Federal Office
for Information Security

German eID based on Extended Access Control v2

Overview of the German eID system

Version 1.4

20. October 2020

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

Figures

Tables

1 Introduction

In the course of the digitisation of business and governmental processes, secure electronic identification is of crucial importance in order to enable trust in electronic services.

This document gives an overview of the ***German eID based on Extended Access Control v2*** (in the following also abbreviated by ***German eID***). The German eID is based on government-issued chip cards (***eID cards***) using certified chips and strong cryptographic protocols.

The following types of eID cards are currently part of the scheme:

1. **German identity cards** (***Personalausweis***) issued to German nationals living in Germany or abroad,
2. **German resident permits** (***Aufenthaltstitel***) issued to non-EU nationals living in Germany, and
3. **German eID card for Union citizens** (***Unionsbürgerkarte***) issued to citizens of the European Union and nationals of the European Economic Area.

Figure 1: German ID card, Residence Permit and eID card for Union citizens

The issuance of eID cards started in 2010. Amongst other functions[1], the eID cards contain an eID functionality that enables secure electronic identification of **natural persons** based on a two-factor authentication. As a governmental eID scheme, the system benefits from well-defined regulations by national laws and ordinances; cf. [PAuswG], [AufenthG] and [eIDKG].

The German eID fulfils all requirements of the eIDAS Level of Assurance '**high**', cf. [LoA Mapping]. IT security as well as data protection considerations, usability and ease of integration are the central basis for the design of the whole eID system. In this respect, the German eID combines the following features into a single eID system:

- strong and secure mutual authentication between the relying party and the user,
- secure storage of personal data and cryptographic keys,
- high resistance against duplication and tampering,
- reliable prevention of illicit use by others,
- data protection and data minimisation by design, i.e.
  - encrypted data transmission,
  - full control over the release of personal data by the user,
  - no use of global or persistent unique identifiers,
  - no monitoring option on the use of the eID, neither by government institutions nor by other parties,

1 The additional applications, i.e. the ePassport Application and the eSignature Application, are not part of the German eID scheme and therefore out of scope of this document.

- the strict regulation of governmental processes in accordance with German law,
- online and offline capability, and
- easy use by all parties involved.

2 The German eID card

The identification means of the German eID scheme is the national eID card issued by the German government. The eID card is a card in td-1 format [ICAO 9303] containing a contactless chip that communicates in accordance with the international standards [ISO/IEC 14443] and [ISO/IEC 7816] [ISO/IEC 7816] and has a maximum validity period of 10 years.

The technology of the German eID is based on the **eIDAS token specification** [BSI TR-03110] with the detailed system architecture as defined in [BSI TR-03127]. The chip of the German eID card stores the personal data of the holder and serves as security anchor for the protection of this data and the authentication of the holder.

Figure 2: Integrated chip

The eID card utilises **two authentication factors** to perform authentication, "**possession**" (eID card) and "**knowledge**" (6-digit PIN). The chip of the eID card stores the personal data and the relevant keys to enable authentication. The PIN must be entered by the card holder to start the authentication process.

Furthermore, the PIN serves to express the holder's consent to the authentication.

2.1 Stored data

The chip of the German eID includes a dedicated eID application that securely stores the personal data of the card holder. The following personal data are contained within the eID application and may be transmitted during authentication[2]:

1. family name,
2. name at birth (optional),
3. given names,
4. doctoral degree (optional),
5. date of birth,
6. place of birth,
7. address,
8. type of document,
9. expiry date,
10. nationality,
11. service- and card-specific identifier (pseudonym),
12. indication whether the card holder is older or younger than a particular age,

2 For data that may be transmitted via the eIDAS Interoperability Framework, see chapter 5.

13. indication whether a place of residence matches the requested place of residence, and
14. religious name / stage or pen name (optional).

Furthermore, to check whether the German eID card is valid or not, a card-specific revocation token for comparison with the relying party's revocation list and the indication whether the eID card is expired are transmitted as part of the authentication (upon request by the relying party).

Access to any data is only possible after successful authentication of the relying party as described in sections 2.2 and 2.3.

2.2 Mutual authentication

Looking at the real world, the holder of an ID card usually knows to whom or which institution she or he proves her/his own identity, since the identification takes place at the premises of a company/a government office, or both persons involved use their ID cards to identify each other. In such situations, the holder shows his or her ID card directly to the relying party without third parties involved.

