Federal Office
for Information Security

fido ALLIANCE
simpler
stronger
authentication

eIDAS Regulation

Opportunities for Strong Authentication

Outline

1. What is eIDAS?
2. Electronic Identification
3. eIDAS - Levels of Assurance
4. Trust Services
   - General Requirements
   - Electronic Signatures
   - Registered Delivery Services

1. What is eIDAS?

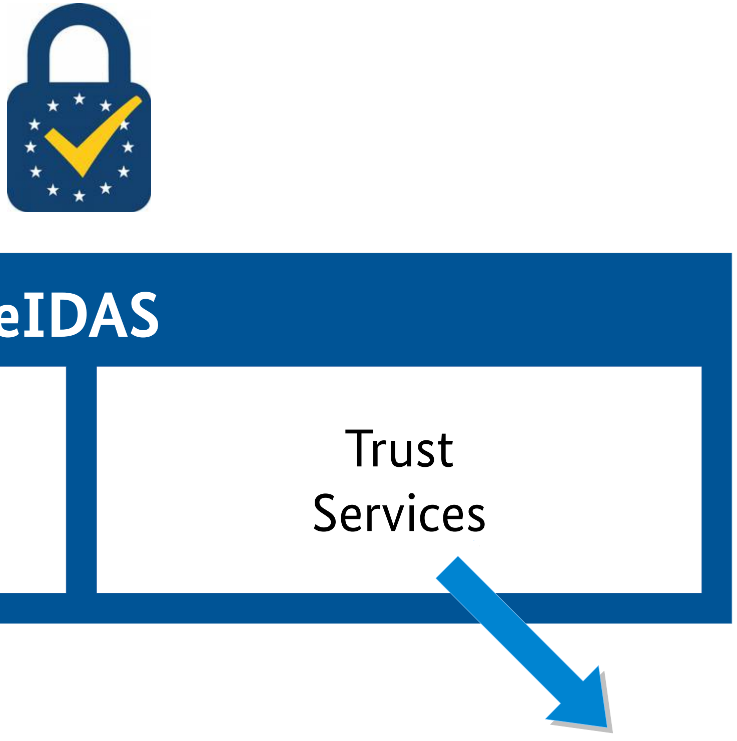
eIDAS-Regulation

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

eIDAS provides:

- **legal framework** for **cross-border usage** of eID means for on line access to public services (world première)
- **legal certainty to cross border use** of a trust services which may any generic electronic transaction
- comprehensive “toolbox” of services to boost trust and confidence in electronic transactions

eIDAS-Regulation



eIDAS

Electronic Identification

Trust Services

Mutual recognition of national eID schemes

legal certainty in cross border use of electronic trust service

2. Electronic Identification

Aims of Electronic Identificaction via eIDAS
Elements of an eID scheme
Implementation of Strong Authentication

Electronic Identification

Aims of Electronic Identifaction via eIDAS

- Interoperapibility of National eIDs instead of one EU eID
  - Interoparability framework connects different kind of electronic identities

- Cross-boarder recognition
  - Public services are obliged to recognize notified eIDs (of LoA substantial or higher)

- Notification only possible by Member-States

- Notified eIDs are categerorized into three **Level of Assurance (LoA)**
  - LoA is evualuated through peer review by the EU member states

