Bundesamt
für Sicherheit in der
Informationstechnik

Technical Guideline TR-03107-1 Electronic Identities and Trust Services in E-Government

Part 1: Assurance levels and mechanisms

Version 1.0

This translation is informative only. The normative version is the German text.

Federal Office for Information Security
P.O.B. 20 03 63
D-53133 Bonn (Germany)
Tel.: +49 22899 9582-0
e-mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

List of Tables

1 Introduction

The goal of this Technical Guideline is the evaluation of methods on electronic identities and trust services for various e-government processes and the assignment to assurance levels. For this purpose, generic criteria applicable to all processes as well as special criteria for different processes are specified.

In this respect, the term *trust service* covers services offering further functions based on electronic identities, such as declarations of intent, transmission of documents or federated identity methods. Trust services are to enhance the trust of citizens / companies and the government agency in their communication with each other and thus promote the use of e-government[1]. The term *trust service* (German: *Vertrauensdienst*) must be distinguished from the term "*confidentiality"* (German: *Vertraulichkeit*) which refers to to the protection of data against unauthorised notice and disclosure. In addition to the technical security of the methods, the trustworthiness / credibility of the respective manufacturers and service providers is also required to ensure trust in these services.

1.1 Identities

The *identity* of natural or legal persons is defined by different features such as name, address, date of birth, e-mail addresses or also pseudonyms. Identities, however, do not only denominate and characterise persons but also entities, resources, services and other objects. In the virtual world, names and features are illustrated by attributes of an electronic identity.

In order to enable access to systems, processes and services, users must be identifiable, i.e. the system must be provided with certain identity information. In order to ensure the secure use of the system, the *authenticity* of this identity data is of essential importance. If this data is falsified, obsolete or not verifiable, it is not possible to generate reliable communication, even for a secure infrastructure.

Once a user is authenticated, the system must decide on the scope of authorisations this user may be assigned. This scope of authorisations includes the assignment and verification of access rights on data, services and resources.

Administration processes can now be initiated and carried out on the basis of this authentication and determined authorisation.

1 The term "*trust service"* is also used in the EU Commission's proposal for a "Regulation on electronic identities and trust services for electronic transactions in the internal market". In this proposal, further processes are covered (e.g. timestamp), but it has a narrower meaning as regards technology (e.g. for declarations of intent, only signatures are considered).

1.2 Content

Various technical solutions for different fields of application have been developed and implemented over the years. These solutions cover different identity management processes on different security levels.

This Technical Guideline assesses and classifies mechanisms for electronic administration processes between citizens / legal persons on the one hand and government agencies on the other hand. The following processes are distinguished:

- Identification of persons, organisational units or resources
- Declaration of intent made, for example, to approve certain administration services or document contents
- Electronic transmission of documents and identity data.

The functions which must be fulfilled by a mechanism to be suitable for a certain process is specified for each of these processes. Furthermore, criteria are defined for the assignment to assurance levels, and suitable mechanisms are assigned to the assurance levels on the basis of these criteria. In addition to the mechanisms considered in this Guideline, the criteria can also be used to assess other mechanisms.

For these processes / mechanisms, only electronic methods are contemplated. Non-electronic methods which would also be possible are beyond the scope of e-government and are not evaluated.

The assessment of the mechanisms takes into account the threats to the communication between communication partners via public networks. If the communication takes place via closed systems with limited user groups, the assessment might deviate, in particular if the closed space for communication already counteracts threats by means of additional safeguards.

1.3 Overall system

This Technical Guideline does not consider the overall system of the administration process (or general government agency processes), but only the access to them by means of identities, declarations of intent and transmission of documents. Taking the overall system into consideration requires the preparation of a comprehensive security and data protection concept.

In this concept, general and application-specific requirements exceeding pure communication between persons and government agencies must also be taken into account. This might cover, for example, the protection of information collected in the government agency system, but also further requirements such as the revision security of the processes.

This Guideline can also be used to support the preparation and development of a corresponding concept.

2 Definitions

2.1 Basic terminology

Basic terminology of identity management as used in this Guideline is defined below (following [ISO24760-1]):

- An **entity** is a person, an organisation, an object, a subsystem or a definable group of several of the aforementioned. Within the scope of this Guideline, entities are citizens, government agencies / companies and resources such as services and websites.
- An **identity attribute** or an **identity date** is a characteristic or property of an entity. Examples of identity attributes of persons are name, date of birth or the feature of having reached a certain age. Identity attributes of government agencies include the name of the government agency or its web address.
- An **identity** is a set of identity attributes assigned to an entity. An entity may have several identities, as well as several entities may have the same identity. Thus an identity is usually not unique but may be unique within a certain application context.
- A **unique identity** is an identity which clearly represents the corresponding entity within a certain application context; different entities have different unique identities. An identity (i.e. a certain amount of attributes) which is unique within a certain application context is not necessarily unique within a different context.
- A **relying entity** is an entity which relies on the authenticity and validity of an identity or other transmitted data. Depending on the application, several relying entities may be involved in a process. Examples of relying entities are government agencies (identification of citizens by the government agency, citizens submitting a declaration of intent to a government agency) or citizens (identification of services by citizens, transmission of documents from government agencies to citizens).

The following terms are used additionally for processes which are based on identities (see section 2.2):

- A **document** is the representation of a defined set of associated data in physical or electronic form. Examples are a contract or a completed form.
- A **process** is a defined set of associated data in the form of one or several documents which unambiguously describe a business transaction. A process may for example include the identity of a citizen, the identity of a government agency and the unique description of a service requested by a citizen.
- A **transaction** in terms of this Guideline is the execution of a process.

The following terms are relevant for the processing of identities or other data:

- **Authentication** is the process of providing identities or other transmitted data with metadata which enable relying entities to check the origin, authenticity and validity of the identity or data. The process of checking by the relying entity is also referred to as the **authentication** of the identity / data.[2]
- **Authentication means** are technical means which enable its owner to authenticate an identity (i.e. an amount of identity attributes) or other transmitted data. Examples of authentication means are passwords, an ID card or a signature card. If several technical means are required (such as a chip card and a PIN), the complete *authentication mean* includes several **authentication factors**.

2 The German language differentiates between authentication of data by the sender (*Authentisierung*) and by the relying entity (*Authentifizierung*).

- An **authentication system** comprises of the entire technical infrastructure including organisational processes and the legal framework which allow for the authentication using authentication means.
- The **enrolment** is the registration of an entity in an authentication system, mostly associated with an identity check which results in the provision of authentication means.

2.2 Processes

Based on identities, different processes can be implemented which support electronic business processes in e-government:

- **Identification** is the transmission of application-related suitable identity attributes (i.e. an identity) including authenticated metadata as well as the check of this identity (authentication) by relying entities.
- The **authorisation** of an entity is the assignment and check of the rights related to an entity, for example access rights or the right of using a certain application. Authorisations are always carried out in relation to an application. Therefore, they are not included in this Guideline.
- A **declaration of intent** is the expression of a will aimed at bringing about a legal effect: It expresses the intention of a legal consequence. Within the scope of this Guideline, the declaration of intent may include the approval of a process or the content of a document. The declaration of intent will only become effective when received by the recipient.
- The **transmission of a document** is the wilful transmission of a document to a defined recipient.

In this Guideline, the processes of identification, declaration of intent and transmission of documents are considered.

In general, only mechanisms which do not include any further functions as required for the process should be used in e-government processes as far as possible. For instance, a qualified electronic signature should not be used for identification, since using a qualified electronic signature for the declaration of intent cannot be distinguished technically from using it for identification. Thus, there is a risk that an unintended legal consequence is triggered unintentionally.

2.3 Assurance levels

For the characterisation and comparison of the quality and trustworthiness of mechanisms, different organisational and technical factors must be taken into consideration within the respective context. The assignment to a assurance level takes into account

- the technical security of the process into account, for example the security
  - of the authentication means used (token, passwords, ...),
  - of the relevant IT infrastructure and
  - of the cryptographic processes used;
- the organisational security of the process, for example
  - the quality of the identification process, i.e. how reliable the proof of personal data is at the registration authority as well as the proving which data belong to which person;
  - the quality of issue and delivery processes of the authentication means (for example by e-mail, by post, download or personal handover),
  - the trustworthiness of the authority issuing documents (for example the government, certification authority, private organisation),

- the trustworthiness of the persons involved in the application phase (for example identity provider, third parties for data transmission);

- the legal framework in particular regulations of the legal procedures (e.g. rules for the onus of proof such as refutable legal assumptions) of particular legal requirements of the involved parties.

Furthermore, any concrete vulnerabilities or security gaps or attacks against mechanisms are taken into account.

The criteria are detailed in section 3 and/or the following process-specific sections.

Three assurance levels are used in this Guideline:

- **normal**: The effects of the damage caused by compromising are limited and manageable. This assurance level corresponds approximately to the *normal* security level according to IT-Grundschutz [BSI100-2].
- **high**: The effects of damage caused by compromising may be considerable. This assurance level corresponds approximately to the *high* security level according to IT-Grundschutz [BSI100-2].
- **high** +: In addition to the *high* assurance level, special legal protection[3] of the method is required on the basis of a legal principle. The violation of legal requirements would have serious effects. The effects of an incorrect identification or incorrect assignment of a process to an identity is to be regarded as serious.

The *high +* assurance level does not correspond to the v*ery high* security level according to the IT-Grundschutz. The v*ery high* security level in terms of the IT-Grundschutz cannot usually be achieved with mechanisms which use the IT systems of the citizen.

The *high +* assurance level requires a governmental operation or governmental control of the method and/or the acknowledgement of the parties involved. Compared to the *high* assurance level, the requirements for the enrolment, i.e. for the initial identity verification, are increased.

In the chapters 4 to 6, different mechanisms of the identity management are assigned to processes and assurance levels.

2.4 Determination of protection requirements

The operator of a business process, for e-government this means the responsible government agency, must determine and define the application-related assurance level required for the processes, taking into account the specific threats and legal framework.

Following [BSI100-2], the threats can be assigned to a ***normal* / *high*** assurance level on the basis of possible effects / impairments according to table1.

