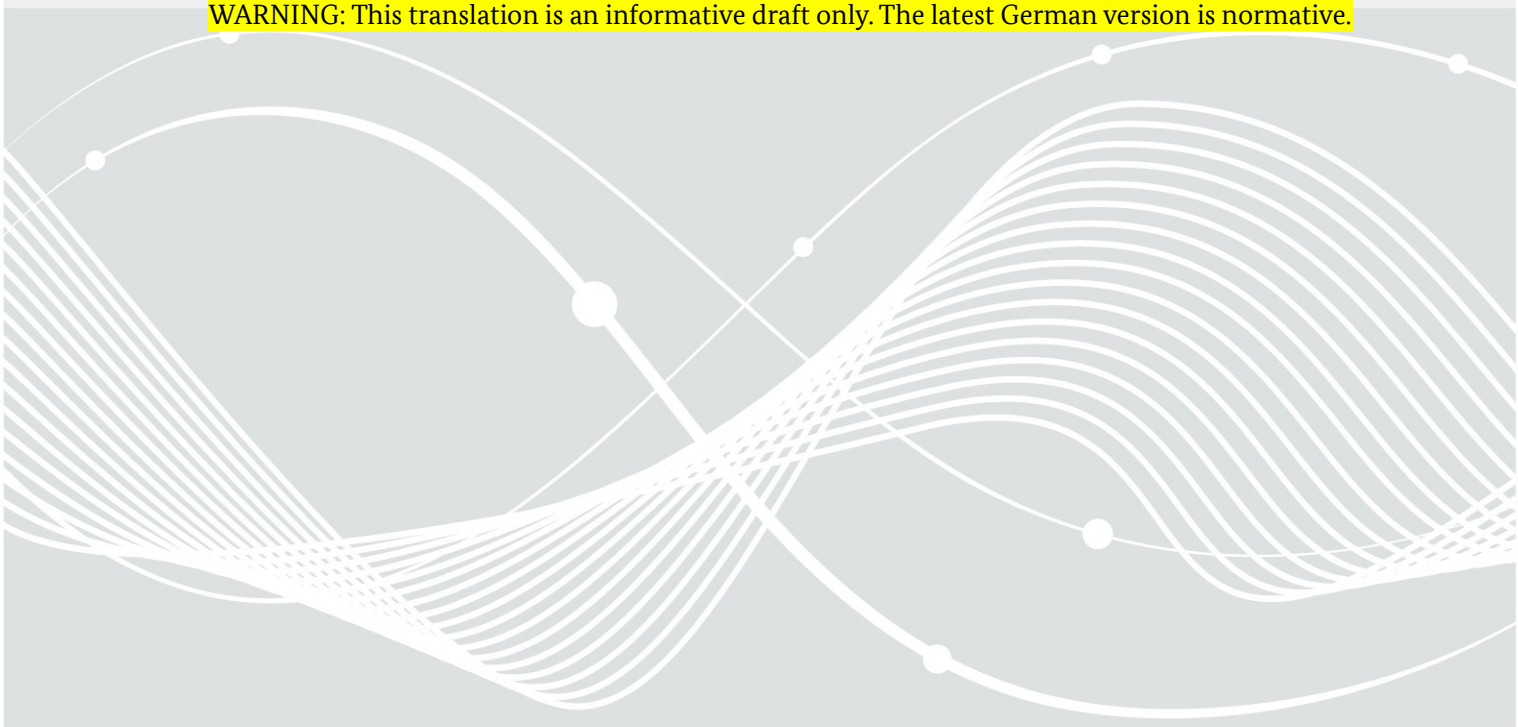
Bundesamt
für Sicherheit in der
Informationstechnik

Technical Guideline TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons

Version 1.0.4
08.11.2018

WARNING: This translation is an informative draft only. The latest German version is normative.



Federal Office for Information Security (BSI)
PO Box 20 03 63
53133 Bonn, Germany
Phone: +49 22899 9582-0
E-mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

Table of Contents

1 Introduction

1.1 Objective and content of the Technical Guideline

The (initial) identification of natural persons is decisive for the security of e-government and multiple other digital business processes. Critical aspects of identity checks are the reliable prevention and detection of fraud, for instance identity theft or the usage of a non-existent identity. Based on the threats to identity checks, proper requirements for the identity checks have to be defined and implemented.

Complementary to the Technical Guideline [TR-03107-1] (Electronic Identities and Trust Services in E-Government), the present Technical Guideline examines threats and requirements for identity proofing and verification procedures which are based on the usage of ID documents (e.g. ID cards or passports). Just as [TR-03107-1], the present Technical Guideline takes into account that the (minimum) required level of assurance varies, depending on the kind of e-government or business process. For the assessment of identity verification procedures, the same assurance levels as in [TR-03107-1] are used. These assurance levels are *normal*, *substantial* and *high*.

Additionally, the present Technical Guideline defines the requirements for the assurance levels in such a manner, as to fulfil also the requirements of [eIDAS LoA] as far as identity proofing and verification of natural person is concerned. That is, with the requirements according to the present Technical Guideline for the assurance levels *normal*, *substantial* and *high*, the requirements according to [eIDAS LoA] for the assurance levels *low*, *substantial* and *high*, respectively, are fulfilled.

The assurance level required for a specific e-government or business processes needs to be determined by the process owner of the service in question. This aspect of determining the **required** assurance level for specific processes is out of scope of this Technical Guideline. Also, aspects like service availability or non-reputability of identification / registration processes are not considered. Furthermore, this Technical Guideline does not address necessary measures to ensure the confidentiality of transmitted or stored data or other data protection aspects.

1.2 Structure of the Technical Guideline

Section 2 explains some terms and definitions used throughout this document to describe identity proofing and verification procedures, and to evaluate attack scenarios on these procedures.

