



German eID based on Extended Access Control v2

Supporting Documentation

20 February 2017

Version 1.0

This document lists supporting documentation of the German eID scheme. The list is divided into national laws and ordinances, administrative directives, Technical Guidelines and Protection Profiles, journal articles and other supporting documentation.

National laws and ordinances

This section lists the relevant laws and ordinances of the German eID. The referenced laws and ordinances are published in the Federal Gazette (*Bundesanzeiger*), and are additionally available online at <https://www.gesetze-im-internet.de>.

- **[PauswG]**

Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG),

Act on Identity Cards and Electronic Identification

- Defines the legal basis of the German ID card and the electronic identification with the German eID system. 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].
- Link: <http://www.gesetze-im-internet.de/pauswg>
- Informational English version available at (not necessarily the current version):
 - https://www.gesetze-im-internet.de/englisch_pauswg

- **[PauswG_AMD]**

Regierungsentwurf für ein Gesetz zur Förderung des elektronischen Identitätsnachweises

Government draft for an Act on the promotion of electronic identification

- Amends [PAuswG] with regard to the promotion of the German eID and the notification of the German eID according to the eIDAS Regulation.
- Not yet available online, currently in the legislative process, will enter into force before notification

- **[PauswV]**

Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung – PauswV)

Ordinance on Identity Cards and Electronic Identification

- Defines the details of [PauswG].
- Link: <http://www.gesetze-im-internet.de/pauswv>
- No English version available.

- **[AufenthG]**

Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet

Act on the Residence, Economic Activity and Integration of Foreigners in the Federal Territory

- Defines the legal basis of the German residence permit. 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].
- Link: https://www.gesetze-im-internet.de/englisch_aufenthg
- Informational English version available at (not necessarily the current version):
 - https://www.gesetze-im-internet.de/englisch_aufenthg

- **[AufenthV]**

Aufenthaltsverordnung

Ordinance Governing Residence

- Defines the details of [AufenthG].
- Link: <http://www.gesetze-im-internet.de/aufenthv/>
- No English version available.

Administrative directives

- **[PassVwV]**

Allgemeine Verwaltungsvorschrift zur Durchführung des Passgesetzes (Passverwaltungsvorschrift – PassVwV)

- Defines the administrative procedures for the German passport and is also applies to applications for and issuance of the German ID card.
- Link:
http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_17122009_IT464400311.htm
- No English version available.

- **[AufenthVwV]**

Allgemeine Verwaltungsvorschrift zum Aufenthaltsgesetz

- Defines the administrative procedures for the German residence permit.

- Link:
http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_26102009_MI31284060.htm
- No English version available.

Technical Guidelines

This section lists the Technical Guidelines that are relevant for the German eID system [German eID]. The Technical Guidelines are also available at <https://www.bsi.bund.de/EN/eID-TR>.

- **[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
 - Defines the architecture of the German eID system based on Extended Access Control v2.
 - Informative English version available at:
 - <https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03127/tr-03127.html>
- **[BSI TR-03110]**
BSI, Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token
 - Specifies the security mechanisms for Machine Readable Travel Documents and eIDAS Token. The Technical Guideline is the technical basis for the German eID as well as for European passports and driving licenses, but also provides additional mechanisms.
- **[BSI TR-03112]**
BSI, Technical Guideline TR-03112 eCard-API-Framework
 - Specifies the API and the message format between the eID client software of the user and the eID-Server of the service provider.
- **[BSI TR-03116]**
BSI, Technische Richtlinie TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung
 - specifies the cryptographic requirements of the whole German eID system.
- **[BSI TR-03119]**
BSI: Technische Richtlinie TR-03119, Anforderungen an Chipkartenleser mit ePA-Unterstützung
 - Specifies technical requirements for card readers.
- **[BSI TR-03121]**
BSI: Technische Richtlinie TR-03121, Biometrics in public-sector applications
 - Defines requirements and recommendations for components to capture biometric data (fingerprint scanners, software for capture and quality assurance of facial images and fingerprints).

