INTERNATIONAL STANDARD

ISO/IEC 29191

First edition
2012-12-15

Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication

Technologies de l'information — Techniques de sécurité — Exigences pour l'authentification partiellement anonyme, partiellement non reliable

Reference number
ISO/IEC 29191:2012(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Terms and definitions **1**
3 General **2**
4 Framework **2**
5 Requirements **4**
Annex A (informative) **Use cases** **5**
Annex B (informative) **Application of the mechanism for the purpose of data authentication and data protection** **7**
Bibliography **9**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC should not be held responsible for identifying any or all such patent rights.

ISO/IEC 29191 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, subcommittee SC 27, *IT Security techniques*.

Introduction

The current state of the art for entity authentication requires the revelation of the identifiable information of an entity being authenticated. In many types of transactions, the entity would prefer to remain anonymous and unlinkable, which means that when two transactions are performed, it is difficult to distinguish whether the transactions are performed by the same user or two different users. However, in some circumstances there are legitimate reasons to enable subsequent reidentification (e.g., the interest of accountability). The term ‘partially anonymous, partially unlinkable’ means that an a priori designated opener, and that designated opener only, can identify the authenticated entity. For example, a library may need to identify an entity that has not returned a borrowed book in order to send a late notice to the entity. Current cryptographic technologies are available to provide partially anonymous, partially unlinkable authentication. This International Standard defines a framework and requirements for partially anonymous, partially unlinkable authentication.

Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication

1 Scope

This International Standard provides a framework and establishes requirements for partially anonymous, partially unlinkable authentication.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
authentication
provision of assurance in the claimed identity of an entity

[SOURCE: ISO/IEC 18014-2]

2.2
claimant
entity which is or represents a principal for the purposes of authentication

[SOURCE: ISO/IEC 9798-1:2010]

2.3
credential
representation of an identity

[SOURCE: ISO/IEC 24760-1]

2.4
designated opener
entity who can re-identify the claimant from the transcript of authentication

NOTE The selection of the designated opener should be made in advance of transactions. The entity or entities that make that selection may vary with the implementation. As the designated opener has the capability of identifying the claimant, the selection of the designated opener and the selection of the transcript of authentication to be provided to the designated opener need to be carefully performed.

2.5
identity
set of attributes related to an entity

[SOURCE: ISO/IEC 24760-1]

2.6
re-identification
identification of a claimant following a partially anonymous, partially unlinkable authentication

NOTE Re-identification is also called opening.

2.6
transcript of authentication
record of sequences of exchanged data from a process of authentication

3 General

Many cryptographic mechanisms are available and in use today to improve the security of the authentication process. This leads to greater trust when, following a successful authentication, an entity is given appropriate access to protected resources using some authorization process. Note that the details of authorization are out of scope for this standard and thus marked in parentheses. A typical authentication and authorization model includes the following steps (with each step usually including a number of sub-steps, many of which are covered in ISO/IEC 29115):

a) Enrollment

b) Authentication

c) (Authorization)

Most cryptographic mechanisms in use today require the revelation of the identifiable information and enable tracking of an entity across transactions. For example, the use of public keys could hide an entity's real name. However, if the same public key or pseudonym is used for multiple authentications, it can be used to link information about the entity across transactions and so build a profile.

But complete anonymity and unlinkability may not always be desirable. For example, an entity could use anonymity to escape punishment for exploiting a system. So, while anonymity and unlinkability may be appropriate in some situations, there are cases where it may be necessary to give certain parties the ability to re-identify an entity.

To achieve the goal of partially anonymous, partially unlinkable authentication, the process steps now look like:

a) Registration/enrollment, including setup to achieve anonymity

b) Authentication

c) (Authorization)

d) Re-identification (when appropriate)

4 Framework

For the sake of understanding an overview of the framework, a typical scenario is exemplified, where a claimant begins by enrolling with a service. The service includes an issuer that generates credentials and issues them to the claimants. The claimants then use the credentials for authentication. If the authentication is successful, a transcript of authentication is created. Although it may contain other things, this transcript shall include information necessary to enable re-identification by the designated opener. If re-identification is required, the transcript of authentication is given to the designated opener who, a priori to any transactions, must be established and provided with the necessary cryptographic components required for re-identification. Each system will have its own set of practices and principles for determining when re-identification is appropriate or necessary. Those details are not within the scope of this standard. Principles such as openness, transparency and notice are explained in ISO/IEC 29100.

