Federal Office
for Information Security

German eID based on Extended Access Control v2

LoA mapping: Mapping of the characteristics of the German eID scheme to the eIDAS Level of Assurance

Version 1.0

20 February 2017

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0

E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Introduction

This document maps the characteristics of the **German eID based on Extended Access Control v2** (in the following abbreviated as ***German eID***), to the requirements of the eIDAS Levels of Assurance defined in Commission Implementing Regulation (EU) 2015/1502 pursuant to Article 8(3) of the eIDAS Regulation [(EU) 910/2014].

For that purpose, we consider each requirement of the Implementing Regulation and explain how the German eID meets the requirements for Level of Assurance '**high**'.

The German eID is a scheme based on government-issued chip cards using strong cryptography. Currently, two types of ID cards are part of the eID scheme:

1. **Identity cards (Personalausweis)** issued to German nationals living in Germany or abroad, and
2. **Residence permits (Aufenthaltstitel)** issued to non-EU nationals living in Germany.

An overview of the system is given in [German eID].

The following national regulations and documents are relevant for the assessment of the Level of Assurance of the German eID:

- **Act on Identity Cards and Electronic Identification ("Personalausweisgesetz")** [PAuswG][1],
- **Ordinance on Identity Cards and Electronic Identification ("Personalausweisverordnung")** [PAuswV],
- **Residence Act ("Aufenthaltsgesetz")** [AufenthG],
- **Ordinance Governing Residence ("Aufenthaltsverordnung ")** [AufenthV]**,**
- **Technical Guidelines and Protection Profiles of the German Federal Office for Information Security (BSI)** referred to in Appendix 4 of [PAuswV].

The referenced laws and ordinances are published in the **Federal Gazette ("Bundesanzeiger")**, and are additionally available online at

- https://www.gesetze-im-internet.de.

The Technical Guidelines and Protection Profiles are available on the website of the BSI at

- Technical Guidelines: https://www.bsi.bund.de/EN/eID-TR,
- Protection Profiles: https://www.bsi.bund.de/EN/eID-PP.

As the German eID is part of different official documents (i.e., the German ID card and the German residence permit), this document distinguishes between the underlying documents, whenever applicable national laws and regulations differ.

1.1 Terminology

In the following, this document also uses the following terms:

- '***eID card***' for the official document if the statement holds for any of the official documents containing the German eID, i.e. for the German ID card as well as for the German residence permit;

1 The notification of the German eID will be based on an amendment of the [PAuswG] which is currently in the legislative process and will enter into force before notification, cf. [PAuswG_AMD].

- '***issuing authority***' for the authority responsible for enrolment and issuance of the eID cards, i.e.
  - the identity card authority for the German ID card and
  - the foreigner´s authority for the German residence permit.

2 LoA mapping

2.1 Enrolment

2.1.1 Application and registration

LOW, SUBSTANTIAL, AND HIGH

1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.

The terms and conditions related to the use of the German eID are defined by [PAuswG] and [PAuswV] for the German ID card and by [AufenthG], [PAuswG], [PAuswV] and [AufenthV] for the German residence permit. As part of the national legislation, the terms and conditions related to the use of the German eID are publicly available and legally binding for the applicant, as well as for other involved parties.

Additionally, the issuing authority is obliged to inform the applicant about the German eID and the measures necessary to ensure the secure use of the German eID as part of the application according to §11 (3) [PAuswG]. It must offer the applicant corresponding information material.

In addition, the German government operates a web portal 'https://www.personalausweisportal.de' that informs users (as well as businesses and government entities) about the functions, use and security aspects of the German eID.

2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means.

The mandatory and recommended security precautions related to the electronic identification means and its use are defined in §27 [PAuswG].

As stated above, §11 (3) [PAuswG] requires the issuing authority to inform the applicant about the German eID and the measures necessary to ensure the secure use of the German eID. It must offer the applicant corresponding information material. This includes information and links to information on mandatory and recommended security precautions.

In addition, the German government operates a web portal 'https://www.personalausweisportal.de' that informs users (as well as businesses and government) about the functions, use and security aspects of the German eID.

3. Collect the relevant identity data required for identity proofing and verification.

According to §9 (3), (4) and §5 (2), (5) [PAuswG], §86 [AufenthG] and [AufenthV], the responsible issuing authorities collect the relevant identity data required to verify the identity of the person beyond doubt at the time of application. In particular, this includes the data stored on the German eID (see §5 (2), (5) [PAuswG].

In addition, the relevant data are stored by the responsible authorities in dedicated (local) registers[2] (see §23 [PAuswG]) and §91a [PAuswG]. These data include the photograph of the card holder, the necessary processing notes, and at least the following data:

1. family name and name at birth,

2 The registers of the identity card authorities are local registers (generally the responsibility of the corresponding local municipality). For persons who need a residence permit, the register of the foreigner´s authority is a central register.

2. given names,
3. date of birth,
4. place of birth,
5. sex (residence permit only),
6. height (ID card only,
7. eye colour (ID card only),
8. signature (ID card only,
9. address (ID card only),
10. nationalities,
11. document number,
12. blocking code (for revocation purposes)
13. references to data records in which information on the foreigner is kept (residence permit only),
14. any former names, divergent spellings of names, aliases and other names used by the foreigner such as names pertaining to religious orders, pseudonyms or a family name under German law which differs from the family name entered in the passport (residence permit only).