The ***high +*** assurance level should be selected if, compared to the *high* assurance level, particular legal security is required, very sensitive data is processed or if the reliable identification of the user is very important. This is the case, for example, if processes are used which replace the written form.

In complex business processes of government agencies, the determination of protection requiremnts for different subprocesses or different subsets of the data processed can lead to different results.

3 Specific legal protection is often also associated with a legal privilege of a mechanism as regards the legal effectiveness, value of proof or other legal characteristics.

It is recommended to determine the necessary assurance level on the basis of a protection requirement determination according to [BSI100-2] taking legal provisions into account.

There is no need for mechanisms according to this Guideline for business processes which do not entail any major damage in case of misuse.

2.5 Evaluation of mechanisms

For the processes

- identification (chapter 4)
- declaration of intent (chapter 5)
- transmission of documents (chapter 6)
- transmission of identity data (chapter 7)

functions which must be mapped by the mechanisms are defined in the corresponding chapters. The assignment of mechanisms which comply with these functions to a assurance level is made on the basis of criteria which are generally listed in section 3; additional specific criteria are added in the process-specific chapters.

<table>
<tr><th rowspan="2">Threat</th><th colspan="3">Assurance level</th></tr>
<tr><th>Normal</th><th>High</th><th>High +</th></tr>
<tr><td>Violation of laws/regulations</td><td>Violation entailing minor consequences</td><td>Violation entailing considerable consequences</td><td>Violation entialing grave consequences</td></tr>
<tr><td>Incorrect identification or incorrect association of assets to an identity</td><td>Minor consequences</td><td>Considerable consequences</td><td>Grave consequences</td></tr>
<tr><td>Impairment of the right to informational self-determination</td><td>Impairment of the confidentiality of personal data</td><td colspan="2">Considerable impairment of the confidentiality of personal data</td></tr>
<tr><td>Impairment of the physical integrity of a person</td><td>Impairment does not appear possible</td><td colspan="2">Impairment cannot be ruled out</td></tr>
<tr><td>Impaired performance of duties</td><td>The impairment is assessed to be tolerable.</td><td colspan="2">Impairment would be assessed as intolerable by some of the individuals concerned</td></tr>
<tr><td>Negative internal or external effects</td><td>Minor / only internal impairment of reputation or trust expected</td><td>Considerable impairment of reputation or trust possible</td><td>Statewide impairment of reputation or trust possible</td></tr>
<tr><td>Financial consequences</td><td>Tolerable financial loss</td><td colspan="2">Considerable financial losses, however not existence-threatening</td></tr>
<tr><td colspan="4">Attention must be paid to the following: The aggregation of threats my increase the required assurance level. For example, the processing of personal data with normal protection requirement might have to be increased to a necessary high assurance level if many persons are effected by an impairment.
If several threats are relevant, the maximum of each determined necessary assurance level must be assumed for overall evaluation.</td></tr>
</table>

Table 1: Threats and assurance levels

3 General criteria for assurance levels

This chapter provides general criteria for the classification of mechanisms with regard to assurance levels which are amended by process-specific criteria in the following chapters. These criteria are only minimum requirements; the classification of concrete mechanisms must always be made on the basis of the evaluation of the overall system.

3.1 Authentication means

An important criteria for the evaluation of a mechanism is the control of the owners over the authentication means assigned to them. Different factors may be used to secure the authentication means:

Knowledge in terms of this Guideline is the knowledge which is exclusively known by the authorised owner and the verifying entity (e.g. the server in case of passwords, chip cards in case of a chip card PIN).

- If knowledge is used as the sole security factor, it is necessary to comply with the requirements provided in safeguard S 2.11 “Provisions governing the use of passwords” of the BSI IT-Grundschutz catalogues (see [GS]).
- If knowledge is used in combination with possession, both security factors must be linked, for example using the PIN for the activation of a chip card. This is to avoid that attackers can combine the knowledge and possession of different owners to get a valid authentication mean.
  If a retry counter is used which only allows for max. three trials for guessing the right PIN, the PIN must have at least 5 (*normal* assurance level) or 6 (*high / high +* assurance level) decimal digits (see [AIS 20/31]).

		Assurance level		
		Normal	**High**	**High+**
Authentication mean (section 3.1)		One factor	Two factors	Two factors
Enrolment / issue (section 3.3)		Known authority (see section 3.2.1)	Trustworthy authority (see section 3.2.2)	Government agency / authority approved by a government agency (see section 3.2.3)
Revocation (section 3.4)		24h	1h	immediately
Securing the communication link (section 3.5)		Securing on the transport level	End-to-end link / securing by trustworthy authorities (see section 3.2.2)	End-to-end link / securing by a government agency / authority approved by a government agency (see section 3.2.3)
Crypto-graphy (sec. 3.6)	**Algorithms / key lengths**	[TR-03116] / [TR-02102]		
	Key storage	Protect against unauthorised access	Use of certified hardware for private keys	Use of certified hardware for private keys

Table 2: General criteria for assurance levels

Knowledge should generally be defined by the owners, i.e. the owners select their own passwords / PINs (except for one-time passwords and passwords which cannot be used for authentication).

Possession as a security factor in terms of this Guideline is a physical token which is solely controlled by the owner. For this purpose it is important that reproduction of the token is not possible. This can be achieved by using suitable hardware and suitable cryptographic processes (see section 3.6).

Biometry as a security factor is not further contemplated in this Guideline because biometry is usually not suitable for use in online processes. Among other things, the protection against replay (i.e. the reuse of a previous record of a biometric characteristic) and biodetection are problematic in online scenarios. The use of biometry to replace knowledge as a security factor is usually possible under certain circumstances. This does, however, not play a role in practice and is thus not given any consideration in this Guideline.

In order to achieve a *high* assurance level, it is essentially necessary to use two factors for securing the authentication means which ensure the sole control of the users over their authentication means.

3.2 Trustworthiness of authorities

For most mechanisms, further authorities assume relevant tasks for the security of the mechanism in addition to the owner of the authentication means and the relying entity, for example enrolment and issue of authentication means (section 3.3), communication security (section 3.5) or storage of data. All authorities must establish and observe a set of rules for their respectively assumed tasks.

If the owner of an authentication means or the relying entity directly commissions a third party (order data processor in terms of the BDSG), this third party must meet the requirements for the owner / relying entity and the requirements provided in this section are thus not relevant.

3.2.1 Known authority

For all assurance levels, these tasks may only be assumed by authorities which are identified by the system operator for each task and which are known in the system. The number of authorities should be reduced to the required minimum.

For all authorities, it is recommended to prepare and update a security concept as well as to have an associated regular auditing carried out according to IT-Grundschutz. In this respect, the audit must include all tasks assumed by the authority and the compliance with the assigned protection objectives.

3.2.2 Trustworthy authorities

In order to achieve the *high* assurance level, these authorities must be recognised as trustworthy.

Preparing and updating a security concept as well as associated regular auditing including an attestation according to IT-Grundschutz are binding at the *high* security level. The audit must be carried out by a neutral entity (for example, a recognised auditor).

The security concept and the audit must include all tasks assumed by the authority and the compliance with the assigned protection objectives. If Technical Guidelines of the BSI, standards or other state-of-the-art technology for the verification are available for the task assumed by the authority, they must be complied with.

3.2.3 Government agency / authority approved by the government agencies

For the *high +* assurance level, the authorities must be government agencies and authorities approved by government agencies, since government agencies act in the public interest and are subject to special requirements for care and diligence.

In addition to the requirements for trustworthy authorities, it must be verified whether the authority has a certificate according to IT-Grundschutz on the *high* security level. In this respect, the audit / certificate must include all tasks assumed by the authority and the compliance with the assigned protection objectives.

Unless the authority is a government agency, the approval for the task assumed must be given by a government agency on the basis of legal provisions or a formalised process.

3.3 Enrolment and issue of authentication means

Enrolment is the registration of an entity with an authentication system. An identity check of the entity is typically carried out as part of the enrolment and authentication means (consisting of several factors, if necessary) are subsequently issued and/or available authentication means are registered. The identity check can be carried out on the basis of physically presented documents or electronically using an eID system on a suitable assurance level.

The identity attributes available in the authentication system can thus include proven (external) identity attributes as well as (internal) identity attributes which are then generated only in the system. For both external and internal attributes, it must be defined to what extent their validity expires if the underlying proven identity of the entity changes (see also section 3.4).

The identity check must at least be carried out on the is assurance level of the authentication system for which the enrolment is intended. Information on the evaluation of mechanisms for the identity check are provided in section 4 and in chapter 10.1 of [ISO29115].

Authentication means for the *high* assurance level must be issued such that both security factors (see section 3.1) are issued on different ways of transmission. Security means based on possession must be issued such that the authorised owner can see after its receipt whether the security mean has been used without authorisation, for example by using a transport PIN for securing a chip card.

- In order to reach the *high* assurance level, the authentication means must be enrolled and issued by authorities which are considered as trustworthy for this task (see section 3.2.2). Identity must be checked on the basis of suitable documents or database entries which are proven to belong to the entity, for example by the comparison of photos. The documents and/or databases must be issued and/or maintained by trustworthy authorities (section 3.2.2).

  Alternatively, the identity can be checked by means of a mechanism according to section 4 on a *high* assurance level.

- The enrolment and issuing of authentication means for authentication systems with a *high +* assurance level must be carried out by government agencies or by authorities approved by government agencies (see section 3.2.3). Identity must be checked on the basis of official documents / registers. Here, it must be proven that the documents / register entries belong to the entity, for example by the secure comparison of photos.

  Alternatively, the identity can be checked by means of a mechanism according to section 4 on a *high +* assurance level.

Part of the issuing of authentication means is to provide the owner with appropriate and necessary information on how to use these authentication means.

3.4 Revocation / blocking

It must be possible for all assurance levels for the owner to revoke or block authentication means.

- For the *normal* assurance level, the blocking of the authentication means must be effective no later than 24 hours after the blocking message of the owner. The transmission of blocking messages (hotline or the like) must at least be possible during the general business hours.
- For the *high* assurance level, the blocking of the authentication means must be effective no later than 60 minutes after the blocking message of the owner. The transmission of blocking messages (hotline or the like) must be possible at any time.
- For the *high +* assurance level, the blocking of the authentication means must be effective immediately after the blocking message of the owner. The transmission of blocking messages (hotline or the like) must be possible at any time via generally known means.