Electronic Identification

Elements of an eID scheme

Enrolment

- application
- registration
- identity proofing

eID means management

- design
- issuance
- suspension
- renewal and replacement

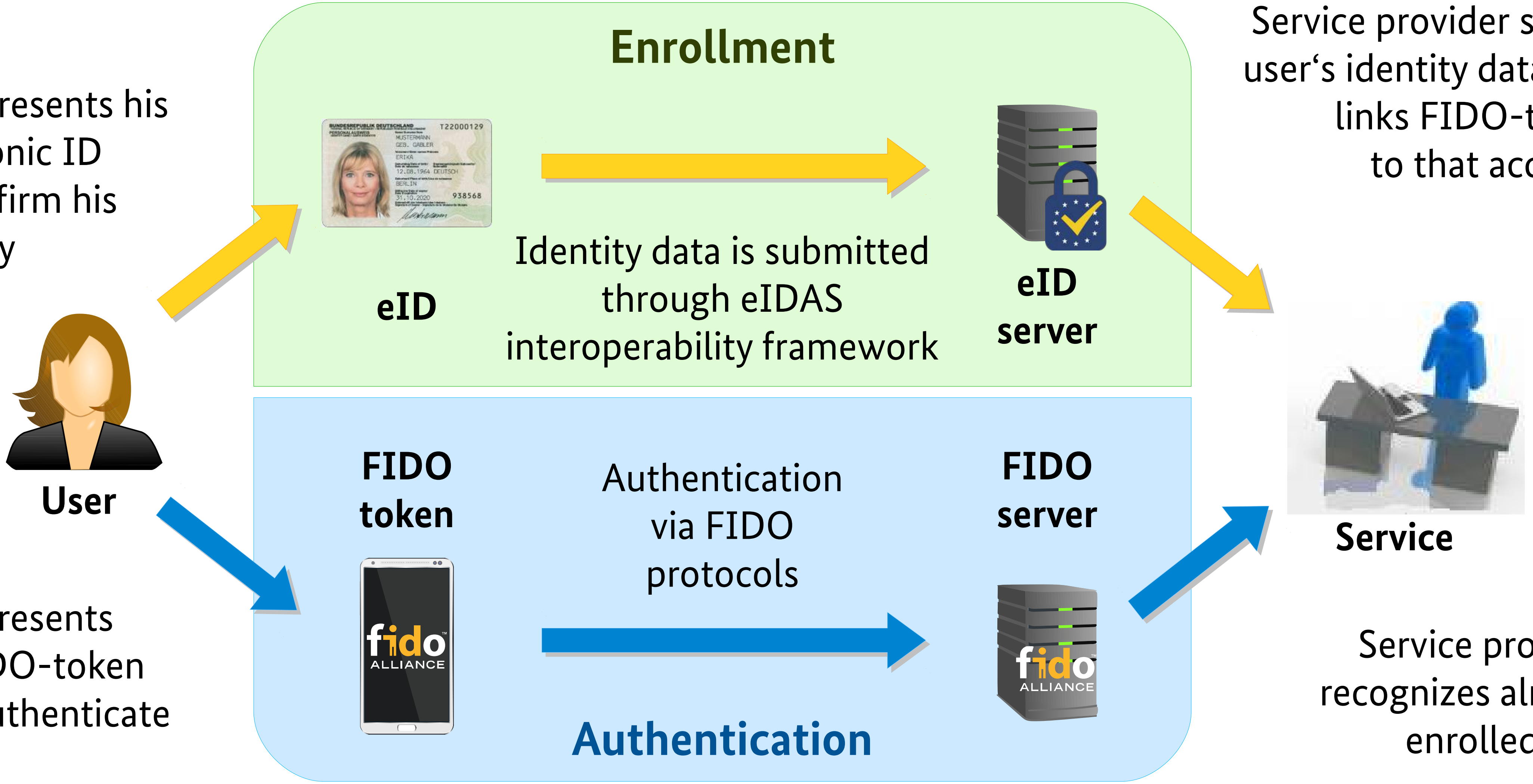
Authentication

- requirements for confirming an identity to a relying party

Management, organisation

- Information Security Management (ISM)
- record keeping
- facilities and staff
- controls
- compliance and audit

Derived Identities



User presents his electronic ID to confirm his identity

Enrollment

Identity data is submitted through eIDAS interoperability framework

Service provider stores user‘s identity data and links FIDO-token to that account

