronous communications can yield important benefits [RCMA01]. For instance when an authority needs to request a document from another authority (possibly in another country), an asynchronous use of Web services makes sense. A document request can then be dispatched even if the organisation that is to process the request is currently off-line. Asynchronous messaging can in such scenarios lessen availability requirements and also contribute to a higher overall scalability of the system.

An architecture based on Web services has advantages both from a technical and from a business perspective. From a technical perspective, we can mention the following advantages:

- **Support for loose coupling of components:** Web services can support an architecture that consists of loosely-coupled software components. Web services support both synchronous and asynchronous communication models.

- **High scalability:** Web Services are not connection-oriented. The HTTP protocol with its request/response-style communication is highly scalable.

- **Easier integration of heterogeneous systems:** as Web services are platform and language agnostic, they are well suited to integrate heterogeneous legacy systems that are running on different platforms or are written in different programming languages. A highly heterogeneous IT infrastructure is typical of e-government environments, especially in countries with a federated administration.

- **Flexibility:** services are published in a registry and can be dynamically discovered and invoked. It becomes easier to exchange one service provider for another or to change an interface to a given service without changing the whole system.

- **Use of standard technology:** Web services build on standard technology such as XML, SOAP, HTTP, FTP etc. This means that existing

infrastructure can be leveraged and that know-how already exists regarding the use of these technologies. As Web services are based on well-accepted standards, the danger of vendor lock-in is greatly reduced.

- **Service oriented architecture (SOA):** Web services enable a migration towards a service oriented architecture (SOA). In a service oriented architecture, functionality of components that needs to be accessible to other components is exposed as a service. Such architectures are expected to increase flexibility and make integration with legacy systems easier.

From a business perspective, Web services are an enticing choice as well. The use of standard technology means that existing infrastructure can be leveraged and that development staff may already be familiar with technologies such as XML or HTTP. These advantages are expected to have a positive impact on both development costs and total cost of ownership (TCO) [LK03].

Much more important however is the notion of a service oriented architecture (SOA). Government can expose some of their services as Web services. Such an approach makes it easier for business customers to access government services and even to integrate them seamlessly into their business processes. The fact that Web services are language and platform agnostic greatly reduces the effort needed for the integration of heterogeneous components. At the same time, government can access services provided by other administrative entities or private sector companies and use these services as building blocks for their applications.

Some authors expect that Web services have the potential to change value chains in public administration. Meir and Spahni describe the vision of a network state where governmental organisations form a network of cooperating entities that offer services to and consume services from participating organisations. Such a cooperation is based on services and service level agreements. Meir and Spahni expect that networks of cooperating entities will lead to innovative process designs and help to uncover new strategic potentials for public administration [MS03].

The author expects that Web services will be increasingly used for integration of distributed components, both in the private and the public sector. Within our architecture, Web services are well suited as they offer a lightweight approach to integration that is built on well-accepted standards. Web services can enable a loosely coupled architecture and are inherently highly scalable. From the perspective of deployment, Web services have the advantage that existing infrastructure can be used. There is no need to deploy

'heavy-weight' middleware such as CORBA. Consequently, there is no need to maintain additional components (e.g. a CORBA ORB) on the citizen's machine.

7.1.2 4-tier Architecture

The architecture in part follows the multitiered approach proposed by the J2EE specification. However, the client tier differs from a standard J2EE architecture. Normally, the J2EE client tier only comprises presentation logic and does not contain business logic or store data. In contrast, the client tier of our architecture also contains an integration layer and a smart card. The client tier thus comprises a small amount of application logic and data that would in a standard J2EE architecture be located in the business and EIS tiers. The data in the client tier is information that is related to the citizen's digital identity and is stored and managed in the tamper-proof card environment.

Normal Web browsers are used to access services. Next to using the HTTP protocol to fetch HTML pages from Web servers, the architecture leverages Web services in order to integrate credentials into a Web-based service delivery. All credential-related protocol steps between adapter layer and server are executed using SOAP (Simple Object Access Protocol) over HTTP. As in a standard 4-tier architecture, the Web tier services all client calls. Servlets in the Web tier communicate with EJB components in the business tier in order to provide services. Figure 7.1 depicts the 4-tier approach taken by our architecture.

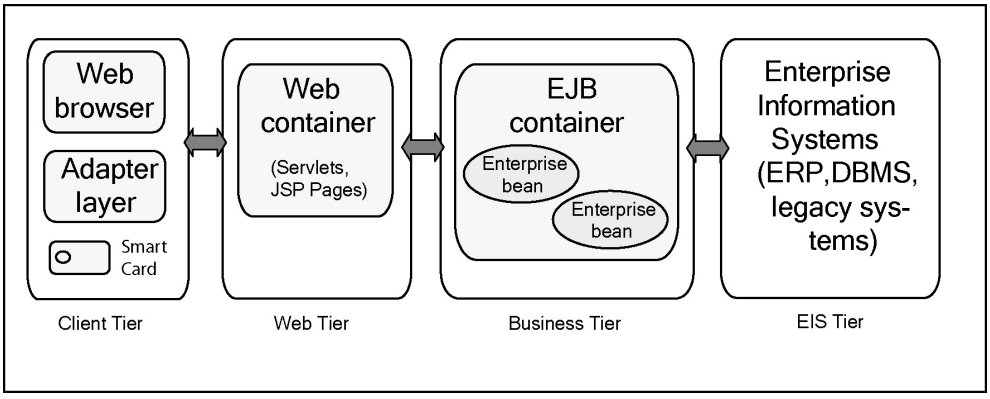

Figure 7.1: The J2EE platform takes a 4-tier approach to distributed computing

The architecture features four tiers with the following functionality:

- **Client tier:** In the proposed architecture, the client tier comprises three elements: the Web browser, the adapter layer and the citizen card. The Web browser is used as a front end. The adapter layer is an integrative element that makes the card's functionality available to applications and serves to connect the client with remote components. The citizen card stores and manages all elements of the citizen's digital identity.

- **Web tier:** the Web tier handles requests from clients for Web pages. This tier is responsible for generating the presentation logic for clients in the client tier. The Web tier comprises HTML pages, servlets and Java server pages (JSP). Servlets and Java server pages both run inside a Web container. The Web tier also comprises servlets that act as an end-point for Web services. The business logic behind the Web services is implemented by EJB beans. Clients invoke the servlet which then calls the EJB bean in the business tier.

  Components in this tier receive calls from clients, interact with components in the business tier to service these calls and return the answer to clients.

- **Business tier:** the business tier contains the core business logic of an application. The business logic is encapsulated in enterprise Java beans that run inside an EJB container. This layer is concerned with application logic only. With regard to credentials, we expect that commercial vendors will offer Java beans that handle all processes related to credentials. For a credential issuer, such beans address the functionality of establishing pseudonyms and of issuing credentials. For a service provider, these beans offer the functionality of checking credentials for validity.

- **Enterprise information systems (EIS) tier:** this tier comprises enterprise information systems: database systems, enterprise resource planning systems (ERP) and other types of legacy systems might need to be exposed to beans in the business tier. This layer is also needed to achieve persistence. Entity beans from the business tier access databases in the EIS tier in order to store application data. With regard to credentials, issuers need a database to store data about pseudonyms, credentials, credential public keys and transaction records.

7.1.3 Motivation for the Use of Enterprise Java Beans

The Java 2 Platform, Enterprise Edition (J2EE) provides developers with a platform-independent, component-based approach to the design, development, assembly and deployment of enterprise applications. The J2EE standard comprises a set of APIs and a standard for server side components, so called Enterprise Java Beans (EJB). J2EE builds on existing technologies from the Java 2 Platform, Standard Edition. The J2EE platform is a specification, which is then implemented by vendors in the form of J2EE-compliant products [Rom99].

Our architecture builds on J2EE technology and thus allows a component-oriented development approach on the server side. We cite a number of advantages that are obtained from using the J2EE platform. The first three advantages apply to component-based software development in general and are not specific to the J2EE platform [Rom99].

- **Decreased time to market:** software engineers can buy third-party components when developing applications. Companies thus write less code themselves, resulting in a decreased time to market.

- **Reduced development cost**: the overall cost of application development is normally reduced by the use of components, as less code needs to be developed, documented and tested.

- **Reduced need for in-house competence:** ready-made components can be bought for many parts of an application, thus reducing the need for programmers with specialised skills.

- **Open standard:** the J2EE platform is a standard. Products from many vendors are available. Thus, the danger of vendor lock-in is greatly reduced.

- **Platform independence:** J2EE application servers are available for many different platforms. J2EE applications are thus not bound to any single operating system and are easy to re-deploy on different platforms.

- **Wide range of APIs:** The J2EE platform includes a wide range of APIs addressing issues such as directory services, database connectivity, message-oriented middleware, legacy integration and other aspects of application development. These APIs further facilitate the development of applications.

- **Container services for enterprise Java beans:** enterprise beans run inside a container that offers many middleware services, including resource pooling, transaction management, security services and life-cycle management of beans. These services greatly facilitate the development of scalable server side applications.

The J2EE platform has rapidly gained popularity. Many implementations of J2EE servers are on the market and even open source implementations of such servers are available. This is a further motivation to build an architecture based on the J2EE platform, as open source products have received growing attention lately in the e-government community.

With regard to the support of credentials, we expect that software vendors will offer EJB components that handle protocols related to credentials. Issuers of credentials and organisations that offer credential-based services can thus buy such components instead of developing credential-related components themselves. Due to the fact that the J2EE specification defines a component model, pre-defined components become easier to integrate. The use of third-party components for the handling of credentials can thus accelerate the shift towards credential-based services.

7.1.4 Mapping to J2EE Roles

Java 2 Enterprise Edition applications are made up of components. In the J2EE framework, different roles are defined for the development of EJB components and the actual assembly and deployment of applications. In this section, we discuss what kind of roles must be assumed by an organisation that wants to act as a credential issuer or offer credential-based services.

The following roles can be distinguished with regard to the development and deployment of J2EE applications [Rom99]:

- **Container and server provider:** enterprise beans execute within an EJB container, which manages the execution of the beans. This container in turn runs on an J2EE application server. Although the role of container and server provider are often treated as two different roles, both server and container are in practice provided by the same vendor. This party typically also supplies tools that facilitate the deployment of beans to the application server.

- **Bean provider:** the bean provider develops enterprise beans. These beans encapsulate the business logic of an application. The bean developer may be a component vendor or an in-house entity.

- **Application assembler:** the application assembler develops applications by combining several J2EE components into an application. For that end, the application assembler may also write additional beans. This party is furthermore responsible for creating deployment descriptors and creating the enterprise archive (EAR) file, which is then deployed.

- **Deployer**: the deployer is responsible for adapting the application to the specific operational environment in which it will run. They adapt beans by manipulating property files and settings in the deployment descriptor. The deployer is also responsible for setting security parameters (such as permissions for the users) related to a given application.

- **System administrator:** the system administrator is responsible for the administration of an enterprise's computing infrastructure which also comprises administration of the J2EE application servers. Once the application is deployed, system administrators monitor it (with the help of monitoring tools supplied by server providers) and ensure the stability of the deployed application.

An organisation that wants to deploy credential-based services needs to assume three roles. J2EE servers (which also comprises the bean container) are available from commercial vendors. We expect that enterprise Java beans that handle credentials will be developed by software companies. Such beans can cover the issuing of credentials and authentication based on credentials.

Consequently, governmental entities can buy these components instead of developing them on their own. Thus, an administration needs personnel to fulfil the roles of application assembler, deployer and system administrator. They must assume the following tasks:

- **Application assembler**: the application assembler uses beans from software vendors that encapsulate credential-related protocols and integrate them with existing applications. Due to the use of beans, the application assembler does not have to change the code of beans related to the handling of credentials. These beans merely need to be integrated with the presentation tier and other EJB beans that encapsulate the application logic. The integration with existing systems (legacy systems) is also a responsibility of the application assembler.

- **Deployer:** after the application is assembled, a deployer further adapts the beans for deployment in the organisation's environment. A deployer

applies settings to customise the system with regard to the use of credentials. The deployer also makes the necessary security settings. For providers of credential-based services, settings must be made that describe which credentials are needed for a given service.

- **System administrator:** the system administrator ensure the stability of the solution once it has been deployed. We expect that most administrations have in-house IT departments that can assume the task of administering a J2EE application server.

7.1.5 Service Discovery Based on Portal

The architecture makes use of Web browsers as a front end. We presume that services are discovered by help of a service portal. Citizens use their Web browser to access the portal. Many countries have implemented service portals for e-government services that serve as a single point of entry for all services (see section 3.2). Our architecture is geared towards the use of a portal as well. Figure 7.2 illustrates the function of the portal as a point of entry.

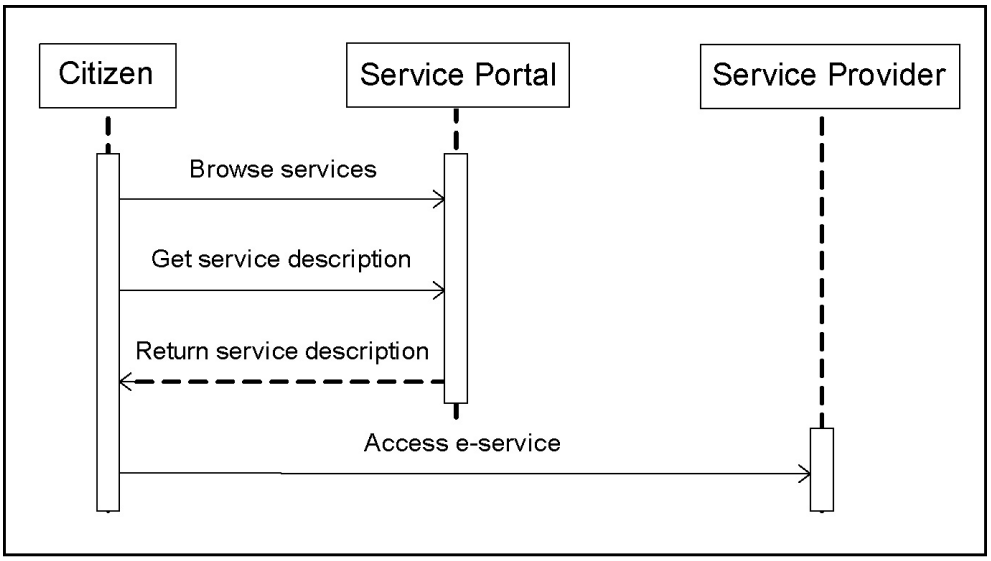

Figure 7.2: The central portal serves the purpose of service discovery

Citizens use the portal to discover services that are useful for them. A citizen who wants to find a service connects to the portal and browses the services that are presented on the portal. Once citizens have identified a useful service, they can retrieve a service description and follow the link to that service. Services themselves are not delivered through the portal.

The portal is merely used for service discovery and to retrieve a service description in XML format. The portal supplies a description of the service that comprises the location of the service in the form of a uniform resource locator (URL) and the information whether this service is delivered anonymously or not. This information is required by the adapter layer: all communication with providers of anonymous services must be routed through an anonymous channel in order to hide the citizen's IP address. With the help of the service descriptions it can be assured that only connections to anonymous services are routed through the mix network, thereby reducing the load on this infrastructure.

7.2 Client Components

The client tier of the architecture comprises three components: a Web browser as a front-end, the citizen card and an adapter layer. The layer serves as an integrative element and to extend the bowser's capabilities. It is responsible for the integration of the smart card and the interfacing with distributed system components such as the off-card storage. The adapter layer also interfaces to the infrastructure for anonymous communication. Another important function of the adapter layer is to support an authentication by pseudonymous credentials within Web-based services. The adapter layer handles all credential-related protocols for the Web browser and thereby enables the use of credentials in services that are accessed through an unmodified Web browser. Figure 7.3 illustrates the components of the adapter layer.

The adapter layer comprises the following components:

- **User interface logic:**

  The adapter layer contains a low amount of application logic related to the presentation of the user interface:

  - **Viewer for citizen card content:** citizens must be able to view the data that is stored on the citizen card. The adapter layer can retrieve identity elements from the card and display them to the user.
  - **Transformation of XML-encoded content:** service providers can send XML content back to the client together with an XSLT style sheet (eXtensible Style Sheet Language Transformations). The adapter layer can then transform the XML content to HTML with the help of the style sheet.