The possibility of transmitting blocking messages must be provided via public communication channels and appropriately made known to the owners of authentication means.

In order to revoke the blocking, the owner of an authentication mean must be identified at least on the assurance level of the authentication system.

Authentication means must also be revoked if the authenticated identity attributes are no longer valid (e.g. change of name) or if the owner is longer entitled to own the authentication means (see also chapter 10.2.2 in [ISO29115]).

3.5 Securing the communication link

It is generally recommended to prefer authentication systems with are based on relationship of trust between the owner of the authentication means and the relying entities, i.e. which do not require third parties or intermediaries for communication.

Any third parties or intermediaries which are included in the authentication system must be included in the evaluation of the assurance level. The requirements of section 3.2 are applicable.

3.6 Cryptography

For different mechanisms, specific cryptographic requirements are defined in each part of [TR-03116]. The description of the mechanisms includes a reference to each part. If [TR-03116] does not include any specifications for a mechanism, the requirements contained in [TR-02102] must be observed.

The private keys of all entities of an authentication system must be stored securely, i.e. confidentially. This requires that the private key is protected against being copied and that the key is prevented from being used by unauthorised persons.

Public keys which are used for authentication must also be stored securely, i.e. protected against manipulation.

- In order to reach the *high* assurance level, suitable hardware (for example chip cards or HSMs certified according to Common Criteria on Assurance Level EAL 4 augmented with AVA_VAN.5 on the basis of a suitable protection profile) must be used. When operating the hardware in a protected environment, augmentation with AVA_VAN.4 is sufficient.
- For the *high +* assurance level, certification must be performed on the basis of a protection profile provided by BSI for this purpose.

The cryptographic methods must be designed in such a manner that they can be adjusted to the latest cryptographic knowledge. This includes especially the possibility of exchanging keys, exchanging cryptographic primitives and increasing key lengths. It is recommended to already prepare a migration concept when developing a system.

In addition to the mechanism-specific requirements such as integrity / confidentiality of the data transmitted, the cryptographic methods used must particularly defend against the attacks specified in section 10.3.2 of [ISO29115]. If confidentiality is a security objective for a mechanism, cryptographic methods are to be used, which offer forward secrecy (i.e. the confidentiality is also maintained when long-term keys or passwords / PINs are compromised).

3.7 Requirements for the user environment

The BSI provides citizens with recommendations how to secure their local computer (https://www.bsi-fuer-buerger.de). These recommendations include:

- Installation of firewall, virus scanner and all security updates
- Deactivation of active contents in the browser, as far as possible
- Deactivation of cookies in the browser which are persistent after the session time

This list is not complete; the current status according to https://www.bsi-fuer-buerger.de is applicable. It must be ensured that the mechanisms can be used with computers which are configured in accordance with these recommendations; mechanisms must not have any requirements which are contrary to the recommendations of BSI.

When evaluating the mechanisms, it must be taken into account that these recommendations may not implemented extensively.

Moreover, it is recommended to select mechanisms which are compatible with as many operating systems and browsers as possible so that the users can freely select their local computer, and that they have alternatives in case of security warnings for certain systems.

4 Identification

The basis for many electronic administration services is the initial identification or enrolment of citizens or legal persons. For a reliable identity management, this identification (or the identification made for enrolment) is the basis for all further activities such as the granting of authorisationa.

According to the definition in section 2, identities and thus identification is not necessarily unique. The necessary attributes of an identity are defined by the application context; the identity for a certain application may for example include the place of residence, whereas in a different context, only the age is required.

A legal person is identified by the identification of a natural person who is authorised to represent the legal person for the intended special application. For example, the authorisation to represent can

- be made by an authorisation on the part of the service provider (for example a database entry assigned to the identity),
- be provided as identity attribute by the identification mechanism or a mechanism for the transmission of identity data or
- be made by using a derived identity including the authority to represent.

The proof of the authorisation to represent must be provided on the same (or higher) assurance level as the identification of the natural person.

The terms “citizen (natural person)” and “legal person” are combined in the term *person* hereinafter.

4.1 Functions

4.1.1 Identification of persons

For the identification of a person it is necessary to distinguish whether there is already a verified identity for the service to be used (“user account”), or whether a new account must be created or whether the service should be used without any explicit creation of an account. For the first case, the application purpose is the *login*, for the latter case it is the *registration* or *initial identification*. Identification within the meaning of this section is always the registration and/or login, usually with the goal of using services afterwards, i.e. a synchronous process. For asynchronous processes, for example the transmission of a document in connection with identity data, see sections 6 and 7.

Assurance level	**Identification of persons**	
	Registration / Initial Identification	**Login**
High+	Electronic proof of identity with ID card / residence permit (section 4.3)	
High	--	Cryptographic hardware token (section 4.4)
Normal	--	Cryptographic software token (section 4.5) / password (section 4.6)

Table 3: Mechanisms for the identification of persons

In general, initial identification and login can be performed on different assurance levels; for example it is possible to create an account by means of an electronic identity whereas it is used on the basis of a password. In this case, the assurance level of the login is the minimum assurance level of both processes.

The identification of persons is a volatile process which is only valid for the moment; it is not possible to provide proof to third parties. This corresponds to the term of non-electronic identification, i.e. natural persons presenting their ID cards. The mere identification (checking the ID card) is not suitable to provide proof to third parties; it is not permanent. Due to data protection reasons, this volatility of the identification should usually also be reflected in the technology used for identification ("deniability"), contrary to the "non-repudiation" for declarations of intent.

In some cases, however, verifiability at a later point in time is required, nonetheless. In these cases, additional process steps or safeguards to be taken by the relying government agency are required, such as the secure storage of the identification data in the systems of the government agency. This corresponds to the preparation of a copy of the ID card[4] which might be necessary as an additional safeguard for non-electronic identification. Corresponding safeguards, if necessary, must be taken into account when planning the concept for the application.

The identification is not linked to any other transaction or further processes. If this is required for certain applications, the identification must be linked to the application context.

The functions for the identification of persons for a service are:

- Authenticity / integrity of the identity attributes transmitted
- Confidentiality of the identity attributes transmitted; this requires the identification of the recipient, in e-government, this is the service / government agency, see section 4.1.2.
- Linking the identity attributes transmitted to the authorised person
- Data economy and volatile identification

4.1.2 Identification of services

On the other hand, not only the identification of the user of a service is required but, in particular, also the (unambiguous) identification of the service to the user. This is also the prerequisite for the confidentiality of the identity attributes of the person. Only in this way it is possible to ensure that the attributes are not transmitted to unauthorised third parties.

This Guideline only contemplates publically accessible services, i.e. it is not necessary to treat the identity of the service confidentially. Only authentication and integrity must be ensured. Equally, data-economic identification is not required but the services can be clearly identified by the person.

In most cases, the identification of the service is necessary to prepare further interactions with the service, i.e. the identification must be linked with a "session" or a connection between persons and services. This

Assurance level	Identification of services and secure connections
High +	Electronic proof of identity with ID card / residence permit (section 4.3)
High	SSL certificates (*high* only with limitations) (section 4.7)
Normal	

Table 4: Mechanisms for the identification of services

4 Here, the regulations on the legal admissibility of ID card copies must be observed.

function is not required if the business process is completed by the identification, which means that no additional “session” is necessary.

Thus the functions of service identification are:

- Authenticity / integrity of the transmitted identity of the service
- Establishment of a reliable connection between persons and service linked with the identity of the service which can be used for the following processes.

4.2 Criteria for assurance levels

In addition to the basic criteria mentioned in section 3, the following specific criteria for identification can be used to assign mechanisms to certain assurance levels (see tables 5 / 6).

4.2.1 Level of assurance according to [ISO29115]

[ISO29115] is an international standard for the assignment of identification systems to assurance levels. There are levels 1 – 4. On level 1, the identity attributes are assigned by the entity itself without being checked by any registration authority. Therefore, this level is only suitable for e-government if no authenticated identity is required.

For the *normal* assurance level, the mechanism must fulfil at least assurance level 2, for *high* level 3, for *high +* level 4. This applies both to mechanisms for the identification of persons as well as for the identification of services.

4.2.2 Criteria for the identification of services and secure connections

In addition to 3 and 4.2.1, the following criteria apply to the identification of services. The assurance level required for the identification of the service depends on the assurance level required for the data transmitted itself and might thus deviate from the assurance level required for other functions. The assessment assumes a uniform assurance level for all functions.

4.2.2.1 Granularity of service identification

Services can be identified either by identifying the service provider which offers a certain service, or by identifying the service itself.

Identification of services	**Assurance level**		
	Normal	**High**	**High+**
Level of assurance according to [ISO29115]	2	3	4
Granularity of service identification	Identification of the service domain	Identification of the service domain	Identification of the service itself
Securing the connection	On transport level	End-to-end protection	End-to-end protection
Linking identity to the session context	Organisational	Cryptographic	Cryptographic

Table 5: Additional criteria for the “identification of services and secure connections”

For the *normal* or *high* assurance level, it is sufficient to identify the service provider. Due to the specific legal situation, however, it is necessary to identify the service itself for the *high +* assurance level.

This requirement does not usually preclude the use of a joint gateway / portal within the meaning of a data processor contracted by the data controller.

4.2.2.2 Securing the connection

As the established connection is used for further business processes, more than just the mere identification is required for a secure connection. Therefore, a re-encryption by third parties or similar is not allowed for the *high / high +* assurance level. An end-to-end protection is required.

4.2.2.3 Linking identity to the session context

As one part of the establishment of a session context, it is necessary to ensure that the identification of the service is linked with this session. This includes that the identity must be clearly assigned to a certain session and not just to a certain communication endpoint, and that it may only be valid there. For the *high / high +* assurance level, this link must be established with suitable technical / cryptographic mechanisms such as cryptographically secure session identifiers / cookies.

4.2.3 Criteria for the identification of persons

In addition to 3 and 4.2.1, the following criteria apply to the identification of persons.