Section 3 gives an overview of the basic security objectives (existence, legitimacy and, if applicable, uniqueness), threats and requirements of the identity proofing and verification procedures. The specified requirements on the identity proofing and verification procedures aim at achieving the security objectives in face of the existing threats.

The requirements from Section 3 are refined in Sections 4 to 8. The threats related to the security objectives are analysed top-down and the resulting refined requirements are surveyed, differentiated according to the assurance levels *normal*, *substantial*, *high*. Section 4 deals with the requirements on secure ID documents. Section 5 discusses the security of any intermediary transmission channels, i.e. interfaces between presenting a proof of identity and its verification. Sections 6 and 7 discuss the verification of proof of identities with respect to the utilised ID documents and the (biometric) check against persons. Having regard to applications where unique identities are required, threats and requirements for the registration of unique sets of ID attributes are discussed in Section 8. Section 9 discusses general risks and related security requirements for organisations that perform identity verification procedures.

2 Definitions and assessment methodology

2.1 Terminology

Proof of identity: Identity information (e.g. ID documents, biometric characteristics, or biometric data) available about a natural person in combination with all known properties of this information (like, for instance, metadata) to confirm the authenticity and integrity of the identity information. This Technical Guideline presumes that the proof of identity is always provided by the natural person to be identified. In other words, any proofs of identity that are provided for or on behalf of third persons are out of scope of this Technical Guideline.

Identity check (ID check): Identity verification procedure, i.e. check of consistency and authenticity of the data that is provided by a proof of identity. In the context of this Technical Guideline, an ID check is always based on a proof of identity.

Authoritative source: "any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity" [eIDAS LoA].

ID document: A physical object issued by an authoritative source (e.g. residents' registration office, foreigners' registration office) that can be used to provide a proof of identity. An ID document is therefore a special kind of authoritative source. ID documents can be issued by both public or private entities. Examples of ID documents are the German national ID card, electronic residence permit, passports, driving licences[1].

ID register: Authoritative source that is not or can not be provided in the form of an ID document. Examples of ID registers are public registers of residents or the Central Register of Foreign Nationals in Germany.

For ID checks considered in this Technical Guideline, it is always assumed that they are based on the checking of ID documents that are used as authoritative sources. Additional information may be used, for instance from an ID register. The classification of any source of information as authoritative source shall be based solely on the correctness and integrity of the data a provided directly by the source of information. That is, possible subsequent manipulations and protection mechanisms for data transmitted from an authoritative source are to be taken into account separately.

The terms **entity**, **identity attribute** (ID attribute), **identity** and **unique identity** are used as defined by [TR-03107-1].

2.2 Attack potential

Attack potential denotes a measure for the resources necessary to implement and execute a specific attack on the target of evaluation (TOE). Normally, the categories expertise, resources and motivation describe the attack potential of an attacker [CC1]. TOEs in the sense of this Technical Guideline are procedures for ID verification. Scope of a TOE assessment according to this Technical Guideline are products (e.g. ID documents, software/hardware used for verification) as well as processes, procedures, and work instructions (e.g. verification of a hologram by a human inspector). More specifically, for the assessment of the attack potential the necessary resources from the following five categories have to be assessed:

- **elapsed time**: Time required to prepare, implement and execute the attack.

1 This exemplary list of documents does not imply any assessment of ID documents regarding their possible suitability for certain assurance levels. The term "explicit ID document" refers to ID documents issued for the explicit purpose to be used for identity proofing and verification. For example, European driving licences conforming to Directive 2006/126/EC are ID documents but no explicit ID documents.

- **specialist expertise**: required or applied **generic**[2] expertise on technologies and techniques that are employed in the TOE.
- **knowledge of the TOE**: required or applied **insider** knowledge about a specific TOE, e.g. about a specific ID check.
- **window of opportunity**: opportunities to access a TOE in order to prepare and/or execute an attack. For example, online or offline access to the TOE has to be considered. Also, any restrictions in the feasibility of attacks have to be considered. For instance, if a method for a certain manipulation requires for its calibration repeated access to (parts of) the TOE.
- **equipment:** availability and costs of material and other equipment that is used or required for an attack.

For the overall assessment of the attack potential necessary for a successful attack [CEM], Appendix B.4 has to be taken as basis. Based on the resources required for an successful attack the overall calculation of attack potential shall be done according to [CEM] Appendix B.4.2.3, Table 3. The attack potential against which a requirement can still be considered as sufficiently secure follows from [CEM], Appendix B.4.2.3, Table 4 (“Rating of vulnerabilities and TOE resistance”).

2.3 Successful attack

The execution of an attack is to be considered as successful if and only if an illegitimate proof of identity is provided and the implemented ID check does confirm the illegitimately claimed identity. If there is any successful and reproducible attack that is relevant within the attack potential to be considered (see Section 2.4), the ID check is not suitable for the pursued assurance level. If the attack under consideration has a certain statistical probability of success, it has to be considered as successful if the resulting false acceptance rate (FAR[3], false positive) is above the maximum permissible value for a certain application or assurance level. Here, it is presupposed that a maximum permissible FAR is pre-defined for an ID check (or its related e-government / business processes). Within the attack potential that is to be considered as relevant according to the aspired assurance level, it must not be possible to exceed the pre-defined FAR.

When assessing attacks on cryptographic procedures, protocols, or their concrete implementations in software or hardware, a binary evaluation is sometimes possible. That is, it may be possible to decide whether, for example, a key stored on a chip card can be reproducibly compromised by a specific attack. This is in contrast to probabilistic statements on security, i.e. quantitative information on the probability with which a TOE can be compromised during the execution of an attack.