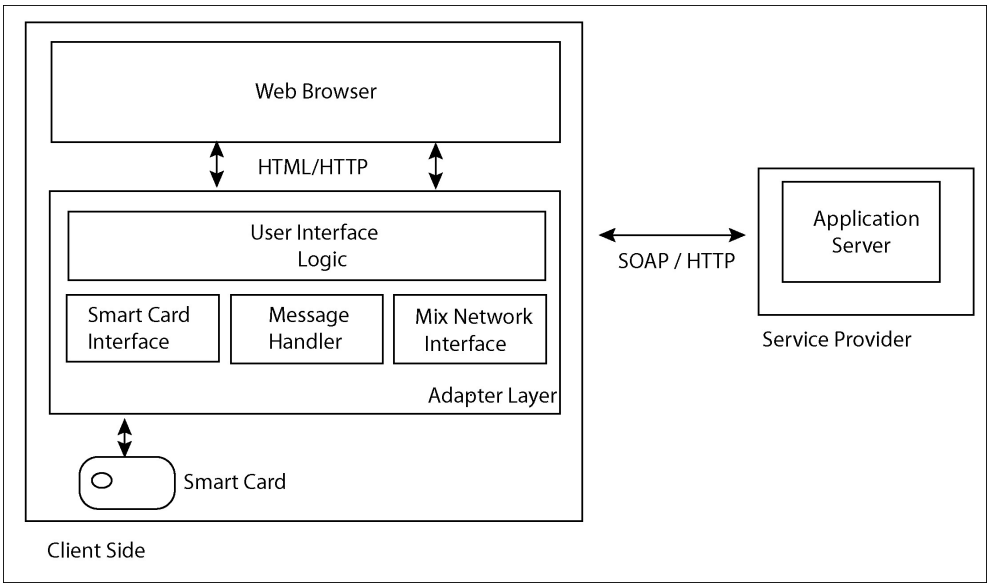

Figure 7.3: Components of the adapter layer

  - **User interaction with regard to credential protocols:** as Web browsers do not contain user interface elements to support credential protocols, the adapter layer generates such dialogues. For instance, the adapter layer generates a dialogue box before engaging in the credential show protocol in order to ask a citizen for consent.

- **HTTP proxy for Web browser:** the browser directs HTTP requests at the adapter layer. The adapter layer then communicates with service providers. Using the adapter layer as a proxy facilitates integration with the mix network (see below) and allows to integrate credentials into Web-based services.

- **Smart card interface:** This component interfaces to the citizen card. It exposes the card's functionality in the form of a high-level interface. Smart cards communicate via an APDU-based interface (Application Protocol Data Unit). If a Java client is used instead of a Web browser, the Java client can directly access this interface in order to get access to citizen card functions.

- **Message handler:** The message handler serves the purpose of integration with remote system components. The middleware based on Web services connects the adapter layer with other system entities such as

the off-card storage. The middleware layer addresses protocols related to the use of pseudonymous credentials (such as obtaining or showing a credential).

- **Mix network interface:** The interface establishes an anonymous communication channel for the communication with providers of anonymous services. This component acts as a proxy service that can set up a TCP/IP connection through a mix network, thereby masking the user's IP address. The existence of the mix network is completely transparent to the user. The service description retrieved from the portal service must indicate which services are anonymous, so that the respective communications can be routed through the mix cascade.

The prototypical implementation makes use of XSLT style sheets to transform content from service providers into HTML. A transformation of XML by style sheet has the advantage that the presentation of content can be changed easily by adapting the style sheet.

The adapter layer was prototypically implemented as a servlet. Implementation as a servlet has the advantage that the handling of HTTP requests from the browser to the adapter layer is handled by the servlet engine, which saved development time. The interaction diagram in Figure 7.4 shows the interplay between the browser, the adapter layer and the Web browser in credential-based service access. The specific steps that are performed as part of access control on the server side are considered in more detail in section 7.4.

The following steps are performed when accessing a service:

1. The citizen has discovered a service by use of the portal and points the Web browser to the desired address.

2. The adapter layer retrieves the HTML pages of the service.

3. Upon trying to access a part of the service that requires the possession of a credential, the Web server checks whether the client has already shown the required credentials. This is achieved by looking up whether the client possesses the role that is associated with the given credentials. If the credentials have not been shown yet, access is denied.

4. The adapter layer requests a description which credentials need to be shown in order to be granted access.

5. The service provider sends an XML file that specifies which credential or which set of credentials needs to be shown in order to use the service.

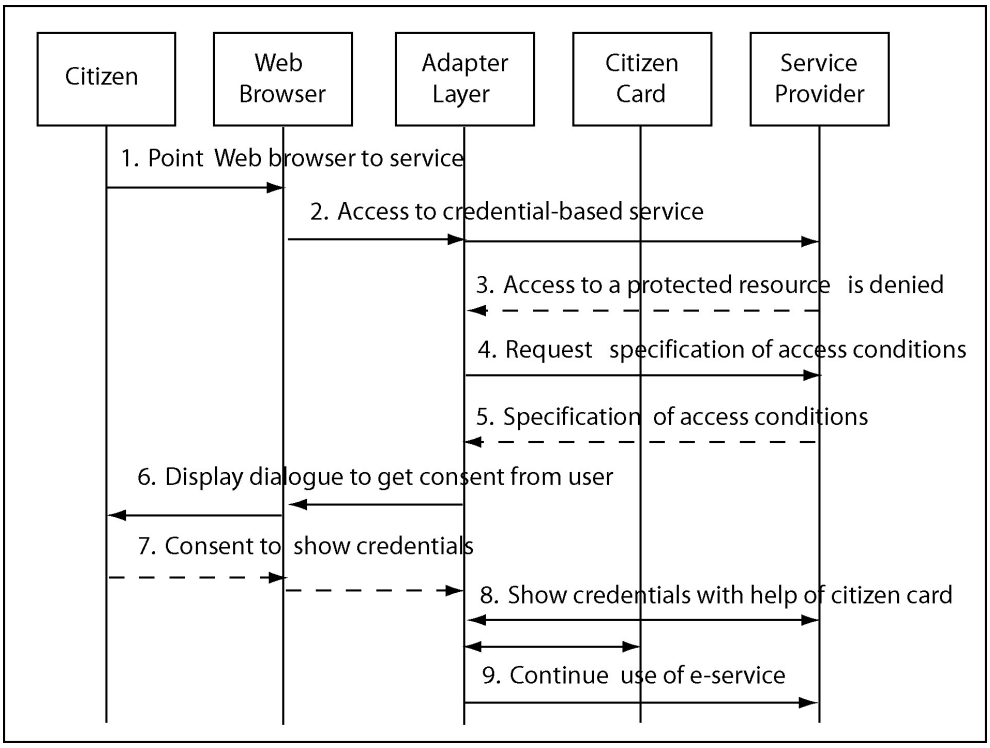

Figure 7.4: Interplay between Web browser and adapter layer in service access

6. The adapter layer displays a dialogue (by sending the dialogue in HTML form to the Web browser) and asks whether the citizen wants to show the required credentials.

7. The citizen gives consent.

8. The adapter layer engages in the credential show protocol with the service provider. The show protocol is implemented as a Web service. The adapter layer handles the message exchange with the service provider. However, the messages of the protocol are passed on from the adapter layer to the citizen card. All cryptographic calculations are performed on the smart card. The show protocol comprises three rounds, i.e. three calls to a Web service are effected by the adapter layer. As a result of showing the credentials, the server now associates the client with a role as specified in the access control settings.

9. After successfully showing the credential, the adapter layer resumes the access to the service and continues the session. The application server now lets the client access the resource.

7.3 Web and Business Tier

The architecture on the server side comprises three tiers: Web tier, business tier and EIS tier. Our design aims at a Web-based service delivery. Accordingly, service providers represent services as a series of HTML pages. The citizen navigates through these pages in order to obtain services.

Figure 7.5 gives an overview of the Web and the business tier. Components for service representation are located in the Web tier. The business tier comprises components that encapsulate all application logic related to credentials, i.e. establishing pseudonyms, issuing credentials and verifying credentials. Furthermore, the business tier comprises components to implement application logic that is specific to a given service. The design only models application logic related to credentials.

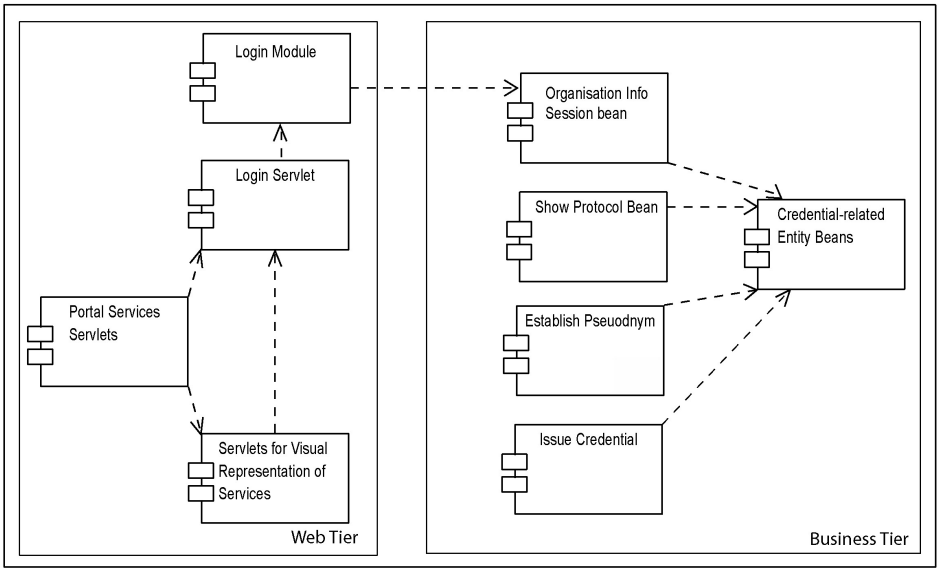

Figure 7.5: An overview of components in the Web and the business tier

7.3.1 Web Tier

This tier contains components that are concerned with generating the user interface. Furthermore, authentication of users is done in the Web tier. This tier usually does not contain any business logic. The Java 2 Enterprise Edition offers servlets and Java Server Pages (JSP) as technologies for this layer. The components of the Web tier run inside a Web container.

The architecture makes use of servlets within the Web tier for the portal service, a login servlet and for servlets that generate HTML pages of services. Furthermore, the Web tier comprises servlets that are deployed on the Web container as end-points for Web services. These servlets are invoked by clients who call a Web service. The servlet then forwards the call to a session bean that implements the business logic behind the Web service. A stateful session bean requires a servlet as an end-point in order to expose its methods as Web services. In contrast, stateless session beans can directly expose their methods as Web services without making use of a servlet.

In order to enhance the readability of diagrams, we do not show these end-point servlets in the component and class diagrams. The Web tier comprises four types of servlets, as shown in Figure 7.5:

- **Portal service servlets:** these servlets are operated by the authority that provides the portal service. An organisation that issues credentials or offers credential-based services does not host servlets of this type. The servlets generate the portal pages and provide XML descriptions of services.

- **Servlets related to visual representation of services:** citizens use services by help of a Web browser. An organisation represents services as a series of HMTL pages which the citizen can access. An approach based on HTML pages has the advantage that existing tools and know-how can be leveraged to create service pages.

- **Login servlet:** the login servlet is called by clients who wish to enter a particular role. It communicates with the login module in order to authenticate users who wish to access services. Both login servlet and login module are necessary to achieve an authentication and authorisation based on credentials.

- **End point servlets:** every session bean in the business tier that exposes its functions as a Web service has a servlet as an end-point.

Next to these three types of servlets, a login module must be provided:

- **Login Module:** the login module is not a servlet but a normal Java object. The login module serves the purpose of authenticating users and associating them with roles. After a user has shown a credential and called the login servlet, the login module associates the user with a specific role based on the credentials that were shown. The login module must correspond to the JAAS (Java Authentication and Authorisation Service) specification.

This design thus separates visual representation of services from credential-related application logic. Service providers design their services as usual as HTML screens and deploy them on the Web tier. Access control settings are made at the time of deployment.

7.3.2 Business Tier

The business tier of a J2EE application comprises the business logic. This tier communicates with the Web tier and the EIS tier. In order to create a manageable EJB application, the business tier is usually split into two parts that each contain a different type of enterprise Java bean. The first type of beans are session beans. This type of beans encapsulate the business logic of the application. The second type of beans are entity beans. These beans store data persistently and generally correspond to data in the underlying database layer [Rom99]. We will first discuss the layer of session beans for the handling of credentials and then discuss the entity beans of the design. Figure 7.6 illustrates the session beans in the business layer comprising session and entity beans.

7.3.3 Session Beans in the Business Tier

Session beans model the business-specific parts of an application. The design addresses only logic that is specific to the handling of credentials. For an actual deployment, further beans must be added that contain logic related to the services that are to be provided by an organisation. All session beans in the session layer expose their services to clients as Web services.

With regard to the handling of credentials, the following functions must be provided:

- establishing a pseudonym with a user
- issuing a credential to a user
- verification of a credential, optionally with regard to a pseudonym

The above list of credential-related functions does not comprise the establishing of the root pseudonym: this pseudonym should be established as a part of the card personalisation process. Verification of a credential happens when a user accesses a service which is only accessible upon demonstration of a credential. Demonstrating a credential with regard to a pseudonym means that the user must also prove possession of a pseudonym. Next to beans

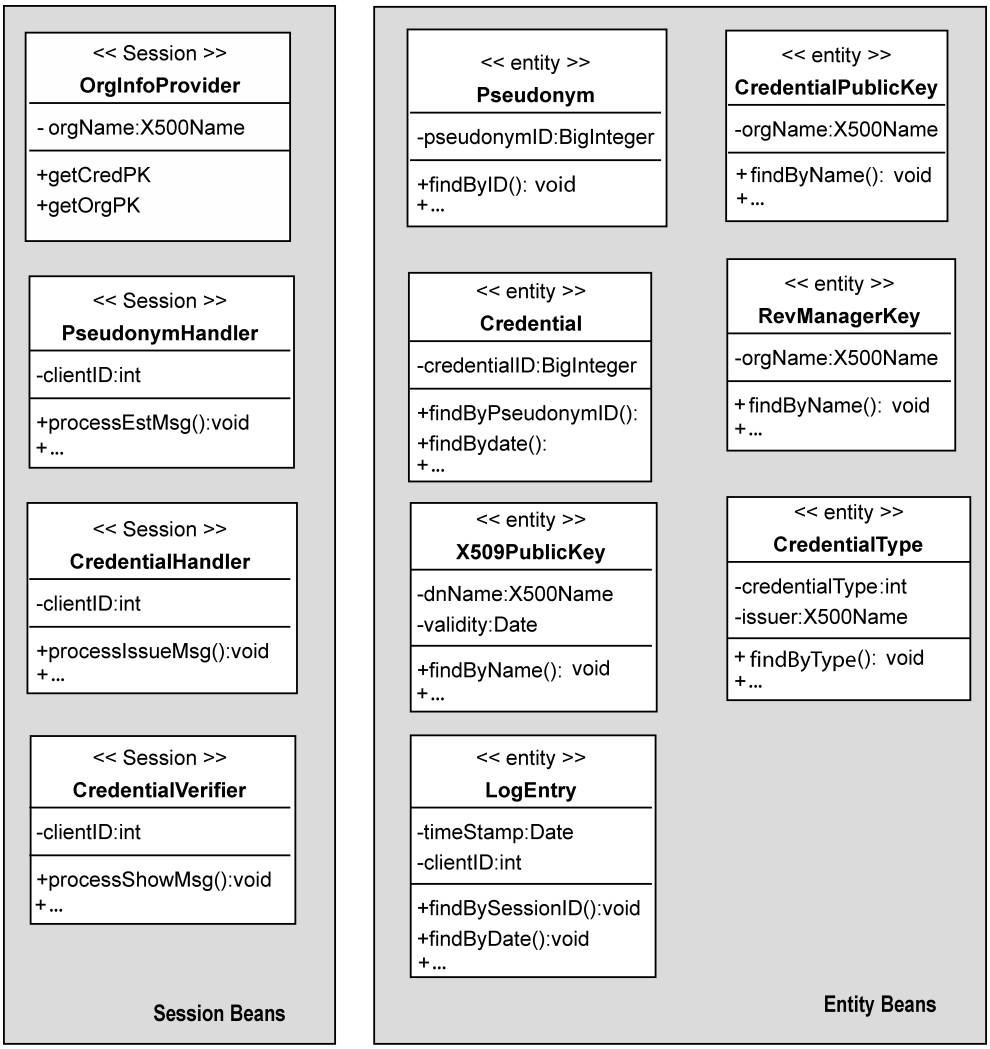

Figure 7.6: An overview of session and entity beans in the business tier

for these three functions, the business tier also comprises a session bean for credential-based authentication of clients.