Every application will have its own requirements so any particular implementation may have variations from the flow described above. For example, the cryptographic-based credentials could be generated by the claimant, rather than the issuer; or credentials may be issued electronically or in person. But such variations do not change the fundamental aspects of the framework.

This framework defines a set of roles and operations, which are shown in Figure 1.

The four roles are:

a) Issuer – the entity who issues credentials to claimants

b) Claimant – the entity who will be authenticated by a verifier

c) Verifier – an entity that checks whether the claimant possesses credentials that are valid

d) Designated opener – the entity that can re-identify the claimant

Among the above four roles, there are four basic operations in this framework.

1) A process between an issuer and a claimant to perform a credential issuing process. After this process a claimant has a credential.

2) A process for the designated opener to setup the cryptographic information necessary for re-identification.

3) A process between a claimant and a verifier to perform authentication, which produces a transcript of authentication. Authentication is successful if the verifier can determine that the claimant possesses a valid credential.

4) A process by a designated opener to identify the claimant from the transcript of authentication, called re-identification. In this process, a designated opener uses the transcript of authentication and may use other information, where appropriate, to enable re-identification

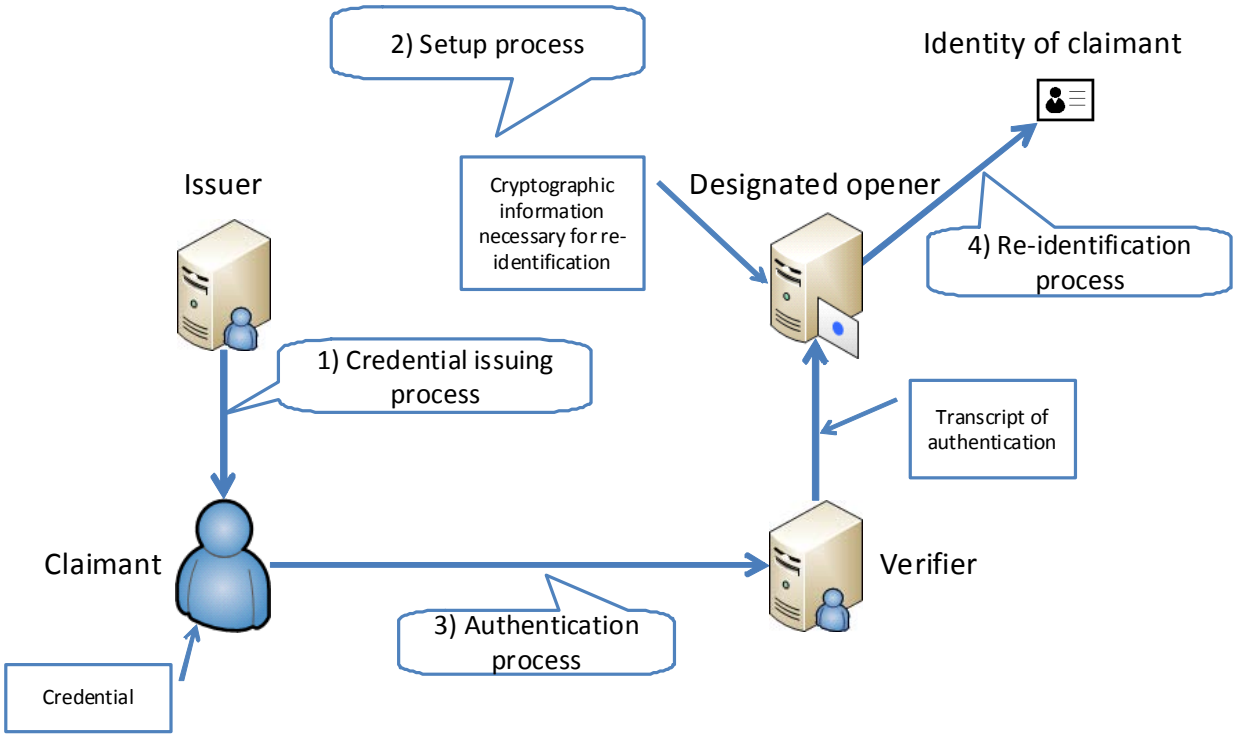

Figure 1 — Framework of partially anonymous, partially unlinkable authentication

5 Requirements

Partially anonymous, partially unlinkable authentication shall satisfy all requirements described below.

a) A claimant shall be authenticated by a verifier without being identifiable by the verifier.

   For a claimant to remain anonymous to a verifier, the transaction shall not provide any information to identify the claimant, while allowing the verifier to corroborate that the claimant possesses a valid credential.

b) The transcript of authentication shall not by itself provide information that can link multiple authentication transactions by the same claimant.