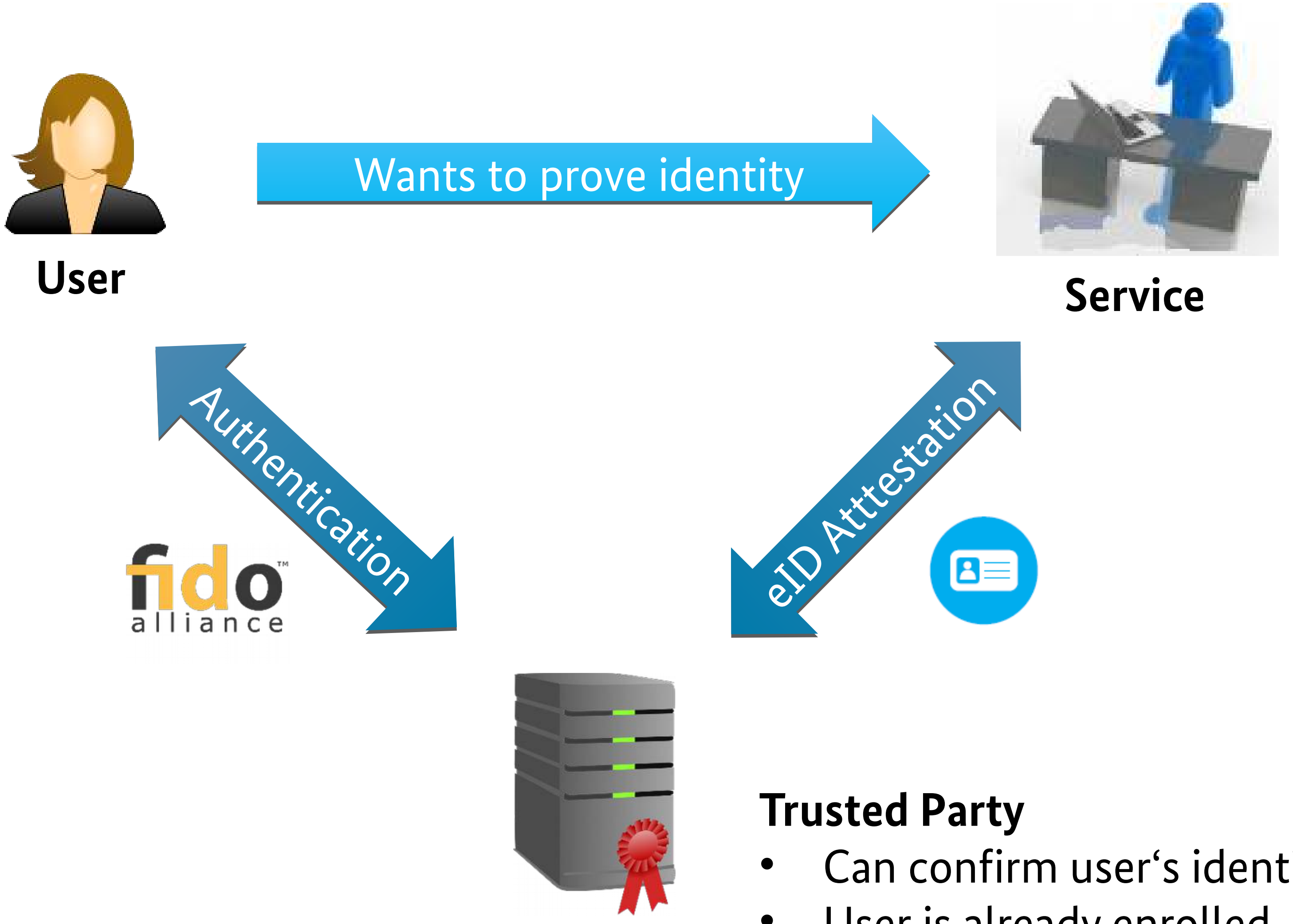
Authentication via FIDO protocols

Authentication

User presents his FIDO-token to reauthenticate

Service provider recognizes already enrolled user

Identification Service Provider



Trusted Party

- Can confirm user‘s identity
- User is already enrolled

Federal Office
for Information Security

3. eIDAS - Levels of Assurance

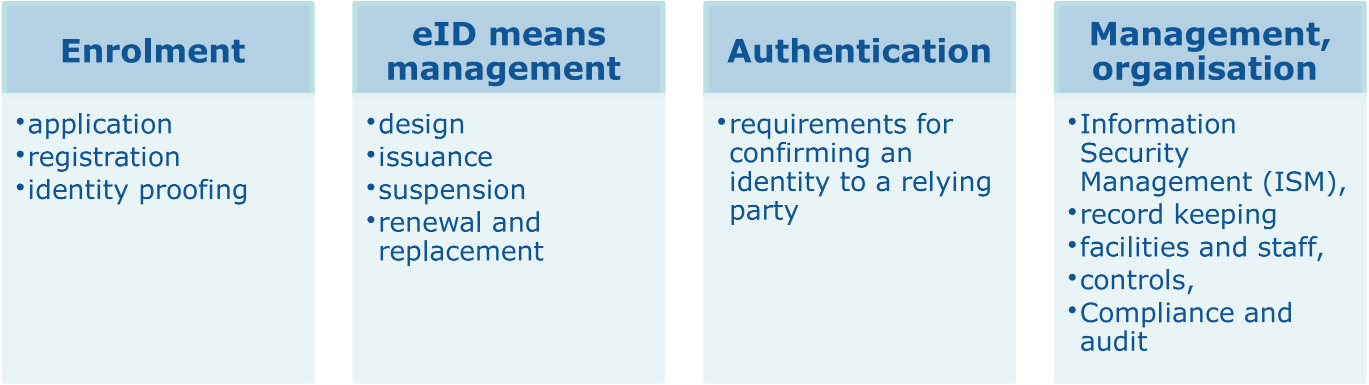
Levels of Assurance

- eIDAS defines three **Level of Assurance (LoA)**
  - low, substantial and high

- Minimum technical specifications and procedures are laid out in Commission Implementing Regulation (EU) 2015/1502

- The regulation cover all elements of an eID scheme

- higher assurance level fulfil the equivalent requirement of a lower assurance level
  - e.g. LoA substantial is covered by LoA high



Enrolment	eID means management	Authentication	Management, organisation
• application • registration • identity proofing	• design • issuance • suspension • renewal and replacement	• requirements for confirming an identity to a relying party	• Information Security Management (ISM), • record keeping • facilities and staff, • controls, • Compliance and audit

Levels of Assurance
Requirements on Authentication

Level low:

- Implementation of security controls against guessing, eavesdropping, replay or manipulation

Level substantial:

Low plus

- Dynamic authentication
- At least two factors from different categories

Level high:

Substantial plus

- protection against duplication and tampering

LoA Low

LoA Substantial

LoA High

Levels of Assurance
Requirements on Authentication

Level low:

- Resistance against enhanced-basic attack potential

Level substantial:

- Can be assumed to be used only if under control of the person to whom it belongs
- Resistance against moderate attack potential

Level high:

- Can be reliably protected by the person to whom it belongs against use by others
- Resistance against high attack potential

LoA
Low

LoA
Substantial

LoA
High

Levels of Assurance
Opportunities for FIDO

Potential LoA’s for FIDO:

LoA Substantial

LoA High

- Challenge: Currently, many FIDO products have not been subject to an independent security evaluation
- Raising security of FIDO to meet eIDAS LoA’s opens up new market perspectives