With regard to the choice of stateful or stateless implementation of session beans, all credential-related beans are implemented as stateful beans. All credential protocols are essentially three-round protocols, i.e. they comprise three consecutive protocol steps. As a consequence, the server must retain the state of the protocol in between the rounds. Thus, stateful session beans are an appropriate choice.

We directly map the above mentioned functions to session beans. Each functionality is mapped to a single session bean. This leads to a design where each bean represents exactly one business process. Furthermore, there is one session bean to handle information requests regarding keys and credential types. The design comprises the following session beans:

- **PseudonymHandler:** this bean establishes a pseudonym with a citizen. Once a pseudonym is established with a citizen, the pseudonym is committed to a persistent storage by help of entity beans. The pseudonym handler also creates a log record to document the event of establishing a pseudonym.

- **CredentialHandler:** this bean issues a credential to a citizen. A precondition is that the citizen has already established a pseudonym with the organisation. There may be pre-conditions for obtaining a credential: the issuance of a credential can depend on the possession of other credentials which the citizen must first show. A record that describes the credential is saved to a database. This record also contains a reference to the pseudonym to which the credential was issued. Furthermore, the credential handler creates a log record to document the event of issuing a pseudonym.

- **CredentialVerifier:** this bean implements the credential show protocol. Credentials can be shown on their own or with regard to a pseudonym. Thus, this bean also implements steps to have a citizen prove possession of a pseudonym. Whenever a credential was shown, a transcript of the show protocol is committed to the log (persistent storage).

- **OrgInfoProvider:** this bean serves as a manager of information and cryptographic keys related to the organisation. The information handler is implemented as a stateless session bean. It services key and information requests that are issued by the three session beans described above. It is also be accessed by components in the Web tier.

The bean also provides information related to access control. Clients who have tried to access a protected resource can query this bean. The bean then informs the client what credentials need to be shown in order to access the resource.

Next to these four session beans, one further helper class is needed:

- **ProtocolProcessor:** this class encapsulates application logic specific to the protocols of the Camenisch and Lysyanskaya credential system. A protocol processor object performs all calculation steps of a credential-related protocol. It thus encapsulates the cryptographic algorithms of the credential system.

Figure 7.7 shows a more detailed view of the 'CredentialVerifier' bean. This bean uses an instance of the 'ProtocolProcessor' class for the processing of credential messages. The show protocol is directly exposed as a Web service.

There is no need for a data transfer object (DTO) to encapsulate credentials: such objects are often used to transfer information between clients and session beans. However, credential holders and credential issuers each use a different representation of a credential (comprising different secret values). There can thus be no common representation of a credential beyond the credential description.

These beans only implement logic related to the use of credentials. An organisation adds these beans to existing beans that encapsulate the organisation's business processes. The session beans depend on entity beans to store data that is necessary for the execution of credential protocols. These entity beans are described in the next section.

7.3.4 Entity Beans in the Business Tier

In contrast to session beans, entity beans do not contain business logic - they encapsulate data. In our design, entity beans are used to store data related to the handling of pseudonymous credentials. Such data are e.g. pseudonyms, credentials, a log file, credential keys and system parameters.

The data is usually kept in databases in the EIS tier. The entity bean represents that data and makes it available to session beans. For reasons of performance, clients must never directly access entity beans. Instead, all access to entity beans must be routed through a session bean. Entity beans are used to create data records in the database, retrieve data from the database and also to delete data from the database. Every entity bean

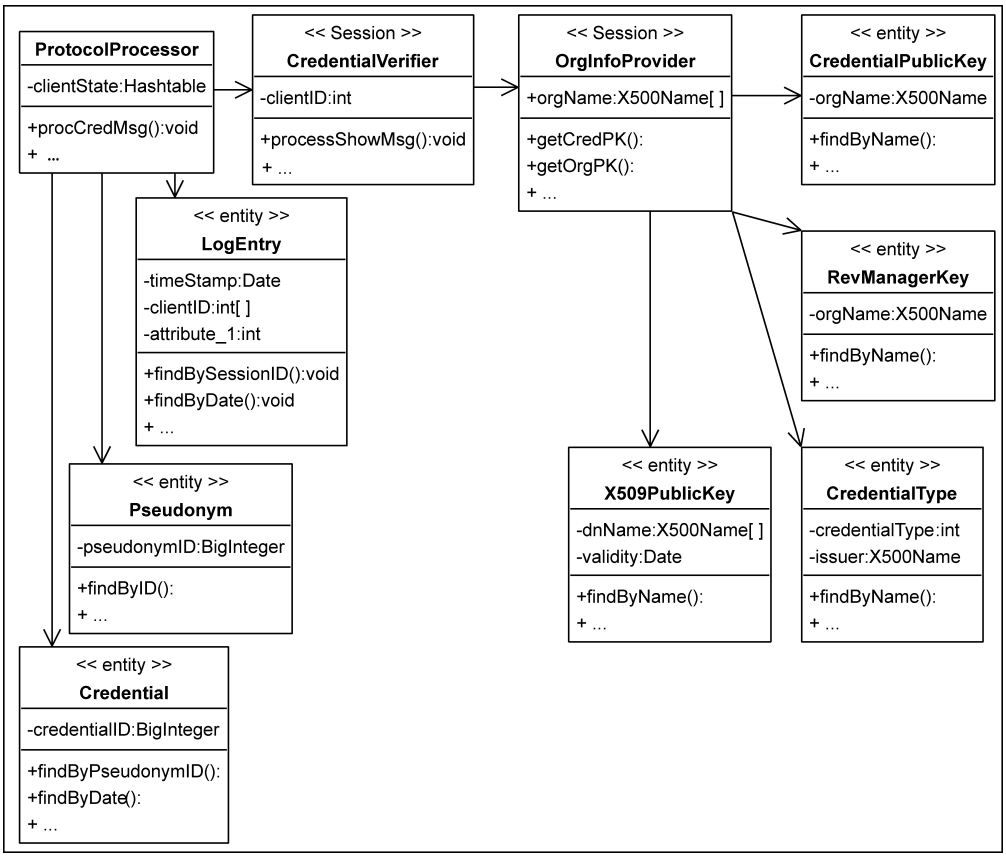

Figure 7.7: The 'CredentialVerifier' bean and its relation to other beans in the business tier

contains methods for the management of the bean and may provide further user-defined methods to implement business logic.

Entity beans comprise methods for the creation, updating and removal of data in the underlying storage. Entity beans also have finder methods: these methods are used to retrieve instance data from the persistent storage based on search criteria. One or more data instances can be retrieved from the database.

Every entity bean has a primary key that uniquely identifies the data record that the bean represents. The primary key can be an atomic data item or a class comprising several attributes.

Our design comprises the following entity beans:

- **Pseudonym:** a citizen establishes a pseudonym with an organisation before obtaining credentials. An organisation keeps a list of all pseudonyms that were established with citizens. Pseudonyms do not

expire. The entity bean has a finder method that allows a session bean to retrieve all pseudonyms established within a given period. Pseudonyms are not deleted but are archived when no longer needed. A pseudonym has a unique number that serves as a primary key for the bean.

- **Credential:** credentials are obtained only after establishing a pseudonym. A citizen can obtain several credentials under the same pseudonym. As credentials depend on a pseudonym, the credential entity bean contains a reference to a pseudonym entity bean. Credentials usually have an expiry date. They are not deleted from the database but are archived when they expire. The credential object has a finder method which allows to retrieve all credentials that belong to a given pseudonym. Every credential has a credential type, which together with the pseudonym number and the expiry date serves as a primary key.

- **Credential public key**: every organisation who issues credentials has a credential key pair. This entity bean represents a credential public key. In order to determine the validity of a credential that is presented to a relying party, an organisation must possess the credential public key of the organisation that has issued the credential. An organisation's X.500 distinguished name serves as a primary key for this bean.

- **X.509 public key certificate:** this entity bean represents an X.509 public key certificate. Every organisation that participates in a credential-based system possesses both a credential public key and an X.509 public key (for digital signatures). As a primary key, the organisation's X.500 distinguished name is used.

- **Revocation manager public key:** the public key of a revocation manager has a key format that is different from a normal credential public key. Therefore, an entity bean class of its own is used to store the revocation manager's keys. As is the case with other public key related beans, the revocation manager's X.500 name serves as primary key.

- **Log entry:** events related to credentials are recorded in a log entry in a database. The events that are logged are the creation of a pseudonym, the issuance of a credential and the verification of a credential (i.e. when a user shows a credential). All of these events result in a transcript of a cryptographic protocol. Next to this transcript, every log entry comprises a time stamp and the SSL session ID of the client.

This session ID is necessary so that several events of a client within one session can be linked together. The time stamp together with the SSL session ID serve as a primary key for the bean.

- **Credential type:** an organisation can issue many different types of credentials. This entity bean represents the description of a credential. The description comprises a name for the credential, a short description, a type number and dependencies between credentials (e.g that a citizen must show a specific credential before obtaining another credential). For every type that is issued, one entity bean is created. The type number serves as a primary key.

Every organisation who acts as an issuer of credentials has a credential key pair that consists of a credential public key and an associated secret key. The public key is stored in the database and represented by an entity bean. In an actual deployment, the secret key must be stored in a tamper-proof environment such as a smart card or a hardware security module (HSM).

A service provider also needs to store a number of global parameters for the credential system. A credential system usually has system-specific parameters that are shared by all participants in the system. Such a parameter is e.g. the length of public keys. It does not make sense to represent these parameters as entity beans, as only a single set of parameter data exists within the system.

In practical deployments it may be desirable to bypass the entity bean layer and write directly to the underlying database. Some bean instances are too short-lived to justify the overhead of creating a bean in order to persist data. This is the case with the log entry bean: after an entry is committed to the database, it is never updated and possibly seldom read. As these records serve purposes of documentation only, it is acceptable to directly write them to the database to reduce server load. Thus, a session bean should be able to write a log entry directly to the database without creating a 'LogEntry' entity bean first. The J2EE specification explicitly allows the bypassing of an entity bean.

There are several options with regard to the storage of these objects: they can be stored in a relational database (through an object-relational mapping) or saved to an object database management system (ODBMS). With regard to storage in a database system, two options can be distinguished, namely bean-managed persistence and container-managed persistence. If bean-managed persistence is chosen, the entity bean is responsible for storage of objects to and retrieval of objects from the database. This could happen by e.g. writing objects to the database by use of the Java Database Connectivity (JDBC) API.

In settings with container-managed persistence, the administrator informs the container what fields to persist by manipulating bean properties. Persistence is then managed by the middleware (i.e. the bean container). Subsequently, the container can manage storage and retrieval operations. Container-managed persistence has the advantage that less code needs to be written by developers. The mapping of the entity beans described above to a relational database scheme is outside the scope of this thesis. For the prototypical implementation, all objects were serialised into XML files.

7.4 Authentication and Authorisation based on Credentials

In our architecture, credentials are integrated into a Web-based service model. Services are thus represented as a series of HTML pages (respectively servlets and Java server pages). In Web-based service delivery, the J2EE platform usually authenticates users by a pair of username and password. In an anonymous setting however, users cannot be authenticated by user names and passwords, as users shall stay anonymous.

Instead, we directly map credentials to roles. Users show credentials to the server and thereby enter roles. Such an approach integrates well with the role-based access control model of the J2EE platform. An authentication based on credentials can be achieved on the J2EE platform by use of a customised login module which handles the authentication of users. This login module is then deployed to replace the standard authentication mechanism that relies on user names and passwords. A customised login module can be developed by the use of JAAS (Java Authentication and Authorization Service) which is a part of the J2EE specification as of release 1.3. Users thus show credentials to the application server to enter roles. On the basis of these roles, users can be authorised to access specific resources. For all credential-related protocols, Web services are used.

7.4.1 Java Authentication and Authorization Service

The Java Authentication and Authorization Service (JAAS) can be used to implement arbitrary authentication mechanisms. By use of the JAAS framework for authentication, Java applications can remain independent from underlying authentication technologies [Sun03]. JAAS is a part of J2SDK, v 1.4 and is also integrated into the J2EE specification as of version 1.3.

In order to use JAAS for an authentication based on credentials, a developer must implement a login module that replaces the password-based

authentication mechanism. The login module must implement the interface 'javax.security.auth.spi.LoginModule'. The login module verifies that a client has shown the respective credentials. If the client has shown all necessary credentials to enter a role, the login module includes the user in the list of authenticated subjects and associates the subject with the given role.

The login module must implement the following methods:

- **Initialize**: this method initialises the login module. An object representing a user and further necessary context information are passed to the login module for initialisation.
- **Login**: this method authenticates a subject. In a credential-based setting, the login method consults the log file to find out whether all credentials necessary for a given role have indeed been shown.
- **Commit:** after a successful authentication, the commit method is invoked. It associates the subject with the role that belongs to the given set of credentials.
- **Logout:** this method removes the subject from the current set of authenticated users.
- **Abort:** this method is called if the authentication has failed.

The login module is invoked by the Web container when a user is to be authenticated. The deployment file must specify for which security realm the given login module is to be invoked. As a name for a subject, the SSL session ID is used. Based on the login module, a user can be authenticated and associated with roles. The mapping from credentials to roles is described in the next section.

7.4.2 Mapping from Credentials to Roles

The Java 2 Enterprise Edition platform supports a role-based access control model. Subjects are authorised based on the roles they have entered. This implies that access rights are not attributed to subjects but instead to abstract roles that exist in a system. In role-based access control, a subject is authenticated and then enters one or more roles. When accessing a resource, the access control subsystem checks whether the role the user currently holds has the right to access the given resource. Authorisations are always specified and enforced with regard to roles.

An identity concept comprising credentials aims to provide anonymous and pseudonymous services to citizens. When accessing services, users must

be authenticated and authorised while staying anonymous. Role-based access control can easily be combined with an authentication based on credentials: a citizen shows credentials and thereby enters a role that is associated with a set of credentials. All authorisation decisions are made based on roles. The application server only checks whether a client is associated with a given role and does not need to know about the identity of a client (respectively a citizen) who accesses a service.

The mapping from credentials to roles can be done at the time of deployment. This mapping is in many application scenarios straightforward: the deployer specifies a number of roles that exist in the system in an XML file. For each credential - respectively for each combination of credentials - a separate role is defined. Entering a role can thus necessitate the possession of several credentials. Mapping credentials to roles is a natural solution: for instance, a citizen who holds a social benefit credential acts in the role of 'benefit recipient'.

We can illustrate the mapping with an example system from the domain of social benefits where two types of credentials exist: a credential for citizens on a low income and a credential for citizens who receive old age pension. In order to map these credentials to a role-based access control model, we first define the roles 'pensioner' as well as 'income support recipient'. Let us assume that a specific service exists for old age pensioners who have a low income. For this category of users, we specify the role 'pensioner income support'. A user requires both credentials in order to enter this role. Figure 7.8 shows a fragment of the resulting XML file that specifies the mapping to roles. The XML format of the specification of roles complies with the J2EE standard.

After having defined the roles in an XML file, a mapping from credentials to roles needs to be specified in another file. We map each credential respectively each combination of credentials to one of the defined roles. The role definition and the mapping from credentials to roles is then used for access control in the Web and the business tier. Figure 7.9 shows the resulting mapping as an XML file. The format of this file can be chosen freely, as credential-based authentication is not part of the J2EE standard. The resulting XML file is interpreted by the login module bean in the business tier.