   For a claimant to remain unlinkable to verifiers, the transaction shall not provide any information to link multiple transactions performed by the same claimant.

c) The transcript of an authentication shall contain information necessary for the designated opener to re-identify the claimant.

   For the designated opener to be capable of later re-identifying the claimant, the transcript resulting from a successful transaction shall provide information to identify the claimant. Note, the designated opener may use other information, where appropriate, to enable re-identification.

d) The designated opener shall be able to provide evidence that the claimed identity is correct.

   In order to avoid fraudulent claim(s) by the designated opener, the designated opener shall be able to provide evidence that the procedure for re-identification was properly performed.

Annex A
(informative)

Use cases

A.1 Library use case

In some countries, the list of books that an individual has borrowed from a library is considered to be sensitive because the list can reveal the individual's thoughts, conscience, or religion. Due to this sensitivity, borrowers may not want their name linked to the list of books they have borrowed. At the same time, the library may need to associate the title of a borrowed book with the name of the borrower (e.g., if the book is not returned by the due date). Partially anonymous, partially unlinkable authentication can be applied to this scenario.

The registration desk librarian (issuer) at the library will provide a membership card and rules for re-identification to an individual (claimant) who would like to borrow books. When the individual wants to borrow a book, he/she will present the membership card to the librarian (verifier) who will check that the individual is a member of the library and will perform the book checkout procedure. A transaction record is created and stored in a database so the library can manage and track books on loan. All individuals remain anonymous in this database, and checkout transactions cannot be linked together.

If the individual keeps a book for longer than the allowed borrowing period, the database will notify the head librarian (designated opener) who can determine the name of the borrower for the overdue book and use it to send the individual an appropriate notice.