- **[BSI TR-03122]**
BSI: Technische Richtlinie TR-03122, Conformance Test Specifications for TR-03121.
 - Specifies test criteria to check the correct implementation of the communication according to [BSI TR-03132]
- **[BSI TR-03124]**
BSI: Technical Guideline TR-03124 eID-Client
 - Specifies the client software for online authentication with the German eID.
- **[BSI TR-03129]**
BSI, Technical Guideline PKIs for Machine Readable Travel Documents - Protocols for the Management of Certificates and CRLs
 - Specifies web service messages between the entities of the PKIs of the German eID system.
- **[BSI TR-03130]**
BSI: Technical Guideline TR-03130 eID-Server
 - Specifies the eID-Server for online authentication with the German eID.
- **[BSI TR-03131]**
BSI: Technische Richtlinie TR-03131, EAC-Box Architecture and Interfaces
 - Specifies the architecture and interfaces of the reader component used within municipalities to read or change data stored on the German eID.
- **[BSI TR-03132]**
BSI, Technische Richtlinie TR-03132 Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente
 - Defines requirements for the communication between the issuing authorities and the card manufacturer of the German eID card.
- **[BSI TR-03133]**
BSI: Technische Richtlinie TR-03133, Prüfspezifikation zur Technischen Richtlinie BSI-TR 03132 Sichere Szenarien für Kommunikationsprozesse im Bereich hoheitlicher Dokumente
 - Specifies test criteria to check the correct implementation of the communication according to [BSI TR-03132].
- **[BSI TR-03105]**
BSI: Technische Richtlinie TR-03105, Conformity Tests for Official Electronic ID Documents
 - Specifies conformity tests of the official electronic eID documents according to [BSI TR-03110] and corresponding reader components.

Protection Profiles

This section lists the Protection Profiles that are relevant for the German eID system [German eID]. The Protection Profile are also available online at <https://www.bsi.bund.de/EN/eID-PP>.

- **[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)
 - Specifies functional and assurance requirements for smartcards according to [BSI TR-03110]. The protection profile is designed to allow a modular approach with regard to the implemented applications and protocols. It serves as one alternative for the security certification of the German ID card or the German residence permit.
- **[BSI-CC-PP-0061]**
BSI, Common Criteria Protection Profile BSI-CC-PP-0061, Electronic Identity Card (ID_Card PP)
 - Specifies functional and assurance requirements for the German ID card. It serves as one alternative for the security certification of the German ID card.
- **[BSI-CC-PP-0069]**
BSI, Common Criteria Protection Profile BSI-CC-PP-0069 Electronic Residence Permit Card (RP_Card PP)
 - Specifies functional and assurance requirements for the German residence permit. It serves as one alternative for the security certification of the German residence permit.
- **[BSI-CC-PP-0064]**
BSI, Common Criteria Protection Profile BSI-CC-PP-0064 for Inspection Systems
 - Specifies functional and assurance requirements for inspection systems operated by government or law enforcement organisations, e.g. police. It serves to certify the reader component used within municipalities (EAC-Box).

Journal articles

- **[SecProof EACv2]**
Ö. Dagdelen, M. Fischlin, Security Analysis of the Extended Access Control Protocol for Machine Readable Travel Documents, ISC 2010, Lecture Notes of Computer Science, Springer
- **[SecProof PACE]**
J. Bender, M. Fischlin, D. Kügler, Security Analysis of the PACE Key-Agreement Protocol, ISC 2009, Lecture Notes of Computer Science, Springer
- **[RevConcept]**
J. Bender, D. Kügler, M. Margraf, I. Naumann: Privacy-friendly revocation management without unique chip identifiers for the German national ID card, Computer Fraud and Security, 09/2010.

Additional documentation

- **[German eID]**
BSI, German eID based on Extended Access Control v2 - Overview of the German eID system
 - Gives an overview of the German eID system and the underlying technical requirements.
- **[LoA Mapping]**

BSI: 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

- Maps the characteristics of the German eID to the requirements of the eIDAS Levels of Assurance defined in (EU) 2015/1502.

- **[IF-Mapping]**

BSI: German eID based on Extended Access Control v2 - Fulfilment of interoperability requirements according to (EU) 2015/1501

- Describes how the German eID meets the interoperability and minimum technical and operational security requirements under Commission Implementing Regulation (EU) 2015/1501.