The definition of roles and the specification of access control settings (i.e. which role a user must hold in order to access a resource) are handled by the deployer at the time of deployment. Access control settings are thus separated from application logic. These declarative settings can be adapted at any time without having to modify application code. The protection of resources in the Web tier relies on the role definitions and is described in the section 7.4.3.

```
<!-- SECURITY ROLES -->
<security-role>
  <role-name>pensioner</role-name>
  <description>Citizen on old age pension</description>
</security-role>
<security-role>
  <role-name>income_support_recipient</role-name>
  <description>Citizen on income support</description>
</security-role>
<security-role>
  <role-name>pensioner_income_support</role-name>
  <description>Old age pensioner on income support</description>
</security-role>
...
```

Figure 7.8: A definition of roles for the use in the J2EE role-based access control model

The mapping from credentials to roles was a straightforward process in the example presented in this section. This is the case because we had chosen quite a simple example. Conversely, much more complicated situations can arise in practical implementations and a mapping from credentials to roles can become quite complex.

For instance, we did not consider negative credentials. An example for such a negative credential is a credential that states that a citizen is not allowed to drive a car. In our system, entering a role always requires an affirmative set of credentials (i.e. the absence of a credential is not tantamount to a negative credential). The existence of negative credentials can make a mapping more challenging [BFK99]. Trust establishment with the help of credentials can thus become quite a complex task depending on the application scenarios. Trust establishment and the specification of trust policies are still a subject of academic research (see e.g. [Sam02], [NA02], [HMM+01]).

7.4.3 Protection of Resources in the Web Tier

The J2EE Web tier supports a declarative setting of access rectrictions for components in this tier. HTML pages, servlets and Java server pages can thus be protected by manipulating deployment descriptors. In this section we continue our example and show how to restrict access to components in the Web tier based on roles.

Access to resources is declaratively restricted on the basis of URL (Uniform Resource Locator) patterns. If no security constraint is defined for a

```
<CredentialRoleMapping>
  <role-name>pensioner_income_support</role-name>
   <CredentialList>
    <Credential>
     <Issuer>C=UK,O=Newcastle City Council, OU = Pension Benefits
        Administration,  CN = Benefits Credential Issuer</Issuer>
     <description>Old Age Pension Credential</description>
     <CredentialType>10010<CredentialType>
    </Credential>
    <Credential>
     <Issuer>C=UK,O=Newcastle City Council, OU = Social Benefits
      Administration, CN = Benefits Credential Issuer</Issuer>
     <CredentialType>10020<CredentialType>
     <description>Income Support Credential</description>
    </Credential>
   </CredentialList>
  </role-name>
 ...
</CredentialRoleMapping>
```

Figure 7.9: A mapping from roles to credentials

given page or servlet, it is assumed to be publicly accessible. For each URL pattern, the deployer can enumerate the roles that are needed to gain access. Furthermore, the deployer can make settings that ensure that access is only possible via a connection secured by SSL (secure sockets layer). Settings for access control are made in the 'web.xml' file in the directory 'WEBINF' on the J2EE server. Figure 7.10 shows a fragment of an XML file that builds on the roles defined earlier. Again, this XML fragment is compliant with the J2EE standard.

The file restricts access to all servlets in the specified directory. Similarly, access to all Web pages in this directory could be protected by adding another 'web-resource-collection' tag. Users who want to access these resources must have entered the role of 'pensioner income support'. In order to enter this role, users must have shown the respective credentials for this role. Credentials are shown by accessing a Web service provided by the 'CredentialVerifier' bean in the business tier. By defining a 'user-data-constraint' statement we enforce that the services can only be accessed via a secure connection.