4.2.3.1 Prior “identification of services and secure connection”

The prior identification of the service combined with the establishment of a secure connection is required for the following criteria and must therefore be made on the basis of the intended assurance level for the identification of persons.

Identification of persons	**Assurance level**		
	Normal	**High**	**High+**
Level of assurance according to [ISO29115]	2	3	4
Identification of services and secure connection	*Normal*	*High*	*High +*
Linking identity to the session context	Organisational	Cryptographic	Cryptographic
Confidentiality of the identity attributes	Identification of the service on the *normal* assurance level and communication according to section 3.5	Identification of the service on the *high* assurance level and communication according to section 3.5	Identification of the service on the *high +* assurance level and communication according to section 3.5

Table 6: Additional criteria for the “identification of persons”

4.2.3.2 Linking identity to the session context

The transmitted identity must be linked to the sessions context. This means among others that the identity of a person must be clearly assigned to a certain session and not just to a certain communication endpoint, and that it may only be valid there. For the *high / high +* assurance level, this link must be established with suitable technical / cryptographic mechanisms.

4.2.3.3 Confidentiality of the identity attributes

The identification of the received service on the same assurance level as the identification of the person is a prerequisite for the confidentiality of the identity attribute of the person.

Section 3.5 must be observed for the actual transmission of the identity attributes.

4.3 Electronic proof of identity with ID card / residence permit

The *electronic proof of identity* is standardised by the Federal ID Card Act [PAuswG]. Similarly, the electronic proof of identity for the electronic residence permit is standardised by the German Residence Act [AufenthG]. Both in combination are implemented as a technically consistent system. The technical description is specified in [TR-03127] and the documents referenced therein.

The electronic proof of identity is used for the secure mutual authentication of citizens on the one hand and the electronic services from the business and administration sector on the other hand in business processes on the internet. Service providers must at first prove their identity on the basis of an authorisation certificate and the fact that they are authorised to query certain data. Then the citizens must provide the service provider with electronic proof of their identity.

The following identity attributes are available within the scope of the electronic proof of identity:

- First name, surname, religious / artistic name and doctor's degree, if any; birth name available in ID cards issued from Q2/2012[5];
- Date of birth and place of birth, or proof of age if only the exceeding of a certain age limit must be ensured;
- Address or proof of residence if not the complete address is required;
- Pseudonym (service-specific and card-specific identification for pseudonymous access);
- Document type and issuing state;

In addition, nationality and auxiliary residence conditions are provided in the residence permit.

The authorisation of the *Vergabestelle für Berechtigungszertifikate* VfB [German office for authorisation certificates] in the BVA [Federal Administrative Office] is required for the use of the electronic proof of identity of citizens in business processes. The *Vergabestelle* verifies the identity of the service provider and determines which personal data and ID card data from the ID card may be transmitted. It depends on the body which is responsible for the use of the data in terms of the data protection act which specific authority as a service provider in terms of §2 (3) [PAuswG] will apply for the authority at the office for authorization certificates. This can be a service provider or an association which was assigned the task of identifying the citizens and provides access services for several government agencies.

In addition, the new ID card is prepared for a *qualified electronic signature* (see section 5.3). Signature certificates are offered by certification service providers according to [SigG] for reloading on the ID card (possibly subject to charge).

5 The availability of the birth name for online authentication was implemented by the eGovernment act.

The electronic proof of identity offers the identification of citizens and services in one step. At the moment, this is thus the only system mentioned where both endpoints of the connection between citizen and service are securely identified without further safeguards.

4.3.1 Functions

The electronic proof of identity implements all functions of identification both of the services and the citizens.

4.3.1.1 Authentication / integration of the transmitted identity of the service

The identity of the service is checked by the procurement office for authorisation certificates, cryptographically secured and stored in the authorisation certificates. The authorisation certificate – and thus the authentication / integrity of the identity of the service – is checked by the ID card chip.

4.3.1.2 Secure connection linked with the identity of the service

If eID clients are used according to [TR-03124], the identification of the service is linked to the connection between web browsers and services (“channel linking”).

4.3.1.3 Authenticity / integrity / confidentiality of the identity attributes transmitted

The identity attributes are entered during the application process of the ID card authorities and stored within the scope of ID card production on the chip of the ID card in a way which is secure and protected against falsification. During the electronic proof of identity and on the basis of the encryption, the service checks the authenticity of the chip and directly reads out the data from the ID card via an authenticated, encrypted and integrity-secured channel.

4.3.1.4 Linking the identity attributes transmitted to the authorised person

In order to read out the identity attributes, a secret PIN which only the ID card owner knows must be entered.

4.3.1.5 Data economy and volatile identification

The VfB determines the maximum of attributes to be transmitted, and the ID card owner can make further restrictions. The electronic proof of identity is designed such that the authenticity of the identity attributes can be checked by the service at the moment of identification, however cannot be proven to third parties.

4.3.2 Assurance level

The *high +* assurance level is reached.

4.4 Cryptographic hardware tokens

Besides the new ID card, other suitable hardware-based identification mechanisms can also be used. Examples of such hardware tokens are electronic staff ID cards, specific USB sticks or key cards from the *Deutschland-Online-Infrastruktur* DOI [German online infrastructure].

Most of the identity attributes are stored on the token as an integral part of a certificate. Depending on whether the token is assigned to a natural or a legal person, the certificate includes the identity of a natural or legal person. Moreover, the certificate of a natural person can be assigned further certificates which for example describe the role of a natural person as the representative of a legal person (attribute certificates).

Authentication is usually carried out by a challenge-response process which proves that the private key to this certificate is owned.

4.4.1 Functions

4.4.1.1 Authenticity / integrity / confidentiality of the identity attributes transmitted

The identity attributes are an integral part of the certificate and thus, the authenticity / integrity of the attributes is cryptographically ensured by the signature of the certificate.

The conventional systems based on hardware tokens transmit the identity attributes in a non-encrypted way. For reasons of confidentiality, a secured connection between service and person including the service identification on an appropriate assurance level is required, e.g. by SSL (see section 4.7).

4.4.1.2 Linking the identity attributes transmitted to the authorised person

Depending on the specific system, the transmitted identity attributes are linked to the authorised person by owning the token or additionally by securing the token with a secret PIN.

4.4.1.3 Data economy and volatile identification

Most of the available hardware tokens do not offer any mechanism for data economy similar to the mechanisms for the electronic proof of identity of the ID card but only offer a certificate which statically includes all relevant identity details. Therefore, these tokens can only be used for closed systems / networks which always require the same set of identity attributes for identification, i.e. it does not have to be possible to transmit individual attributes selectively.

4.4.2 Assurance level

A prerequisite for assigning the token to an assurance level is its assignment to a level of assurance according to [ISO29115]. The requirements for authentication means as per section 3.1 apply to the token; in particular, the mechanism for reaching a *high* assurance level requires a two-factor authentication.

The requirements as per section 3.6 apply. There must not be any private cryptographic keys outside the token (no key backup or key escrow). If keys are generated outside the token, this must be carried out in a secure environment and any private keys available outside the token must be deleted before the token is handed out.

The assurance level depends on the context and the process selected for the identification of the token owner (enrolment) and the issuing of the token (section 3.3). Each individual case must be assessed.

4.5 Cryptographic software tokens

In addition to the storage of the private key for a certificate-based authentication on a hardware token (see section 4.4), it is also possible to store the key on the computer of the owner (software token or "software certificate"[6]).

Here, the identity attributes are stored as a part of the certificate. Depending on whether the certificate is assigned to a natural or a legal person, it contains the identity of a natural or legal person. Moreover, the certificate of a natural person can be assigned further certificates which for example describe the role of a natural person as the representative of a legal person (attribute certificates).

Authentication is usually carried out by a challenge-response process which proves that the private key to this certificate is owned.

4.5.1 Functions

4.5.1.1 Authenticity / integrity / confidentiality of the identity attributes transmitted

The identity attributes are an integral part of the certificate and thus the authenticity / integrity of the attributes is cryptographically secured by the signature of the certificate.

The conventional systems based on software tokens transmit the identity attributes in a non-encrypted way. For reasons of confidentiality, a secured connection between service and person including the service identification on an appropriate assurance level is required, e.g. by SSL (see section 4.7).

4.5.1.2 Linking the identity attributes transmitted to the authorised person

The transmitted identity attributes are linked to the authorised person by means of password-based access protection on the private key in most cases. The access protection can be either forced by the operating system ("access control") or the password is used to decrypt the private key which was stored in an encrypted manner.

4.5.1.3 Data economy and volatile identification

Most of the available software tokens do not offer any mechanism for data economy similar to the mechanisms for the electronic proof of identity of the ID card but only offer a certificate which statically includes all relevant identity details. Therefore, software tokens can only be used for closed system / networks which always require the same set of identity attributes for identification, i.e. it does not have to be possible to transmit individual attributes selectively.

4.5.2 Assurance level

As a software token does not implement a two-factor authentication, only the *normal* assurance level can be reached. The requirements provided in safeguard S 2.11 "Provisions governing the use of passwords" of the IT-Grundschutz catalogues of the BSI (see [GS]) must be met for the password protecting access to the private key.

6 This (usual) description is not precise, because the storage of the private key is decisive, not the storage of the corresponding (public) certificate.

4.6 User name / password

Software-based processes can also be used in addition to hardware-based identification and authentication mechanisms. In particular for log-on, i.e. the authentication of already registered persons, a user name / password approach is usual. Initial registration is not possible with this mechanism. In general, preference should be given to methods based on cryptography over purely password-based methods.

The requirements provided in safeguard S 2.11 “Provisions governing the use of passwords” of the BSI IT-Grundschutz catalogues (see [GS]) must be met.

4.6.1 Functions

4.6.1.1 Authenticity / integrity / confidentiality of the identity attributes transmitted

The user name is the only transmitted identity attribute. In order to protect the authenticity / integrity / confidentiality of the identity attribute during transmission, a secure connection must be established with a suitable mechanism prior to transmission.

4.6.1.2 Linking the identity attributes transmitted to the authorised person

The transmitted identity attributes are linked to the authorised person by means of a (secret) password.