These data include the Minimum Data Set of the German eID except the uniqueness identifier (pseudonym) that is only present on the German eID. Instead of the uniqueness identifier, the register stores the document number of the eID card which is in turn, for reasons of privacy, not stored in the German eID.

2.1.2 Identity proofing and verification (natural person)

The German eID is issued as part of the German ID card or the German residence permit. Therefore, registration for the German eID benefits from the strict regulation of official national procedures according to German law, particularly with regard to identity proofing and verification performed by the responsible issuing authorities. In particular, the procedures used at German national level by the entity responsible for the registration to obtain recognised ID evidence are inherently applied.

In addition to the fact that registration uses the very same procedures as for obtaining an official ID document, in the following, we also elaborate in detail on the common case that identity proofing and verification of the person is done via a recognised official photo ID document and/or data of the (local) register of the issuing authority to highlight how the technical controls of rationale 1a of level 'high' are also fulfilled in this case.

Details of the application process are as follows:

According to §9 [PAuswG], application for the German eID card must be carried out in person or – if necessary – by the applicant's legal representative and not by an authorised representative. The application for a German residence permit may also be submitted by an authorised representative according to the administrative directive §81.1.2 [AufenthVwV].

Exceptions to this general rule are only possible in very specific cases e.g. if the applicant is incapable of action or of providing consent and needs to be represented by a power of attorney, which in turn has to be publicly or notarially certified for this purpose. For minors under the age of 16 and for persons who are legally incapable and who do not have an authorised representative, the only person who may file an application on their behalf is the custodial adult responsible for supervising their residency.

In order to verify identity, the applicant and his/her legal or authorised representative must appear in person at the issuing authority. In equivalence to personal appearance, a staff member of the issuing authority may visit the applicant to receive the application for the German eID and to perform identity proofing and verification (cf. [PassVwV] §6.1.1.3), e.g. if the applicant is not able to visit the authority´s office.

The procedures for identity verification ensure that the eID is only issued if the identity of the applicant is verified beyond doubt[3]. These procedures are laid down in §9 [PAuswG] and further specified in §6 [PassVwV] for the German ID card and §49 [AufenthVwV] for the German residence permit. In general, identity verification as part of the registration procedure according to national law is done via an existing recognised official photo ID document, cf. § 6.3.1.1 [PassVwV] and §49.1.0 [AufenthVwV]. In addition, issuing authorities may use data of their dedicated registers for identity proofing and verification (cf. §23 (2) [PAuswG] and §64 [AufenthV]).

Note that in this case, the official photo ID document is itself an authoritative source.

However, there may also be cases where other procedures in accordance with the national administrative regulation have to be applied, e.g. if the person is not (yet) in possession of an official document because the ID card is the first such document.

In case of doubt regarding the applicant's identity, the issuing authority must request appropriate additional evidence and/or initiate the necessary measures to determine the applicant´s identity. The authority may arrange to have applicants photographed and fingerprinted by the police if it would otherwise be impossible or extremely difficult to determine the applicant's identity.

LOW

1. The person can reasonably be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.

See rationale 1.a of level 'high' (below).

2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.

See rationale 1a. of level 'high' (below).

3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.

Application for the German eID is carried out in person by the applicant and his/her legal or authorised representative. The official document used for identity verification (and/or registers of the issuing authorities) are authoritative sources. Hence, it is verified that the claimed identity exists. Part of the identity verification procedure is the verification that the applicant matches with the claimed identity on the official document comparing the person´s face with the photo on the document.

In case of doubt regarding the applicant's identity, the issuing authority must request appropriate additional evidence and/or initiate the necessary measures to determine the applicant´s identity before issuing the German eID. The authority may arrange to have applicants photographed and fingerprinted by the police if it would otherwise be impossible or extremely difficult to determine the applicant's identity.

Hence, this control is satisfied.

3 In the special case where the identity of an applicant for a residence permit cannot be verified, the residence permit is issued without eID and contains a remark, stating that the residence permit is not fit to be used for identification of the holder ("Identification information is based on information provided by the holder").

SUBSTANTIAL

Level Low, plus one of the alternatives listed in points 1 to 4 have to be met:

First, we provide the rationale why the German eID fulfils all requirements for the level 'substantial'. This provides the base for fulfilling the requirements of the level 'high', based on the alternative listed in point 1. Thus the points 2, 3, and 4 below are not applicable.

1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity

See rationale 1.a of level 'high'.

and

the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person

See rationale 1.a of level 'high'.

Further, if a recognised official photo ID document (and/or register data of the issuing authority) is used for identity verification, this document is checked to determine that it is genuine, and it is known that the evidence relates to a real person.

and

steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence;

See rationale 1.a of level 'high'.

or

2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it

N/A

and

steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;

N/A

or

3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for the registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council or by an equivalent body

N/A

or

4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.

N/A

HIGH

Requirements of either point 1 or 2 have to be met:

Here we provide the rationale why the German eID fulfils all requirements for level 'high' based on the alternative point 2. Additionally, we elaborate in detail on how the common case of identification via official photo ID documents (and/or register data of the issuing authority) complies with point 1.a. of level 'high'.