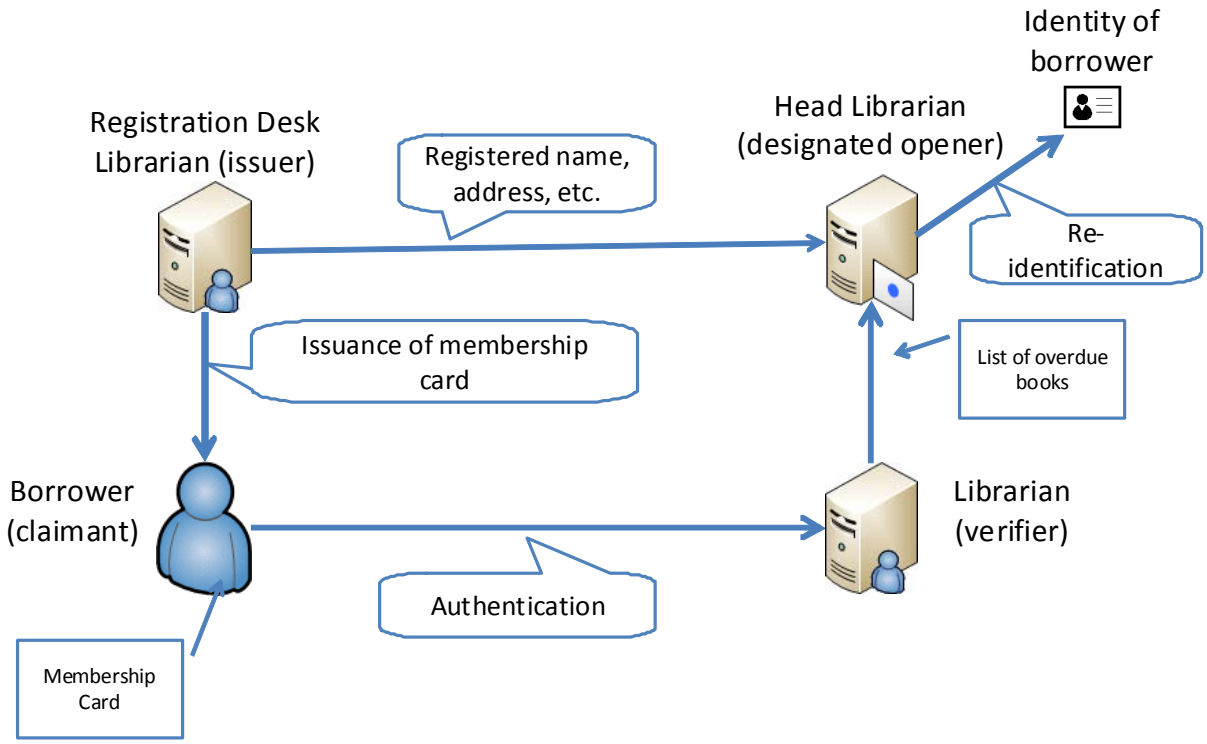

Figure A.1 — Library use case

A.2 Intelligent Traffic System use case

Precise measurements, real-time analysis, and predictions of traffic densities and flows on intercity highways are important contributors to improve traffic flow, safety, and sustainability. A precise trace of the cars on the highway is of great importance. On the other hand, being able to track the real-time location of each car in a continuous manner has potential privacy implications. Partially anonymous, partially unlinkable authentication can be used in this scenario to support the needs of the intelligent traffic management system while preserving the privacy of the drivers.

The frequent users of a route are issued a tag that can be read in a contactless manner. At the entrance of the intercity highway, the tag authenticates itself using partially anonymous, partially unlinkable authentication and receives a temporary identifier that is used until the car exits the highway.

By logging this temporary identifier, an intelligent traffic control center can create a list of each car, the time of entry onto the highway, and time of exit, without knowing a permanent identifier of any car. The list can be used to perform real-time analysis of the traffic flow or used to control the flow by denying the access of the cars in the congested section of the highway. It can also be used in capacity planning based on actual usage patterns.

When a car with a temporary identifier passes through a tolling station, the toll billing system is authorized to use the identification service, which can convert the temporary identifier to a billing account for the vehicle. The other conditions in which authorities may demand re-identification should be made known to the user in advance.

This use case demonstrates how a system using partially anonymous, partially unlinkable authentication can be used with multiple purposes.