4.6.1.3 Data economy and volatile identification

The only identity attribute which is transmitted is the user name which is minimal in terms of the purpose of use. This is not a permanent identification, since no cryptographic mechanisms are used.

4.6.2 Assurance level

With this mechanism, only the *normal* assurance level can be achieved.

4.7 SSL connection and certificates

The usual mechanism on the internet for the establishment of a secure connection to a service, and in this context the identification of the service, is the establishment of an SSL connection with certificate-based identification of the service and/or domain (host name) on which the service is provided. SSL stands for *Secure Socket Layer p*rotocol, TLS is the abbreviation for the subsequent *Transport Layer Security* protocol. Following general usage, the abbreviation "SSL" is used hereinafter.

For evaluation, this Guideline assumes the use of SSL according to the requirements provided in [TR-03116], part 4, i.e. in particular, the use of suitable protocol versions and suitable cipher suites.

When using SSL, a certificate for the service is required for the application of SSL by means of which the service and/or domain identifies itself to the citizen. In the World Wide Web, i.e. outside closed systems, the certificates are based on the “Internet PKI” according to [RFC5280]. In order to ensure that the citizen can trust this certificate, it must be issued by a certification authority which is considered trustworthy in common browsers. The protocol establishes an end-to-end connection between the identified service and the browser, i.e. the citizen.

In general, different types of SSL certificates are classified which mainly differ in how profoundly they verify the authentication and authorisation of the persons applying for a certificate for a specific domain:

- *Domain Validation* (DV): The only thing which is checked is whether the person applying for a certificate can receive the e-mails sent to the domain. No other checks regarding the service or the authorisation of the applicant are carried out. The process does not provide any protection against man-in-the-middle attacks. DV certificates must not be used for e-government applications.
- *Organisation Validation* (OV): The authorisation of the applicant to use the domain is checked. Additionally, a limited check is carried out to determine whether the service provider exists.
- *Extended Validation* (EV): An additional explicit identity check of the service provider on the basis of official registers is carried out. Furthermore, the authorisation of the applicant for the application process is checked. The domain must be controlled by the service provider only.

The exact processes depend on the certification authority.

4.7.1 Functions

4.7.1.1 Authentication / integration of the transmitted identity of the service

The identity of the service is cryptographically secured as an integral part of the SSL certificate. During the establishment of the SSL connection, the association of the certificate with the service is proven by proving the corresponding private key.

4.7.1.2 Secure connection linked with the identity of the service

A secure connection is established by a cryptographic key agreement (SSL handshake). The identity of the service is used for the establishment of the connection in the form of a certificate and/or its corresponding key.

4.7.2 Assurance level

The *high* assurance level for the identification of the service can only be achieved subject to the following conditions:

- It is necessary to use extended validation certificates of trustworthy certification authorities. In this context it must be ensured that citizens actually check that an extended validation certificate is provided for connection establishment. This can, for example, be accomplished by checking the address bar of the browser.
- There are numerous certification authorities for SSL certificates worldwide each of which can issue SSL certificates for all websites. If one certification authority is compromised, all websites are at risk, not only those websites which use a certificate of this certification authority. In case of the acute compromising of a certification authority, the *high* assurance level for the service identification on the basis of a SSL certificate cannot be achieved – irrespective of the assurance level of the certificate which is used by the service itself.

If an SSL connection is authenticated by means of the channel linking of the electronic proof of identity (see section 4.3), the assurance level of the connection does not depend on the SSL certificate because the service is identified by the enrolment process of the procurement office for authorisation certificates.

The compliance with the requirements provided in [TR-03116], part 4, is the prerequisite for the use of SSL connections as a secure connection and SSL certificates for the identification of services.

5 Declaration of intent

A declaration of intent is the expression of a will aimed at the implementation of a legal effect by the person declaring this will. Within the scope of this Guideline, a declaration of intent includes the approval of a process or the content of a document. As the approval of a process can be replaced by the approval of a document which includes the process data, only the case of the approval of a document will be given consideration hereinafter.

The declaration of intent will only become effective when received by the recipient, which means that the document must be transmitted "on behalf of" after the declaration of intent has been made.

5.1 Functions

As per administrative law, the highest assurance level for the declaration of intent is achieved in written form, thus mapping the characteristics of a typical signature from which the following functions are derived (quoted from [BRSchriftform]):

- *Perpetuation function: In administrative law, as well, the written form always requires the embodiment of the declaration in a document. The embodiment of the declaration in a document (document unit) ensures that the declaration is recorded on a sustained basis. Thus it is possible to check its content.*

- *Warning function: In order to adhere with the written form, a genuine signature of the declaration is required. Thus, by the conscious act of signing, the person declaring the will is advised of the increased statutory liability and the personal responsibility of signing the declaration. This is to protect the persons declaring their will against precipitance.*

- *Conclusion function: The declaration is concluded spatially by the genuine signature; only the part above the signature is part of the declaration. For declarations which do not have to be received, the genuine signature also separates the binding declaration from the draft.*

- *Identity and verification function: The person issuing the document can be recognised and identified by the distinctive signature by name because the unique signature establishes a unambiguous connection with the person behind the signatory. In case of a dispute, for example, the identity can be verified by comparing the signatures.*

<table>
<tr><th rowspan="2">Assurance level</th><th colspan="3">Declaration of intent</th></tr>
<tr><th>Electronic signatures
(section 5.3)</th><th colspan="2">Not signature-based</th></tr>
<tr><td>High +</td><td>Qualified electronic signature</td><td colspan="2">Form in association with the electronic proof of identity (section 5.4) /
De-Mail with secure login
(section 5.5)</td></tr>
<tr><td>High</td><td>Advanced electronic signature with hardware token</td><td>--</td><td rowspan="2">TAN process
(section 5.6)</td></tr>
<tr><td>Normal</td><td>Advanced electronic signature with software certificate</td><td>User interaction
(section 5.7)</td></tr>
</table>

Table 7: Mechanisms for the declaration of intent

- *Authenticity function: The spatial connection of the signature with the document containing the declaration establishes a connection between the declaration and the signature. This is to guarantee that the content of the declaration originates from the signatory and that it cannot be falsified at a later time.*

- *Function of proof: The embodiment of the declaration in a document which bears the genuine signature of its originator constitutes a piece of evidence. The document provides proof for the content and the originator of the document. This proof can be shown on the basis of the verification function of the signature, in particular by means of a signature comparison.*

These functions must be implemented by means of an electronic mechanism which is to cover the written form in general for the communication between citizens and government agencies.

However, for many applications, the written form is not essentially mandatory. According to § 10 [VwVfG], administrative actions in general do not require any form. The written form due to statutory formal requirements is only mandatory for some administrative services. Thus, the operators of e-government business processes must assess which functions are relevant for the business process and which functions can be gone without.

If the written form is required by law, it can be replaced by the electronic form according to § 3 a [VwVfG] unless otherwise regulated by a legal provision; it can be replaced:

1. by a qualified electronic signature (see section 5.3);
2. by the declaration of intent on a form at the authority in association with the electronic identity function (see section 5.4), or
3. by De-Mail with the sending option "confirmed by the sender" (see section 5.5)[7].

In the cases 2 and 3, the functions of the written form which are not directly covered by the mechanism, must be replaced by appropriate measures provided for by the authorities (see section 5.4 and 5.5).

Processes which are not based on signatures can generally not secure all functions of the written form themselves. For example, the completion function can usually not be implemented by means of TAN processes. If required for the business process, the functions which are not represented by the process itself must be replaced by technical and organisational processes such as the recipient of a declaration of intent or reliable third parties.

5.2 Criteria for assurance levels

In addition to the basic criteria mentioned in section 3, the following specific criteria for issuing a declaration of intent can be used to assign mechanisms to certain assurance levels (see table 8).

5.2.1 Assurance level of the identification of the person declaring a will

The identification of the person declaring a will must be at least carried out on the aimed assurance level of the mechanism for issuing a declaration of intent, see section 4.

5.2.2 Integrity protection of the document

The integrity of the document must be ensured in the long term. The required period results from the requirements of the specialised process and the statutory retention periods. In cases in which the document

7 The possibility of using De-Mail as a replacement for the written form according to VwVfG will come into effect on July 1st, 2014.

Declaration of intent	Assurance level		
	Normal	**High**	**High+**
Assurance level of the identification of the person declaring a will (see section 4)	*Normal*	*High*	*High +*
Integrity protection of the document	Organisational	Cryptographic or organisational by a trustworthy authority (see section 3.2.2)	Cryptographic or organisational by a a government agency / authority approved by the government agency (see section 3.2.3)
Linking identity to the document	Organisational	Cryptographic or organisational by a trustworthy authority (see section 3.2.2)	Cryptographic or organisational by a a government agency / authority approved by the government agency (see section 3.2.3)
Triggering of the declaration	Simple user interaction	Attributable to the user on a *high* assurance level	Attributable to the user on a *high* + assurance level

Table 8: Additional criteria for the “declaration of intent”

consists of several parts, all parts of the document must be protected (concluding function). For example, the document consists of the form and the data entered if it has been submitted via a web form.

For the *normal* assurance level, organisational safeguarding the integrity, e.g. storage of the document by the recipient in a database, is sufficient.

In order to achieve a *high* assurance level in this way, the document must be stored by an authority which has been approved as trustworthy authority for this process.

For the *high +* assurance level, the document must be stored in an electronic file by a government agency and/or an authority which has been verified by the government agency for this purpose (see section 3.2).

As an option, the document can also be stored by encryption, e.g. by the cryptographic signature of the document by a trustworthy authority / government agency or by permanent archiving according to [TR-03125].

5.2.3 Linking identity to the document

The identity must be linked to the document representing the declaration of intent in such a way that it is permanently verifiable. This can be achieved in different ways. For the *normal* assurance level, an organisational linking is sufficient, e.g. the storage of document and identity on one database. In order to achieve a *high* assurance level in this way, the organisational linking must be made by an authority which is reliably approved for this process; for the *high +* assurance level, it must be done by a government agency and/or an authority which has been approved by the government agency for this purpose (see section 3.2).

As an option, cryptographic linking is also possible, e.g. by a cryptographic signature on the document together with the identity data put together by a trustworthy authority / government agency, or by a signature on the document including a key with clear attribution of the identity (certificate).