1. Level substantial, plus one of the alternatives listed in points a to c has to be met:

a. Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source;

If an existing recognised official photo ID document (and/or register data of the issuing authority) is used for identity verification, §6.3.1.1 of [PassVwV] and §49.1 of [AufenthVwV] ensure that the identity of the applicant is verified based on this document (and/or register data) and that the German eID is only issued if the identity of the applicant is verified beyond doubt. The official document and registers both are authoritative sources.

Part of the identity verification using the official document is the verification that the document is genuine and valid and that it represents the claimed identity. Hence, this control is satisfied.

In particular, the result of the verification is whether the official document relates to a real person (cf. 1. of level 'substantial') or not.

Otherwise, see also alternative 2. of level 'high'.

and

the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source;

If an existing recognised official photo ID document (and/or register data) is used for identity verification, §6.3.1.1 of [PassVwV] and §49.1 of [AufenthVwV] ensure that the identity of the applicant is verified based on this document and that the German eID is only issued if the identity of the applicant is verified beyond doubt. This includes at least the comparison of the applicant with the photo on the document. As the official document is itself an authoritative source, this control is satisfied.

or

b. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for the registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of

Regulation (EC) No 765/2008 of the European Parliament and of the Council or by an equivalent body

and

steps are taken that the results of this previous procedure remain valid;

N/A

or

c. Where, electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body

and

steps are taken that the results of this previous issuance procedure of a notified electronic identification means remain valid.

N/A

OR

2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level of the Member State of the entity responsible for the registration to obtain such recognised photo or biometric identification evidence are applied.

As the German eID is part of the German ID card or the German residence permit, application for the German eID always implies the issuance of a new eID card[4]. Consequently, the procedures used at German national level by the entity responsible for registration to obtain recognised ID evidence are inherently applied.

2.1.3 Identity proofing and verification (legal person)

As the German eID is only used for the identification of natural persons, 2.1.3 is not applicable.

LOW

1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made.

2. The evidence appears to be valid and can be assumed to be genuine, or to exist according to an authoritative source where inclusion of a legal person in the authoritative source is voluntary and is regulated by an agreement between the legal person and the authoritative source.

3. The legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person.

-

SUBSTANTIAL

4 In case of eID cards issued before application of [PAuswG_AMD] the eID functionality may disabled at time of issuance and can be enabled afterwards. However, the German eID is already present at time of issuance and a new application is not necessary. To enable the German eID in this case, the applicant has to appear in person at the issuing authority and is identified via a recognised photo ID document.

Level low plus one of the alternatives listed in points 1 to 3 has to be met:

1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and (if applicable to the legal person) its registration number-

and

the evidence checked to determine whether it is genuine, or known to exist according to an authoritative source, where inclusion of the legal person in the authoritative source is required for the legal person to operate within its sector

and

steps have been taken to minimise the risk that the legal person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;

2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 for the assurance level substantial, then the entity responsible for the registration need not repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body;-

or

3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.

HIGH

Level substantial plus one of the alternatives listed in points 1 to 3 has to be met:

1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and at least one unique identifier representing the legal person used in a national context-

and

the evidence is checked to determine that it is valid according to an authoritative source;

or

2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 for the assurance level high, then the entity responsible for the registration need not repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body

and

steps are taken to demonstrate that the results of this previous procedure remain valid;

or

3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body

and

steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.

N/A.

2.1.4 Binding between the electronic identification means of natural and legal persons

As the German eID is only used for the identification of natural persons, 2.1.4 is not applicable.

LOW

1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level low or above.

2. The binding has been established on the basis of nationally recognised procedures.

3. The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person.-

SUBSTANTIAL

Point 3 of level low plus:

1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level substantial or high.

2. The binding has been established on the basis of nationally recognised procedures, which resulted in the registration of the binding in an authoritative source.

3. The binding has been verified on the basis of information from an authoritative source.

HIGH

Point 3 of level low and point 2 of level substantial, plus:

1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level high.

2. The binding has been verified on the basis of a unique identifier representing the legal person used in national context; and on the basis of information uniquely representing the natural person from an authoritative source.

N/A.

2.2 Electronic identification means management

2.2.1 Electronic identification means characteristics and creation

LOW

1. The electronic identification means utilises at least one authentication factor.

N/A.

2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.

N/A.

SUBSTANTIAL

1. The electronic identification means utilises at least two authentication factors from different authentication factor categories.

The German eID requires mutual authentication of the service provider and the card holder via a sequence of cryptographic protocols, called General Authentication Procedure, as defined in [BSI TR-03110].

The corresponding private keys are securely stored on the chip of the eID card (German ID card or residence permit) of the card holder. As part of the cryptographic protocols, a corresponding PIN of the card holder is required to unlock the chip of the eID card.

Consequently, the German eID utilises two authentication factors from the different authentication factor categories “possession” (eID card) and “knowledge” (PIN).

2. The electronic identification means is designed so that it can be assumed to be used only if under the control of the subject to whom it belongs.

See rationale 2. of level 'high' (below).

HIGH

Level substantial, plus:

1. The electronic identification means protects against duplication and tampering against attackers with high attack potential.

The private keys required for authentication with the German eID and the identification data of the subject are stored on the chip of the card holder´s eID.