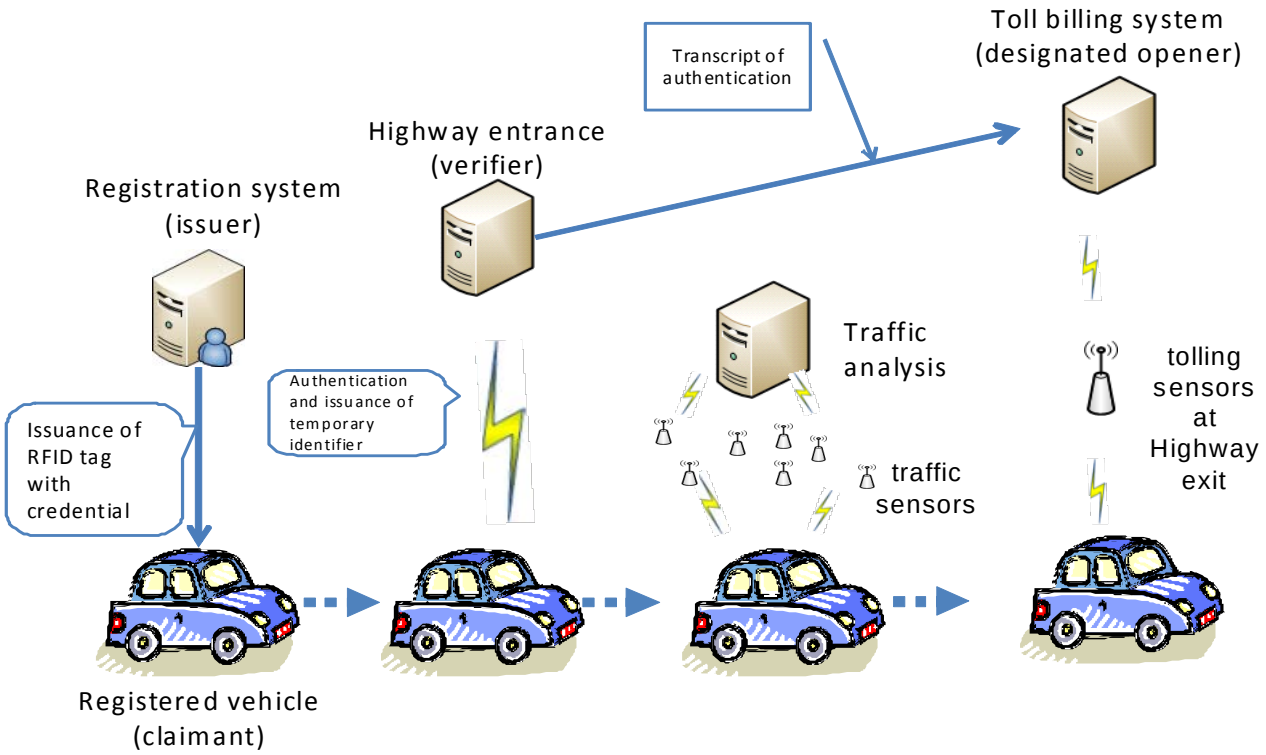

Figure A.2 — ITS Use case

Annex B
(informative)

Application of the mechanism for the purpose of data authentication and data protection

In this Annex, we provide an application where the same mechanism serves for data authentication while hiding some information of the user although the user is not anonymous. In the exemplified scenario below, the hidden information will be an account number, such as bank account number and credit card number.

Users have billing accounts, such as bank accounts and credit card accounts. When shopping at a web store, it is important that the user has a legitimate billing account. However, there is a risk of conveying the exact account number to the web store, as it may be abused by the web store. On the other hand, there is a risk for the web store on receiving such exact account number of the customer, and the web store may need to pay extra cost to keep these data secured from being breached. Partially anonymous, partially unlinkable authentication can be used in this scenario for the purpose of data authentication and data protection.

There will be a bank or credit card company, who will be issuing accounts to the users. There will be users who want to buy some goods from a web store. There will be a piece of software at a web store that checks if the user has a legitimate billing account, and if the user does have one, performs the sales procedure of the goods. The bank or the credit card company will play the role of the designated opener.

A user when opening his bank account or credit card account engages in issuing process with either a bank or credit card company. The user receives a credential. When the user wants to buy some goods at the web store, the user engages in user authentication at the web store and proves the user has a legitimate billing account at the claimed bank or the credit card company. Through the use of partially anonymous, partially unlinkable authentication, the web store can verify that the user indeed has a legitimate account at the claimed organization, without learning the user's exact account number. The log entry would be the name of the goods, the date of purchase, and the name of the bank or the credit card company that the user claimed to have account at, with a transcript that was generated through the data authentication. The transcript does not reveal the exact account number. The transcript is unlinkable, that is, it is impossible to find from the log entries other goods that have been purchased using the same account number. The web store passes this transcript to the claimed organization. The organization, the bank or credit card company, performs the re-identification process on the transcript and successfully obtains the exact billing account.

The user is comfortable that the web store does not learn his account number, and the web store is comfortable that it need not learn such private information.