The German eID transfers these principles into the digital world. The basic principles of electronic identification via the German eID are based on

- the **mutual authentication** between the chip of the eID card and the relying party (or service provider), meaning that not only the holder of the eID authenticates via the eID to the relying party but also the relying party authenticates directly to the chip of the German eID, and
- the **direct communication** via a **secure end-to-end protected channel** between the relying party and the chip of the eID.

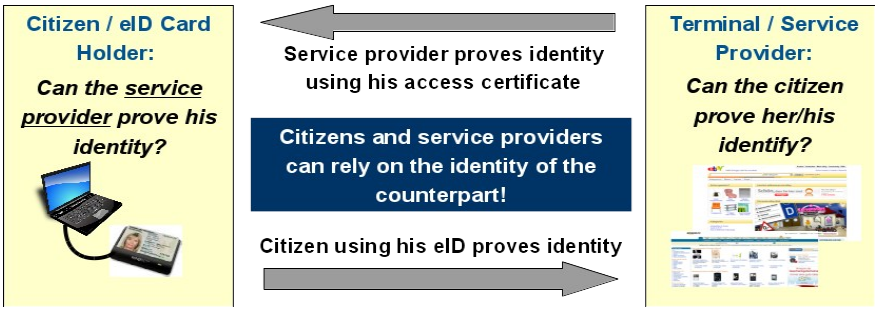

Figure 3: Mutual authentication between eID card holder and service provider

The principle of mutual authentication allows both communication parties to

- have proof of the identity of the counter-part and
- establish a trusted and secure end-to-end-protected channel.

As part of the mutual authentication, the relying party has to prove authorisation to get access to the relevant data. Access to any data is only possible after successful authentication of the relying party and verification of the corresponding access rights. The authentication of the communication parties and the assignment of access rights are realised via dedicated public key infrastructures; cf. Section 3.4.

However, unlike transactions such as a signature, showing the ID card does not lead to permanent proof of identity in the physical world. Instead, the identification process is ephemeral and cannot be proven to a third party.

The German eID maps this principle to the electronic identification, too. As the personal data are securely stored on the eID card's chip and transmitted via an authenticated channel, the authenticity and integrity of the data are ensured without the need to sign the data. Hence, unlike signature-based

eID schemes, the relying party receives no permanent proof of identity. From a data protection point of view, this has the advantage that the relying party cannot prove the authentication vis-à-vis a third party.

2.3 Authentication mechanism

The authentication mechanism of the German eID is called the ***General Authentication Procedure***. It consists of the following sequence of cryptographic protocols. Technical details can also be found in the eIDAS token specification [BSI TR-03110]:

1. **PIN Verification via *PACE***

   The PACE protocol serves to verify that the user has knowledge of the PIN of his/her German eID and to establish an encrypted and integrity-protected channel with strong session keys (Secure Messaging) between the card holder's (local) user device (e.g. computer or card reader) and the chip of the German eID. After PACE is successfully executed, the further communication with the local user device is protected.

2. **Mutual authentication via *Extended Access Control v2***

   - **Authentication of the service provider (*Terminal Authentication Version 2*)**

     This protocol provides a (challenge-response-based) proof of authenticity and access rights of the relying party. The protocol is based on the ***authorisation PKI*** with the German Federal Office for Information Security (BSI) as national trust anchor. The access rights of the terminal are assigned via authorisation certificates.

     The proof of access rights via Terminal Authentication is required for all personal and document-related data stored in the applications of the chip. These access rights can be exercised only within the channel encrypted by Chip Authentication.

   - **Authentication of the German eID's public key (*Passive Authentication*)**

     This step 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 using the ***document PKI***.

   - **Authentication of the document (*Chip Authentication Version 2*)**

     This protocol 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 German eID. Furthermore, the Chip Authentication establishes a secure, cryptographically end-to-end-protected channel between the chip of the German eID and the relying party.

     Only after the encrypted channel has been established, the relying party can access personal or document-related data stored on the chip of the German eID.

3. **Validity check and reading personal data**

   The service provider checks the validity of the document, i.e. whether the document is revoked or expired. The service provider may access the data stored on the German eID according to his or her access rights and perform special functions.