The chip hard- and software of the German eID card are certified according to the Common Criteria ([ISO/IEC 15408]) using one of the following protection profiles depending on the generation and the technical platform of the corresponding eID card:

- [BSI-CC-PP-0087] (MR.ED-PP) for German eID cards in general,
- [BSI-CC-PP-0061] (ID_Card PP) for the German ID card, or
- [BSI-CC-PP-0069] (RP_Card PP) for the German residence permit.

These Protection Profiles define the functional and assurance requirements for the chip hard- and software of the German eID card. This includes security functional requirements (SFRs) to protect the private keys and identity information against duplication and tampering.

The evaluation is performed on evaluation assurance level (EAL) 4, augmented with ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5 (Advanced methodical vulnerability analysis) to evaluate resistance against attackers with high attack potential.

The Common Criteria certificate of the German ID Card and the German residence permit consists of a composite certificate of the eID card's operating system and the underlying chip.

Consequently, the Common Criteria certificate proves protection against duplication and tampering against attackers with high attack potential.

2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

The authentication mechanism of the German eID is based on a mutually authenticated and end-to-end-protected channel between the service provider and the chip of the eID card via a sequence of cryptographic protocols. This protects against attacks such as Man-in-the-Middle. Since the authentication is dynamic (see 2.3.1), the mechanism also prevents replay attacks.

Furthermore, the Common Criteria certification of the eID card provides a high assurance against duplication (see rationale 1.).

The two authentication factors (possession of the eID card and knowledge of the corresponding PIN) are used in conjunction. The PIN is only known to the person to whom the eID belongs and the German [PAuswV] obliges the user to keep it secret. The PIN is necessary to give user consent to perform an electronic identification, to unlock the chip of the eID card and to get access to the stored identification data.

The PIN has a length of 6 digits and is blocked by the eID card after 3 failed attempts. This protects against guessing by attackers with high attack potential, cf. [AIS 20/31].

After authentication, the card holder can remove the card from the reader. Furthermore, the card holder is able to use dedicated card readers that allow the PIN to be entered in the reader itself. This allows the user to prevent phishing attacks on the PIN, even on compromised computers.

Hence, the design of German eID ensures that the person to whom it belongs can reliably protect it against use by others.

2.2.2 Issuance, delivery and activation

LOW

After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.

N/A.

SUBSTANTIAL

After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.

N/A.

HIGH

The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.

As the German eID is part of the German ID card or the German residence permit, issuance and delivery of the German eID are official procedures based on national law. These procedures ensure that the two authentication factors (eID card and PIN) of the German eID are delivered in different ways into the possession of the person to whom the eID belongs.

For that purpose, the holder of the German eID receives a letter (PIN letter) from the card manufacturer that is sent via regular mail to the address of the person to whom the eID belongs ([PAuswV], §17). The letter contains an initial randomly generated activation PIN, together with a PIN unblocking key (PUK) and a revocation password. Both, PIN and PUK are protected by a tamper-evident scratch code, enabling the holder of the German eID to detect unauthorised notice by others.

In general, the responsible issuing authority hands the eID card itself over to the applicant in person or to a person entitled by the applicant to receive the card. Before the eID card is handed over, the card holder has to confirm to the issuing authority that he or she has received the PIN letter (§18 (2) [PAuswV]). Further, in the special case where the German eID is issued outside Germany (e.g. consulates) and personal collection by the applicant would cause unreasonable inconvenience, the issuing authority may send the German ID card via mail to the applicant. In this case, the issuing authority must use personal registered mail with return receipt to ensure that the eID card is delivered into the possession of the applicant §6.3.3 [PassVwV]. In particular, the PIN letter and ID card are delivered in separate steps.

After delivery of the eID card and before its first use for authentication, the German eID must be activated by the card holder by means of a dedicated activation procedure that requires not only possession of the card but also knowledge from the PIN letter[5]. Activation can be performed at the issuing authority or locally by the card holder.

These processes ensure that the German eID is delivered only into the possession of the person to whom it belongs and only after reception of the eID activation PIN is confirmed, thereby fulfilling this criterion.

2.2.3 Suspension, revocation and reactivation

LOW, SUBSTANTIAL, and HIGH

1. It is possible to suspend and/or revoke an electronic identification means in a timely and efficient manner.

If the ID card is lost or stolen, it is possible to revoke/suspend the German eID in a timely and efficient manner. Revocation of the German eID is regulated by national laws (see §25 of [PAuswV]).

The revocation report process is as follows:

1. The card holder reports the eID card as lost. This can be done at the issuing authority or by calling a revocation hotline. The revocation hotline is publicly known and available 24/7.
2. The issuing authority or hotline retrieves a revocation code from the card register or calculates it from the revocation password from the PIN letter and the card holder's first name, family name and date of birth.
3. The revocation code is sent to the operator of the revocation list without undue delay.

5 Technically, the activation procedure of the German eID requires the user to enter the activation PIN that is contained in the PIN letter to set a new PIN before the German eID can be used for identification (cf. [BSI TR-03127] for details).

4. Using the revocation code received, the operator of the revocation list then determines a unique revocation key of the corresponding eID and puts this key on the revocation list without undue delay.
5. The corresponding authorisation CAs retrieve the revocation list and provide the specific revocation information to the service providers. This completes the revocation process of the eID.