When assessing attacks on ID checks that are based on biometric recognition (by trained staff or automated procedures), frequently only probabilistic statements are possible. The overall “quality” of biometric recognition is usually measured by contrasting the FAR and the false rejection rate (FRR, "false negative"). Both measures are essential for the practical usability of methods, and there is usually an inherent trade-off in the optimization of FAR and FRR. For the security aspects considered in the Technical Guideline, only the FAR is relevant. The FRR is not considered within the scope of this document. To determine the FAR that is achieved by a specific attack, the procedures used for checking whether a claimed identity does exist and whether it matches with the person claiming the identity, have to be analysed. Again, this applies likewise to procedures carried out by trained staff or automated procedures. Depending on the type of procedure, any applicable data capturing (e.g. reading of ID attributes, biometric or other reference data), data transmission and data analysis / matching needs to be considered.

The maximum admissible FAR must be defined before the audit is conducted. As stated above, it depends on the application and the required assurance level. For example, the Technical Guideline Biometrics for Public

2 In the context of *specialist expertise* the term *generic* is used to differentiate specialist expertise in a certain field from specific knowledge of the TOE, i.e., to differentiate if from specific insider knowledge.

3 In the literature, the more specific term "false match rate" is frequently used. In this Technical Guideline we use the more general term "false acceptance rate" in the sense that an illegitimately claimed identity is erroneously accepted.

Sector Applications [TR-03121-3] stipulates that the FAR for the biometric matching (finger print or face) must not exceed 0.1% (1:1,000).

For determining the FAR of an ID check without any malicious manipulation efforts, a random selection of the person to be identified from the relevant population and the biometric data between which the comparison is carried out, must be taken as a basis[4].

2.4 Assessment of the attack potential

For a successful attack that has been theoretically identified or practically implemented and executed, it must be assessed whether it is relevant for the TOE and the intended assurance level. An attack is relevant for a specific assurance level if and only if the attack potential necessary for its design and execution is to be taken into account according to Table 1.

	Assurance level		
	normal	**substantial**	**high**
Attack potential (according to [CEM]) to be taken into consideration	up to and including enhanced-basic	up to and including moderate	up to and including high

Table 1: Maximum attack potential to be taken into consideration for the different assurance levels

For example, due to technological progress or the disclosure of previously confidential information, additional attack options that require a lower attack potential may become feasible. For instance, the attack potential required for a successful attack may be reduced from high to moderate in the course of time. In such a situation, a previously obtained assurance level remains valid for the date at which the assurance level assessment was conducted, except it turns out that such attacks requiring a lower attack potential had already been known and in use.

2.5 Execution of attacks

There is a risk of manipulation with any type of ID check. To assess the assurance level of an ID check, possible attacks need to be analysed. An approach to analyse attacks is their practical execution and evaluation of the required resources, i.e. the required attack potential. In case there is a sound empirical or theoretical base, possible attacks can also be analysed without a (complete) practical execution. Of course, to analyse the feasibility of attacks, all safeguards against manipulation implemented by the ID checking procedure must be considered. For example, the utilization and quality of inspection equipment or minimum requirements for illumination or resolution of video transmissions have to be taken into account.

4 The case that (by chance) an actually correct matching pair of person to be identified and biometric data are selected from the respective populations is not relevant in determining the FAR.

3 Proof of identity and identity checks

3.1 Security objectives

Possible security objectives of ID checks procedure are:

S1. **Existence**: Existence of an entity (natural person) to which all claimed ID attributes apply.

S2. **Legitimacy**: All stated ID attributes apply to the natural person claiming them (implies S1. Existence).

An ID checking procedure does not necessarily require a unique identification of an entity (natural person). Frequently, however, a unique identity is required (for instance in [eIDAS]).

S3. **Uniqueness**: No two persons have identical values for all captured ID attributes.

The relevance and any relative priority of the security objectives depends on the intended use for which the ID checking is required. Security objectives that are not relevant for a specific use case may be ignored. It needs to be ensured, however, that all relevant security objectives and the related threats and requirements are taken into consideration.

3.2 Threats

To ensure the security objectives existence, legitimacy, and uniqueness are achieved, measures to prevent and detect the following threats need to be implemented:

B1. Claimed ID attributes apply neither to the person claiming them[5] nor to a different person.

B2. Successfully and correctly checked ID attributes become invalid (for instance, due to a change of name).[6]

B3. A person uses illegitimately the ID attributes of another person (impersonation or identity theft).

B4. Claimed ID attributes are valid for more than one person.

3.3 Requirements

From the security objectives existence, legitimacy, and uniqueness and the threats described in Section 3.2, the following requirements can be derived to ensure secure ID checking procedures:

A1. Trustworthy ID documents (as an authoritative source according to [eIDAS LoA]).

A2. Trustworthy transmission channels. This is relevant if entities performing the ID checking have no immediate access to the ID document, no immediate contact to the natural person to be identified, or both.

A3. Reliable checking of the ID documents.

A4. Reliable control of used transmission channels.

A5. Reliable comparison between the person to be identified and the presented ID document (integrity of the proof of identity).

A6. Collected ID attributes allow a unique identification.

5 If the claimed ID attributes are no longer up-to-date (for example, after a change of residence or name) they may still be suitable for a unique identification, provided they had been valid in the past. If, in addition to the unique identification of a person, specific ID attributes are required for a certain use case, the up-to-dateness of these attributes may need to be ensured on top of the actual identification process.

6 This threat is only relevant for use cases where a permanent validity of recorded ID attributes is relevant. For one-time ID checks at a single point in time, this threat as no relevance.

A7. Correct registration (and, if applicable, recording) of all required ID attributes.

A8. Ensuring the integrity of all process steps.

A9. Binding and documented specifications for all steps of the ID check. The specifications need to be compliant with all requirements on the ID verification.