As the channel is authenticated, the card holder is authenticated, too. Moreover, as the transmission is encrypted, only the authenticated service provider may read the data.

As described above, each protocol of the General Authentication Procedure has well-defined security objectives. The security of the protocols is proven in cryptographic security proofs [SecProof PACE], [SecProof EACv2].

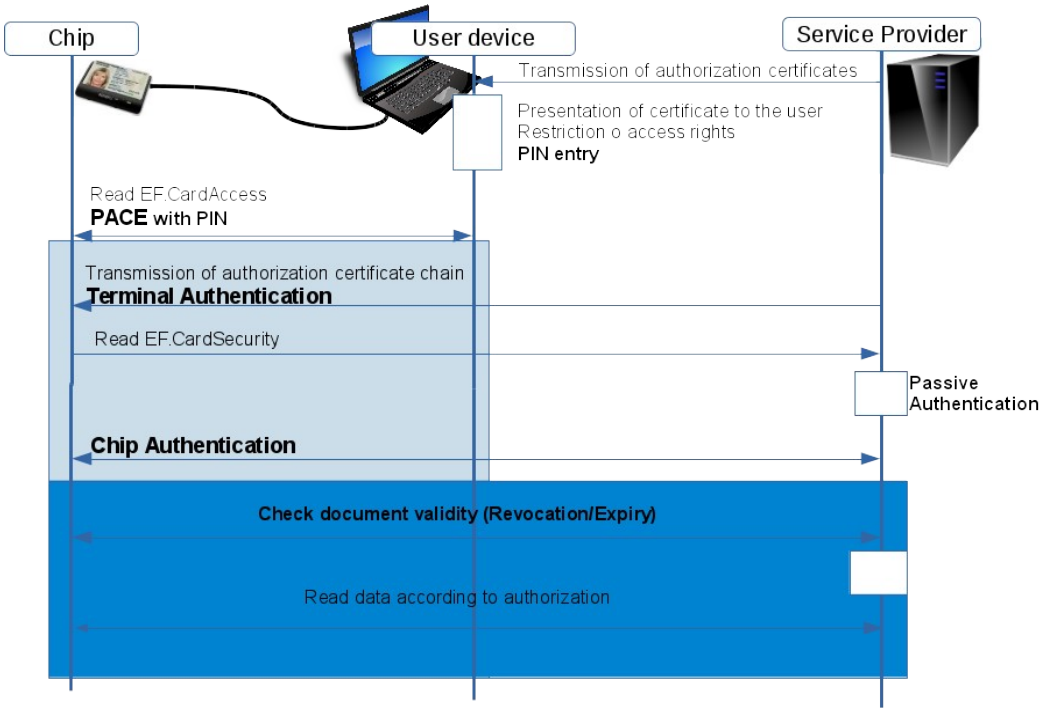

Figure 4: General Authentication Procedure

2.4 Authorisations

In order to get access to data stored on the German eID, the relying party needs authorisation. Public sector bodies of other Member States of the European Union are authorised to request person identification data from the German eID[3] of a user (cf. also Section 5 for eIDAs integration).

Authorisations for further relying parties are issued by the ***Issuing Office for Authorisation Certificates (VfB)*** upon application in accordance with [PAuswG], [eIDKG] and [PAuswV].

Technically, the authorisation of a relying party is assigned via authorisation certificates issued within the authorisation PKI. The relying party needs an authorisation certificate to perform online authentication and to get access to the relevant data of the German eID.

3

3 eID Infrastructure

Online authentication with the German eID is based on a direct mutual authentication between the relying party and the user. This allows managing authentication without the need for a third party – e.g. (central) ID provider – to perform the authentication procedure. Instead, the authentication procedure is directly performed by the relying party and the German eID. An advantage of this setting is that it avoids the risk of a central security hotspot and/or tracking entity. Furthermore, the direct relationship allows the relying party to define availability of its own service without needing service level agreements with the other party of the system. Instead, the service provider can define availability of its services as needed. A connection to the background system is only necessary on a temporary basis to retrieve new certificates and current revocation lists; in particular, no connection at the time of authentication of an eID card holder is necessary.

The **eID infrastructure** to perform authentication with the German eID online consists of the following components and communication relationships.