4. Trust Services

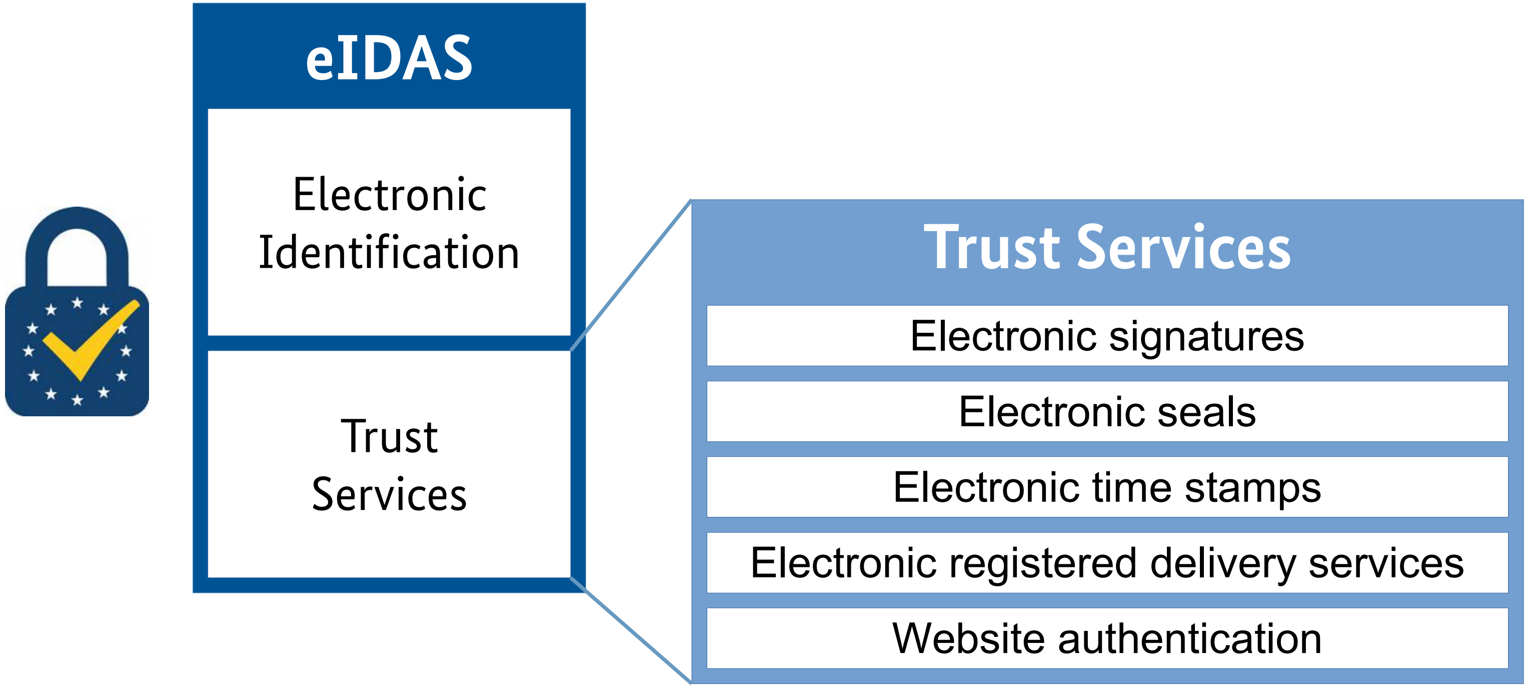
Aim of Trust Services
Remote electronic signatures
Electronic Registered Delivery Services

eIDAS – Trust Services

- Trust Services are intended to enable electronically cross-border transactions with legal certainty
- It should be possible to use trust services as evidence in legal proceedings in all Member States
- Qualified Trust Services shall have the equivalent legal effect as the corresponding paper-based processes
- National Regulations of the Member States should be largely harmonized
- Technological Neutrality

eIDAS – Trust Services

Trust services covered by eIDAS:



eIDAS

Electronic Identification

Trust Services

Trust Services

- Electronic signatures
- Electronic seals
- Electronic time stamps
- Electronic registered delivery services
- Website authentication

eIDAS – Trust Services

Legal effects of qualified trust services:

- Art. 25(2) - A qualified electronic signature shall have the equivalent legal effect of a handwritten signature

- Art. 35(2) - A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

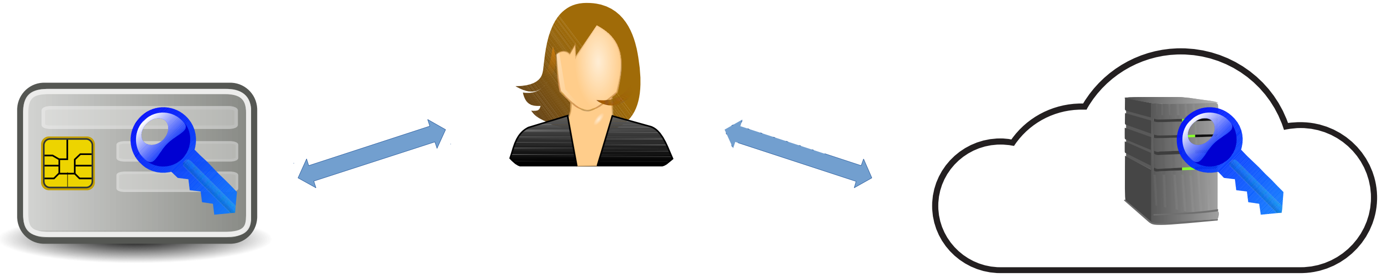
- Art. 41(2) - A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

- Art. 43(2) - Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

Qualified Electronic Signatures (QES) in the context of eIDAS

- based on an Advanced Electronic Signature
- Must be created using a qualified signature creation device (QSCD)
- legally equivalent to handwritten signature

Local Signatures



Remote Signatures

- Signatures are created by local QSCD owned by the user (i.e. a smart-card)

- Signatures are created by a qualified trust service provider (QTSP)
- QSCD is operated by QTSP

Remote electronic signatures
- Strong Identification

- Signatory's signing key is created, managed and stored by the Trust Service Provider on behalf of the signatory
- Trust Service Provider for Remote Signature is obliged to unambiguously identify the signatory
- Identification must be at the same Level of Assurance as for issuing a qualified certificate
  - by personal presence
  - using identification means that are conforming with LoA substantial, and that require personal presence during their issuance

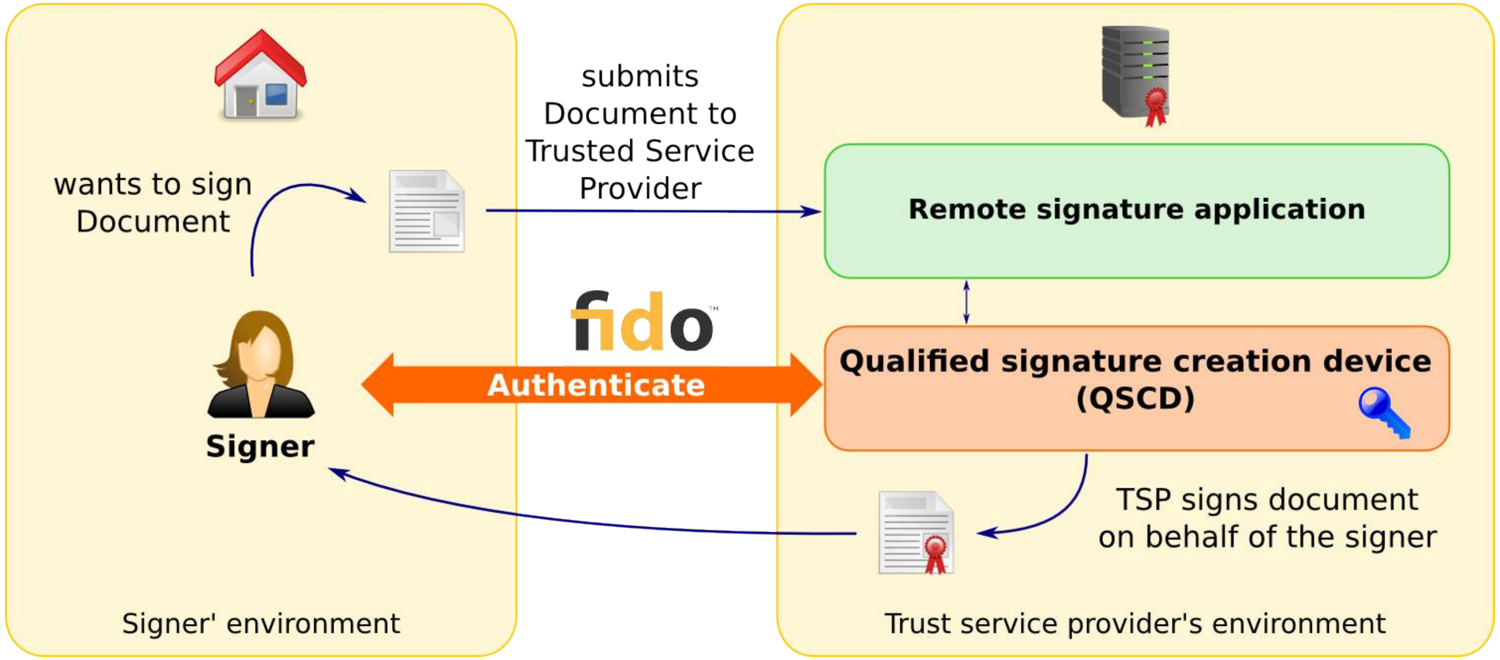
Remote electronic signatures - Strong Authentication

- Trust Service Provider must ensure that the signatory's signing key used for electronic signature creation can be reliably protected by the
- legitimate signatory against use by others.

  - At least 2 authentication factors from different categories
  - Level of Assurance substantial for user authentication is required
  - It can be assumed that the authentication factors can only be used if they're under the control or possession of the person to whom they belong

- Authentication must be linked to the document to be signed

Remote electronic signatures

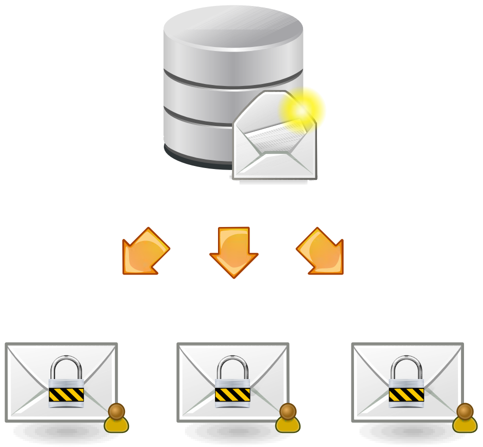

wants to sign Document
submits Document to Trusted Service Provider
Remote signature application
fido
Authenticate
Signer
Qualified signature creation device (QSCD)
TSP signs document on behalf of the signer
Signer' environment
Trust service provider's environment

- Trust service provider stores user’s signing key
- User authorizes usage of signing key by help of FIDO authentication

Federal Office
for Information Security

Electronic Registered Delivery Services

- Legal admissibility of data sent and received
- Presumption of integrity of for data sent and received and for accuracy of the date of the data sent and received
- Services are provided by qualified trust service provider (QTSP)
- Sender must be identified with a high level of confidence
- Sending and receiving of data have to be secured by AdES or AdESeal of the QTSP
- The date and time of sending, receipt and changes have to be indicated with a qualified time stamp



De-Mail

FIDELIO

ID-card

- Reliable Electronic Identification
- Level of Assurance High
- Certified Hardware

BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
T22000129
MUSTERMANN
GEB. GABLER
ERIKA
12.08.1964 DEUTSCH
BERLIN
31.10.2020
938568

FIDO

- based on asymmetric crypto
- high acceptance due to better market penetration

Yubikey 4, Yubico AB

- German ID-card does not natively speak FIDO
- Restricted-Identification offers similar functionality
  - e.g. strong cryptography, service provider dependent keys

- FIDELIO service translates between German ID-card and FIDO bases authentication
- German ID-Card can be used as FIDO token

Conclusion

- eIDAS demands for strong identification and authentication in many applications
- FIDO based solutions offer a path for strong authentication, but fulfilment of regulatory requirements needs to be demonstrated

fido ALLIANCE simpler stronger authentication

Thank you for your attention!

Contact

Dr. Michael Hoppe
michael.hoppe@bsi.bund.de
Tel. +49 (0) 228 99 9582-6135

Federal Office for Information Security
Godesberger Allee 185-189
53133 Bonn
www.bsi.bund.de

Federal Office
for Information Security