See [BSI TR-03127] and [BSI TR-03110] for technical details.

2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation.

Revocation of the German eID requires appearing in person at the issuing authority or the local municipality or using the revocation hotline.

The authorities are able to identify the card holder by checking the corresponding (local) registers. To revoke the eID via the revocation hotline, knowledge of the revocation password of the PIN letter sent to the card holder is required.

This prevents unauthorised revocation/suspension of the German eID.

If the ID card is recovered after revocation, the corresponding eID may be reactivated. This requires the card holder to appear in person at the issuing authority and to present the corresponding ID card.

This prevents unauthorised reactivation of the German eID.

3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.

The German eID may be reactivated after revocation/suspension. Reactivation is based on an official national procedure according to [PAuswV] (§26). In particular, the card holder is required to appear in person and to present the corresponding eID card to the issuing authority. Reactivation only takes place after the issuing authority has identified the card holder.

2.2.4 Renewal and replacement

The German eID can be neither renewed nor replaced (without new enrolment). If a person needs a new German eID (because the old eID expired or was lost or stolen), a new enrolment is required, cf. 2.1. Hence, this section is not applicable.

LOW and SUBSTANTIAL

Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or be based on a valid electronic identification means of the same, or higher, assurance level.

HIGH

Level low, plus:

Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

N/A.

2.3 Authentication

This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section controls are understood to be commensurate to the risks at the given level.

2.3.1 Authentication mechanism

The authentication mechanism of the German eID consists of a sequence of cryptographic protocols, called the **General Authentication Procedure**, according to [BSI TR-03110] (**eIDAS Token specification**). The General Authentication Procedure consists of the following steps:

1. **PACE**

   The PACE protocol verifies the PIN entered by the user and establishes a secure messaging channel (i.e. an encrypted and authenticated channel) with strong session keys between the card holder's local device (e.g. computer or card reader) and the chip of the German eID.

2. **Extended Access Control v2**

   - **Terminal Authentication Version 2**

     This protocol provides a challenge-response based proof of the authenticity and the access rights of the relying party. The protocol is based on an official PKI (**authorisation PKI**) with the German BSI as national trust anchor.

   - **Passive Authentication**

     Provides proof of the authenticity of data stored on the German eID, specifically of the public key of the chip. For this purpose, the public key of the chip of the German eID is signed by the card manufacturer.

     The verification of the authenticity of the public key is based on an official PKI (**document PKI**) with the German BSI as national trust anchor.

   - **Chip Authentication Version 2**

     Provides proof of the possession of the eID´s private key (which corresponds to the public key verified during 'Passive Authentication'). Thus, together with the Passive Authentication, the protocol verifies the authenticity of the eID card's chip. Furthermore, the protocol establishes a secure, cryptographically end-to-end-protected channel between the German eID and the relying party).

     This is done via an ephemeral-static Diffie Hellman key agreement using the service provider's ephemeral key pair of Terminal Authentication and the chip's static key pair. Only after the encrypted channel has been established, the relying party can access personal or document related data stored on the German eID's chip.

All protocols of the General Authentication Procedure have well-defined security objectives. The fulfilment of the security goals is proved by means of cryptographic security proofs published in cryptographic journals, cf. [SecProof PACE], [SecProof EACv2]. In particular, these proofs demonstrate resistance of the protocols against passive and active attackers.

Since Extended Access Control is based on an ephemeral-static Diffie-Hellman key agreement in which the ephemeral key is generated by the relying party, the authentication mechanism is dynamic.

Furthermore, correct and secure implementation of the protocols is asserted as part of the Common Criteria certification of the corresponding eID card to resist attackers with high attack potential.

LOW

1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.

See rationale 1. of level 'substantial' (below).

2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.

The personal data stored on the German eID are subject to strict access control. The Common Criteria certification of the eID card proves a high assurance against compromise of the data.

The PACE protocol ensures that the user has given his/her consent to the use of the eID and to the release of person identification data by entering the PIN. Furthermore, the relying party is authenticated via Terminal Authentication using the authorisation PKI. After mutual authentication, person identification data are only transmitted in a secure, cryptographically end-to-end-protected channel between the German eID and the relying party. This implies that no person identification data are processed or stored in plain text by the card reader or device of the holder, i.e. the security of these components is not relevant for the protection of person identification data. Furthermore, the explicit cryptographic check of the identity and authorisation of the relying party ensures that no person identification data are transmitted to unauthorised entities.

The algorithms, key sizes and parameters used within the cryptographic protocols are re-evaluated yearly and selected according to the state of the art by the BSI in line with [SOG-IS Crypto]. The selected parameters are mandatory for the involved parties and published in corresponding algorithm catalogues [BSI TR-03116].

Consequently, this control is satisfied.

3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.

See rationale of level 'high' (below).

SUBSTANTIAL

Level low, plus:

1. The release of person identification data shall be preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process.

On the German eID, the release of person identification data is preceded by the General Authentication Procedure as described above. As part of the General Authentication Procedure, the EAC protocol provides an ephemeral-static Diffie-Hellman key agreement in which the ephemeral key pair is provided by the relying party, thereby providing dynamic authentication. To ensure a high entropy of this ephemeral key pair, [BSI TR-03116] contains requirements for suitable random number generators to be used by the relying party.