7.4.4 Protection of Business Tier Components

In this section we discuss access control measures with regard to resources in the business tier that are exposed to client calls. Three components in the business tier expose services to clients as a Web service: these are the session

```
<!-- SECURITY CONSTRAINT -->
<security-constraint>
 <display-name>constraint_pensioners_income_support</display-name>
 <description>Services for old age pensioners on income support</description>
  <web-resource-collection>
   <web-resource-name>PensionerIncPages</web-resource-name>
   <url-pattern>/WEB_INF/pensionerIncServices/classes/*</url-pattern>
   <http-method>GET</http-method>
  </web-resource-collection>
 <auth-constraint>
  <description>Only pensioners on income support have access</description>
  <role-name>pensioner_income_support</role-name>
 </auth-constraint>
 <user-data-constraint>
 <transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

Figure 7.10: An example XML specification that only allows users in the role of 'pensioner income support' to access protected servlets

beans that serve to establish pseudonyms, to issue credentials and to verify credentials. These three services are provided by the 'PseudonymHandler' bean, the 'CredentialHandler' bean and the 'CredentialVerifyer' bean. We will briefly discuss whether access control measures to these three functions must be provided. In cases where access restrictions make sense, we consider how access control measures can be implemented.

We consider access control measures for the three credential-related functionalities provided by the session beans:

Verification of a credential ('CredentialVerifyer' bean): it does not make sense to restrict the access to the 'CredentialVerifyer' bean. After all, a citizen must be able to show a credential to the organisation in order to enter a role. Thus, the Web service that verifies a credential must be accessible to unauthenticated clients. Thus, no access control measures are necessary for this bean.

Establishing a pseudonym ('PseudonymHandler' bean): in a practical deployment it does not make much sense to restrict access to the 'PseudonymHandler' bean. Citizens do not have a use from establishing a pseudonym. A pseudonym without a credential cannot be used to access services. Thus, it would be feasible to allow any citizen to establish a pseudonym and to only make restrictions with regard to the issuing of credentials. We will nevertheless briefly describe how access restrictions for the 'PseudonymHandler' bean can be implemented with the help of declarative access control measures.

The methods of the pseudonym handler bean are exposed as a Web service through a servlet that is called by clients. Consequently, access can be restricted to credential holders by specifying in the 'web.xml' file of the Web container the roles that a citizen must hold in order to call the servlet. Thereby, a citizen must first show the required credentials in order to access the Web service with which a pseudonym is established.

Issuance of a credential ('CredentialHandler' bean): with regard to the 'CredentialHandler' bean, access control measures make sense. It must be possible to configure the system so that citizens can only obtain credentials if they have previously proved possession of other credentials. Such cases can be handled by restricting access to the 'CredentialHandler' session bean. Dependencies between credentials are part of the credential type description (represented by the 'CredentialType' entity bean). Every type description states what credentials a citizen must already possess in order to be issued the given credential.

Access control measures for this bean must be implemented in part programmatically. When a client calls the 'CredentialHandler' bean, the bean looks up dependencies in the credential type description. The bean can then call a method from the container to verify whether the caller has already shown the required credentials (and thus possesses the associated role). This is achieved by calling the method 'isCallerInRole'. This method is provided by the EJB container and allows a session bean to learn about the roles that the caller holds. If a client does not hold the required roles, the Web service returns an error code. Thereby, dependencies between credentials are specified as part of a credential type description. The dependencies are enforced by the 'CredentialHandler' bean that handles the issuing protocol for credentials.

7.4.5 Access Control Steps performed as Part of a Service Access

This section provides an illustrative example to demonstrate the interplay of different components that are involved in authentication and authorisation. The example builds on the previous sections and illustrates the use of a login module to enable an authentication based on pseudonymous credentials. It explains the steps that are performed on the server side if a user accesses a credential-based service. Figure 7.11 illustrates the access to a service based on credentials in more detail.

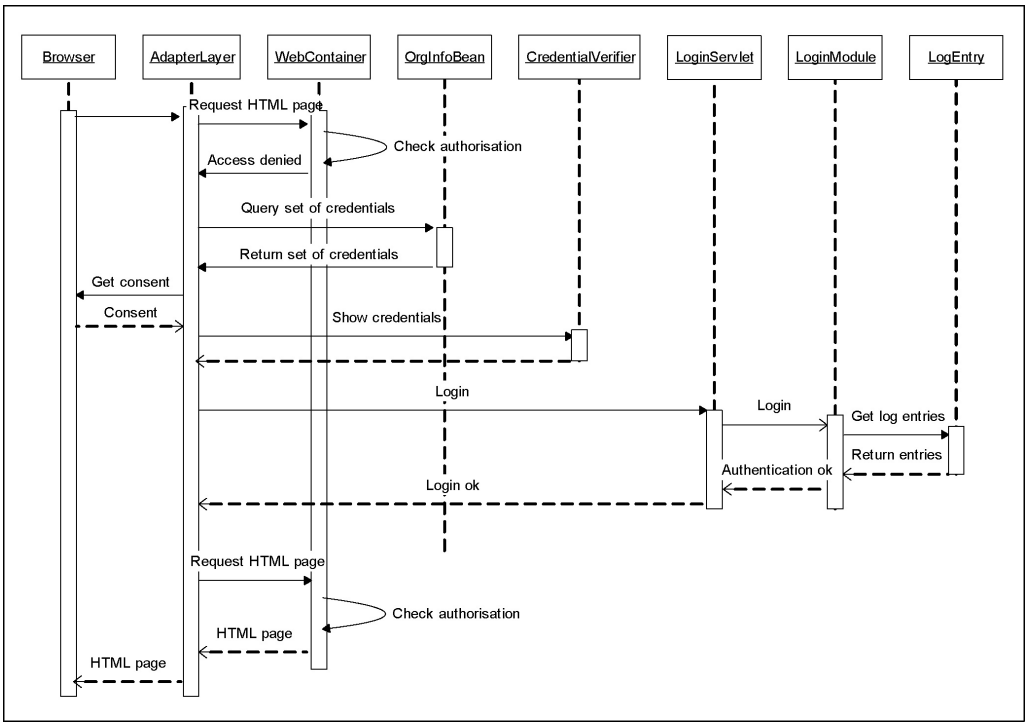

Figure 7.11: Accessing a credential-based service

The following steps are performed when accessing a credential-based service:

1. The browser requests an HTML page that is a protected resource. The request is sent from the browser to the adapter layer. The adapter layer then sends the HTTP request to the Web server.

2. Check authorisation: the Web container checks whether the caller holds the right role in order to access this page. The user is still unauthenticated and so does not hold any role.

3. The Web container denies access and sends an HTTP error message.

4. The adapter layer invokes a Web service provided by the OrgInfoBean in order to find out which credentials must be shown to access the resource.

5. The OrgInfoBean returns the set of credentials.

6. The adapter layer displays a dialogue (by sending the dialogue in HTML form to the Web browser) asking whether the citizen wants to show the required credentials.

7. The citizen gives consent.

8. The adapter layer engages in the credential show protocol with the service provider. The adapter layer only relays messages between service provider and the citizen card. All cryptographic calculations are performed on the smart card. The show protocol comprises three rounds, i.e. the adapter layer effects three calls to the service provider.

9. In order to be authenticated, the adapter layer calls the login servlet. The layer sends the SSL client ID and the role that the citizen would like to enter to the login servlet.

10. The Web container invokes the login module. The login module queries the EventLog entity bean in order to find out which credentials have been shown by the citizen. It adds the client to the list of authenticated users and associates the client with the given role. The SSL session ID serves as name for the client.

11. The adapater layer again requests the protected page from the Web server.

12. The Web server checks whether the client holds the right role. This is now the case, as the login module has associated the client with the required role.

13. The Web container returns the requested HTML page.

14. The adapter layer sends the HTML page to the Web browser.

7.5 Prototypical Implementation

The architecture described in this section was in part prototypically implemented. The prototypical implementation of a system for credential-based service access based on Web services was undertaken as part of a diploma thesis by András Kiraly [Kir03a]. The prototypical implementation of the architecture validates the approach that is taken in the design of the system. The prototype implements several key concepts of the architecture. In the prototype, credentials are integrated into a Web-based service delivery through a standard Web browsers. Protocols related to credentials are implemented as calls to Web services. All server side components of the prototypical implementation were based on the Java 2 platform, Enterprise Edition. For details on the prototypical implementation, the reader is referred to [Kir03a].

The prototypical implementation is based on the pseudonymous credential system proposed by Camenisch and Lysyanskaya. A prototypical implementation of the system was developed by IBM Research in Rüschlikon, Switzerland. The implementation is called Idemix, which is an acronym for Identity Mix. In the course of this thesis, a research cooperation was established by the author between University of Zurich and IBM Research Rüschlikon which made it possible to use parts of the code developed by IBM.

The prototype by IBM was in part leveraged for the prototypical implementation. All classes related to cryptographic calculations were taken from Idemix. This includes classes for basic cryptographic algorithms as well as classes that are specific to Camenisch and Lysyanskaya's credential system. Neither classes for the graphical user interface nor for the communication between distributed entities were reused.

In the prototypical implementation, Web services are used for all communications between client and server. The prototype demonstrates that credential protocols can be implemented as Web services. On the client side, the adapter layer acts as a proxy for the Web browser. It handles all communication with service providers. Furthermore, it translates responses from servers that contain presentation logic from XML into HTML. On the server side, all calls to Web services are handled by servlets, not by EJB beans. As the system by Camenisch and Lysyanskaya cannot be implemented on smart cards yet, no implementation on card environments was undertaken.

The prototype differs from the design depicted in this chapter as follows:

- **Client side:** cryptographic classes were prototypically implemented in Java 2, Standard Edition, as a Java Card implementation is not yet feasible. The adapter layer was implemented as a servlet, running inside a Tomcat Web container. The transfer of HTML and XML pages of services was implemented as a Web service in order to avoid the parsing of HTTP messages in the servlet.

- **Server side:** all server side components were implemented within the Web tier. The prototypical implementation thus does not make use of an EJB business tier. Furthermore, persistence is based on XML in the prototype. Objects are thus serialised into XML files instead of into a database.

The prototypical implementation shows that credentials can seamlessly be integrated into a Web-based service delivery. The prototype enables a user to discover services from a portal. Pseudonyms and credentials can be

obtained from service providers and services can be accessed anonymously and pseudonymously by use of credentials [Kir03a].

7.6 Summary

Credentials can be integrated into an application architecture comprising Web-based service delivery and J2EE components. The architecture proposes that credential-based services are delivered through a standard Web browser that is complemented with an adapter layer. The adapter layer makes the functionality of the smart card available to Web-based applications, interfaces with remote system components and enables the use of credentials in Web-based services.

On the server side, credential-based services can be integrated into an architecture based on enterprise Java beans. As credential protocols span several rounds, these protocols must be mapped to stateful session beans. All services related to credentials can be offered as Web services. A credential-based authorisation can be achieved by mapping credentials and combinations of credentials to roles. Such an approach facilitates an integration with the role-based access control model used by the J2EE platform.

We expect that component manufacturers will offer EJB components that encapsulate credential protocols. Providers of credential-based services can thus reduce their development effort when migrating towards anonymous and pseudonymous services.

Chapter 8

Discussion

This chapter discusses the concept for an extended digital identity with regard to its potential and with regard to problems that may arise when implementing the concept. We will first discuss to what extent we expect the public and private sector to migrate towards anonymous services. With regard to the use of credentials in e-government, we will also discuss whether a fully anonymous administration based on pseudonymous credentials is feasible. We will equally examine barriers that currently exist for an implementation of credentials as part of the citizen's digital identity, both with regard to technological and non-technological factors.

8.1 Potential of the Extended Digital Identity in Public and Private Sector Services

The concept for an extended digital identity proposed in this thesis adds pseudonymous credentials to the citizen's digital identity. Since credentials are an additional feature that complements the existing functionality of digital citizen cards, both identified and anonymous service delivery becomes possible. We have argued that adding pseudonymous credentials contributes to the protection of privacy, as credentials pertain to the privacy goals of data avoidance and data minimisation. However, measures at the level of the digital identity are only effective if the respective technologies are adopted by service providers. The extent to which credentials enhance the citizen's privacy directly depends on the amount of anonymous services that are available.

The public sector should take a pioneering role with regard to credential-based services: as the government acts as an issuer of citizen cards it should also act as an early adopter of anonymous services. By delivering some ser-

vices in an anonymous way as pilot services, the viability of this technology can be demonstrated. Citizens can become acquainted with this new feature of citizen cards and learn how to use digital credentials in electronic transactions. Both service providers and users would have an opportunity to build up trust in the new technology.

With regard to the use of credentials in administrative services, we expect that most administrative services will remain identity-based. An administration will thus offer some of its services in an identified manner and others in an anonymous manner. Despite the availability of credentials, we expect that many government services will in the future nevertheless require the disclosure of an identity. This is mainly because of the many interdependencies that exist between administrative entities. Such interdependencies make it harder to deliver anonymous services. The vision of a fully anonymous administration is discussed in section 8.2. We expect that some services will be provided in an identified and in an anonymous version in parallel. For instance, the social benefits scenario presented in section 6.1.5 may be delivered anonymously with the help of citizen cards. At the same time, citizens who do not want to interact by citizen card can still use the social benefits booklet. There is thus room for a duality of identified and anonymous delivery of a service.

We expect that an important application of credentials as an additional feature of the digital identity will be to create anonymous versions of documents that today still state the identity of the holder. Services that are re-engineered by government for electronic delivery could make use of such credentials. The social security scenario described in section 6.1.5 is an example for such a re-engineered service. We furthermore expect that many credentials will be used not only within administrative services but as well to access services in the private sector.

Once government has demonstrated that credential-based services are feasible, private sector companies can be expected to take up the technology as well. We believe that organisations can obtain an advantage over competition by offering privacy-enhanced services based on credentials. Users who are aware of privacy problems will prefer services that are offered anonymously over those in which they have to disclose their identity. By favouring companies that offer services anonymously, consumers can exert pressure on organisations and accelerate a shift towards privacy-enhanced services. In this way, anonymous services could become a marketing instrument for organisations: after all, an organisation that values the customer's privacy is perceived as more consumer-friendly. We expect that pressure from consumers and privacy organisations may be necessary to motivate providers to

offer services anonymously, as many companies deem personal data important for marketing decisions (see section 8.3).

If anonymous services are to reach their full potential, whole value chains should become anonymous. In scenarios where several organisations are involved in the provision of a service, all services making up the composed service should be anonymous. For instance, buying a book anonymously is impossible unless some financial institution supplies an anonymous payment service and another organisation delivers the goods to the customer without disclosing the customer's identity to the seller. Anonymous e-cash is available today already. In contrast to this, privacy-enhanced shipping services are not available yet, although such services would be easy to implement based on credentials.

As an example, we will consider how the shopping of goods on the Internet can be implemented anonymously. Customers first establish a contract with their preferred parcel service (which entails disclosing their address) and receive a credential from the parcel service. The parcel service also acts as an anonymity revocation manager for this particular credential and can thus map the credential to the customer's address. When the customer buys books in an on-line store, he or she shows the credential issued by the parcel service and pays for the books with anonymous cash. The book store hands the books over to the parcel service together with the transcript of the credential that the customer has shown. The parcel service can determine the customer's address from the credential transcript (by anonymity revocation) and deliver the books to the customer. The book store thus does not learn anything about the customer's identity.

The fact that privacy-enhancing technologies are becoming available creates a need for legitimisation for organisations which want to record personal data in their systems. Technologies for anonymous transactions cannot simply be dismissed anymore as being technically unfeasible. When designing new systems, business analysts will have to consider anonymisation as an option. For the citizen, pseudonymous credentials can thus provide more privacy in service access.

8.2 The Vision of a Fully Anonymous Administration

David Chaum originally envisioned an anonymous transaction system where only a single trustworthy entity knows about a subject's identity. Any organisation a person conducts business with will know the person only under

a pseudonym. With regard to e-government, the question needs to be discussed whether such an approach would be feasible and could lead to a fully anonymous administration. Of course, laws governing administrative processes would have to be adapted in order to move towards a fully anonymous administration. Also, existing information systems would have to be modified, resulting in significant cost and a possibly lengthy transition period.

From a theoretical point of view, one could argue that a credential system such as the one proposed by Camenisch and Lysyanskaya would be suitable to institute a fully anonymous administration. In such a system, the citizen's identity would only be known to a single administrative entity. The registry of births could for example perform this function and issue the root pseudonym to the citizen at the time of birth. After obtaining the root pseudonym, further pseudonyms can then be established with the population register, the income tax administration and so on. A citizen would in such an approach be known to all governmental organisations but the registry of births only under a pseudonym. Each authority would know the citizen under a different pseudonym, thus preventing authorities from linking records concerning a citizen.

While such a concept might seem promising from the perspective of privacy protection, it would be rather difficult to implement in practice. There are several arguments why a fully anonymous administration will not become reality in the near future and why it will possibly never be enacted.

In our opinion, a first severe hindrance to a purely anonymous administration is the need for an equality of paper-based and electronic processes in public administration. Despite the existence of electronic communication channels, a citizen also needs to be able to enter into contact with administration through traditional channels (e.g. by sending a letter). After all, some people may not want to use a citizen card and, more importantly, not all people may be able to use them. However, pseudonymous credentials are impractical to use in paper-based processes. Credential technology is specifically designed for the use in electronic settings and relies on support from information systems to handle the calculations involved in such a system. An exclusive use of digital credentials to model the citizen's digital identity would make it hard - if not impossible - to carry out a process through more traditional channels. Thus, we consider a purely anonymous administration as unpracticable if a parallelism of traditional interactions and electronic interactions is to be achieved.