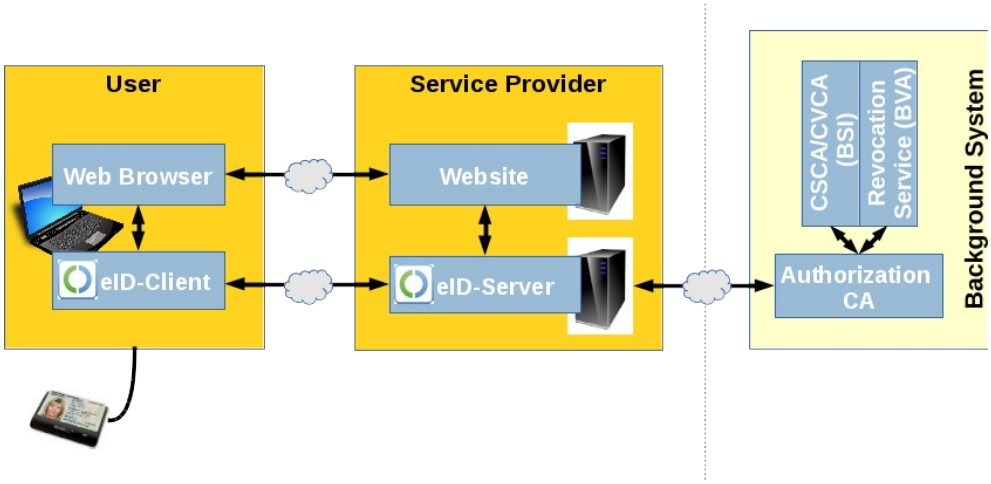

Figure 5: eID infrastructure – Communication relationships during online authentication

3.1 Online authentication

The online authentication process flow consists of the following steps:

1. The holder of the German eID requests a web service that requires an authentication.
2. The service provider sends an authentication request to the eID-Server and activates the eID Client via the user's application (e.g. browser).
3. The eID Client is redirected to the eID Server of the service provider.
4. The eID Client enables the holder of the German eID to view the information on the service provider and the corresponding access rights. The holder of the eID may deselect particular access rights or deny authentication.
5. The holder of the eID gives consent to the authentication process and proves the required 'knowledge' by entering the PIN.
6. The General Authentication Procedure is performed. As part of the authentication, the eID-Client verifies that the certificates of the web session fit with the authorisation certificate of the relying party. Only after successful verification are the relevant personal data transmitted from the German eID to the eID Server.

7. The eID Server transmits the authentication response containing the corresponding personal data to the service provider and redirects the eID Client back to the web session.
8. The service provider checks the authentication response and the corresponding personal data and decides whether to give the holder of the German eID access to the requested service.

3.2 User environment

The environment of the user consists of a computer (e.g. desktop PC, notebook, tablet, cell phone,...), eID Client software and a card reader.

The local ***eID Client*** software manages the online authentication process on the client side and serves as the link between the German eID, the user and the service provider. As such, it can display information about the service provider, may provide options to deselect access rights, enables PIN entry, and ensures the binding between the web session with the service provider and online authentication session with the service provider's eID server.

The eID Client software is based on open specifications that can be implemented by different vendors[4]. Using certified eID Client software is recommended. One certified implementation – the ***AusweisApp2*** – is provided by the German Federal Government.

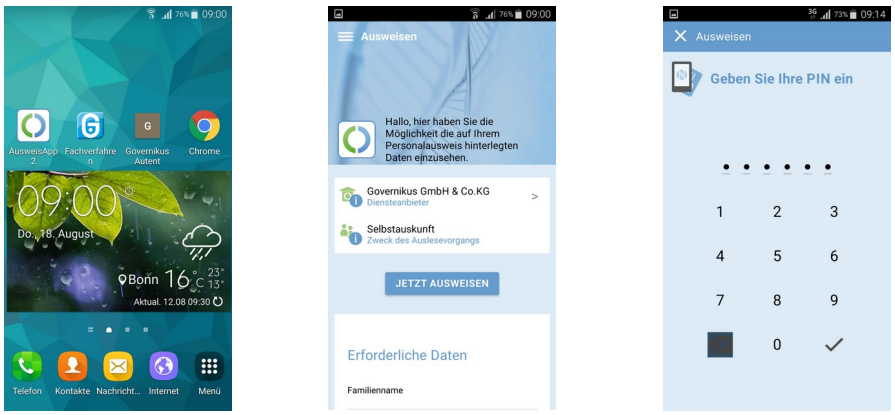

Figure 6: Screenshots of AusweisApp2 for NFC compliant Android smartphones

Furthermore, the user needs a **card reader** for the physical communication with the eID card. Different types of readers ensure a flexible integration into different user environments. Examples are