5.2.4 Triggering the declaration of intent

The easiest way to make a declaration of intent is by user interaction (e.g. clicking on a button). On the *high* / *high +* assurance level, it must be possible to attribute the triggering of a declaration on a certain level to the user. This can, for example, be accomplished by triggering the declaration within a secure connection according to section 4 after having identified the user on the desired assurance level during connection establishment. If the identification is programmed accordingly (e.g. PIN entered directly prior to the declaration of intent), it is possible that the identification itself will trigger the declaration.

5.3 Electronic signatures

The use of electronic signatures for securing the declaration of intent is regulated in the Digital Signature Act [SigG]. The Digital Signature Act defines three different forms of electronic signature:

- *(Simple) electronic signatures* are data in electronic form which are added to other electronic data or are logically linked with them and which are used to authenticate a document or a process. This can, for example, be a signature at the end of an e-mail or a scan of a handwritten signature.
- *Advanced electronic signatures* are electronic signatures which
  1. are exclusively attributable to the owner of the signature key,
  2. allow for the identification of the owner of the signature key,
  3. are generated by means which are under the sole control of the owner of the signature key, and
  4. are linked with the data to which they refer such that any additional modification of the data can be detected.

  In general, advanced electronic signatures are technically implemented by asymmetric cryptographic signatures. Here, it is essential that the private key is under the sole control of the owner. In this context, it must be distinguished between storing the private key in the owner's computer system (software token or "software certificate"[8]) or storing it on a dedicated secure hardware token.
- *Qualified electronic signatures* are advanced electronic signatures which
  5. are also based on a qualified certificate valid at the time of generation, and
  6. are generated with a secure signature creation unit (i.e. with a hardware token which meets the requirements of the Digital Signature Act).

(Ordinary) electronic signatures are not given further consideration in this Guideline.

5.3.1 Functions

Advanced / qualified electronic signatures are basically suitable for fulfilling the functions regarding the declaration of intent.

- The functions of authenticity and conclusion are implemented by the creation of a cryptographic signature for the whole document. It is not possible to subsequently add or change data without impairing the validity of the signature.

8 This (usual) description is not precise, because the storage of the private key is decisive, not the storage of the corresponding (public) certificate.

- The functions of identification and verification are implemented by the certificate attributed to the key which includes the identity of the key owner. A corresponding certificate is clearly attributed to the signed document by means of the signature.
- The warning function is implemented by the key owner triggering the signature creation. Automatically created signatures do not meet the requirements which exist for warning functions.
- The functions of proof and perpetuation are implemented by the cryptographic verifiability of the signature. If the maintenance of the value of proof / perpetuation is required beyond the forecast period for suitable cryptographic algorithms and key lengths as per [SigKat], the value of proof must be maintained by means of mechanisms according to [TR-03125].

5.3.2 Assurance level

The *high* assurance level is only achieved if the creation of an electronic signature is secured by two factors, i.e. for an advanced electronic signature with suitable hardware token (see section 3.1) or with a qualified electronic signature. The requirements of the algorithm catalogue [SigKat] must be met.

According to the Digital Signature Act (([SigG] §6 (2)) and [VwVfG] §3 a, the qualified electronic signature has the same legal status as the typical written form (replacement for the written form), thus achieving the *high +* assurance level.

5.4 Form in association with the electronic proof of identity

According to § 3 a [VwVfG], a declaration of intent substituting the written form can be made by means of an electronic form provided by the government agency if the person declaring the will can be identified by the electronic proof of identity (see section 4.3):

> *§3 a sentence 4 VwVfG*
>
> *The written form can also be substituted*
>
> *1. by directly making a statement on an electronic form provided by the government agency on an input device or via networks accessible to the public;*
>
> *2. - 4. [...]*
>
> *In the cases of sentence 4 number 1, a reliable proof of identity according to § 18 of the Identity Card Act or according to § 78 section 5 of the Residence Act is required for the input via networks accessible to the public.*

Using a form in combination with the electronic proof of identity in order to make a statement can be compared to the typical declaration of intent for the record / by appearance in person, when an employee of the government agency identifies the person declaring the will and records the statement. A signature by the person declaring the will is not required in this case. The use of forms in association with the electronic proof of identity as a replacement of the written form is described in part 2 of this Guideline ([TR-03107-2]).

5.4.1 Functions

The electronic identity of the ID card / residence permit with secure administrative actions fulfils the indicated functions under the following conditions (translated quote from [BRSchriftform], details are provided there):

According to its primary purpose, the electronic proof of identity allows in particular the implementation of the identity function of the written form. The warning function can also be fulfilled by entering the elD PIN, if necessary, together with a note regarding the planned transaction. [...]

If required, the remaining functions of the written form (conclusion, perpetuation, authentication, verification and proof of the written form) can be mapped for the communication with state authorities by technical / organisational measures within the involved state authority meeting appropriate security requirements.

If the functions of conclusion, perpetuation, authentication, verification and proof are required for the business process, they can be implemented for example by means of a secured transmission from the citizen to the government agency in connection with the subsequent cryptographic signature of the processed data by the government agencies or their storage in a trustworthy IT system of the government agency (for details in this respect, see [TR-03107-2]). For the perpetuation function, see also section 5.3.

5.4.2 Assurance level

The identification on the *high +* assurance level is ensured by using the electronic proof of identity. The assurance level of the whole process depends on the implementation of further functions – as necessary – by the government agency.

5.5 De-Mail

According to § 3 a [VwVfG], a declaration of intent substituting the written form can also be made by De-Mail (see section6.3) if the person declaring the will can be identified by using the option "confirmed by the sender" according to §5 (5) [De-Mail-G]:

§3 a sentence 4 VwVfG

The written form can also be substituted

1. [...]

2. for applications and notifications by sending an electronic document to a government agency using a mode of dispatch according to § 5 section 5 of the De-Mail Act;

3. for electronic administration files or other electronic documents of the government agencies by sending a De-Mail message according to § 5 section 5 of the De-Mail Act, if the issuing government agency can be identified as the user of the De-Mail account through the confirmation of the accredited service provider;

4.[...]

5.5.1 Functions

De-Mails fulfil the indicated functions and the conditions specified in the Federal Administrative Procedures Act [VwVfG](see above):

The option "confirmed by the sender" according to §5 (5) [De-Mail-G] is only available after the owner of the account has logged on to his De-Mail account on the basis of "secure login" according to §4 (1) sentence 2. Details on how to fulfil the perpetuation function are provided in section 5.3.

5.5.2 Assurance level

When logging on to the user account with "secure login" (see [VwVfG] §3 a), the *high +* assurance level is reached.

5.6 TAN systems

A user account is required for every TAN system. In order to achieve a certain assurance level, it is necessary to create the user account at least on this level. Since there are numerous different TAN systems, it is not possible to completely classify the systems.

Examples of TAN systems:

- The typical TAN system (TAN list using any TAN from the list) is not admitted for e-government applications due to the many known practical attacks.
- iTAN system: Indexed TAN lists are used; the TAN to be used is provided by the relying entity.
- The mTAN system (mobile TAN, also referred to as smsTAN) uses the connection with a registered mobile phone for the transmission of the TAN specific for the process.
- Systems based on TAN generators (also referred to as chipTAN) use a separate hardware - the TAN generator - to create transaction-specific TANs.

5.6.1 Functions

The use of TAN systems can cover the following functions:

- The warning function is covered by the citizen by TAN input.
- The identification function is fulfilled by the attribution of the TAN list / mobile phone / TAN generator to a certain person. The *high* assurance level can only be achieved if suitable mechanisms against brute-force attacks on the TAN (such as a maximum operating error counter) are used. The stipulations contained in section 3.1 apply accordingly.
- The functions of authenticity and conclusion can be implemented for the data which are used for creating a TAN. Due to the low entropy of the TAN (typically six characters), only the *normal* assurance level can be achieved for this function.

If required for the business process, any further function must be covered by additional safeguards.

5.6.2 Assurance level

The *high* assurance level can only be achieved with TAN systems which include the major process data in the creation of the TAN and is shown to the user independently of the primary connection between the citizen and the government agency. Furthermore, the system must implement a two-factor authentication (see section 3.1) irrespective of the primary connection between citizen and government authority.

- It is presently still possible to use the iTAN system for the *normal* assurance level; however, it no longer corresponds to the state-of-the-art technology and should be replaced by another system as soon as possible. For new systems, the iTAN system must no longer be used.

- The *high* assurance level can be achieved for the mTAN system under the following conditions only:
  - The mobile phone (or the phone number, to be precise) is registered on the account of the citizen at the government agency only after the identification of the citizen at least on the *high* assurance level (see section 4).
  - The primary connection between citizen and government agency is not established via the mobile phone but via a separate end device and a different network.
  - The mTAN system implements a two-factor authentication via the mobile phone (possession factor) and the access code (PIN; gesture – knowledge factor) of the mobile phone. Therefore, the system may only be used by mobile phones which have an enabled and effective access locking mechanism.

  According to the current status of evaluation, the mTAN system for new systems should no longer be used for the *high* assurance level.
- The *high* assurance level can be achieved with a TAN generator under the following conditions:
  - The TAN generator must be individual, i.e. the generators of different owners may not be exchangeable. This condition is also fulfilled if the generator itself is individualised by a chip card.
  - The generator / chip card (possession factor) is protected by a PIN or the like (knowledge factor). The criteria of section 3.1 are applicable.

  Due to the large number and different forms which are specific to the respective manufacturer, it is not possible to provide a concluding evaluation of all systems. Such an evaluation must be carried out on the basis of these defined criteria by reference to the specific system and its implementation.

5.7 User interaction

A declaration of intent on *normal* assurance level can also be made by an ordinary user interaction such as clicking on an accordingly labelled push-button. It is, however, required that a secure connection between citizen and government agency has been established before and that a mechanism identifies the citizen at least on the *normal* assurance level (see section 4). The functions of identification and warning are then both covered on the *normal* assurance level.

If required for the business process, any further function must be covered by additional safeguards.