As part of the authentication, the German eID is checked to ensure that it is authentic (cf. section 2.3.1) and valid, i.e. not revoked or expired.

Furthermore, the authentication mechanism of the German eID is dynamic.

2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.

See rationale of level 'high' (below).

HIGH

Level substantial, plus:

The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

The authentication mechanism of the German eID consists of the General Authentication Procedure according to [BSI TR-03110] (eIDAS Token specification). As described above, all cryptographic protocols of this procedure as well as the procedure as a whole have cryptographic security proofs which ensure that the protocol design is resistant against active and passive attackers, including, but not limited to, resistance against guessing, eavesdropping, replay and manipulation.

The use of a PIN consisting of 6 digits that is blocked after 3 failed attempts, protects against guessing attacks also by attackers with high attack potential.

The authentication mechanism provides a mutual authentication between the chip of the German eID and the relying party. Authenticity of the static keys of the German eID and the relying party is provided by dedicated national Public Key Infrastuctures (document PKI and authorisation PKI), both with the German BSI as trust anchor.

The cryptographic algorithms, key lengths and parameters to be used within the protocols are selected according to the state of the art and ensure a security level of at least 120 bits, cf. [BSI TR-03116]. This prevents eavesdropping on the communication.

The dynamic authentication mechanism of the German eID prevents replay attacks.

Further, the implementation of the protocols is evaluated as part of the Common Criteria certification of the German ID card and of the residence permit, whence the certifications particularly confirm resistance of the implementation against attackers with high attack potential. Besides activities listed in this control, the certification also considers side-channel attacks and includes an advanced methodical vulnerability analysis.

Hence, this control is fulfilled.

2.4 Management and organisation

All participants providing a service related to electronic identification in a cross-border context ("providers") shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for the electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.

The German eID scheme is based on official documents. Hence, the scheme is managed directly by the German government, and requirements are defined by national laws, decrees and subordinate guidelines.

The requirements hold for the participants providing a service related to electronic identification and corresponding auditing rules. Furthermore, the complete German eID scheme is covered by a "Framework Security Concept for the Overall System of the Electronic ID Card" [FrSecConcept] that identifies the relevant threats for the different components of the scheme and is the basis for corresponding security controls of the participants involved. The concept applies to the German residence permit as well.

With regard to the services within the German eID scheme, there are basically two types of parties that have to be distinguished within the German eID scheme:

- **Public authorities**

  Public authorities act in the public interest according to laws and regulations and are subject to special obligations of due diligence.

- **Private parties**

  Private parties take over tasks as contractors of public authorities or carry out market roles within the German eID scheme that are not executed by public bodies.

The following roles provide a service related to electronic identification in the cross-border context:

- **The (local) issuing authorities of the German eID**
  - verify the identity of the applicant and
  - issue the German eID.

  The issuing authorities are public authorities. The duty of the issuing authorities is fulfilled based on a legal mandate, performed according to formalised processes which are defined in dedicated procedural guidelines. Furthermore, the issuing authorities are supervised according to national law.

- **The eID card manufacturer (Bundesdruckerei GmbH)**
  - produces and personalises the German eID card and
  - cryptographically signs the document.

  The card manufacturer Bundesdruckerei is a private company that is fully owned by the Federal Republic of Germany. The Bundesdruckerei operates a certified Information Security Management System according to [ISO/IEC 27001].

- **The CSCA – Country Signing Certification Authority (BSI)**
  - is the root CA of the Public Key Infrastructure for document validation (document PKI).

  The CSCA is a public certification authority. The BSI operates a certified Information Security Management System according to [ISO/IEC 27001].

- **The revocation service operated by the Federal Office of Administration (BVA)**
  - generates and provides the generic revocation lists.

  The revocation service is a public service operated Germany´s Federal Office of Administration (BVA). The duty of the revocation service is fulfilled according to a decree of the Ministry of the Interior and performed according to formalised processes which are defined in dedicated

procedural guidelines. Furthermore, the revocation service is supervised in accordance with national law.

- **The revocation service of the authorisation CAs**
  - generates and provides the relying party specific revocation list to the relying parties.

  Authorisation CAs must comply with the requirements of the Certificate policy of the authorisation PKI. This policy defines specific controls to be fullfiled by the authorisation CAs, in particular with regard to revocation. The authorisation CAs of the German eID scheme are trust centres that operate a certified Information Security Management System according to [ISO/IEC 27001].

The following roles are part of the German eID infrastructure, but not part of the German scheme in the sense of the notification, as the role of these participants is related to providing trust in the relying party, which is not a requirement for the eID scheme according to the eIDAS Level of Assurance. Hence, these roles are not considered in the following.

- The Issuing Office for Authorisation Certificates (VfB)
  - issues licences for service providers.
- The CVCA – Country Verifying Certification Authority (BSI)
  - is the root CA of the authorisation PKI and issues certificates to authorisation CAs.
- The authorisation CAs
  - issue certificates to the service providers.
- Service providers
  - provide a service that can be used with the German eID.

2.4.1 General provisions

LOW, SUBSTANTIAL, and HIGH

1. Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognised as such by national law of Member State, with an established organisation and fully operational in all parts relevant for the providing of the services.