- external, integrated or embedded readers,
- readers with or without PIN pad,
- readers with PC/SC, CCID or Bluetooth interface, or
- NFC-compliant smartphones.

3.3 Service provider

A service provider wishing to integrate online authentication with the German eID into their IT systems has to deploy an ***eID Server***. The eID server communicates with the application of the service provider, the eID Client software of the user and the background system. For that purpose, the eID Server stores the authorisation certificates of the service provider and the corresponding private keys and revocation list to be used during authentication.

4 For a list of currently available interoperable implementations see http://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Online-Ausweisen/das-brauchen-Sie/Software/software-node.html.

3.4 Background system

3.4.1 Document PKI

The document PKI is used to ensure authenticity of the German eID.[5] It consists of the following two entities:

1. ***Country Signing Certification Authority (CSCA)*** operated by the Federal Office for Information Security (BSI),
2. ***Document Signer (DS)*** operated by the card manufacturer, i.e. the Bundesdruckerei.

The chip of the eID card holds a static Diffie-Helmann key pair where the public key is signed by the Document Signer. The authenticity of the signature is verified as part of the General Authentication Procedure described in Section 2.3. The relevant certificates of the document PKI are stored on the chip (DS certificate), or can be obtained from the CSCA.

3.4.2 Authorisation PKI

The authorisation PKI serves to ensure the authenticity and to determine the maximum access rights of the service provider. It is a three-tier PKI consisting of:

1. ***Country Verifying Certification Authority (CVCA)*** operated by the Federal Office for Information Security (BSI),
2. ***Authorisation CAs (BerCAs)*** which are operated by certified Trust Centres,
3. **Service providers** holding at least one authorisation certificate.

The service provider certificates have only a short validity period (~1 day) to avoid the need for a revocation management of authorisation certificates.

3.4.3 Revocation system

In order to impede illegitimate use of lost or stolen eIDs, the holder of the German eID must be able to revoke them. Due to the design principles of the German eID, the eID system does not use global revocation lists of unique public keys or serial numbers of all revoked cards for service providers, as this would constitute a global (card-specific) identifier of the holder of the eID.

Instead, the German eID system makes use of service provider-specific revocation lists. That is, each eID card provides a service-provider and card-specific revocation token to the service provider who verifies it against its individual service-provider-specific revocation list. The individual service provider revocation lists are generated by the authorisation CAs using a generic revocation list obtained from the revocation service. As part of the authentication procedure, revoked eIDs are detected.

5 The document PKI is the same as used for German ePassports.

4 Life cycle

4.1 Enrolment, issuance, delivery and activation

Upon application by an entitled person, the German eID is issued by the responsible issuing authorities in accordance with the procedures defined by the underlying national laws. The issuing authority captures the necessary personal data of the applicant and subsequently transmits these data to the manufacturer of the eID card.

The card manufacturer produces and personalises the eID card. As part of production, a PIN letter containing an initial randomly generated activation PIN, together with a PIN unblocking key (PUK) and a revocation password is produced. The PIN letter is sent by the card manufacturer to the applicant. Both PIN and PUK are protected by a tamper-evident scratch code.

The eID card itself is delivered by the responsible issuing authority in person to the applicant or to a person authorised by the applicant to receive the card.

After the eID card is delivered and before its first use, the holder of German eID must activate the eID card by changing the initial PIN to some operational PIN. Activation can be performed at the issuing authority or locally by the card holder.