6 Transmission of documents

A major process in e-government is the transmission of documents between persons and government agencies, such as the transmission of applications or messages, or vice versa the query of government agency information by an identified person.

A distinction must be made between the mere transmission of documents which is explained in this section, and a possibly associated declaration of intent made for example to conclude an application (see section 5).

6.1 Functions

Any system for the secure transmission of documents must cover the following functions:

- Confidentiality of the document during transmission. The required level of confidentiality protection of the document mainly depends on the content of the document.
- Integrity of the document during transmission. This function only ensures that the document is not changed during transmission. The authenticity of the document requires the identification of the sender and that the integrity during transmission is ensured.
- Identification of the recipient. This is required to ensure the confidentiality of the document because only by identifying the recipient is it ensured that the recipient is the only person who receives the content of the document.
- (Optional) Identification of the sender. For the mere transmission of the document, the identification of the sender is not required. Depending on the application, it may, however, be relevant for the administrative processes triggered by the transmission.

Depending on the operational scenario and/or the documents transmitted, it may be necessary to identify /address an organisational unit of a government agency or also an individual employee of the government agency directly as the recipient and not a government agency.

6.2 Criteria for assurance levels

In addition to the basic criteria mentioned in section 3, the following specific criteria for the transmission of documents can be used to assign mechanisms to certain assurance levels (see table 10).

<table>
<tr><th rowspan="2">Assurance level</th><th colspan="3">Secure transmission of documents</th></tr>
<tr><th colspan="2">Person ↔ government agency</th><th>Government agency ↔ government agency</th><th>Web upload</th></tr>
<tr><td>High +</td><td colspan="2" rowspan="2">De-Mail
with secure login</td><td></td><td>... with electronic proof of identity</td></tr>
<tr><td>High</td><td rowspan="2">OSCI with end-to-end encryption / signature</td><td></td></tr>
<tr><td>Normal</td><td>De-Mail</td><td>e-mail with S/MIME</td><td>OSCI with transport encryption / signature</td><td>... with SSL certificate (assurance level according to section 4.7)</td></tr>
</table>

Table 9: Mechanisms for the secure transmission of documents

Transmission of documents	Assurance level		
	Normal	**High**	**High+**
Identification of the recipient according to section 4	*Normal*	*High*	*High +*
Identification of the sender according to section 4 (opt.)	*Normal*	*High*	*High +*
Encryption and integrity protection	On transport level	End-to-end / recoding only by trustworthy authorities (see section 3.2.2)	End-to-end / recoding only by a government agency / authorities approved by the government agency (see section 3.2.3)
Linking the identity of the recipient and sender to the transmitted document	Organisational	Cryptographic or organisational by a trustworthy authority (see section 3.2.2)	Cryptographic or organisational by a government agency / authority approved by the government agency (see section 3.2.3)

Table 10: Additional criteria for the “transmission of documents”

6.2.1 Identification of sender and recipient

The mechanisms provided in section 4 may be used for the identification of sender and recipient. The *high/high +* assurance level can only be achieved if the identification of the recipient and possibly also the identification of the sender have achieved this assurance level.

6.2.2 Encryption and integrity protection

The encryption / authentication on transport level is sufficient for the *normal* assurance level.

The use of a secure transport network (such as IVBB / IVBV, TESTA, Deutschland-Online-Infrastruktur) is sufficient for the *normal* assurance level provided that only trustworthy authorities are connected to the transport network. The use of a secure transport network is not sufficient for the *high* assurance level.

The *high / high +* assurance level for the transmission of documents can only be achieved if

- the end-to-end transmission is encrypted and authenticated, or
- the intermediate stations of the transmission have special, legally secured trustworthiness, and if the transmission between these stations is encrypted and authenticated. The requirements to be met for the trustworthiness of authorities (section 3.2) according to the assurance level apply to the intermediate stations.

The virtual mail centre (see [VPS]) and mechanisms for specialised processes based on it (such as the electronic court and administration inbox, see [EGVP]) are special cases of the second variant. If the virtual mail centre is used, the cryptographic functions of encryption / decryption and signature generation / verification on behalf of the actual sender / recipient are carried out in a central authority operated by the addressed government agency. The virtual mail centre is thus an intermediate station between sender and

final recipient which is operated by the receiving government agency itself and is thus trustworthy and does not preclude assigning the method to the *high* / *high +* assurance level.

6.2.3 Linking the identities to the transmitted document

For the *normal* assurance level it is sufficient if the identities of the recipient (and possibly the sender) are linked organisationally to the transmitted document. For the other assurance levels, the linking must be accomplished by cryptographic mechanisms or organisationally by trustworthy authorities (*high* assurance level) or government agencies / authorities approved by the government agencies (*high +*).

If several authorities are involved in the transmission of documents, and the identities are linked organisationally, the assurance level of the linking is the lowest assurance level of the involved authorities.

6.3 De-Mail

The De-Mail concept allows for the authentic, confident and binding exchange of messages and documents via the internet. These De-Mail features are ensured by the following basic statutory requirements (see [De-Mail-G]) for operation:

As a closed system, De-Mail may only be operated by accredited De-Mail service providers (DMDA) and provided for potential users.

On the other hand, De-Mails can only be sent and received by users who have been clearly identified by the respective DMDA.

De-Mails are transmitted via encrypted channels. For inter-DMDA transmission, an additional content encryptions is used.

Accessing the account / login is possible on the basis of two different authentication levels.

- On the one hand, access on the basis of the *normal* authentication level is possible by a combination of user name and password. Compared to the *high* authentication level, the scope of functions is restricted here.
- On the other hand, if a token is used (possession and knowledge), the *high* authentication level can be achieved and thus the complete scope of functions is available (and thus the *high* + assurance level).

6.3.1 Functions

The functions are covered as follows:

6.3.1.1 Confidentiality and integrity of the document

Securing is carried out by means of SSL encryption and partially(inter-DMDA) by means of S/MIME encryption.

In some specialised sectoral legislation (for example, §67 (6) SGB X with respect to social data, §87a (1) AO), it is standardised that this securing in connection with the safeguards defined by [De-Mail-G] is suitable for the transmission of corresponding specialised data.

In general, it must be observed that end-to-end encryption might be additionally necessary when sending documents with particularly sensitive data (§3 (9) BDSG). This requires encryption and decryption by the communication partners themselves, i.e. it implies that corresponding software is installed on the systems of the communication partners which is supported by the De-Mail infrastructure. The communication

partners are responsible for agreeing upon the specific mechanisms for encryption; in this respect, the requirements provided in [TR-03116], part 4, must be complied with.

Identification of sender and recipient

Initial identification of the recipient according to section 4 by the DMDA according to the provisions provided in [De-Mail-G] and [TR-01201]. Initial identification to be accomplished by means of valid pieces of identification (e.g. ID card) or equivalent methods. Identification can be made electronically, for example, by means of the electronic proof of identity of the ID card / residence permit in order reach the *high +* assurance level.

Each authentication prior to an application (sending and receiving De-Mails) is possible on the basis of two different authentication levels:

- *Normal* authentication level using the user name / password with the resulting restriction of the account functionality regarding the subsequent use (e.g. no use of the sending options “personal” and “confirmed by the sender” when sending De-Mails, and no reading access of De-Mails received in the inbox with the sending option “personal”)
- *High* authentication level by additionally using a token (e.g. electronic proof of identity) with resulting complete account functionality.

6.3.2 Assurance level

Depending on the authentication level of the sender at the time of sending, at least the *normal* assurance level is applicable to messages / documents transmitted by De-Mail services in compliance with [De-Mail-G] and [TR-01201]. If the authentication level of the sender is *high*, the *high +* assurance level is achieved due to statutory regulations.

6.3.3 Delivery

If the option ”Collection confirmation” according to §5 (9) [De-Mail-G] is used, documents can be officially delivered by De-Mail. This option is only available, if “secure login” is used.

6.4 E-mail with S/MIME

S/MIME (Secure / Multi-purpose Internet Mail Extensions) is an IETF standard (see [RFC5750], [RFC 5751]) for the cryptographic protection of e-mails and files. With S/MIME messages can be cryptographically signed and/or encrypted. Technically, the encryption is implemented by hybrid cryptography and the signature by asymmetric cryptography. To this end, S/MIME provides appropriate cryptographic processes and message formats (based on the CMS standard [RFC 5652]).

The communication partner for S/MIME is authenticated by X.509 certificates. They must be issued by a confidential certification authority in order to ensure the trust of the communication partners in the certificates. In most cases, the same PKI structures are used as for issuing SSL certificates (see section 4.7).

6.4.1 Functions

When using e-mails with S/MIME, the necessary functions of secure document transmission are covered as follows.

6.4.1.1 Confidentiality and integrity of the document

Confidentiality is implemented by the S/MIME encryption of the transmitted document. Only the owner of the key can decrypt the transmitted encrypted document.

The integrity of the document is protected by a signature across the complete transmitted document. Therefore, with any modification of the document, the signature will loose its validity.

6.4.1.2 Identification of the recipient

For the identification of the recipient, the certificate attributed to an encryption key is used which confirms the identity of the appropriate owner of the key. The assurance level of the identification depends on the X.509 certificate of the recipient, i.e. on the confidentiality of the certification authority and the quality of the enrolment.

6.4.1.3 Identification of the sender

The sender is identified by the certificate attributed to a signature key which confirms the identity of the appropriate owner of the key. The assurance level in the identification depends on the X.509 certificate of the sender (see above). Since the protection of integrity for document transmission via S/MIME is made by a signature, the identification of the sender is mandatory.

6.4.2 Assurance level

With document transmission by e-mail with S/MIME, the *normal* assurance level can be achieved when using the Internet PKI (see section 4.7) for the identification of sender / recipient. When using a dedicated PKI and excluding the Internet PKI, it might be possible to reach a higher assurance level.

The cryptographic requirements for the use of S/MIME as specified in [TR-03116], part 4 must be complied with. For the identification of recipient and sender, the provisions made in section 4 as well as in [TR-03116], part 4, are decisive.

6.5 OSCI

The OSCI transport standard is a protocol which is used by many XML standards of public administration (XÖV projects in most cases). In this context, the protocol offers a framework which is used by the respective standards.