A further obstacle is that many processes could potentially become harder to use when delivered anonymously. This problem concerns processes where

data has to be exchanged with other administrative entities. Depending on the administrative culture of a country, some services may require an exchange of data with several other administrative entities. If anonymity is to be preserved, data can only be communicated in the form of anonymous credentials. Citizens would have to apply for a multitude of credentials when accessing such services, thus making anonymous services more cumbersome to use. This problem especially applies to services in which data related to family relationships needs to be demonstrated. Documenting such relationships is difficult in anonymous settings, unless specific family credentials are introduced.

These problems are best illustrated by example: In many countries, students can apply for grants that are paid out by government if well-defined conditions are met. Often, grants are only paid to students who meet certain criteria with regard to income and assets and whose parents also meet criteria in terms of income and assets. In an anonymous administrative system, it is hard to prove a fact about one's parents without compromising one's own anonymity or the anonymity of the parents. It would be hard to establish a link between parents and their children unless both the parents' and the child's pseudonyms are divulged. This in turn would re-establish a linkability of records. If several such links between records can be made by an administrative body, anonymity could be destroyed.

Disclosing pseudonyms could be avoided with a credential that proves family relationships: the parents can then obtain a credential that certifies their income and that is issued with respect to the family credential. The parents then pass that credential on to their child. The child subsequently shows the income credential of the parents together with the family credential to document that the income credential indeed belongs to the individual's parents. A citizen would thus have to handle numerous credentials in order to obtain a grant anonymously. In the least it can be said that an anonymous grant application process would be hard to implement and probably lead to a service that is not citizen-friendly at all.

A fully anonymous implementation of administration would also render cross-checks between administrative bodies related to fraud detection unpracticable. Depending on the legal framework of a country, administrative entities may consult data from other entities in order to detect fraud. If administrative records are anonymous, such checks are of course unfeasible. In case of a suspected misbehaviour, the anonymity of a citizen towards all relevant authorities would have to be revoked. From the perspective of administration, an impediment to cross-checks constitutes a strong argument against a fully anonymous administration.

We thus do not expect that administration will ever become fully anony-

mous. There are too many processes that require the combination of data from several sources. For technical reasons, a fully anonymous e-government would presumably only be practicable in a world where all administrative services are accessed electronically. It would presumably make quite a number of processes more complicated in comparison to identity-based processes. We thus expect credentials to be used as a feature that complements existing forms of digital identity and not as the sole means of modelling a citizen's digital identity.

8.3 Barriers to the Implementation of Anonymous Services

In this section we are considering barriers that must be overcome when implementing pseudonymous credentials as part of the citizen's digital identity. Barriers arise from technical issues and from non-technical issues. Both kinds of obstacles must be addressed on the way to implementation. We will first discuss three non-technical barriers:

- **Extent of anonymity:** a first non-technical barrier lies in the fact that a consensus must be reached regarding the extent to which anonymous services and communications are to be implemented. Such a consensus necessitates that society engages in a debate on the values of privacy. Citizens need to be made aware of privacy threats posed by electronic data processing. A debate must focus on the question in what areas anonymity is desirable and where the limits of anonymity will have to be drawn. It is to be expected that such a debate on privacy and anonymity will be led by privacy activists, citizens, politicians, academics and practitioners from the administrative domain alike.

  The extent to which anonymous transactions and communications are desirable must be clearly defined. A clear definition is also important with regard to the anonymous communication infrastructure that forms the basis for anonymous Internet-based transactions. A consensus must be reached delineating whether such an infrastructure shall only be used for credential-based anonymous services or also for anonymous Web surfing in general.

- **Value attributed to personal data:** a second non-technical barrier is the value that private sector companies attribute to personal data. Private sector organisations may not want to migrate towards anonymous transactions, as personal data (from identified transactions) is of-

ten deemed valuable for marketing purposes. Personal data may also be deemed necessary in order to engage in customer relationship management (CRM) activities. The government has no means to force the private sector into offering anonymous services. Unless, of course, privacy laws would be adapted to impose anonymous service delivery wherever possible. Unless such legal changes are implemented, pressure from consumers and privacy organisations may be necessary to bring private sector organisations to offer anonymous services. Notwithstanding, we argue that personalised services and marketing activities would still be possible despite credential-based service delivery: pseudonyms constitute a form of identity that allows personalisation of services without disclosing the customer's identity.

- **International interoperability:**The hardest problem with regard to credential technology concerns the international interoperability of credentials. The interpretation of a credential is dependant on legal concepts of the country in which the credential was issued. A citizen who is eligible for social benefits in one European country is not automatically eligible for benefits in other countries. Consequently, a credential issued in one country may not have the same semantics in another country.

  A good example to illustrate the problem of cross-border use of administrative information is the issue of same-sex marriage. In 1998, the Netherlands have enacted a law that allows same-sex couples to marry. The law affords such couples the same rights as married heterosexual couples. Let us consider a homosexual couple that has got married in the Netherlands and moves abroad. Although legally married in the Netherlands, the couple may not be treated as a married couple in many other EU member states [OvdB01a]. A credential certifying the marital status cannot be reliably interpreted in cross-border scenarios without detailed knowledge about the legal framework of the country of origin.

  As long as legal differences in member states persist, an international interoperability at a semantic level is difficult to implement. More standardisation and harmonisation of administrative cultures and legal frameworks is needed before a cross-border use of credentials becomes possible.

From a technical perspective, three factors may cause problems when implementing credential-based services in the domain of e-government. They concern the adaptation of legacy systems, smart card technology and the

lack of industry standards. These barriers are ordered by their significance, beginning with the problems that we consider the least difficult to solve:

- **Migration of legacy systems and infrastructure:** the majority of today's information systems was designed for transactions involving personal data. Once processes are re-engineered for the use of credentials, existing information systems must be modified accordingly. Administrations who want to act as credential issuers will have to adapt their legacy systems and add additional infrastructure components. This could lead to potentially high cost and to a lengthy transition period towards anonymous services. Systems in both the public and the private sector would have to be adapted. Another problem is the infrastructure for anonymous communication in the Internet. We have stated that such an infrastructure is a prerequisite for anonymous services (see section 4.6). The infrastructure will have to support a high number of concurrent users. Due to the high overhead of mix networks, an anonymising infrastructure on a large scale can be expected to cause higher cost.

- **Smart card technology:** we have stated in section 6.7.5 that today's generation of smart cards can hardly handle the mathematical operations required by advanced credential systems. In order to implement advanced credential systems in smart card environments, the application programming interfaces (APIs) of cards will have to include support for big integer arithmetic. Consequently, standards such as the JavaCard standard would have to be revised. In order to deal with the lack of processing capability, stronger processors or even general purpose cryptographic co-processors will have to be embedded on cards.

- **Lack of standards:** currently, there are no standards yet for credential systems and related protocols. Both governmental and private sector organisations may be reluctant to invest in credential technology unless technical standards exist. Standards are an essential requirement for interoperability between several vendors. A standard has the potential to reduce the danger of vendor-lock in and protect investment in technology. A situation where every country or vendor uses proprietary formats for credentials and protocol messages should be prevented. Standardisation should comprehend credential formats, key lengths and the format of credential protocol messages. The standardisation process could be driven by an organisation such as the World Wide Web Consortium (W3C) or by a consortium consisting of several vendors. We expect that a standard by an industry consortium would

probably be more effective in advancing credential technology, as standardisation processes by standardisation bodies often take a long time. An industry standard that takes up best practices would ensure that products become available soon while maintaining technical interoperability.

8.4 Technological Considerations for an Accelerated Implementation

The concept for an extended digital identity has the potential to enhance the citizen's privacy and to lessen the privacy threats posed by electronic identity cards. However, the concept also poses significant technological and non-technological challenges on the way to an implementation. In this section, we discuss pragmatic trade-offs that can be taken with regard to technology in order to enable a faster deployment of credentials in e-government. The trade-offs concern on the one hand a simpler solution to replace mix networks and on the other hand the use of mobile phones as carrier of a smart card that stores pseudonymous credentials. The use of mobile phones would in particular allow a roll-out of credentials without having to issue an official electronic identity card. Of course, the proposed measures necessitate the introduction of further trust assumptions. Still, the two measures would allow a much faster migration towards credential-based services while only requiring trust assumptions that can be regarded as reasonable.

8.4.1 Anonymising proxies

A first technological trade-off concerns the deployment of mix networks. We have stated that an infrastructure based on mix networks that scales to a large number of users would cause significant costs. We can achieve a reduction of costs and complexity by introducing the assumption that citizens trust their Internet service provider (ISP) not to divulge identities behind IP addresses. We further assume that anonymity is maintained to a large degree even if the provider of an anonymous service can trace an IP address back to a given ISP. Such assumptions allow to replace the mix network by simpler mechanisms. For instance, an ISP (or other trusted entity) could operate a simple anonymising service. Such a service would consist of a single proxy that forwards IP packets between citizens and service providers, thereby masking the citizen's IP address. An alternative solution would be to change the citizen's IP address after every transaction by use of the DHCP

protocol [DL99]. As a drawback, this solution would potentially affect other Internet-based applications that are running on the citizen's machine.

8.4.2 Mobile Phones

The second trade-off concerns the use of mobile phones as a carrier for smart cards. The smart card is inserted into a second card terminal inside the mobile phone. Thereby, credentials are still stored inside the tamper-proof card environment.

The smart card can either contain all elements of the digital identity or merely pseudonymous credentials. Pseudonyms and credentials can be established over the network with the help of a personal computer as a host. The mobile phone communicates with the host computer via the Bluetooth protocol [Blu03]. As a prerequisite for this scenario, the smart card must feature a co-processor to support the mathematical calculations involved in credential systems.

Leveraging mobile phones yields two benefits: most importantly, the mobile phone serves as a trustworthy client terminal and provides a trustworthy user interface. Citizens do not have to trust a service provider's card terminal anymore when using credentials in local settings. In addition, mobile phones are very well accepted. By interacting through their own mobile phone, citizens may build up trust in credential technology faster which in turn can lead to a faster uptake of pseudonymous credentials.

Credentials can be used with the help of the mobile phone in local settings and in Web-based applications:

- **In Web-based applications** the citizen needs a personal computer that features a Bluetooth adapter but in turn does not have to operate a card terminal. The adapter layer must be configured to communicate with the mobile phone instead of with a card terminal. Citizens can then establish pseudonyms, obtain credentials and access credential-based services over the network. It is important that the connection between personal computer and mobile phone is encrypted with a suitable security product. All cryptographic calculations are still executed within the protected card environment.

- **In local settings** (e.g. in the office of an authority), citizens can also establish pseudonyms, obtain credentials or show credentials. Citizens do not have to insert their cards into a card terminal operated by the service provider. Instead, the service provider communicates with

the phone via Bluetooth and indicates the credentials that are to be shown. The citizen merely has to select 'yes' or 'no' in order to show the credentials or not. All dialogues are effected on the citizen's mobile phone.

The use of Bluetooth as a protocol for the communication between host computer and mobile phone does not affect the anonymity of the citizen. As of version 1.2, the Bluetooth protocol provides a the so-called 'Anonymity Mode' that masks the unique Bluetooth hardware address of a device [Blu03]. Bluetooth is thus well-suited as a protocol between host and mobile phones in conjunction with pseudonymous credential technology.

However, the use of mobile phone technology impacts the anonymity of the citizen, as phone users are not anonymous towards their network provider (unless by use of an anonymous pre-paid phone card). The network provider is able to tell in which cell of the network a user currently is (provided the phone is switched on and within reach of the network). Anonymity is thus compromised to a certain degree.

The technological trade-offs thus affect trust assumptions in the sense that additional trust assumptions become necessary on the part of the citizen. Citizen's must trust their ISP (respectively the provider of the proxy server) not to divulge connection data. Similarly, citizens must trust their network provider not to pass on location data to third parties. We consider both trust assumption as reasonable.

At the same time, these trade-offs can be expected to enable a faster migration towards credential-based services, as complexity is reduced and infrastructure cost is lowered. In particular, these modifications would solve the problem that citizens have to trust card terminals in local services. Also, we expect that the use of mobile phones will positively impact the acceptance and uptake of credential-based service provision. Of course, pilot projects will have to be undertaken to find out about the average citizen's readiness to trade security for usability. However, an accelerated uptake and an increased acceptance through the use of mobile phones would be a particularly important benefit, as privacy-enhancing technologies are only effective if they are indeed leveraged by citizens.

8.5 Summary

Credentials as part of the citizen's digital identity are an enabling technology for anonymous services. Since government acts as citizen card issuer, it should also act as an early adopter of credential technology and offer

credential-based services. Once public sector services make successful use of credentials, private sector companies can be expected to follow.

We presume that the majority of public services will remain identity-based. A fully anonymous administration is unlikely to be implemented for several reasons: first and foremost, a fully anonymous administration based on pseudonymous credentials would probably necessitate the exclusive use of electronic service access. All citizens would have to use citizen cards in order to interact with administration. Furthermore, many administrative services are potentially hard to implement anonymously and could result in a service that is harder to use than its identity-based counterpart. However, we expect that credentials will be widely used to create anonymous versions of documents that today state the citizen's identity. Such credentials can be used in many processes in the private sector.

There are of course, also certain barriers to the implementation of credentials. A first hurdle to be surmounted is a consensus on the extent to which anonymity is desirable in electronic systems. Another obstacle may be the acceptance on the side of service providers. As private sector companies are interested in keeping personal data for purposes of data mining, pressure from consumers and privacy activists may be necessary to accelerate a migration. From a technical perspective, potential obstacles are the large number of legacy systems that would have to be modified, the lack of processing power on current smart cards and the current lack of standards with regard to technology. Much harder than these technological problems is the problem of international interoperability: before credentials issued by government can be used in cross-border transaction, a further harmonisation of legislation between participating countries is necessary.

Chapter 9

Conclusions and Further Research

This final chapter summarises the thesis and presents the conclusions from this work. An overview on the scientific contributions has already been given in section 1.1 and shall not be repeated here. As an outlook, we suggest issues for further research in the field of anonymous digital identity.

9.1 Conclusions

Digital identity cards are already in productive use in European countries. The current generation of electronic identity cards aims to provide a strong form of authentication for use in electronic transactions, coupled with the ability of issuing digital signatures. However, we have argued that these multi-application digital identity cards also pose a threat to the privacy of citizens. All of today's electronic identity cards model the digital identity of the citizen solely with an authentication and a signature certificate. As these cards are to be used in a multitude of applications ranging from e-government to e-commerce and possibly in the future e-health, there is the danger that citizens will leave a dense transaction trail when using these cards. Such a trail potentially allows service providers to link all transactions by a given card.

In order to offset some of these privacy dangers posed by electronic identity cards, we propose that digital identity should be extended by an anonymous component. We thus propose that the digital identity should not only be modelled with elements that disclose the holder's identity but also with elements that describe a subject's characteristics in an anonymous way. This leads to a concept of digital identity that differs from the approach taken

by the current European identity card initiatives. Including an anonymous component enables support for an anonymous service access with the help of citizen cards.

