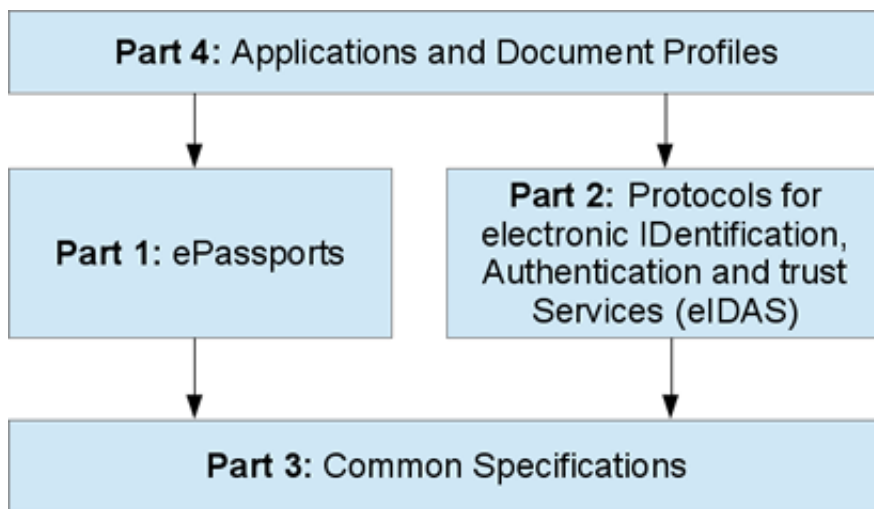


You are here: [Homepage](#) [Publications](#) [Technical Guidelines](#) **BSI TR-03110 Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token**

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

The BSI TR-03110 specifies security mechanisms for Machine Readable Travel Documents and eIDAS token. In particular, this specification is the technical basis for the German ID card (Personalausweis) and the German Residence Permit (cf [TR-03127](#)) as well as for European Passports and Driving Licenses, but also provides additional mechanisms.

BSI TR-03110 is organized as follows:



Structure of TR-03110

Protocols

This Technical Guideline specifies the following protocols to protect personal data stored on electronic documents:

Password Authenticated Connection Establishment (PACE)

PACE is a mutual authentication mechanism between terminal and chip that is based on a shared password,

e.g. a secret PIN (Personal Identification Number) that is only known to the holder or a CAN (Card Access Number) that is printed on the document. This mechanism is a replacement for Basic Access Control and is used to set up the initial communication.

Extended Access Control (EAC)

Extended Access Control is a mutual authentication mechanism between the terminal and the chip based on public key infrastructures (PKI). Terminal Authentication restricts access to data stored on the chip to authorized terminals. Chip Authentication not only authenticates the chip as genuine, it also enforces strong encryption and integrity protection of the transmitted data.

Restricted Identification (RI)

Restricted Identification may be used to generate a chip-specific pseudonym for a certain terminal sector. The terminal sector is an identifier shared by all terminals of a certain service provider.

This allows an (authenticated) terminal to recognize a chip based on the pseudonym previously received from the chip without reading out any personal data. Furthermore, it is computationally impossible to link pseudonyms across terminal-sectors.





Pseudonymous Signatures (PS)

Pseudonymous Signatures is a protocol that allows to sign data under a chip and sector specific pseudonym. The protocol can be used as alternative to Restricted Identification and is part of a version of Chip Authentication.


Enhanced Role Authentication (ERA)

Enhanced Role Authentication is a mechanism that may be used store requests for additional attributes on the chip. Attribute Providers can read these requests and may provide corresponding attributes for authorized Service Providers via storage in the chip. In contrast to the model of an Identity Provider, this may be realized such that the Attribute Provider does not learn to which Service Provider the Chip is communicates.

Downloads

-  [BSITR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 - Version 2.10 \(pdf, 626.7 KB\)](#)
-  [BSITR-03110-2 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 - Version 2.20 \(pdf, 1.03 MB\)](#)
-  [BSITR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Version 2.20 \(pdf, 3.05 MB\)](#)
-  [BSITR-03110-4 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 4 – Version 2.20 \(pdf, 1.17 MB\)](#)

Former versions referred by international standards

-  [BSITR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 - Version 2.10 \(pdf, 2.49 MB\)](#)

Worked Example to TR-03110

-  [EAC Worked Example \(zip, 1.46 MB\)](#)