The specification is updated and issued by the KoSIT (coordination authority for IT standards) in the [OSCI] document.

OSCI transport offers a variety of configuration options. These refer in particular to the different types of basic message process (synchronous / asynchronous, etc.) as well as to the alternatives for communication protection. The starting point for the communication scenario is the implementation of the principle of double envelope. Thus, a distinction is made between author and sender as well as between recipient and reader.

The specification is available in two relevant versions:

- Version 1.2 is an established standard focussing on government agency communication; communication is based on the transmission of messages by a third authority(intermediary);
- Version 2.0 focuses on the interoperability with standard implementations as web service profiling, supplements it by acknowledgement mechanisms / inbox functionality and, if synchronous, also

allows direct communication. When using public networks / asynchronous communication, end-to-end encryption must be used.

OSCI transport is used both for the communication between government agencies and for the communication between persons and public authorities (e.g. notary / court). In this Guideline, only the second case is relevant.

6.5.1 Functions

6.5.1.1 Confidentiality and integrity of the document

Since OSCI itself does not stipulate any mandatory safeguards, the concrete measures to secure the confidentiality and integrity of the transmitted documents must be defined by each application using OSCI.

6.5.1.2 Identification of sender and recipient

In order to identify and address inboxes and intermediaries, if necessary, external services which must be involved when assessing the assurance level are used.

Most of the individual inboxes and intermediaries in this context are identified and addressed by the German Administrative Services Directory [DVDV]. In the DVDV, government agencies and authorities commissioned by government agencies can register services which in turn are available for others under the parameters registered there. This allows for the secure communication of the authorities with each other.

For the application of OSCI in the Electronic Court and Administration Inbox [EGVP], the SAFE infrastructure is used for identification and addressing.

6.5.2 Assurance level

The assurance level achieved with the OSCI transport solely depends on the provisions made by the appropriate OSCI-using standard. For the implementation of specific safeguards in the context of OSCI transport, the use of XML signature and XML encryption is provided for content data and user data. The contemplations made in chapter 3.6 apply accordingly.

Finally, it should be noted that the use of OSCI transport may cover a wide spectrum of assurance levels ranging from the *high* assurance level to completely waiving all security safeguards and thus achieving no assurance level.

6.6 Web upload

For document transmission via browser-based web upload, a secure connection (SSL connection) between citizen and service is established on the basis of the identification process according to section 4. Depending on the process used, only the service (for the identification of services on the basis of an SSL certificate) or also the citizen (when an electronic proof of identity is used) is identified. Then the document is transmitted within the established connection (“upload”).

Within this service, the document transmitted is either kept available for collection by means of a specialised process and/or by an authorised person in a government agency or transmitted to them. For this purpose, the sections 6.1 and 6.2 apply accordingly, whereby criteria can also be covered by organisational safeguards of the government agency and/or within the framework of the security concept of the government agency.

6.6.1 Functions

The functions are covered as follows:

6.6.1.1 Confidentiality and integrity of the document

Protection by the SSL connection, see section 4.7.

6.6.1.2 Identification of the recipient

Identification of the recipient according to section 4. If the electronic proof of identity is used, the recipient is identified on this basis, i.e. the recipient is identified on the *high +* assurance level, irrespective of the kind of SSL certificate used ("channel linking", see section 4.3). If the electronic proof of identity is not used, the assurance level of identification depends on the SSL certificate (see section 4.7).

If documents with particularly sensitive personal data are to be transmitted, additional safeguards to protect the identity of the final recipient (organisational unit in the government agency, employee of the government agency) might have to be taken.

6.6.1.3 (Optional) Identification of the sender

If the electronic proof of identity is used, the sender (citizen) can be identified as well. If an SSL certificate is used, the sender must be identified by additional identification according to section 4 (if required for the application).

6.6.2 Assurance level

For SSL connections, the requirements provided in [TR-03116], part 4, must be met. For the identification of the recipient and, if necessary, of the sender, the provisions of section 4 must be observed.

7 Transmission of identity data

The transmission of identity data must be considered to be a special case of transmitting a document. What is meant is the transmission of personal attributes stored with an identity provider to an identified recipient. Here, the transmission of the identity attributes must be explicitly initiated by the person identified by means of the data (in the following, referred to as data holder).

7.1 Functions

A system for the secure transmission of identity data must include the following functions, see also section 6.1:

- Confidentiality of the identity data during transmission.
- Integrity of the identity data during transmission. This function only ensures that the identity data is not changed during transmission. The authenticity of the data requires the identification of the sender and that the integrity during transmission is ensured.
- Identification of the recipient. This is required to ensure the confidentiality of the identity data, because only by identifying the recipient is it ensured that the recipient is only person who can receive the data.

In addition to the functions derived from the functions for the transmission of documents, a mechanism must include the following functions for the transmission of identity data:

- Identification of the data holder. The data stored with the identity provider must be collected by means of the secure initial identification of the data holder.
- Secure storage of the identity data with the identity provider. The identity provider keeps and maintains an account with the identity data collected. The data must be stored in a secure (confidential, authentic) manner.
- Logging on to the account of the data holder and triggering the data transmission. It must be ensured that only the data holder can initiate the transmission of the identity data.

The assurance level required for the confidentiality of the identity data / identification of the recipient depends on the data itself and might thus deviate from the assurance level required for the other functions. The assessment assumes an uniform assurance level for all functions.

7.2 Criteria for assurance levels

In addition to the basic criteria provided in section 3, specific criteria for the transmission of identity data are mentioned in table 11, which are used to assign a mechanism to an assurance level. Explanations of the criteria can be found in sections 4, 3.2 and 6.2.2.

Transmission of identity	Assurance level		
	Normal	**High**	**High +**
Identification of the recipient according to section 4	*Normal*	*High*	*High +*
Encryption and integrity protection according to section 6.2.2	*Normal*	*High*	*High +*
Initial identification of the data holder according to section 4	*Normal*	*High*	*High +*
Secure storage of the identity data according to section 3.2	*Normal*	*High*	*High +*
Logging on to the account of the data holder according to section 4	*Normal*	*High*	*High +*

Table 11: Additional criteria for the “transmission of identity data”

7.3 Identity confirmation service according to De-Mail-G

The identity confirmation service according to [De-Mail-G] §6 uses the De-Mail infrastructure (see section 6.3) for the transmission of identity data. Here, the De-Mail service provider keeping and maintaining the account of the data holder acts as identity provider.

7.3.1 Functions

The functions are covered by the corresponding functions of the De-Mail infrastructure, see section 6.3. The requirements to be met in order to reach an assurance level apply accordingly.

7.3.2 Assurance level

The identity confirmation service is only available for “secure login”. For the functions of integrity protection, identification of the data holder, storage and logging on to the account, at least the *high* assurance level is therefore applicable to identity data transmitted by De-Mail services in compliance with [De-Mail-G] and [TR-01201]. The assurance level of the other functions depends on the assurance level of the identification of the recipient.

For the identification of the recipient, the initial identification of the data holder and logging on to the account of the data holder on the *high* assurance level, the *high +* assurance level is achieved due to statutory regulations.

References

[DVDV]	BIT: German Administrative Services Directory - process description
[AIS 20/31]	BSI: AIS 20/31 -- A proposal for: Functionality classes for random number generators
[BSI100-2]	BSI: BSI Standard 100-2: IT-Grundschutz Methodology
[GS]	BSI: IT-Grundschutz-catalogues, https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[TR-01201]	BSI: Technical Policy TR-01201, De-Mail
[TR-02102]	BSI: Technical Policy TR-02102, Cryptographic processes: recommendations and key lengths
[TR-03116]	BSI: Technical Policy TR-03116, Technical policy for the eCard projects of the Federal Government.
[TR-03124]	BSI: Technical Policy TR-03124, eID-Client
[TR-03125]	BSI: Technical Policy TR-03125, Retention of evidence of cryptographically signed documents
[TR-03127]	BSI: Technical Policy TR-03127, Architecture of electronic ID card and electronic residence permit
[TR-03132]	BSI: Technical Policy TR-03132, Secure scenarios for communication processes for sovereign documents (TR SiSKo hD)
[SigKat]	Federal Network Agency: Bulletin regarding the electronic signature as per Digital Signature Act and Signature Regulation - Summary of suitable algorithms
[BRSchriftform]	Federal Government: Report of the Federal Government according to article 5 of the law ruling De-Mail services and amending further regulations (http://dipbt.bundestag.de/dip21/btd/17/107/1710720.pdf)
[RFC5750]	IETF: B. Ramsdell, S. Turner: RFC 5750, Secure/Multi-purpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling
[RFC 5751]	IETF: B. Ramsdell, S.Turner, Secure/Multi-purpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, 2010
[RFC 5652]	IETF: R. Housley, Cryptographic Message Syntax (CMS), 2009
[ISO24760-1]	ISO/IEC: ISO/IEC 24760-1: Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts
[ISO29115]	ISO/IEC: ISO/IEC 29115: Information technology -- Security techniques -- Entity authentication assurance framework
[OSCI]	OSCI control centre: OSCI transport 1.2, Specification
[AufenthG]	German Residence Act as amended with the announcement of 25 February 2008 (BGBl. I p.162), last amended by article 4 (5) of the act of 30 July 2009 (BGBl. I p. 2437)
[De-Mail-G]	De-Mail Act of 28 April 2011 (BGBl. I p. 666), amended by article 2 (3) of the act of 22 December 2011 (BGBl. I p. 3044)
[PAuswG]	Act on ID cards and the electronic proof of identity (Federal ID Card Act - PAuswG) of 18 June 2009 (BGBl. I p. 1346)
[SigG]	Digital Signature Act of 16 May 2001 (BGBl. I p. 876), last amended by article 4 of the act of 17 July 2009 (BGBl. I p. 2091)
[VwVfG]	Federal Administrative Procedures Act as amended with the announcement of 23 January 2003 (BGBl. I p. 102), last amended by article 2 (1) of the act of 14 August 2009 (BGBl. I p. 2827)
[EGVP]	Website of the electronic court and administration inbox, http://www.egvp.de
[VPS]	Website of the virtual inbox, https://www.bsi.bund.de/VPS