Such an anonymous component can be implemented with the use of pseudonymous credentials. Pseudonymous credentials allow a subject to prove a statement made by a third party in an anonymous and trustworthy way. Furthermore, subjects can establish pseudonyms for settings in which a provider needs to recognise a subject in subsequent accesses to an e-service. Pseudonymous credentials bring several benefits: first and foremost, anonymous services are the most effective way to prevent the creation of personal data. As every credential only describes a single attribute of a subject, they allow a citizen to only disclose the exact set of attributes that is needed for a given service. Credentials thus also pertain to data minimisation. We have consequently argued that pseudonymous credentials have the potential to enhance the citizen's privacy and that they are to be included as a part of the digital identity. In order to maintain strong trust relationships in anonymous settings, an anonymous form of digital identity needs to be revocable. This implies that the identity of a citizen who behaves in unlawful ways can be discovered by a trusted third party.

A digital identity based on pseudonymous credentials allows both public and private sector organisations to act as credential issuers and to offer credential-based services. A credential issuer needs to publish policy documents that describe the semantics of credentials and the practices that are followed in the issuing process. Furthermore, we propose a credential information base that contains information directed at the end-user. Credential issuers whose credentials implement a revocable form of anonymous identity also need to appoint an anonymity revocation manager. This entity can be an organisation that is part of government, a private sector organisation or even a religious organisation. Such an entity must be trusted by credential issuers, citizens and service providers alike.

Our concept of an extended digital identity proposes that a citizen card is to be equipped with an identity manager that manages the life-cycle of credentials. As a new functionality for citizen cards, the identity manager also provides identity information management functionality: any access to identity elements is logged in order to allow citizens to keep track of where and when they have used their digital identity.

The credential system by Camenisch and Lysyanskaya is currently the most advanced pseudonymous credential system. However, today's low-cost smart cards cannot handle such advanced systems yet. Additional processing capabilities will have to be added and APIs will have to be adapted to support a wider range of algorithms. We have evaluated other ways of

storing pseudonymous credentials in order to overcome the limited resources of smart card environments. Storing credentials in a network-based storage limits functionality and is undesirable for security reasons. Other devices such as mobile phones and PDAs do not provide adequate security features yet to act as a manager of pseudonymous credentials.

Conceptual issues regarding the use of credentials were discussed: we have considered ways to achieve the non-transferability of credentials and have recommended that non-transferability is to be achieved by use of a tamper-proof environment. With regard to a credential namespace, we advocate that a federated, hierarchical name space is chosen so that credential issuers are completely free to choose which attributes to certify. Several methods for the revocation of pseudonymous credentials were assessed. We conclude that there are no algorithms yet that are suitable for an implementation on citizen cards and that scale to a large number of revoked credentials. In order to heighten the usability of credential systems, we have recommended measures to automate storage of pseudonyms and credentials as far as possible. We have also suggested design measures that minimise the decisions that need to be taken when showing a credential.

We have proposed an architecture for the use of credentials in Web based services. The architecture builds on the Java 2 Enterprise Edition, uses Web services for communications related to credential protocols and a Web browser as a front end. A component-based architecture can enable organisations who wish to migrate towards credential-based services to purchase components that encapsulate the credential-related aspects of applications. Web services can facilitate the migration towards a service-based architecture.

We perceive credentials as an additional means to model digital identity. Credentials are beneficial to deliver governmental services anonymously. However, we do not expect that administration will ever become fully anonymous. Much rather we expect that credentials will be used to selectively deliver some services anonymously. Credentials will also be used to create anonymous electronic counterparts of administrative documents that today state the identity of the holder. Such credentials can then be used in a wide range of private sector services.

There are also barriers to the implementation of the proposed concept. Before such a concept can be implemented on a large scale, a consensus must be reached regarding the extent to which anonymity is desirable. With regard to technical barriers, standards regarding credential formats and protocols must first be created in order to protect investments in technology and to promote interoperability. Further obstacles are the large number of legacy

systems that would have to be modified and the lack of processing power on current smart cards. A cross-border use of credentials would necessitate further legal harmonisation efforts by participating countries.

This thesis has focused on conceptual and technical issues regarding anonymous service access. We expect that the anonymous delivery of governmental e-services will be subject to further research in the future. In the next section, we thus present topics for further research activities in the area of credential-based services.

9.2 Further Research

We propose topics that we deem to be important for further research on privacy and anonymity in e-government. As privacy is an interest and depends on personal values, further research should also address social aspects. Our proposals for further research issues comprise both technical and non-technical aspects related to anonymous services:

- **Legal and social aspects:** we have mentioned that a consensus needs to be reached regarding the extent of anonymity in e-services. With regard to social aspects of anonymous transactions, an important research question is to what degree citizens want anonymity and to what extent they are willing to deal with additional technology in order to enhance privacy. A migration towards more anonymous services will also have to be reflected in the legal system. The legal perspective thus also needs to be taken into account.

- **Usability:** in section 6.7.4 we have proposed measures to improve the usability of credential systems. As credential systems have not yet been deployed in any mass-market applications (they have in fact hardly been used outside research institutions), little is known regarding how well average end-users can handle credential technology. Usability tests should be conducted on a larger scale with users from different backgrounds. Such evaluations with a representative set of users are necessary in order to gain a clear understanding of how user interfaces can be made more citizen-friendly. A high degree of usability is a prerequisite for an actual deployment of credential technology in e-government.

- **Administrative process re-engineering:** this thesis has mostly adopted a technical view on pseudonymous credentials. With regard to administrative processes in the governmental domain, researchers and experts from administration should scrutinise processes whether they

can be re-engineered for an anonymous or pseudonymous provision. A further research topic are anonymous versions of administrative documents respectively the question which personal documents should be issued in an anonymous version.

- **Smart card technology**: the current generation of smart cards is equipped with microprocessors that can hardly handle the complexity of advanced credential systems. Although cryptographic co-processors have been available for several years, they only support a limited range of algorithms that are commonly used for digital signature schemes and for symmetric encryption of data (e.g. RSA and DES). In order to implement pseudonymous credential systems such as the one by Camenisch and Lysyanskaya on smart cards, stronger processing capacities are necessary. One possible solution could be to add general-purpose cryptographic co-processors that accelerate a wider range of mathematical operations. A particular challenge is to provide stronger processing capacity without incurring high additional cost.

- **Efficient implementation of pseudonymous credential systems:** research in the area of cryptographic algorithms should address new ways of implementing pseudonymous credential systems respectively ways of implementing credential systems more efficiently. It is desirable to lower the mathematical complexity of such systems. Research could e.g. be directed at finding more efficient ways to implement zero-knowledge protocols. More efficient algorithms could also lead to smaller credential sizes while maintaining security. Both credential sizes and mathematical complexity are prime concerns with regard to a credential implementation in resource-restricted environments such as smart cards.

With the ongoing migration towards digital identity cards, we expect that privacy will become an issue of growing importance. We hope that this work will elicit further research activities in this field by highlighting that digital identity can in part also be implemented anonymously. We expect that the topic of anonymous digital identity will enjoy growing attention in the future and become an issue of increasing importance for researchers in the domain of e-government.

Appendix A

Abbreviations

ACL	Access Control List
ABAC	Attribute-based access control
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
APPEL	A P3P Preference Exchange Language
ASN.1	Abstract Syntax Notation One
BIOS	Basic Input Output System
CA	Certification Authority
CBAC	Certificate-based access control
CIB	Credential Information Base
CMP	Container-Managed Persistence
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CRM	Customer Relationship Management
Cryptoki	Cryptographic Token Interface (PKCS #11)
CSCW	Computer-supported Cooperative Work
DBMS	Database Management System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNA	Deoxyribose Nucleic Acid
DSA	Digital Signature Algorithm
DTO	Data Transfer Object
ECC	Elliptic Curve Cryptography
eEpoch	eEurope Smart Card Charter Proof of Concept
EEPROM	Electrically Erasable and Programmable Read-only Memory
EJB	Enterprise Java Beans

ERM	Electronic Records Management
eESC	eEurope Smart Card Charter
FAR	False Acceptance Rate
FASME	Facilitating Administrative Services for Mobile Europeans
FRR	False Rejection Rate
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
Idemix	Identity Mix
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Information Society Technology
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
J2EE	Java 2 Platform, Enterprise Edition
J2ME	Java 2 Platform, Micro Edition
J2SE	Java 2 Platform, Standard Edition
JDBC	Java Database Connectivity
JMS	Java Message Service
JSP	Java Server Pages
OASIS	Organisation for the Advancement of Structured Information Standards
OCSP	On-line Certificate Status Protocol
ODBMS	Object Database Management System
OECD	Organization for Economic Cooperation and Development
ORB	Object Request Broker
PC	Personal Computer
PCP	Pseudonymous Credential Policy
PCPS	Pseudonymous Credential Practice Statement
PDA	Personal Digital Assistant
PET	Privacy-enhancing Technologies
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure

P3P	Platform for Privacy Preferences
RA	Registration Authority
RAM	Random Access Memory
RDF	Resource Description Framework
ROM	Read-only Memory
RSA	Rivest, Shamir, Adleman
SAML	Security Assertions Markup Language
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TCPA	Trusted Computing Platform Alliance
TLS	Transport Layer Security
TPL	Trust Policy Language
TPM	Trusted Platform Module
UDDI	Universal Description, Discovery and Integration
UMTS	Universal Mobile Telecommunications System
W3C	World Wide Web Consortium
WORM	Write Once Read Many
WSDL	Web Services Description Language
WWW	World Wide Web
XML	Extensible Markup Language
XSL	Extensible Style Sheet Language
XSLT	Extensible Style Sheet Language Transformation

Bibliography

All on-line references have been revisited in January 2004.

[ACJT00] Giuseppe Ateniese, Jan Camenisch, Marc Joyce, and Gene Tsudik. A Practical and Provably Secure Coalition-resistant Group Signature Scheme. In Mihir Bellare, editor, *Advances in Cryptology - CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 255–270. Springer, Berlin, 2000.

[ACR99] Mark S. Ackermann, Laurie F. Cranor, and Joseph Reagle. Privacy in e-Commerce: Examining User Scenarios and Privacy Preferences. In Stuart Feldman and Michael Wellmann, editors, *Proceedings of the 1st ACM Conference on Electronic Commerce*. ACM Press, Denver, Colorado, 1999.

[AM02] Niklas Auerbach and Nico Maibaum. FASME - A Step Towards European E-Government Solutions. In Stanislaw Wrycza, editor, *Proceedings of ECIS 2002*. Gdansk, 2002.

[And02] Ross Anderson. TCPA and Palladium Frequently Asked Questions. Available from: http://www.againsttcpa.com/what-is-tcpa.html, 2002.

[Ash00] Julian Ashbourn. *Biometrics: Advanced Identity Verification: The Complete Guide*. Springer, London, 2000.

[Aue03] Niklas Auerbach. Smart Card Support for Anonymous Citizen Services. In Pedro Isaias, editor, *Proceedings of e-Society 2003*. IADIS Press, Lisbon, 2003.

[Bah97] Anke Bahl. *Zwischen On- und Offline. Identität und Selbstdarstellung im Internet*. KoPäd, München, 1997.

[BBC02] BBC News, 4.7.2002. State Racism Fears Over ID Cards. Available from: http://news.bbc.co.uk/1/uk_politics/2094000.stm, 2002.

[BBC03] BBC News, 19.6.2003. Public Oppose ID Card Scheme. Available from: http://news.bbc.co.uk/2/hi/technology/3004376.stm, 2003.

[BdM94] Josh C. Benaloh and Michael de Mare. One-Way Accumulators: A Decentralized Alternative to Digital Signatures (Extended Abstract). In Tor Helleseth, editor, *Advances in Cryptology - Eurocrypt '93*, volume 765 of *Lecture Notes in Computer Science*, pages 274–285. Springer, Berlin, 1994.

[Ber00] Hal Berghel. Identity Theft, Social Security Numbers and the Web. *Communications of the ACM*, 43(2):17–21, 2000.

[BFK99] Matt Blaze, Joan Feigenbaum, and John Keromyzis. The Role of Trust Management in Distributed Systems Security. In Jan Vitek and Christian D. Jensen, editors, *Secure Internet Programming*, volume 1603 of *Lecture Notes in Computer Science*, pages 185–210. Springer, Berlin, 1999.

[BFK01] Oliver Berthold, Hannes Federrath, and Stefan Köpsel. Web MIXes: A System for Anonymous and Unobservable Internet Access. In Hannes Federrath, editor, *Designing Privacy Enhancing Technologies. International Workshop on Design Issues in Anonymity and Unobservability*, volume 2009 of *Lecture Notes in Computer Science*, pages 113–129. Springer, Berlin, 2001.

[BG02] Heide Brücher and Michael Gisler. E-Government - von den Grundlagen zur Anwendung. In Andreas Meier, editor, *E-Government. HMD - Praxis der Wirtschaftsinformatik, Band 226*. Dpunkt, Heidelberg, 2002.

[Blu03] Bluetooth Special Interests Group. Specification of the Bluetooth System, Version 1.2, November 2003. Available from: http://www.bluetooth.com, 2003.

[Bür03] Urs Bürge. Digitale Identität und eID-Karte - Das Projekt einer schweizerischen elektronischen Identitätskarte. In Hanna Muralt Müller, Andreas Auer, and Thomas Koller, editors, *E-Voting*. Staempfli, Bern, 2003.

[Bra00] Stefan Brands. *Rethinking Public Key Infrastructure and Digital Certificates - Building in Privacy.* MIT Press, Cambridge, Massachusetts, 2000.

[BS01a] Glenn B. Bell and Anil Sethi. Matching Records in a National Medical Patient Index. *Communications of the ACM*, 44(9):83–88, 2001.

[BS01b] Emmanuel Bresson and Jacques Stern. Efficicent Revocation in Group Signatures. In Kim Kwangjo, editor, *Public Key Cryptography. Proceedings of 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2001*, volume 1992 of *Lecture Notes in Computer Science*, pages 190–206. Springer, Berlin, 2001.

[Bun03] Bundesministerium des Innern, Bundesrepublik Deutschland. BundOnline 2005. Available from: http://www.bund.de/BundOnline2005.6164.htm, 2003.

[Bur03] Better Business Bureau. BBB On Line Privacy Seal. Available from: http://www.bbbonline.org/privacy/, 2003.

[Cab03] Cabinet Office. Identity Fraud: A Study. Available from: http://www.homeoffice.gov.uk/docs/id_fraud_report.pdf, 2003.

[Cam98] R.D. Campbell, editor. *Collins English Dictionary.* Harper Collins, Glasgow, 1998.

[Cap02a] Cap Gemini Ernst & Young. Web-based Survey on Electronic Public Services. Results of the First Measurement October 2001. Available from: http://verdi.unisg.ch/org/idt/ceegov.nsf, 2002.

[Cap02b] Cap Gemini Ernst & Young. Web-based Survey on Electronic Public Services. Results of the Second Measurement April 2002. Available from: http://verdi.unisg.ch/org/idt/ceegov.nsf, 2002.

[Cap03] Cap Gemini Ernst & Young. Web-based Survey on Electronic Public Services. Results of the Third Measurement October 2002. Available from: http://verdi.unisg.ch/org/idt/ceegov.nsf, 2003.

[Cap04] Cap Gemini Ernst & Young. Online Availability of Public Services: How is Europe Progressing? Web-based Survey on Electronic Public Services. Report of the Fourth Measurement October 2003. Available from: http://europa.eu.int/

information_society/eeurope/2005/doc/highlights/whats_new/capgemini4.pdf, 2004.

[Cat97] Fred H. Cate. *Privacy in the Information Age*. Brookings Institution Press, Washington D.C., 1997.

[Cav97] Ann Cavoukian. Identity Theft: Who's Using Your Name? Available from: http://www.ipc.on.ca, 1997.

[CE87] David Chaum and Jan-Hendrik Evertse. A Secure and Privacy-protecting Protocol for Transmitting Personal Information Between Organizations. In Andrew M. Odlyzko, editor, *Advances in Cryptology - CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 118–167. Springer, Berlin, 1987.

[CEN00] CEN - European Committee for Standardization. Smart Card Systems: Interoperable Citizen Services: User Related Information: Workshop Agreement CWA 13987-1. Available from: http://www.cenorm.be/isss, 2000.

[CG02] Sébastien Canard and Marc Girault. Implementing Group Signature Schemes With Smart Cards. In Peter Honeyman, editor, *Smart Card Research and Applications. Proceedings of CARDIS 2002*. Kluwer Academic Publishers, Bristol, 2002.

[Cha81] David L. Chaum. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[Cha85] David Chaum. Security Without Identification: Transaction systems to Make Big Brother Obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[CL01] Jan Camenisch and Anna Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, Berlin, 2001.

[CL02] Jan Camenisch and Anna Lysyanskaya. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 61–76. Springer, Berlin, 2002.

[Cla93] Roger Clarke. Computer Matching and Digital Identity. Proceedings of the Computers, Freedom and Privacy Conference, San Francisco. Available from: http://www.cpsr.org/conferences/cfp93/clarke.html, 1993.

[CM98] Jan Camenisch and Markus Michels. A Group Signature Scheme with Improved Efficiency (extended abstract). In Kazuo Ohta and Dingyi Pei, editors, *Advances in Cryptology - ASIACRYPT '98*, volume 1514 of *Lecture Notes in Computer Science*, pages 160–174. Berlin, 1998.

[CM01] Clemens H. Cap and Nico Maibaum. Digital Identity and its Implications for Electronic Government. In Beat Schmid, Katarina Stanoevska-Slabeva, and Volker Tschammer, editors, *Towards the E-Society: IFIP Conference on E-Commerce, E-Business and E-Government*, pages 803–816. Kluwer Academic Publishers, Boston, 2001.

[CMH01] Clemens H. Cap, Nico Maibaum, and Lars Heyden. Extending the Data Storage Capabilities of a Java-based Smartcard. In *Proceedings of the 6th IEEE Symposium on Computers and Communications*. 2001.

[CMH02] Clemens H. Cap, Nico Maibaum, and Lars Heyden. JavaCard-kontrollierter, sicherer Zugriff auf persönliche Dokumente und Berechtigungen. In Sigrid Schubert, Bernd Reusch, and Norbert Jesse, editors, *Informatik bewegt: Informatik 2002 - 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI)*, pages 433–436. Köllen, Bonn, 2002.

[CvH91] David Chaum and Eugene van Heyst. Group Signatures. In Donald W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science*, pages 257–265. Springer, Berlin, 1991.

[Dat97] Data Protection Commissioner Berlin. Arbeitspapier Datenschutzfreundliche Technologien. Available from: http://www.datenschutz-berlin.de/to/datenfr.htm, 1997.

[Dav01] Simon Davies. Reckless ID Card Plan Will Destroy Nation's Freedom. Daily Telegraph, 29 September, 2001.

[Del00] Deloitte & Touche. Through the Portal. Available from: http://www.deloittte.com/dt, 2000.

[DH76] Whitfield Diffie and Martin E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DL99] Ralph Droms and Ted Lemon. *The DHCP Handbook: Understanding, Deploying, and Managing Automated Configuration Services*. Macmillan Technical Publishing, Indianapolis, 1999.

[Dör90] Nicola Döring. *Sozialpsychologie des Internet. Die Bedeutung des Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen und Gruppen*. Hogrefe, Göttingen, 1890.

[Eck01] Claudia Eckert. *IT-Sicherheit: Konzepte, Verfahren, Protokolle*. Oldenbourg, München, 2001.

[eEu99] eEurope Smart Card Charter Steering Committee. The eEurope Smart Card Charter. Available from: http://www.eeuropesmartcards.org, 1999.