4.2 Revocation management

The revocation report process is performed as follows:

1. The card holder reports the eID card as lost. This can be done at the issuing authority or by means of a revocation hotline. The revocation hotline “116 116”[6] is publicly known and available 24/7. Alternatively, if the issuing authority becomes aware that an identity card with an activated electronic identification function has been lost or stolen (e.g., via a police report), or a card holder has passed away, it will immediately initiate revocation of the eID.
2. The issuing authority or hotline generates a revocation request that is transmitted to the revocation service.
3. The revocation service adds the corresponding revocation key of the German eID to the generic revocation list without undue delay.
4. The authorisation CAs retrieve the generic revocation list from the revocation service and generate individual service-provider-specific revocation lists for the service providers.
5. The service provider can detect whether a German eID is revoked or not by checking the service-provider and card-specific revocation token against the individual service-provider-specific revocation list.

6 +49-116 116 or +49-30-40 50 40 50 from outside Germany.

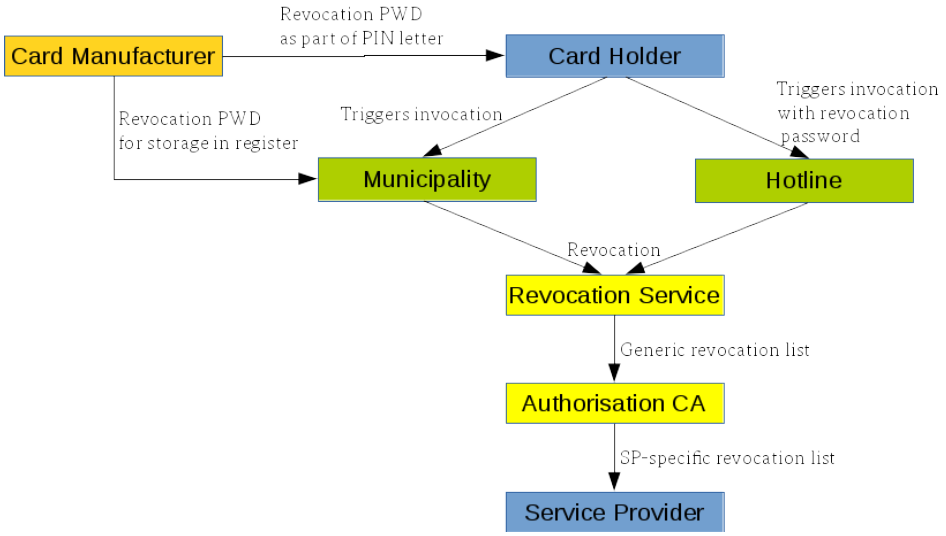

Figure 7: Revocation of the German eID

Further information on revocation management can also be found in [RevConcept]; additional details on the technical design are described in [BSI TR-03127] and [BSI TR-03110].

5 eIDAS integration of the German eID scheme

Due to the nature of the German eID system without a central component, the German eID scheme is integrated into the eIDAS Interoperability Framework [eIDAS IF] via the middleware integration model in accordance with the eIDAS technical specifications; cf. [eIDAS Arch]. How the German eID meets the requirements of [eIDAS IF] is described in [IF Mapping].

5.1 The German middleware

For that purpose, Germany provides middleware (‘***German eIDAS-Middleware***’) to the other Member States and the European Commission. The German eIDAS-Middleware implements an adapted eID-Server with an eIDAS interface based on Part 3 of Technical Guideline [BSI TR-03130] and performs the server side of the authentication procedure with the German eID.

The eIDAS-Middleware is open source (EUPL) and is provided at least as a virtual machine in accordance with the requirements of [eIDAS Arch][7], to be operated by the receiving Member State. To ease integration into the systems, the eIDAS-Middleware is provided to DIGIT for integration into the CEF/DIGIT eIDAS sample implementation package.