Any entity providing services in the German eID scheme that is not itself a public authority must be approved by a public authority and thus be a legal entity recognised by national law.

Hence, this requirement is fulfilled.

2. Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service including, the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long.

Operations of all entities involved in the German eID scheme are directly governed by national law and subordinate regulations.

3. Providers are able to demonstrate the ability to assume the risk of liability for damages, as well as having sufficient financial resources for continued operations and providing of the services.

The authentication mechanisms of the German eID are based on the direct interrelationship between the relying party and the holder of the eID without a third party involved. For this direct end-to-end relationship, national law provides for no liability obligations specific to the use of the German eID.

The provider of the German eID is the Federal Republic of Germany, meaning that no additional insurance is necessary. Furthermore, the revocation service and the CSCA are also operated by public authorities. Arrangements with contractors of the Federal Republic of Germany are managed via contracts.

If an authorisation CA terminates operation, customers of this CA may migrate to another authorisation CA. In this case, the new authorisation CA provides the relying party with relying party-specific revocation lists and continued operation of the service of the terminating authorisation CA is not necessary.

Hence, this requirement is fulfilled.

4. Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.

According to German law, the provider of the corresponding service remains fully responsible for any services offered.

5. Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.

As the German eID scheme is constituted by national law, termination planning is not applicable.

2.4.2 Published notices and user information

LOW, SUBSTANTIAL, and HIGH

1. The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.

For the German eID, all terms and conditions are defined by national laws and decrees and as such publicly available. The laws and degrees also cover the applicable rules for data privacy, thus the German eID includes a privacy policy.

2. Appropriate policy and procedures are in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions and privacy policy for the specified service.

Changes of any service definitions, terms, conditions or privacy policy for the German eID are part of national legislation and therefore made publicly available with the information being in the public domain.

3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.

The Federal Ministry of the Interior provides contact by phone and email for requests for information (http://www.personalausweisportal.de/DE/Service/Kontakt/kontakt_node.html).

2.4.3 Information security management

LOW

There is an effective information security management system for the management and control of information security risks.

See rationale of levels 'substantial and high' (below).

SUBSTANTIAL and HIGH

Level low, plus:

The information security management system adheres to proven standards or principles for the management and control of information security risks.

In accordance with [PAuswV], the German Federal Office for Information Security publishes Technical Guidelines for the German eID scheme, which cover the relevant information on security risks and controls for the German eID. The Technical Guidelines are referenced by [PAuswV] and are mandatory.

Furthermore, the Framework Security Concept serves as a basis for controls against relevant information security threats.

Additionally, the BSI operating the trust anchor of the document PKI and all providers who do not have the status of a public authority have certified information security management systems in accordance with [ISO/IEC 27001] in place.

2.4.4 Record keeping

LOW, SUBSTANTIAL and HIGH

1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.

Recording and maintenance of all relevant information is required by national law and subordinate regulations, as per §23 [PAuswG] and §4 [PAuswV].

Furthermore, suitable recording and maintenance is covered as part of the [ISO/IEC 27001] Information Security Management Systems.

2. Retain, as far as permitted by national law or other national administrative arragement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.

For the issuing authorities, retention of the personal data of participants of the German eID is implemented according to §23-§26 [PAuswG] for the German ID card or pursuant to §62-§65 [AufenthV] for a German residence permit.

For the card manufacturer and the revocation service of the authorisation CAs, compliance with the requirements for retention and destruction is covered as part of the [ISO/IEC 27001] ISMS by control A.18 ‘Compliance’, A.18.1.3.

2.4.5 Facilities and staff

LOW, SUBSTANTIAL, and HIGH

1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.

In the public authorities, staff are employed according to dedicated job profiles. Where relevant, also additional dedicated training programmes for staff members exist. This ensures that procedures are performed by trained, qualified and experienced staff. The duties are performed according to formalised processes, and special obligations of due diligence exist. In particular, this holds for enrolment, identity proofing and verification as well as issuance of the German eID.

For the providers certified or audited according to [ISO/IEC 27001], this control is covered as part of controls A.7 'Human resource security', in particular A.7.2.2.

2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.

The public authorities have been provided with ressources and staff according to the administrative effort of the corresponding services as part of legislative procedure.

For the providers certified or audited according to [ISO/IEC 27001], this control is covered as part of controls A.12 'Operations security', A.12.1.2 'Capacity management'.

3. Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service.

The Framework Security Concept serves as a basis for controls against relevant threats.
Furthermore, for the providers certified or audited according to [ISO/IEC 27001], this control is covered as part of controls A.11 'Physical and environmental security', A.9 'Access control' and control A.12 'Operations security'.

4. Facilities used for providing the service shall ensure access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.

For the providers certified or audited according to [ISO/IEC 27001], this control is covered as part of controls A.11 'Physical and environmental security', A.9 'Access control' and control A.12 'Operations security'.

2.4.6 Technical controls

LOW

1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed.

For the providers certified or audited according to [ISO/IEC 27001], this control is covered as part of controls A.10 'Cryptography', A.12 'Operations security', (relating to availability), A.17 'Information security aspects of business continuity management', and A.18.1.5 'Regulation of cryptographic controls'.

Furthermore, there exist appropriate technical inspections concerning the risk management with regard to the protection of confidentiality, integrity and availability of the information processed.

2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.