Points A1. and A2. take the quality of the of the ID proofing process into consideration, points A3., A4., and A5. the quality of the ID checking procedures. Combined, points A1. to A5. account for the core assurance level of the ID proofing and verification procedures and thus the attack potential necessary for successful (external) attacks based on counterfeited proofs of identity. Point A7. is on quality assurance to prevent any inadvertent errors. Point A8. is on ensuring the integrity of all ID checking procedures, in particular to counteract any insider threats (e.g. from staff). Point A9. is transversal and includes in particular the requirements on documentation for all processes and requirements.

3.4 Coverage of the security objectives and threats

For covering the protection goals existence, legitimacy and uniqueness by the security requirements stated in Section 3.3, the relationships from Table 2 apply.

Protection goal	**Covered by requirements no.**	**Rationale**	
S1. Existence	A1., A2., A3., A4.	A1. ensures that the existence is verified based on trustworthy ID documents. A2., A3. and A4. ensure that the authenticity of ID documents provided for identity proofing is properly checked.	A8. and A9. define organisation wide security measures and ensure their proper implementation.
S2. Legitimacy	A1., A2., A3., A4., A5.	A1., A2. and A3. ensure that a person is (e.g. biometrically) matched only with an actually existing identity (corresponding to the identity of the presented ID document). A4. and A5. ensure that only the legitimate person may successfully claim a specific (i.e., her own) identity.	
S3. Uniqueness	A6., A7.	A6. ensures the uniqueness of the set of ID attributes to be captured, A7. ensures their accurate capture and registration.	

Table 2: Coverage of the protection goals of an ID verification

For the prevention and detection of the threats from Section 3.2 by the security requirements specified in Section 3.3 the relationships from Table 3 hold.

Threat	Covered by requirements no.	Rationale
B.1	A1., A2., A3., A4.	Based on a properly verified, trustworthy ID document, A1., A2., A3. and A4. together ensure that the claimed identity does exist.
B.2	A9.	For possibly required recurrent verifications of the validity of an identity, A9. ensures that all necessary organisational procedures are in place.
B.3	A1., A2., A3., A4., A5.	Based on A1. and A2., the requirements A3., A4. and A5. ensure that the person to be identified has the claimed identity (i.e., the identity corresponding to the presented ID document).
B.4	A6., A7.	A6. and A7. ensure that the set of captured ID attributes defines a unique identity.

Table 3: Coverage of the threats of an ID verification

An incorrect ID verification may occur if any single requirement from Section 3.3 is violated. The overall achieved assurance level of an ID verification is to be determined according to the minimum principle, pursuant to the assurance level achieved for each individual requirement.

4 Trustworthy ID documents

The basis for a regular ID verification is the availability of at least one trustworthy ID document. Such an ID document needs to allow for an authoritative verification of the authenticity and integrity of all relevant ID attributes[7].

ID registers (e.g. register of residents, Central Register of Foreign Nationals) can be used as authoritative source in addition to trustworthy ID documents. The assurance level assessments of this Technical Guideline, however, are solely based on ID documents as proofs of identity. According to the minimum principle, the overall achievable assurance level is to be determined based on the ID document providing the lowest assurance level for a specific ID check. The analogue applies if an admitted ID document has inherently no (i.e. below *normal*), a *normal*, or a *substantial* assurance level, e.g. due to the processes related to the ID document issuance.

4.1 Threats

For the trustworthiness of ID documents, the following threats have to be taken into account:

B1. The source (including the relevant supply chains, i.e. all involved entities like production or logistics) is not trustworthy or compromised.

B2. The ID document is not forgery/tamper-proof.

B3. The ID document does not allow a reliable and tamper-evident check whether a person using the document is its legitimate owner.

B4. Available ID attributes do not allow for a unique identification of a person.

B5. The ID document itself (or relevant ID attributes) is expired or has become invalid.

4.2 Requirements for assurance level assessment

For the prevention and detection of the threats from Section 4.1, the below discussed requirements for trustworthy ID documents have to be taken into account. To evaluate the assurance level for which an ID document is at most suitable, the requirements from Table 4 have to be considered. Those requirements are differentiated according the to the assurance levels. Some requirements are applicable only for assurance level *substantial* or *high*. Other requirements are relevant for all assurance levels, but stipulate an assurance level dependent resilience against potential attacks. At any rate a valid ID document is required, in particular it must not be expired.

7 Requirements and procedures for the issuance of breeder documents (e.g. birth certificates) need to be defined if a trustworthy ID document is not (yet) available for a person (e.g. a newborn). Such requirements and procedures are out of scope of this Technical Guideline.

No.	Requirement	Required for assurance level		
		normal	**substantial**	**high**
A.1	Authoritative source	yes[8]	yes; explicit ID document	yes; officially recognised ID document[9] (implies explicit ID document) or equivalent[10]
A.2	Provides a sufficient set of ID attributes	yes	yes	yes
A.3	Protected against forgery and manipulation	yes; secure against "enhanced-basic" attack potential	yes; secure against "moderate" attack potential	yes; secure against "high" attack potential
A.4	Security features are known and effectively verifiable	yes; secure against "enhanced-basic" attack potential	yes; secure against "moderate" attack potential	yes; secure against "high" attack potential
A.5	Affords a reliable check against its legitimate owner (i.e., allows to detect illegitimate usage)	yes	yes; ID document with facial image data or technically and legally equivalent; not older than 10 years	yes, as *substantial*
A.6	ID attributes are up to date	-	yes[11]	yes, as *substantial*
A.7	Available lost, stolen, or revoked reports are checked	-	yes (as far as available)	yes, as *substantial*
A.8	Periodic check of the set of admitted ID documents	yes	yes	yes

Table 4: Requirements on trustworthy ID documents for the different assurance levels

4.2.1 Authoritative source (A.1)

The ID document is issued by an authoritative source and therefore represents itself an authoritative source. This stipulates the trustworthiness and integrity of all parties involved in the provisioning of the ID document (in particular, the issuing and the producing and personalisation parties). The following requirements have to be fulfilled so that an ID document can be considered as an authoritative source:

1. The entities responsible for issuing the relevant ID documents are known.

8 For instance, possibly a driving licence (which is typically not an explicit ID document).
9 According to the jurisdiction that applies to any underlying contract or according to which a proof of identity is regulated by law. For Germany, see for instance the latest editions of the "Allgemeinverfügung über die Anerkennung eines ausländischen Passes oder Passersatzes".
10 Here, "technically equivalent" refers in particular to an equivalent level of security features and their verifiability of an ID document (i.e. protection against forgery or manipulation).
11 This requirement may also be be omitted for applications requiring level *substantial* or *high* in case the maintenance of up-to-date ID attributes is explicitly not required.