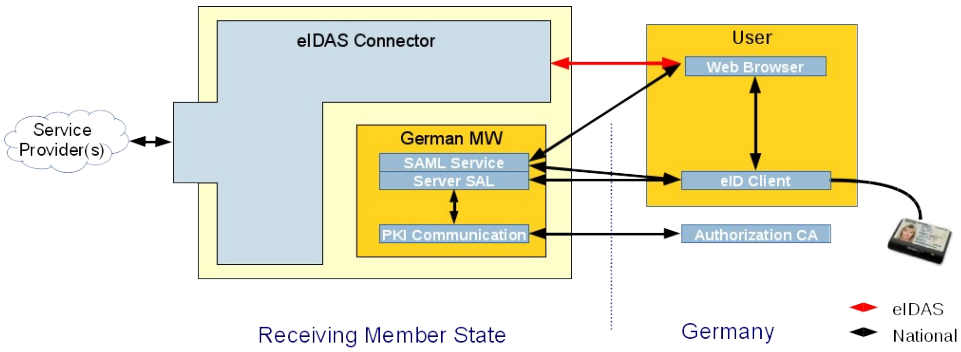

Figure 8: Integration of the German eIDAS-Middleware into the eIDAS network

Public-sector bodies of other Member States of the European Union are authorised to request person identification data from the German eID of a user. For this purpose, Germany will provide an authorisation certificate to each Member State free of charge. Identification and the initial registration at a commissioned authorisation CA will be performed via the Point of Single Contact [eIDAS CN] according to a dedicated procedure [MW Integration]. After initial registration, the German eIDAS middleware automatically updates the authorisation certificates. Provisioning of authorisation certificates also includes the necessary eID revocation lists.

Authorisations for non-public sector bodies are issued by the ***Issuing Office for Authorisation Certificates (VfB)*** upon application via the standard procedure in accordance with [PAuswV].

5.2 Minimum data set

The following **Minimum Data Set (MDS)** is provided by the German eID. Details on the technical mapping to the [eIDAS Attributes] can be found in Part 3 of Technical Guideline [BSI TR-03130].

7 In addition to the requirements of the eIDAS Technical Specifications, the eIDAS-Middleware is also provided in the ways as confirmed in the eIDAS Technical Subgroup, e.g. as jar application and/or Docker image.

eIDAS MDS	German eID
Current family name(s)	Family name
Current first name(s)	First name
Date of birth	Date of birth
Uniqueness identifier	Pseudonym[8]
First name(s) and family name(s) at birth	Birth name (if present on the eID card[9])
Place of birth	Place of birth
Address	Address[10]
Gender	N/A
-	Nationality[11]

Table 1: Minimum Data Set provided by the German eID scheme

8 The pseudonym of the German eID scheme is specific to each eID card and each receiving Member State (for public-sector bodies) or each relying party (for non-public-sector bodies).
9 The birth name is available on eID cards issued since Q2/2012 and residence permits issued since Q4/2014
10 For Germans with no permanent address in Germany, the address may be represented by the string "keine Wohnung in Deutschland" (no permanent address in Germany) in case the address could not be reliably verified by the corresponding issuing authority.
11 In addition to the eIDAS Minimum Data Set, the eIDAS Middleware may also transmit the Nationality of the user.

A. Technical Guidelines and Protection Profiles

From technical side, the German eID is based on a modular system (‘***family concept***’) of technical specifications and protection profiles that define all necessary interoperability and security requirements within this framework. This concept serves as the basis for all official ID documents in Germany.

Within this system, any electronic document is simply a profile of the same technical specification. The profile of the German eID is defined in [BSI TR-03127]. This approach results in synergies, as it enables for instance using the **same technical infrastructure as for European passports.**

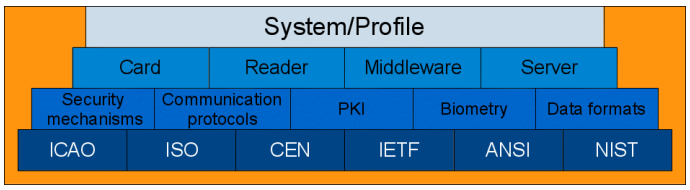

Figure 9: Modular family concept – German eID as a profile

The Technical Guidelines and Protection Profiles relevant for all German official documents are available on the BSI website at

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

The following table gives an overview of the technical specifications and corresponding conformity and Common Criteria certifications of components of the German eID system.