[EG85] Taher El Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In George Blakley and David Chaum, editors, *Advances in Cryptology - CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer, Berlin, 1985.

[ELPW03] Paul England, Butler Lampson, Marcus Peinado, and Bryan Willman. A Trusted Open Platfrom. *IEEE Computer*, 44(2):55–62, 2003.

[EN01] Tommi Elo and Pekka Nikander. Decentralized Authorization with ECDSA: A Software Implementation. In Josep Domingo-Ferrer, David Chan, and Anthony Watson, editors, *Smart Card Research and Advanced Applications*. Kluwer Academic Publishers, Boston, 2001.

[Etz99] Amitai Etzioni. *The Limits of Privacy*. Basic Books, New York, 1999.

[Eur95] European Parliament and the Council of the European Union. Directive 95/46/EC On the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

[Eur99] European Parliament and the Council of the European Union. Directive 99/93/EC On a Community Framework for Digital Signatures, 1999.

[Eur02a] European Commission. From Policy to Practice. Conference on e-Government 7-8 July 2003, Como, Italy. Available from: http://www.europa.eu.int/information_society/eeurope/egovconf/index_en.htm, 2002.

[Eur02b] Eurostat - Statistical Office of the European Communities. E-Commerce in Europe. Results of the Pilot Surveys Carried out in 2001, 2002.

[Eur02c] Eurostat - Statistical Office of the European Communities. Statistics in Focus: Internet and Mobile Phone Usage in the European Union. Eurostat Report KS-NP-02-008-EN-N, 2002.

[Eve92] David Everett. Identity Verification and Biometrics. In K.M. Jackson and J. Hruska, editors, *Computer Security Reference Book*, pages 147–169. Butterworth Heinemann, Oxford, 1992.

[FP97] Hannes Federrath and Andreas Pfitzmann. Bausteine zur Realisierung mehrseitiger Sicherheit. In Günther Müller and Andreas Pfitzmann, editors, *Mehrseitige Sicherheit in der Kommunikationstechnik*, pages 83–104. Addison Wesley Longman, Bonn, 1997.

[Gel98] Robert Gellman. Does Privacy Work? In Philipp Agre and Marc Rothenberg, editors, *Technology and Privacy: The New Landscape*, pages 193–218. MIT Press, Cambridge, Massachussetts, 1998.

[Gen01] Mario Gentili. Italian Electronic Identity Card - Principle and Architecture. In Peter M. G Apers, Paolo Atzeni, Stefano Ceri, Stefano Paraboschi, Kotagiri Ramamohanarao, and Richard T. Snodgrass, editors, *VLDB 2001, Proceedings of 27th International Conference on Very Large Data Bases, Roma, Italy*, pages 629–632. Morgan Kaufmann, San Francisco, 2001.

[Ges00] Gesellschaft für Informatik e.V., Fachausschuss Verwaltungsinformatik und Fachbereich 1 der informationstechnischen Gesellschaft im VDE. Electronic Government als Schlüssel zur Modernisierung von Staat und Verwaltung.

Available from: http://www.gi-ev.de/informatik/presse/presse_memorandum.pdf, 2000.

[GGMM97] Eran Gabber, Philipp B. Gibbons, Yossi Matias, and Alan Mayer. How to Make Personalized Web Browsing Simple, Secure, and Anonymous. In Rafael Hirschfeld, editor, *Proceedings of the First International Conference on Financial Cryptography*, volume 1318 of *Lecture Notes in Computer Science*, pages 17–32. Springer, 1997.

[Gid91] Anthony Giddens. *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford University Press, Palo Alto, 1991.

[Gis01] Michael Gisler. Einführung in die Begriffswelt des eGovernments. In Michael Gisler and Dieter Spahni, editors, *eGovernment: Eine Standortbestimmung*. Haupt, Bern, 2001.

[GK02] Karin Gräslund and Helmut Krcmar. Anonymität. In Gerhard Schwabe, Norbert Streitz, and Rainer Unland, editors, *CSCW Kompendium. Lehr- und Handbuch zum computerunterstützten kooperativen Arbeiten*, pages 429–437. Springer, Berlin, 2002.

[Gla03] Glasner, Joanna. 9-Digit Social Overused as ID. Wired News, 29 January 2003. Available from: http://www.wired.com/news/privacy, 2003.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[Gor92] Ken Gormley. One Hundred Years of Privacy. *Wisconsin Law Review*, (1335), 1992.

[GPR98] Oded Goldreich, Birgit Pfitzmann, and Ron L. Rivest. Self-Delegation with Controlled Propagation - or - What If You Lose Your Laptop. In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 153–168. Springer, Berlin, 1998.

[GPS98] Gunther Gattung, Ulrich Pordesch, and Michael J. Schneider. *Der mobile persönliche Sicherheitsmanager. Technischer Bericht 24*. GMD - Forschungszentrum Informationstechnik GmbH, Darmstadt, 1998.

[Grä01] Karin Gräslund. *Anonymitätseffekte bei der Groupware-Nutzung*. Deutscher Universitäts-Verlag, Wiesbaden, 2001.

[GS01] Michael Gisler and Dieter Spahni. *eGovernment: Eine Standortbestimmung*. Haupt, Bern, 2001.

[GtMJ01] Daniela Gerd tom Markotten and Uwe Jendricke. Identitätsmanagement im e-Commerce. *it + ti Informationstechnik und technische Informatik*, 43(5):236–245, 2001.

[Gui03] Bruno Guissani. You're in the Picture. Time Magazine, 24 February, pages 46-47, 2003.

[HM01] Amir Herzberg and Yosi Mass. Relying Party Credentials Framework. In David Naccache, editor, *Topics in Cryptology - CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 328–343. Springer, Berlin, 2001.

[HMM+01] Amir Herzberg, Yosi Mass, Joris Mihaeli, Dalit Noar, and Ravid Yiftach. Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers. In Michael Reiter and Roger Needham, editors, *IEEE Symposium on Security and Privacy, 2000*, pages 2–14. 2001.

[Hol02] Anna Holmes. Consultation Document for a Future Policy Paper on pan-European Government e-Services. Available from: http://europa.eu.int/ISPO/ida/export/files/en/1359.pdf, 2002.

[HTJ89] Starr Roxanne Hiltz, Murray Turoff, and Kenneth Johnson. Experiments in Group Decision Making, 3: Disinhibition, Deindividuation, and Group Process in Pen Name and Real Name Computer Conferences. *Decision Support Systems*, 5:217–232, 1989.

[ISO97] ISO - International Organisation for Standardization. ISO/IEC 7816-3: Information Technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols, 1997.

[ITU88] ITU-T - International Telecommunication Union - Telecommunication Standardization Sector. *Recommendation X.509: The Directory Authentication Framework*. ITU, Geneva, 1988.

[ITU03] ITU - International Telecommunication Union. Workshop on Challenges, Perspectives and Standardization Issues in e-Government, 5-6 June 2003. Available from: http://www.itu.int/itudoc/itu-t/workshop/e-gov/egov-prg.pdf, 2003.

[Jam90] William James. *Principles of Psychology, Volume I*. Henry Holt, New York, 1890.

[Jen03] Uwe Jendricke. *Sichere Kommunikation zum Schutz der Privatsphäre durch Identitätsmanagement*. Rhombos, Berlin, 2003.

[JGAS02] James Joshi, Arif Ghafoor, Walid G. Aref, and Eugene H. Spafford. Security and Privacy Challenges of Digital Government. In William J. McIver and Ahmed K. Elmagarmid, editors, *Advances in Digital Government*, pages 121–136. Kluwer Academic Publishers, Dordrecht, 2002.

[JM98] Deborah G. Johnson and Keith Miller. Anonymity, Pseudonymity, or Inescapable Identity on the Net. In *Proceedings of the Ethics and Social Impact Component on Shaping Policy in the Information Age*, pages 37–38, Washington, D.C., 1998. ACM Press.

[Kah02] Randolph Kahn. What is a Record? *e-Doc, Journal of the Association for Information and Image Management International*, 16(5):26–29, 2002.

[Köh00] Marit Köhntopp. Generisches Identitätsmanagement im Endgerät. In Rüdiger Grimm and Alexander Röhm, editors, *GI Workshop Sicherheit und Electronic Commerce - WSSEC 2000*. Köllen, Bonn, 2000.

[Kir03a] András Kiraly. Credential-Based Implementations of Digital Identity for Non-Traceable Access to E-Government-Services. Diplomarbeit. Institut für Informatik, Universität Zürich, 2003.

[Kir03b] András Kiraly. A Protoypical Implementation of a BigInteger Library on the Java Card Platform. Semesterarbeit. Institut für Informatik, Universität Zürich, 2003.

[KP98] Joe Kilian and Erez Petrank. Identity Escrow. In Hugo Krawczyk, editor, *Advances in Cryptology - CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 169–185. Springer, Berlin, 1998.

[KP01] Marit Köhntopp and Andreas Pfitzmann. Informationelle Selbsbestimmung durch Identitätsmanagement. *it + ti Informationstechnik und technische Informatik*, 43(5):227–235, 2001.

[LB90] Klaus Lenk and Martin Brüggemeier. Neue Informationsdienste als Bürgerservice. In J. Goller, H. Maack, and B. Müller-Hedrich, editors, *Verwaltungsmanagement. Handbuch für öffentliche Verwaltungen und öffentliche Betriebe*. Raabe, Stuttgart, 1990.

[Len92] Klaus Lenk. Servicebündelung in der Kommunalverwaltung durch 'Bürgerbüros'. *Wirtschaftsinformatik*, 34(06):567–576, 1992.

[Len99] Klaus Lenk. Electronic Government als Schlüssel zur Innovation der öffentlichen Verwaltung. In Klaus Lenk and Roland Traunmüller, editors, *Öffentliche Verwaltung und Informationstechnik - Perspektiven einer radikalen Neugestaltung der öffentlichen Verwaltung mit Informationstechnik*, pages 127–146. Decker, Heidelberg, 1999.

[Lib03] Liberty Alliance. The Liberty Alliance Project. Available from: http://www.projectliberty.org, 2003.

[LK03] Heiko Ludwig and Roland Klüber. Preface to the Special Section on Web Services. *Electronic Markets*, 13(2):104–107, 2003.

[Loc02] Local Government Association, United Kingdom. The Implementation of Electronic Voting in the UK. Available from: http://www.lga.gov.uk, 2002.

[LRSW99] Anna Lysyanskaya, Ron L. Rivest, Amit Sahai, and Stefan Wolf. Pseudonym Systems. In Howard Heys and Carlisle Adams, editors, *Selected Areas in Cryptography*, volume 1758 of *Lecture Notes in Computer Science*, pages 184–199. Springer, Berlin, 1999.

[LT02] Klaus Lenk and Roland Traunmüller. eGovernment - Ein Wegweiser. *eGov Präsenz*, 2002(01):3–6, 2002.

[Mar80] James E. Marcia. Identity in Adolescence. In Joseph Adelson, editor, *Handbook of Adolescent Psychology*. Wiley Interscience, New York, 1980.

[Max02] Maxim Dallas Semiconductor. iButton Overview. Available from: http://www.ibutton.com/ibuttons/index.html, 2002.

[MCH+01] Nico Maibaum, Clemens H. Cap, Lars Heyden, Reinhard Riedl, and Anne-Marie Oostveen. FASME Deliverable 5.1: Final Report on the Prototype of the Complete JavaCard Middleware. Technical report, Nettetal/Brussels, 2001.

[ME02] William J. McIver and Ahmed K. Elmagarmid. *Advances in Digital Government*. Kluwer Academic Publishers, Dordrecht, 2002.

[Mic03] Microsoft Corporation. Microsoft .NET Passport. One Easy Way to Sign in Online. Available from: http://www.passport.net, 2003.

[MR02] Thomas Menzel and Peter Reichstädter. The Role of Citizen Cards in e-Government. In Klaus Lenk and Roland Traunmüller, editors, *Electronic Government, First International Conference, EGOV 2002*, volume 2456 of *Springer Lecture Notes in Computer Science*, pages 446–455. Springer, Berlin, 2002.

[MS03] Joel Meir and Dieter Spahni. Web Services in der öffentlichen Verwaltung. *eGov Präsenz*, (02/2003):13–15, 2003.

[MSV01] Ambros Marzetta, Raoul Stöckle, and Oliver Vaterlaus. Braucht die Schweiz einen amtlichen digitalen Ausweis? Available from: http://www.ofj.admin.ch/themen/riir/digid/studiedigiausweisd.pdf, 2001.

[MvOS96] Alfred J. Menezes, Paul C. van Oorschot, and Vanstone A. Scott. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1996.

[NA02] Zoltán Nochta and Sebastion Abeck. Sichere und effiziente Zugriffskontrolle mit PAMINA. In Sigrid Schubert, Bernd Reusch, and Norbert Jesse, editors, *Informatik bewegt: Informatik 2002 - 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI)*, pages 445–448. Köllen, Bonn, 2002.

[Nak98] Lisa Nakamura. Race In/For Cyberspace: Identity Tourism and Racial Passing on the Internet. In Victor J. Vitanza, editor, *CyberReader*. Pearson Allyn & Bacon, Needham Heights, 1998.

[Nie93] Jakob Nielsen. *Usability Engineering*. Academic Press, San Diego, 1993.

[Nor03] Eric Norlin. The Coming of Digital Identity. Available from: http://www.digitalidworld.com, 2003.

[NT00] Khan Quoc Nguyen and Jacques Traore. An Online Public Auction Protocol Protecting Bidder Privacy. In Ed Dawson, Andrew Clark, and Colin Boyd, editors, *Proceedings of 5th Australasian Conference on Information Security and Privacy - ACISP 2000*, volume 1841 of *Lecture Notes on Computer Science*, pages 427–442. Springer, Berlin, 2000.

[OEC80] OECD - Organisation for Economic Cooperation and Development. OECD Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data, 1980.

[Off00] Office of the e-Envoy. e-Government: A Strategic Framework for Public Services in the Information Age. Available from: http://www.iagchampions.gov.uk/strategy.htm, 2000.

[Off01] Office of the e-Envoy. Benchmarking Electronic Service Delivery. Available from: http://www.official-documents.co.uk, 2001.

[OvdB01a] Anne-Marie Oostveen and Peter van den Besselaar. Linking Databases and Linking Cultures. In Beat Schmid, Katarina Stanoevska-Slabeva, and Volker Tschammer, editors, *Towards the E-Society: IFIP Conference on E-Commerce, E-Business and E-Government*, pages 765–774. Kluwer Academic Publishers, Boston, 2001.

[OvdB01b] Anne-Marie Oostveen and Peter van den Besselar. FASME Deliverable 3.1: Social and Legal Issues and Implications for the Design of Systems. Technical report, Nettetal/Brussels, 2001.

[Ped02] Alan Pedersen. Report Reveals Serious Flaws in Safe Harbor Agreement. Available from: http://www.europamedia.net, 2002.

[Pfl96] Charles Pfleeger. *Security in Computing, 2nd Edition*. Prentice Hall, Upper Saddle River, 1996.

[PK01] Birgit Pfitzmann and Marit Köhntopp. Anonymity, Unobservability and Pseudonymity. A Proposal for Terminology. In

Hannes Federrath, editor, *Designing Privacy Enhanced Technologies. International Workshop on Design Issues in Anonymity and Unobservability*, volume 2009 of *Lecture Notes in Computer Science*, pages 1–9. Springer, Berlin, 2001.

[PKK+02] Reinhard Posch, Gregor Karlinger, Daniel Konrad, Alexander Leiningen-Westerburg, and Thomas Menzel. Weissbuch Bürgerkarte. Bundesministerium für öffentliche Leistungen und Sport, Wien. Available from: http://www.buergerkarte.at, 2002.

[RCMA01] Reinhard Riedl, Clemens H. Cap, Nico Maibaum, and Niklas Auerbach. FASME Deliverable 6.1: System Architecture for the FASME Project. Technical report, Nettetal/Brussels, 2001.

[RE00] Wolfgang Rankl and Wolfgang Effing. *The Smart Card Handbook, 2nd Edition*. John Wiley & Sons, New York, 2000.

[Reg95] Registratiekamer, The Netherlands and Information & Privacy Commissioner of Ontario, Canada. Privacy-Enhancing Technologies: The Path to Anonymity. Available from: http://www.ipc.on.ca, 1995.

[Rie01] Reinhard Riedl. Document-based Inter-organizational Information Exchange. In *Proceeedings of The Nineteenth Annual International Conference of Computer Documentation: Communicating in the New Millennium*, pages 122–131. ACM Press, Santa Fe, 2001.

[Rie03] Reinhard Riedl. Design Principles for E-Government Services. In Maria A. Wimmer, editor, *Quo Vadis e-Government: State-of-the-art 2003. Proceedings of OCG eGov Day Vienna 2003*, volume 165. Österreichische Computer Gesellschaft, Wien, 2003.

[Rom99] Ed Roman. *Mastering Enterprise JavaBeans*. John Wiley & Sons, New York, 1999.

[Ros92] Richard Rosenberg. *The Social Impact of Computers*. Academic Press, San Diego, 1992.

[RR98] Michael K. Reiter and Aviel D. Rubin. Crowds: Anonymity for Web Transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.

[RR02] Reinhard Riedl and Lutz Richter. Digitale Identität - die unbekannt grosse Herausforderung. In Maria A. Wimmer, editor, *Impulse für e-Government: Internationale Entwicklungen, Organisation, Recht, Technik, Best Practices. Proceedings of OCG eGov Day Vienna 2001*, volume 158. Österreichische Computer Gesellschaft, Vienna, 2002.

[RSA78] Ron L. Rivest, Adi Shamir, and Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[RSA97] RSA Data Security Inc. PKCS #11 - Cryptographic Token Interface Standard, Version 2.01, December 1997. Available from: http://www.rsasecurity.com/rsalabs/pkcs/, 1997.

[Sam02] Pierangela Samarati. Enriching Access Control to Support Credential-Based Specification. In Sigrid E. Schubert, Bernd Reusch, and Norbert Jesse, editors, *Informatik bewegt: Informatik 2002 - 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI)*, volume 19 of *Lecture Notes in Informatics*, pages 114–119. Köllen, Bonn, 2002.

[SB96] Rainer Schweizer and Herbert Burkert. Verwaltungsinformationsrecht. Helbling & Lichtenhahn, Basel, 1996.

[SBLB03] Carol Summerfield, Jill Barelli, Henry Langley, and Penny Babb. *National Statistics UK 2003 - The Official Yearbook of the United Kingdom of Great Britain and Northern Ireland.* TSO, London, 2003.

[Sch96] Bruce Schneier. *Applied cryptography.* John Wiley & Sons, New York, 2nd Edition, 1996.

[Sch00] Bruce Schneier. *Secrets and Lies: Digital Security in a Networked world.* John Wiley & Sons, New York, 2000.

[Ser03] Sertifitseerimiskeskus Estonia. The Estonian ID Card and Digital Signature Concept. Available from: http://www.id.ee, 2003.

[SS99] Bruce Schneier and Adam Shostack. Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards. In *Proceedings of the Usenix Workshop on Smartcard Technology (Smartcard '99).* Usenix Association, Berkeley, California, 1999.

[Ste97] Jane Steele, editor. *Information for Citizenship in Europe.* Policy Studies Instutute, London, 1997.

[Sun02a] Sun Microsystems Inc. The Java 2 Platform, Micro Edition. Available from: http://java.sun.com/products/j2me, 2002.

[Sun02b] Sun Microsystems Inc. Java Card 2.2 Application Programming Interface. June 2002. Available from: http://java.sun.com/products/javacard/reference/docs/index.html, 2002.

[Sun03] Sun Microsystems Inc. JAAS Reference Guide. August 2003. Available from: http://java.sun.com/j2se/1.4.1/docs/guide/security/jaas/JAASRefGuide.html, 2003.

[SW89] John Simpson and Edmund Weiner, editors. *The Oxford English Dictionary, 2nd Edition.* Oxford University Press, Oxford, 1989.

[SWR97] Dennis Steinauer, Shukri Wakid, and Stanley Rasberry. Trust and Traceability in Electronic Commerce. *StandardView*, 5(3):118–124, 1997.

[Taj81] Henri Tajfel. *Human Groups and Social Categories: Studies in Social Psychology.* Cambridge University Press, Cambridge, 1981.

[TCG03] TCG - The Trusted Computing Group. Trusted Computing Group Backgrounder. Available from: https://www.trustedcomputinggroup.org/downloads/TCG_Backgrounder.pdf, 2003.

[TCP03] TCPA - The Trusted Computing Platform Alliance. TCPA Frequently Asked Questions, Version 5. Available from: http://www.trustedcomputing.org/docs/, 2003.

[Tra99] Jacques Traoré. Group Signatures and Their Relevance to Privacy-Protecting Off-Line Electronic Cash Systems. In Josef Pieperzyk, Reihaneh Safavi-Naini, and Jennifer Seberry, editors, *Proceedings of 4th Australasian Conference on Information Security and Privacy - ACISP 1999*, volume 1587 of *Lecture Notes on Computer Science*, pages 228–243. Springer, Berlin, 1999.

[Tro00] Maria Trombly. Bank Offers Virtual Safe-Deposit Boxes. Available from: http://www.idg.net, 2000.

[Uni74] United States Department of Jusitice. United States Code Title 5 Section 552a: The U.S. Privacy Act, 1974.

[vB01] Jellen van Buuren. Digital Safe-Deposit for Dutch Citizens. Available from: http://www.heise.de/tp/english/inhalt/te/7393/ 1.html, 2001.

[vLR00] Jörn von Lucke and Heinrich Reinermann. Speyerer Definition von Electronic Government. Available from: http://foev.dhv-speyer.de/ruvii, 2000.

[W3C02a] W3C - World Wide Web Consortium. The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification. Available from: http://www.w3.org/TR/P3P/, 2002.

[W3C02b] W3C - World Wide Web Consortium. XML-Signature Syntax and Processing. Available from: http://www.w3.org/TR/xmldsig-core/, 2002.

[WB90] Samuel D. Warren and Louis D. Brandeis. The Right to Privacy. *Harvard Law Review*, 193(4), 1890.

[Wes67] Alan F. Westin. *Privacy and Freedom*. Atheneum, New York, 1967.

[WGPR02] Merill Warkentin, David Gefen, Paul A. Pavlou, and Gregory M. Rose. Encouraging Citizen Adoption of e-Government by Building Trust. *Electronic Markets*, 12(3), 2002.

[Wil91] Paul A. Wilson. *Computer Supported Cooperative Work : An Introduction*. Intellect, Oxford, 1991.

[Wim02] Maria A. Wimmer. Integrated Service Modelling for Online One-stop Government. *Electronic Markets*, 12(3):149–156, 2002.

[WL02] William H. Winsborough and Ninghui Li. Towards Practical Automated Trust Negotiation. In *International Workshop on Policies for Distributed Systems and Networks - POLICY 2002*, pages 92–103. IEEE Computer Society, 2002.

[WT02a] Maria A. Wimmer and Efthimios Tambouris. A European Perspective Towards Online One-stop Government: The eGOV Project. *Electronic Commerce Research and Applications*, 1(1):92–103, 2002.

[WT02b] Maria A. Wimmer and Efthimios Tambouris. Online One-Stop Government: A Working Framework and Requirements. In Roland Traunmüller, editor, *Information Systems: The e-Business Challenge. Proceedings of the 17th World Computer Congress of IFIP*, pages 117–130. Kluwer Academic Publishers, Boston, 2002.

[ZS95] Miklos Geza Zilahi-Szabo. *Kleines Lexikon der Informatik und Wirtschaftsinformatik*. Oldenbourg, München, 1995.

Curriculum Vitae
Niklas Auerbach

2000 - 2004	Research assistant at the University of Zurich, Department of Informatics Research assistant of Prof. Dr. Lutz Richter (System Architecture & Software Group) and of Prof. Dr. Gerhard Schwabe (Information Management Research Group)
1999 - 2000	Swiss Life: Finance and Risk Management Systems analysis and application development
1998	University of Zürich: Licentiate in Business Administration and Computer Science (lic. oec. publ.)
1995 - 1996	City University, London One year of study as an exchange student Personal tutor: Prof. Dr. Anthony Finkelstein
1992 - 1998	University of Zürich Studies in Business Administration and Computer Science
1984 - 1992	Gymnasium Bäumlihof, Basel-Stadt
1978 - 1984	Primary School Bettingen
1973	Born in Basel, Switzerland