2. For the relevant entities from point 1. above (including any intermediary services or media), publicly available information on any compromise is gathered and taken into account in a timely manner.[12]
3. Available information about counterfeited or manipulated ID documents is gathered and taken into account in a timely manner.
4. ID documents are only issued to the respective authorized person. That is, the eligibility and identity of an applicant is adequately verified before the issuance of the ID document.

Regardless of technical aspects, additional restrictions (e.g. legal or contractual restrictions) may apply on the set of permissible ID documents for some applications. Such restrictions have to be taken into account independent of and in addition to any technical assessment.

The direct use of ID registers may be a legally and technically suitable alternative to the use of ID documents. Such scenarios, however, are out of scope of this Technical Guideline.

4.2.2 Provides a sufficient set of ID attributes (A.2)

The actual set of ID attributes that is required for a proof of identity depends on the specific application. If required by the application, the set of ID attributes has to allow a unique identification. This point is not related to technical security aspects.

4.2.3 Protected against counterfeit and manipulation (A.3)

For the German national ID card, the electronic residence permit[13], and passports issued by EU and EFTA member states, a *high* assurance level w.r.t. protection against counterfeit and manipulation can be presumed, unless contrary indications are available.

For the technical evaluation of the protection against counterfeit and manipulation, the relevant metric is the attack potential necessary for a successful ID verification with a phony ID document. The attack potential has to be classified taking into account the current state of technology and its availability. In any case, the attack potential can not be evaluated in isolation for an ID document but has to be examined in combination with an ID verification procedure. That is, the scope and depth of the ID check must be considered in addition.

Various possible attack scenarios have to be considered. For example, an attacker may

- manipulate certain data of an otherwise genuine ID document,
- design a counterfeited document based on parts from different genuine ID documents,
- design an counterfeited document from scratch.

Depending on the attack scenario, different resources are required. In the following, some resources possibly used for an attack are discussed as examples. Also, some guidance with respect to the corresponding attack potential are provided (on the basis of [CEM] Annex B.4).

Specialist expertise: Irrespective of the specific attack scenario, laymen usually can not produce high-grade manipulations or counterfeits. Usually, the expertise required for a specific attack can not be rated in isolation for a a specific ID document and verification procedures. Additionally, the available / necessary equipment (cf. below) for manipulations needs to be taken into account. Likewise, usage of specialised equipment requires frequently appropriate knowledge and qualification like training in the printing industry or other specialist expertise.

12 For instance, media reports about the relevant entities must be monitored and taken into account. For ID documents that are legally recognised as official ID document and issued by the public administration, the integrity of the issuing entities can be presupposed.

13 Provided the electronic residence permit has been explicitly issued as an ID document, i.e., it is based on verified ID attributes.

Knowledge of the Target of Evaluation (TOE) (i.e., knowledge of non-public information)**:** As a rule, fully personalised ID documents are to be considered as publicly available. Nevertheless, for various attacks non-public information (e.g., composition of used materials, parameters from the production process) may be required.

Window of Opportunity (i.e., possibilities to access the TOE or parts of it that are not publicly available): This includes access to original production and personalization machines or access to original raw or auxiliary materials (like pre-produced blank documents) required for a certain attack scenario. Such access possibilities may also exists at the manufacturer of production / personalisation machines, besides the regular ID document production and personalisation sites. Usually, an unrestricted access to such machines is not possible. For a practical evaluation of the Window of Opportunity in an attack scenario, the criteria from [JILSS] Section 9.3 should be considered.

Equipment: Generally tools and/or materials are required to execute any devised attack in practice. The kind of required equipment depends on the approach of the attack and the security features that need to be circumvented. In case original materials and/or machines are used, the related **Window of Opportunity** needs to be considered. Simple card bodies, foils or holograms are freely available without significant costs. Depending on the security features that are faked or otherwise circumvented, materials (e.g., microlens arrays for tilted images, UV- or IR-Ink) or machines (e.g., laser for optical personalisation, printing machines) are required that typically are to be categorised as “bespoke” or “multiple bespoke”.

4.2.4 Security features are known and effectively verifiable (A.4)

Knowledge about the existing security features of an ID document, together with knowledge and means to verify them is the necessary complement to their existence. For a specific ID check, the attack potential discussed in Section 4.2.3 is relevant insofar, as the ID check does actually verify the specific features. That is to say, for a specific ID check, the necessary attack potential for a successful manipulation or forgery of an ID document is to be determined based on the actual checking of the ID document (w.r.t. the scope and depth of the document checks), not based on the entirety of the existing (security) features of the ID document.

Possibly, an attacker is facing the hurdle that it is not publicly known, which security features are actually checked (and by which means) in a specific ID check. The set of security features could be randomly chosen for each verification procedure or the set of checked security features could be kept secret, or both. Similar to security evaluations of cryptographic protocols, the worst case should be considered in an evaluation, i.e., that an opaque selection of checked features generally does not increase the attack potential required for a successful attack.