Electronic communication channels used to exchange personal or sensitive information between providers of the scheme exist between

- the issuing authorities and the card manufacturer,
- the issuing authorities and the revocation service,
- the card manufacturer and the CSCA,
- the card manufacturer and the revocation service,
- the revocation service and the authorisation CAs,
- the authorisation CAs and the relying parties.

Protection of these channels is defined by Technical Guidelines of the German Federal Office for Information Security ([BSI TR-03116], [BSI TR-03129], [BSI TR-03132]), the Certificate Policy of the CSCA, and the Federal Office of Administration.

For the providers certified or audited according to [ISO/IEC 27001], this control is covered as part of controls A.10 'Cryptography', A.13 'Communications security', and A.18.1.5 'Regulation of cryptographic controls', which may also include references to technical guidelines as stated above.

3. Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plaintext.

For the certified or audited providers, this control is checked as part of the [ISO/IEC 27001] certification (cf. A.9 'Access control' and A.10 'Cryptography').

4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches.

For the certified or audited providers, this control is checked as part of the [ISO/IEC 27001] certification.

5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.

For the certified or audited providers, this control is checked as part of the [ISO/IEC 27001] certification (cf. A.8 'Asset management').

SUBSTANTIAL

Level low, plus:

Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.

The private keys of the CSCA and the card manufacturer used to ensure authenticity of the German eID are stored securely in cryptographic hardware security modules within the secure facilities of the CSCA and the card manufacturer, respectively.

For the providers certified or audited according to [ISO/IEC 27001], this control is covered as part of controls A.10 'Cryptography' and A.11 'Physical and environmental security'.

2.4.7 Compliance and audit

LOW

The existence of periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.

N/A.

SUBSTANTIAL

The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.

N/A.

HIGH

1. The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.

The German eID scheme is directly managed by a government body. Therefore, see 2.

2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.

As the German eID scheme is directly managed by the German government, and requirements are defined by national laws, decrees and subordinate guidelines, this control is fulfilled.

The existing [ISO/IEC 27001] certifications of the relevant providers include periodical independent external audits.

The issuing authorities are public authorities that act according to law and regulations (cf. [PAuswG], [PAuswV], [PassVwV], [AufenthG] and [AufenthVwV]) and in line with formalised processes which are defined in dedicated procedural guidelines. Furthermore, these authorities are supervised according to national law by their respective supervising authority.

Further, the revocation service too is a public service that is operated by the Federal Office of Administration according to a decree of the Ministry of the Interior in line with formalised processes. The Federal Office of Administration has an information security management system and acts according to supervised procedural guidelines.

References

[(EU) 910/2014] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32014R0910

[German eID] BSI, The German eID based on Extended Access Control - Overview

[PAuswG] Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG), https://www.gesetze-im-internet.de/englisch_pauswg/index.html

[PAuswG_AMD] Government draft for an Act on the promotion of electronic identification,

[PAuswV] Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung - PAuswV), http://www.gesetze-im-internet.de/pauswv/

[AufenthG] Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet, https://www.gesetze-im-internet.de/englisch_aufenthg/index.html

[AufenthV] Aufenthaltsverordnung, http://www.gesetze-im-internet.de/aufenthv/

[AufenthVwV] Allgemeine Verwaltungsvorschrift zum Aufenthaltsgesetz, http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_26102009_MI31284060.htm

[PassVwV] Allgemeine Verwaltungsvorschrift zur Durchführung des Passgesetzes (Passverwaltungsvorschrift - PassVwV), http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_17122009_IT464400311.htm

[BSI TR-03110] BSI, Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token

[ISO/IEC 15408] ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security

[BSI-CC-PP-0087] BSI, Common Criteria Protection Profile BSI-CC-PP-0087, Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP)

[BSI-CC-PP-0061] BSI, Common Criteria Protection Profile BSI-CC-PP-0061, Electronic Identity Card (ID_Card PP)

[BSI-CC-PP-0069] BSI, Common Criteria Protection Profile BSI-CC-PP-0069 Electronic Residence Permit Card (RP_Card PP)

[AIS 20/31] BSI, Appendix to AIS20/31, A proposal for: Functionality classes for random number generators

[BSI TR-03127] BSI, Technische Richtlinie TR-03127 eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control - Elektronischer Personalausweis und elektronischer Aufenthaltstitel, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03127/tr-03127.html

[SecProof PACE] J. Bender, M. Fischlin, D. Kügler, Security Analysis of the PACE Key-Agreement Protocol, ISC 2009, pp. 33-48, Lecture Notes in Computer Science, 2009

[SecProof EACv2] Ö. Dagdelen, M. Fischlin, Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Documents, ISC 2010, pp. 54-68, Lecture Notes in Computer Science, 2010

[SOG-IS Crypto] SOG-IS, Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms

[BSI TR-03116] BSI, Technische Richtlinie TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung

[FrSecConcept] Federal Ministry of the Interior (BMI), Sicherheitsrahmenkonzept für das Gesamtsystem des elektronischen Personalausweises (ePA)

[ISO/IEC 27001] ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements

[BSI TR-03129] BSI, Technical Guideline PKIs for Machine Readable Travel Documents - Protocols for the Management of Certificates and CRLs

[BSI TR-03132] BSI, Technische Richtlinie TR-03132 Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente