Federal Office
for Information Security

Technical Guideline TR-03159 Mobile Identities

Part 1: Security Requirements for eIDAS LoA “substantial”

Version 1.0 Draft 2
26. August 2019

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn

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

Table of Contents

Figures

Tables

1 Introduction

Following the ubiquitous market penetration of mobile devices, and their use for online government and business, security relevant processes must also be integrated in those devices. This covers identification and authentication of users, and extends further to transaction authorizations, payments and so on.

In the European Union, the eIDAS-Regulation [eIDAS] provides a technology neutral trust framework for identification processes. At the core, the Regulation defines three *Level of Assurance* (*low*, *substantial* and *high*), which govern mutual recognition of electronic identification means. Details of the Level of Assurance are defined in an Implementing Act [eIDAS LoA] and a corresponding "Guidance" [LoAGuidance] drafted and endorsed by the EU Member States. For the German market, the concept of Level of Assurance is detailed and extended beyond identification to authentication, transaction authorization and other process in the BSI Technical Guideline [TR-03107].

This Technical Guideline comprises two parts

1. The first part concretizes the requirements from [eIDAS] and [eIDAS LoA] for mobile identification scenarios on LoA *substantial*, while staying generic in terms of concrete implementations.
2. The second part defines a concrete implementation scenario for mobile identification based on the generic requirements in the German eID system.

This part of the Technical Guideline specified requirements for mobile identification schemes for Level of Assurance *substantial*. It must be read in conjunction with [eIDAS LoA] including the corresponding guidance [LoAGuidance]. The requirements contained therein must be fulfilled for Level of Assurance *substantial*.

2 Requirements for LoA substantial

This section lists the requirements from [eIDAS LoA] and concretizes them for mobile scenarios, where applicable. Hereby, the quotations from [eIDAS LoA] are highlighted by grey boxes.

In general, the requirement are quantified to resist against attacks by attackers possessing a defined attack potential. The required attack potential to be resisted is

- attack potential *enhanced-basic* for Level of Assurance *low*
- attack potential *moderate* for Level of Assurance *substantial*
- attack potential *high* for Level of Assurance *high*.

Here, the definition of the attack potentials, is to be understood as defined in [ISO18045][1], Annex B.4.

2.1 Enrolment

The enrolment (i.e., application, registration and identity proofing) is independent of the issued authentication means. Therefore, there are no specific requirements for mobile scenarios.

The requirements from [eIDAS LoA] for all parts of the enrolment process must be fulfilled.

For the identity proofing step, either

- a notified identification means on Level of Assurance at least *substantial*, or
- an identification proofing process evaluated to fulfil the requirements for Level of Assurance *substantial* according [TR-03147]

must be used.

2.2 Electronic identification means management

2.2.1 Electronic identification means characteristics and design

SUBSTANTIAL

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

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.

The Guidance of the eIDAS Cooperation Network [LoAGuidance] gives the following explanation of an authentication factor and the different categories of factors (footnotes not part of the original):

> Authentication factors can be divided into the following categories, with further consideration of each given below:
>
> - Knowledge-based factors;
> - Possession-based factors;
> - Inherent factors.
>
> Authentication factors from different categories may also be combined, e.g. a cryptographic token that is protected via a fingerprint or PIN. An identification means that utilises more than one

1 Also available as *Common Criteria Evaluation Methodology* (CEM) at https://www.commoncriteriaportal.org/cc/.

factor from different categories is called multi-factor, *for example: a smartcard (possession) that is activated via a PIN (knowledge) is a multi-factor identification means.*

If multi-factor authentication is used, the different factors should be chosen in a way to counter different threats/attack vectors.

Evaluating the strength of authentication needs to take into account not only the factor(s) itself, but also the mechanism to verify the factor(s)[2].

(a) 'possession-based authentication factor' means an authentication factor where the subject is required to demonstrate possession of it;

The relevant security characteristic of a possession-based authentication factor (e.g. token) is the sole control of it by the owner. This implies that it is important that reproduction of it by a third party is so difficult and unlikely that the risk of this is negligible. The Level of Assurance depends on the level of resistance against reproduction. *For example: asymmetric cryptographic (private) keys, the private keys may be stored on dedicated hardware devices (e.g. smartcards), or software token, uniquely identifiable token (e.g. the SIM card of a cell phone) or devices with one-time-passwords (e.g. "RSA-Token" or printed cards).*

Typical attacks on possession-based authentication factors are theft, duplication or tampering (manipulation), as well as attacks on the proof-of-possession during authentication.

(b) 'knowledge-based authentication factor' means an authentication factor where the subject is required to demonstrate knowledge of it;

The knowledge-based factor likely to be known only by the owner of the factor and the verifying entity, *for example: PINs, passwords, memorable words or dates, pass phrases, pre-registered knowledge and other information likely to only be known by the subject.* In some cases even the verifying entity may not know the actual knowledge-based factor, but are able confirm that they and the applicant know the exact same information, *for example using the hash of a password.*

If knowledge is used as a factor it is necessary to mitigate against guessing (either random or brute force) of the knowledge by an adversary. *For example: where the knowledge is a password, good practice prescribes a suitable password policy (e.g. see safeguard S 2.11 "Provisions governing the use of passwords" of the BSI IT-Grundschutz catalogues, Single token authentication & Password entropy of NIST 800-63-2 Appendix A).*

Typical attacks on knowledge-based authentication factors are guessing, phishing eavesdropping or duplication. A characteristic of knowledge-based factors is that attacks are not necessarily noticed by the subject of the electronic identification means. *For example: brute force/dictionary attacks on a password with low entropy and without retry counter or a password that has been copied from a letter or email without knowledge of the owner or the verifier.*

(c) 'inherent authentication factor' means an authentication factor that is based on a physical attribute of a natural person, and of which the subject is required to demonstrate that they have that physical attribute;

Inherent authentication factors should have a variance even between people of similar characteristics so that a person may be uniquely identified, *for example: fingerprints, palm prints, palm veins, face, hand geometry, iris, etc.*

A key consideration when a biometric factor is being used is to ensure that the person to whom it relates is physically present at the point of verification. This is to mitigate against spoofing or duplication.

2 As an example, this implies that for a biometric factor the quality and false acceptance rate of the sensor used to capture the biometrics for enrolment as well as for verification have to be taken into account. For sensors operated not under supervision, also the resistance to presentation attacks needs to be considered.

Further details on the characteristics of the different categories of authentication factors are given in the table 1, incorporated from [TR-03107], Part 1.

Some additional notes on the different types of authentication means:

- For knowledge based factors, the following requirements hold
  - remotely verified knowledge based means, e.g. passwords, must fulfil the requirements from measure M 2.11 „Regelung des Passwortgebrauchs“ (“Provisions governing the use of passwords”) of the IT-Grundschutz catalogues of the BSI ([BSI-GS])
  - locally verified knowledge based means, e.g. a decimal PIN verified by a smart card, must fulfill the requirements from [AIS 20/31]. If a retry counter of 3 is used, this implies a PIN length of 4 for Level of Assurance *low*, and a PIN length of 5 for Level of Assurance *substantial*. For other locally verified knowledge based factors, e.g. gestures on a touch screen, an equivalent security level must be fulfilled. Equivalence needs to be demonstrated by the operator of the scheme.
  - Except for one time passwords (OTP) or passwords used to protect authentication means during issuance, the value of knowledge based authentication factors should be chosen by the holder to ensure that only the holder knows the value.
- The definition of inherent authentication factor excludes behaviour-based factors.
  - Remotely verified biometrics are not supported by the Technical Guideline, since there are currently no reliable methods for presentation attack detection available in this scenario.
  - For locally verified biometrics, the strength of the mechanism must be comparable to the strength of a locally verified knowledge based factor on the required Level of Assurance, see above. The

	Possession	**Knowledge**	**Inherent**
Prevention			
Linking to Holder	Uniqueness of the possession; Factor must be protected against duplication; holder must not give up possession of means	Only the holder knows the knowledge; Knowledge must not be transferred to others	Holder specific biometric characteristics; Presentation attack detection
Control by holder requires:	Possession under physical control of the holder; Possession is solely used for the scheme s	Knowledge is only used for authentication	Biometric characteristic is only used for authentication
Detection			
Detection of lost control	Loss of possession; Additionally detection of misuse	Only by detection of misuse retroactively	
Reaction			
Revocation of means	Via unique identifier of possession	Locking the corresponding user account (if verified by server) or of the corresponding possession factor (if locally verified)	
Replacement for revoked mean	Via new possession mean	New password / PIN	Registration of another biometric characteristic

Table 1: Characteristics of types of authentication factors

evaluation of the strength must consider the biometric matching characteristics (False Acceptance Rate) as well as the resistance against presentation attacks.

For Level of Assurance substantial, two factors of different categories must be combined. The two factors and the authentication protocol must be designed in such a way that it is not possible to attack both factors independently of each other, i.e. both factors must be linked (e.g. PIN entry is locally verified by the possession based factor). In particular, an attacker must not be able to assign the failure of an authentication attempt to a single authentication factor. Likewise, both factors must not be attackable together by a single attack on the user environment. As an example, the combination of a remotely verified password and a remotely verified biometric characteristic would enable to compromise both factors by simply recording and replaying a transmission.

Additionally, the combination of the factors must ensure, that valid (single) factors from different authentication means cannot be combined into a valid new authentication mean.