Irrespective of the question whether it is publicly known, the selection of the security features to be checked and the criteria for judging the authenticity need to be clearly defined. Ideally, those criteria are defined by or together with the issuing or producing parties. Specimen ID documents may be helpful as reference and for testing and training. Besides, databases with information about the verifiable security features of the ID documents and their verification methods may provide helpful information.

4.2.5 Allows a reliable matching against its legitimate owner (A.5)

This requirement refers to the kind and quality (like used sampling method or a minimum resolution) of data that is available on an ID document. Possible manipulation or forgery of these personalised data is not further considered in this Section (see Section 4.2.3 in conjunction with 4.2.4 instead). To allow a reliable check of the legitimacy of ownership, ID document typically contain knowledge-based and / or biometric data.

- **Knowledge based data**: Typically the security of PIN/PUK based verifications is to be assessed. [RAND] can be used for security assessments related to statistical aspects.

- **Biometric data**: Typically, the quality (possibly including up-to-dateness) from the capture of biometric characteristics during enrolment is decisive, including any subsequent processing or compression. Based on an issued ID document and the corresponding enrolment, only a best case assessment can be done. That is, the attack potential required to surpass the maximum FMR that is permitted for a relevant application can only be assessed based on the assumption that all biometric data available for a comparison with the person to be identified is based on genuine biometric characteristics of the person to be identified. Therefore, spoofing (e.g., presentation attacks) need to be assessed separately. This can only be done in combination with the procedures that are used for capturing and verification of biometric characteristics and data. That aspect is discussed in Section 7.

Fluctuating quality in the capturing of biometric characteristics from different persons during the enrolment process may result in a fluctuating quality of the biometric data recorded in the ID documents. This is not necessarily a weakness of the ID documents or the data capturing processes during enrolment, but needs to be taken into account for the assessment of a possibly increased FMR that may result from a specific attack.

4.2.6 ID attributes are up to date (A.6)

By itself, an ID document can provide only very limited assurance that all ID attributes are still up to date. This is usually also reflected in a limited validity period. Besides, ID attributes (in particular biometric data) may be tagged with metadata that describes the date of data capturing including the date of possible updates.

Very important for ensuring the up-to-dateness of ID attributes (e.g. in case of a change of name or address) are the administrative processes and regulations that are linked to the issuance, update, and revocation of ID documents. Based thereupon, it can be assessed to what extend an up-to-dateness of the ID attributes can be assumed.[14]

4.2.7 Available lost or stolen reports are checked (A.7)

In case a maximum validity period is defined for an ID document, it can be usually checked directly and needs to be verified at all levels of assurance.

To enable a reliable checking for lost or stolen documents, a corresponding system for the systematic recording and tracking of such reports needs to be maintained. If such a system is available, it should also be recorded if a document becomes invalid for any other reason (e.g., due to revocation of the document). Provided such a system is effectively in place, it may depend on the specific ID verification procedure whether lost or stolen reports can be checked. Also for the assurance levels *substantial* and *high*, this Technical Guideline stipulates a checking for lost or stolen reports only if such queries can be legally and technically implemented.

4.2.8 Further requirements

The definition of the set of permissible ID documents needs to be reviewed and possibly updated on a regular basis within appropriate intervals (A.8). This is implicitly also stipulated by A.1 and A.3. For assurance level *normal*, longer time intervals may be defined that for assurance level *substantial* or *high*. When reviewing and updating the set of permissible ID documents, in particular any new information about forgeries and manipulations need to be considered.

14 For example, for a driving licence issued in Germany it can not be assumed that the ID attributes like place of residence are up-to-date. As a driving licence is by law not considered as a document for ID proofing, there is no legal obligation to update such ID attributes in case of a change. Nevertheless, for applications that do not require the current name and address ID attributes, a driving licence can possibly used for assurance level *normal* according to this Technical Guideline. For officially recognised ID documents like the German national ID card, the up-to-dateness can be of the ID attributes can be usually assumed.

4.3 Coverage of the security objectives and threats

For the prevention and detection of the threats from Section 4.1 by the requirements from Section 4.2 the relationships from Table 5 hold.

Threat	Covered by requirements no.	Rationale
B.1	A.1, A.8	A.1 ensures that ID documents are only accepted if they are classified as trustworthy and no indication for any compromise exists. A.8 ensures that the information on the trustworthiness and integrity of ID documents must be frequently updated.
B.2	A.3, A.4, A.8	A.3 ensures that manipulations or forgeries that are not detected are not to be expected. A.4 ensures that effective methods for detecting manipulations and forgeries are known. A.8 ensures that novel methods for forgeries and attacks are promptly taken into account when the authenticity and integrity of ID documents are assessed.
B.3	A.5, A.8	A.5 ensures that an authoritative comparison between the user and the ID attributes of the ID document is possible. A.8 ensures that new manipulation methods are promptly taken into consideration.
B.4	A.2	A.2 ensures that the set of ID attributes that is required for the use-case is recorded.
B.5	A.6, A.8	A.6 ensures that the relevant ID attributes available from the ID document can be assumed to be up-to-date. A.8 ensures that property A.6 is considered as a criterion in the regular revisions of the set of accepted documents.

Table 5: Coverage of the security objectives and threats for trustworthy ID documents

5 Security of transmission channels

Under certain conditions, some laws and regulations (e.g. [De-Mail-G], [eIDAS], anti money laundering directives) may allow the usage of public transmission channels like the internet. Threats related to the use of (remote) transmission channels have to be evaluated w.r.t. a direct, immediate access of the inspecting instance to the ID document and its user (i.e., the person to be identified).