System component	Technical specification	Conformity Certification	Common Criteria Certification
Chip HW and SW	[BSI TR-03110]	[BSI TR-03105], Parts 2 and 3	[PP-Chip], [MR.ED]/[ePA-PP]/[eAT-PP]
Card Readers	[BSI TR-03119]	[BSI TR-03105][12], Parts 4 and 5.2	[PP-0083], if applicable
eID-Client	[BSI TR-03124], Pt. 1	[BSI TR-03124][12], Pt. 2	N/A
eID-Server	[BSI TR-03130], Pt. 1	[BSI TR-03130][12], Pt. 4	N/A
German eIDAS middleware	[BSI TR-03130], Pt. 3	[BSI TR-03130][13], Pt. 4	N/A
Fingerprint scanners	[BSI TR-03121]	[BSI TR-03122]	N/A
Software for capture and quality assurance of facial image and fingerprints	[BSI TR-03121]	[BSI TR-03122]	N/A
Module to secure the authenticity and confidentiality of the application data	[TR-03132]	[TR-03133]	N/A
Module for the change and visualisation service at the issuing authorities	[TR-03131]	[TR-03105], Parts 4 and 5.2	[PP-IS][14]

Table 2: Overview of Technical Guidelines and certifications

12 Certification is recommended
13 Certification in planning/preparation
14 Or a protection profile that provides an equivalent protection level

References

PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG)
AufenthG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet
eIDKG	Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis (eID-Kartengesetz -eIDKG)
LoA Mapping	BSI: German eID based on Extended Access Control v2 - LoA mapping
ICAO 9303	ICAO: Doc 9303, Machine Readable Travel Documents, Part 3
ISO/IEC 14443	ISO/IEC: ISO/IEC 14443 - Identification cards – Contactless integrated circuit(s) cards – Proximity cards
ISO/IEC 7816	ISO/IEC: ISO/IEC 7816 - Identification cards – Integrated circuit cards
BSI TR-03110	BSI: Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token
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, Springer, 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, Springer, 2010
PAuswV	Verordnung über Personalausweise, eID-Karten für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums und den elektronischen Identitätsnachweis (Personalausweisverordnung - PAuswV)
RevConcept	J. Bender, D. Kügler, M. Margraf, I. NaumannPrivacy-friendly revocation management without unique chip identifiers for the German national ID card, Computer Fraud & Security, 09/2010
eIDAS IF	Europäische Kommission: DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1501 DER KOMMISSION vom 8. September 2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
eIDAS Arch	eIDAS Technical Subgroup: eIDAS Technical Specifications - Interoperability Architecture
IF Mapping	BSI: German eID based on Extended Access Control v2 - Fulfilment of interoperability requirements according to (EU) 2015/1501
BSI TR-03130	BSI: Technical Guideline TR-03130 eID-Server
eIDAS CN	European Commission: COMMISSION IMPLEMENTING DECISION (EU) 2015/296of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
MW Integration	BSI: Three steps to integrate the German eIDAS-Middleware
eIDAS Attributes	eIDAS Technical Subgroup: eIDAS Technical Specifications - Attribute Profile
BSI TR-03105	BSI: Technische Richtlinie TR-03105, Conformity Tests for Official Electronic ID Documents
PP-Chip	Eurosmart: Security IC Platform Protection Profile, BSI-PP-0035

MR.ED	BSI: Common Criteria Protection Profile BSI-CC-PP-0087, Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP)
ePA-PP	BSI: Common Criteria Protection Profile BSI-CC-PP-0061, Electronic Identity Card (ID_Card PP)
eAT-PP	BSI: Common Criteria Protection Profile BSI-CC-PP-0069 Electronic Residence Permit Card (RP_Card PP)
BSI TR-03119	BSI: Technische Richtlinie TR-03119, Anforderungen an Chipkartenleser mit ePA-Unterstützung
PP-0083	BSI: Common Criteria Protection Profile BSI-CC-PP-0083 Standard Reader - Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control
BSI TR-03124	BSI: Technical Guideline TR-03124 eID-Client
BSI TR-03121	BSI: Technische Richtlinie TR-03121, Biometrics in public sector applications
BSI TR-03122	BSI: Technische Richtlinie TR-03122, Conformance Test Specifications for TR-03121
TR-03132	BSI: Technische Richtlinie TR-03132, Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente (TR SiSKo hD)
TR-03133	BSI: Technische Richtlinie TR-03133, Prüfspezifikation zur Technischen Richtlinie BSI-TR 03132 Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente
TR-03131	BSI: Technische Richtlinie TR-03131, EAC-Box Architecture and Interfaces
TR-03105	BSI: Technische Richtlinie TR-03105, Conformity Tests for Official Electronic ID Documents
PP-IS	BSI: Common Criteria Protection Profile for InspectionSystems, BSI-CC-PP-0064