The requirement that the authentication mean can be assumed to be only used under the sole control of the holder implies that one of the factors must be knowledge based or inherent. This also implies that some user interaction (either providing the knowledge or the biometrics) is required in the moment of authentication. Re-using stored information or automatically forwarding information (e.g. push OTP) does not fulfill this requirement.

Therefore, in practice, there are only a few possible combinations of authentication factors for mobile scenarios for Level of Assurance *substantial*, e.g.

- a possession based factor with locally verified knowledge, e.g. a smart card or secure element with PIN;
- a possession based factor with locally verified biometrics, e.g. a secure element unlocked with a biometric characteristic.

In all these cases, a possession based factor is necessary for Level of Assurance *substantial*.

Examples for possession based factors in the context of mobile identification are

- a secure external cryptographic token (smart card)
- a secure internal cryptographic token (secure element or SIM card).

Since the rich OS of a mobile hand set cannot be regarded as secure, all relevant security requirements must be fulfilled by the token. For the local verification of knowledge based / inherent factors, they must either be directly verified by the token, or by a secure compartment not under the control of the rich OS.

2.2.2 Issuance, delivery and activation

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.

The basic characteristic of Level of Assurance substantial is a two factor authentication. For the issuance process to deliver the same reliability, the two factors must either be delivered by different channels, or only after identification of the holder by the issuing authority by an identification proofing process on Level of Assurance *substantial*.

If the owner is already in possession of one or more of the authentication factors before identification (e.g. multi-purpose authentication means), the activation procedure must take the following measures:

- The authentication factor(s) must be verified for their suitability for Level of Assurance *substantial*. (e.g. by an attestation mechanism)
- The procedure must demonstrate that the identified person is identical with the person in possession of the authentication factor(s).

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.

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

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

For Level of Assurance substantial, a revocation of an identification means must be effective (i.e. the revocation information must be available to the relying parties) no later than 12 hours after revocation by the holder or another authorized entity. A revocation hotline or similar route for revocation must be available for the holder at all times.

Note that it is not sufficient if the holder is required to de-register his authentication means at each relying party. It must be possible to prevent the use of the authentication means at all relying parties with a single revocation.

Reactivation of authentication means requires the identification of the holder via a process on at least the same Level of Assurance as the authentication means itself. E.g., reactivation of an authentication means on Level of Assurance *substantial* requires identification of the holder on Level of Assurance *substantial* or *high*.

It must be ensured, that e.g. a possession based factor is actually in possession of the holder before reactivation.

2.2.4 Renewal and replacement

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.

In the context of mobile identities, renewal / replacement require the same process as the initial issuance, including identity proofing.

2.3 Authentication

For authenticating the holder of identification means, an authentication mechanism needs to be employed.

2.3.1 Authentication mechanism

LOW

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

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.

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.

For data protection reasons, it is required that the holder of the authentication means is authenticated before personal data are released to the relying party.

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.

The term dynamic authentication is explained by [LoAGuidance] as follows:

> **(3) 'dynamic authentication' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity**
>
> The primary purpose of dynamic authentication is to mitigate against attacks such as 'man-in-the-middle' or misusing verification data from a previously recorded authentication replay to the verifier. This includes:
>
> - replay attacks, i.e. intercepting verification data and reusing them in a different authentication context
> - certain types of session hijacking, e.g. exchanging (parts of) the authentication contexts of two or more simultaneously occurring authentications.
>
> It is important to understand that multi-factor and dynamic authentication are not the same; multi-factor authentication does not require that the authentication is dynamic (e.g. PIN and fingerprint) and can therefore be more exposed to replay attack than a dynamic authentication.
>
> Dynamic authentication might be implemented by the authentication factor (e.g. a one time key from a device) or by the authentication mechanism (e.g. dynamic challenge in a challenge-response authentication).
>
> *Examples for dynamic authentications are:*
>
> - *possession of a private key stored on a smart card and verified using a challenge-response-protocol*
> - *protocols based on an ephemeral Diffie-Hellman and providing authentication (e.g. PACE), cryptographic nonces, timestamps and/or non-repeating sequence numbers.*
> - *protocols based on a static-ephemeral Diffie-Hellman, if the ephemeral key is provided by the relying party (e.g. EAC)*
> - *dynamically generated one time access code (e.g OTP tokens) or challenge response protocols where the one time code has been previously generated and distributed out of band but selected dynamically during authentication (e.g. OTP cards)*
>
> If the subject's private key is stored remotely (centrally stored, e.g. in an HSM operated by the identity provider), the authentication used to access the private key should also be dynamic.

Usually, dynamic authentication involves a cryptographic protocol. The requirements from [SOG-IS Crypto] and [TR-03116] apply. For OTPs the requirements from [AIS 20/31] apply.