Threats resulting from physical manipulations are relevant irrespective from the usage of transmission channels. The usage of (remote) transmissions channels, however, frequently results in increased risks due to restrictions in the type of possible inspections or reduced quality of some inspections. Certain threats, like video manipulations or other forms of information technology based manipulations are only relevant if remote transmission channels are used. In case of digital transmission channels, their security has to be ensured at and/or above the transport layer. This requirement applies irrespective of the authoritative sources (e.g. ID document, ID register) that are used within an ID verification procedure. For the security of the transport layer using TLS [TR-03116-4] has to be considered. Also in case a transport layer with an established end-to-end security can be presupposed, threats at the application layer have to be considered additionally (i.e., in addition to the threats of an ID check without remote transmission channels). For dedicated eID systems the application layer can be secured by cryptographic means so that an assurance level equivalent to processes without remote transmission channels may be achieved. For security measures for the transport layer and dedicated eID systems, [TR-03107-1] and [TR-03116-4], respectively, have to be considered. For the eID function of the German national ID card and electronic residence permits, [TR-03127] [TR-03124-1] and [TR-03130] can be considered.

Without usage of a dedicated eID system, the (visual) checking of physical (optical) features over a remote transmission channel results in a loss of information, for instance due to limits in the available resolution, sampling rate, the transmitted light spectrum, insufficient colour calibration, possible defocus or general bandwidth limitations. Furthermore, signal processing on the application layer (e.g., video or audio manipulations) can be used to modify real world data or create completely artificial data. In summary, two additional types of risks of manipulations have to be considered for the application layer of (remote) transmission channels:

1. Reduced quality / reduced resolution due limitations (e.g. bandwidth) of the transmission media and a possibly two-dimensional representation of transmitted images: As a kind of “transversal” risk, this may affect the complete verification procedure. For instance, tactile security features can not be verified if digital video channels are used. Usually, it is also not possible to check infrared or ultraviolet security features. Optical security features in the visible spectrum can be verified with limited quality. Such limitations reduce the possibilities to detect falsified or manipulated proofs of identity. In other words, the attack potential required for the successful counterfeiting of all security features checked during an ID verification is frequently reduced. Similarly, the possibilities to detect manipulations of biometric characteristics (“presentation attacks”) may be reduced.
2. Malicious manipulations of the transmitted (video) signal of an ID document and / or of the person to be identified. Such manipulations may selectively modify real world data or create completely artificial data. This constitutes a separate risk factor that is specific to the usage of (remote) transmission channels.

5.1 Threats

For the security of transmission channels, the following threats have to be taken into account:

B1. The transmitted biometric data (e.g. facial image) of the person to be identified are manipulated by video technology, so that they match with the proof of identity of a different person.

B2. The data transmitted from the ID document is manipulated by video technology with regard to

1. biometric data (e.g., facial image), so that it matches with a with a different (wrong) person
2. optically personalised ID attributes (e.g., name) or validity attributes (e.g., expiration data)

3. security features (e.g., virtual appearance of features like holograms that do not physically exist on the presented ID document).

B3. Transmission quality, interruptions, video-editing or other manipulations prevent or complicate the detection of physical manipulations (for example masks) of biometric characteristics of the person to be identified.

B4. Transmission quality, interruptions, video-editing or other manipulations prevent or complicate the detection of the absence or manipulation of (security) features of the presented ID document.

B5. Previously recorded and possibly outdated records are re-used (replay attack), possibly without the will or knowledge of the person whose identity is to be verified.

5.2 Requirements for assurance level assessment

For the prevention and detection of the threats from Section 5.1, the below discussed requirements for the security of transmission channels have to be taken into account. Those requirements are differentiated according the to the assurance levels. Some requirements are applicable only for assurance level *substantial* or *high*. Other requirements are relevant for all assurance levels, but stipulate an assurance level dependent resistance against potential attacks. In general, when using (remote) transmission channels in an ID proofing and verification procedure, different kinds of possible manipulations need to be taken into account. This is summarized in Table 6.

No.	Requirement	Required for assurance level		
		normal	substantial	high
A.1	Video-/information technology based manipulation of biometric data of the person to be identified is detected	yes; secure against "enhanced-basic" attack potential	yes; secure against "moderate" attack potential	yes; secure against "high" attack potential
A.2	Information technology based manipulation of data transmitted from the ID document is detected			
A.3	Physical manipulation of biometric characteristics of the person to be identified is detected			
A.4	Physical manipulation of the presented ID document is detected			
A.5	Live transmission of all data is ensured. In particular, any (partial) replay of previously recorded data is detected			
A.6	An exchange of the presented ID document or of the person to be identified during the ID verification procedure is detected			
A.7	A simultaneous manipulation of biometric characteristics (or data) of the person to be identified and the presented biometric reference data from the ID document is detected			

Table 6: Requirements on the security of transmission channels differentiated according to the assurance levels

When using an electronic transmission channel that is not sufficiently secured at the application layer, authentication factors that are originally from different categories (e.g. ID document and face) and therefore require in principle different attack vectors for manipulations may be compromised by a single attack (e.g. video manipulation) if they are both reproduced on a digital transmission channel. This needs to be taken into account for determining the required attack potential for a specific attack.

In the following, some basic guidance is provided that needs to be considered for the evaluation when determining the assurance level with respect to the security of transmission channels.

5.2.1 Video-/information technology based manipulation of biometric data of the person to be identified is detected (A.1)

Here the measures and processes for the prevention and detection of video manipulations have to be evaluated. In particular, software manipulations of biometric data (e.g. digital representations of a face of a person to be identified), so that they match (at least more closely) with a different person, need to be detected. Based on the current state-of-the-art technology, the attack potential required to achieve a FAR above the permissible maximum needs to be evaluated. For the evaluation of the required attack potential, the combined effort for the initial preparation and execution of an attack needs to be considered[15].