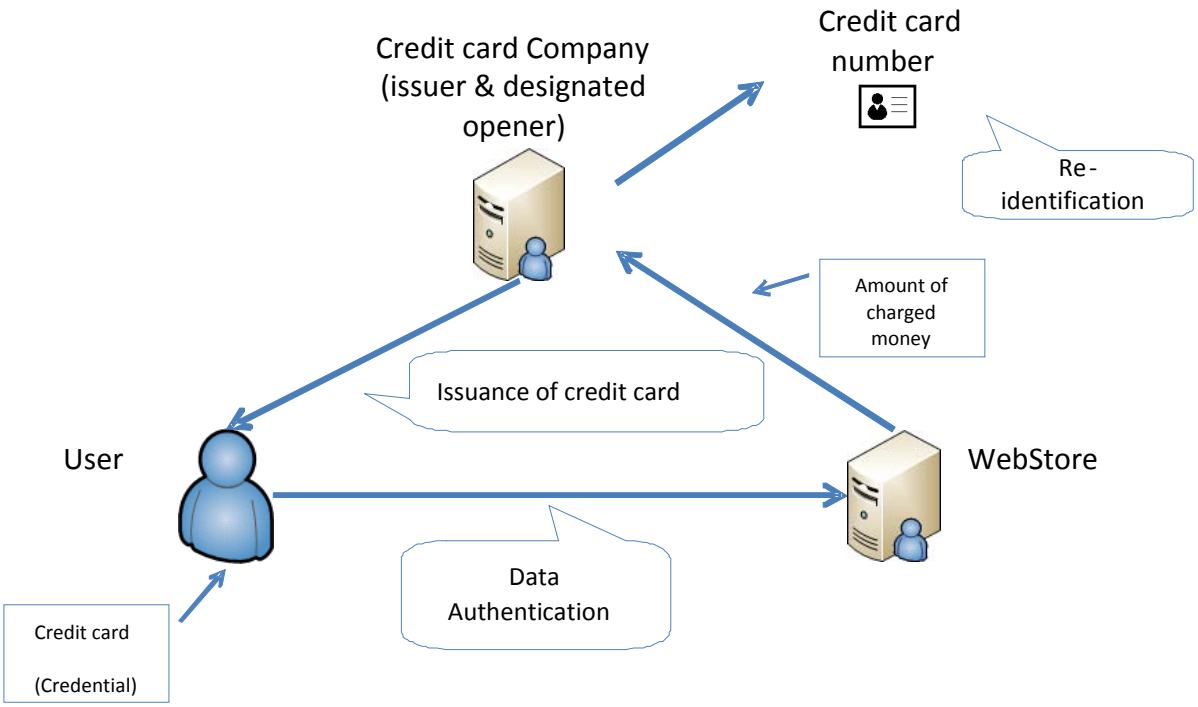

Figure B.1 — Hiding billing account

Bibliography

[1] Chaum and van Heyst: **"Group Signatures**." Advances in Cryptology -- EUROCRYPT '91 Lecture Notes in Computer Science 547 Springer 1991, pp. 257-265.

[2] Kilian and Erez Petrank: "**Identity Escrow**." Advances in Cryptology -- CRYPTO '98, Lecture Notes in Computer Science 1462 Springer 1998, pp. 169-185.

[3] Camenisch and Groth: "**Group Signatures: Better Efficiency and New Theoretical Aspects.**"Security in Communication Networks (SCN 2004) Lecture Notes in Computer Science 3352 Springer 2005, pp. 120-133.

[4] Furukawa and Imai: "**An Efficient Group Signature Scheme from Bilinear Maps.**" Information Security and Privacy, 10th Australasian Conference(ACISP 2005) Lecture Notes in Computer Science 3574 Springer 2005, pp. 455-467.

[5] Isshiki, Mori, Sako, Teranishi and Yonezawa: "**Using group signatures for identity management and its implementation**." Proceedings of the 2006 Workshop on Digital Identity Management (IDM 2006) ACM.

ICS 35.040

Price based on 9 pages