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.

The different Level of Assurance are differentiated by the degree of reliability of the identification the relying party can expect from the identification scheme. This is also reflected by a differentiation of the attack potential the identification means and the authentication mechanisms must resist. For Level of Assurance *substantial* the identification means and the authentication mechanism must resist attack potential *moderate* as defined in [ISO18045], Annex B.4.

In order to validate fulfilment of this control, the following is required:

- The authentication mechanism must be proven to meet the claimed security goals by a cryptographic security proof. The assessment must take the relevant threats into account, e.g. online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attack, session hijacking, man-in-the-middle, credential theft, spoofing and masquerading.
- The security of the identification means must be proven by a Common Criteria certification against a suitable (i.e. covering all relevant assets and threats) protection profile on Assurance Level 4 augmented by AVA_VAN.4. Besides the threats listed for the authentication mechanism, also direct attacks against the identification means must be taken into account, e.g. side-channel or invasive attacks. This requires the use of a secure hardware element, which implements the client-side core security functionalities of the authentication mechanism. Note that Common Criteria certification covers only the identification means as such (the TOE), the overall attack resistance of the authentication mechanism needs to be assessed additionally.
- During assessing attack resistance, the whole authentication mechanism must be taken into account including the risks resulting from verification of the possession of the electronic identification means. If the security mechanism relies on the security of external entities, e.g. the security of a mobile network to transmit an OTP, this needs to be also taken into account.

For the analysis of the authentication mechanism, it must be clear which components of the identification scheme comprise the identification means. Examples:

- For a mechanism based on the possession of a private key, the component in the possession of the subject holding the key is the possession based factor and must mitigate the above attacks. Note that in the case of a remote HSM, the HSM is not a possession factor (it is not actually in the possession of the subject), but the mechanism used to authenticate *towards* the HSM is the authentication mechanism.
- For a mechanism based on a smsOTP, the possession based factor is the phone number the sms is sent to. This implies that the phone number must be guaranteed by the network to be matched against a unique / single SIM, which then can be regarded as a proxy for the phone number. If the phone number is not tied to a unique / single SIM, the smsOTP cannot prove the possession of the possession based factor.

2.4 Management and organisation

The requirements from section 2.4 of [eIDAS LoA] apply.

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.

All security relevant entities in the identification scheme must have a certified Information Security Management System according to [BSI100-2] or [ISO27001]. This covers entities involved in

- the enrolment, identity proofing and issuance of identification means, as well as
- in the operation of identification mechanism including authentication, revocation and validation.

For Certification Authorities in the identification scheme, a certification according to [TR-03145] is required.

3 Additional Requirements

Besides the security requirements based on the Level of Assurance of the eIDAS Regulation detailed in the previous section, additional requirements stemming from other sources must be considered. Some of these are listed in the following.

3.1 Legal Requirements

There are additional relevant legal requirements besides the eIDAS Regulation. Since, by definition, an identification schemes handle personal data, the General Data Protection Regulation (GDPR) must be reflected.

The GDPR requires “Support for Security by Design and Privacy by Design”. This requires that the infrastructure and its components (i.e. the mobile device) support a defined level of assurance and that potential weaknesses or limitations are known to the application developer. Furthermore, implementations based on storage of the identification data under physical control of the subject (e.g. in the handset itself) are favoured from this perspective

3.2 Economic and Market Considerations

The market for mobile electronic identities comprises many different market participants in all areas, e.g. handset vendors, network operators, application developers and so on. In Order to avoid market fragmentation, and in order to foster an interoperable identification infrastructure, mobile electronic identification schemes should be based on open standards.

References

[AIS 20/31]	BSI: AIS 20/31 -- A proposal for: Functionality classes for random number generators
[BSI100-2]	BSI: BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
[BSI-GS]	BSI: IT-Grundschutz-Kataloge, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[TR-03107]	BSI: Technische Richtlinie TR-03107, Elektronische Identitäten und Vertrauensdienste im E-Government
[TR-03116]	BSI: Technische Richtlinie TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung
[TR-03145]	BSI: Technische Richtlinie TR-03145, Secure CA Operation
[TR-03147]	BSI: Technische Richtlinie TR-03147, Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen
[eIDAS LoA]	European Commission: Commission Implementing Regulation (EU) 2015/1502
[eIDAS]	European Parliament, Council of the European Union: 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
[ISO18045]	ISO/IEC: ISO/IEC 18045: Information technology — Security techniques — Methodology for IT security evaluation
[ISO27001]	ISO/IEC: ISO/IEC 27001: Information technology -- Security techniques -- Information security management systems -- Requirements
[SOG-IS Crypto]	SOG-IS: Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms
[LoAGuidance]	: Guidance for the application of the levels of assurance which support the eIDAS Regulation