Specialist expertise: specific knowledge that is required for a certain type of video manipulation needs to be evaluated. Any requirements that do not exceed a standard installation of software components and their common usage through a graphical user interface can be fulfilled by laypersons. The requirement for a special, dedicated training or similar, e.g. for the customization of adaptation of software, should be classified as "proficient". If knowledge of the state-of-the-art in science and technology is required, it should be classified as "expert", and as "multiple expert" in case different and diverse topics are involved at that level.

If a specific **knowledge of the TOE** is relevant and needs to be considered for a certain attack scenario, it has to be assessed according to [CEM], B.4.2.2.

Depending on the details of the assessed video manipulation, a specific **window of opportunity** may be required. For instance, the requirement for the ID document and a previously recorded ("RGB" / "RGB-D") video of the head of an arbitrary person may be assessed as "easy". It can be more difficult if the same document and data is required from a specific person and therefore may be assessed as "moderate" or, depending on the circumstances, even as "difficult".

With respect to **equipment**, in particular the required hard- and software has to be considered. Commercial of the shelf products are to be classified as "standard" equipment. Configurations based on standard products (e.g. arrays of GPUs, integration of different software components) that are tailored for a specific attack scenario may be considered as "specialised" equipment. Hard- or software components that represent the latest state-of-the-art in science and technology and are not directly commercially available may be considered as "bespoke" equipment. Similarly, if bespoke components from different fields (e.g. hardware and software) need to be combined, the equipment is to be rated as "multiple bespoke".

5.2.2 Information technology based manipulation of data transmitted from the ID document is detected (A.2)

This includes video manipulations of optically personalised data as well as manipulations of electronically stored data, e.g., of a facial image stored electronically on the ID document. The methodology for determining the necessary attack potential is basically analogous to those from the previous Section 5.2.1 (A.1). In contrast to (A.1), however, the assessment has to be based on the individual characteristics of each individual ID document that can be used for an ID proofing and verification procedure. The final assessment of the attack potential required to achieve a FAR above the permissible maximum, is to be based on the ID document that requires the lowest attack potential (minimum principle).

5.2.3 Physical manipulation of biometric characteristics of the person to be identified is detected (A.3)

This includes all kind of presentation attacks, where the legitimate owner of a presented ID document is not physically present during an ID proofing and verification procedure. Instead, another person with

15 Presumably, the initial implementation of an attack requires significantly more effort than the marginal costs/efforts required for a (repeated) execution of a single fraudulent identification. A resulting high scalability of a potential attack needs to be considered in a risk analysis for the ID verification procedure.

manipulated biometric characteristics (e.g., using wigs, make up, masks, prosthetics) presents herself. In addition to persons, also objects (e.g., photos, 3-dimensional models) have to be considered.

The circumstances under which a presentation attack has to be considered successful, and therefore the assessment of the required attack potential, depends decisively on how the biometric characteristics of the person to be identified are captured and evaluated.

Specialist expertise: Requirements like a dedicated training (e.g., apprenticeship) for the manipulation of biometric characteristics can be classified as proficient in accordance with [CEM]. Knowledge and skills that represent the best available level of craftsmanship can be classified as “expert”. If such knowledge and skills are required from strictly different fields, the requirements can be classified as “multiple experts”.

If a specific **knowledge of the TOE** is relevant and needs to be considered for a certain attack scenario, it has to be assessed according to [CEM], B.4.2.2.

Depending on the details of the assessed attack scenario, a specific **window of opportunity** may be required. For instance, trial access to the employed methods and techniques for the detection of manipulations may be required for the calibration of an attack. The assessment has to be made in accordance to [CEM], B.4.2.2.

The assessment of necessary **equipment** has to be made in accordance to [CEM], B.4.2.2. Materials (e.g. masks) and equipment (e.g. cameras) that are readily available from specialist trade shops have to be considered as “standard”. Materials or customized products that are not available from commercial suppliers can be classified as “specialised“.

5.2.4 Physical manipulation of the presented ID document is detected (A.4)

The basis for the assessment of the attack potential related to forgery or manipulation of ID documents is described in Section 4.2.3. For the assessment of the attack potential required in the context of a specific ID check, applicable restrictions due to the available inspection possibilities and the actually performed inspections need to be taken into account. If the entity that performs the ID checks has no immediate access to the presented ID document, some types of security features (like ultraviolet or infrared printing, tactile features) can not be not be checked, others (like guilloches) may be more easy to counterfeit successfully due to the limited resolution (spatial resolutions, contrast, colour fidelity) of the transmission channel in comparison to immediate physical inspection. To summarize, the attack potential required for a successful attack has to be assessed according to Section 4.2.3, considering the aforementioned kinds of restrictions which may apply for the ID check.

5.2.5 Live transmission of all data is ensured (A.5)

As a possible attack scenario, the clandestine (partial) re-usage of previously recorded data for subsequent identification procedures needs to be taken into account. Dynamic, randomized verification procedures can help to impede the successful re-usage of such pre-recorded or pre-produced material. Alongside, the utilization of special hard- and software can help to prevent such undetected re-usage of data. For the assessment of the attack potential required for a successful attack, it needs to be evaluated how such data can be pre-produced or pre-computed and possibly used for successful attacks.

Specialist expertise, knowledge of the TOE, window of opportunity and equipment required for such an attack scenario shall be assessed in accordance with [CEM]. In addition, the following criteria shall be considered for the production, composition and undetected usage of pre-produced video data.

Specialist expertise: In analogy to Section 5.2.1.

Knowledge of the TOE: For instance, the (public or restricted) availability of information that is used for the production, composition, or undetected usage of pre-produced video data has to be considered. In addition, information used to circumvent any safeguards for the prevention of feeding in pre-produced data has to be considered.

Window of opportunity: For the preparation of an attack it may be necessary to know the procedure of a (successful) ID check as exactly as possible in advance. For example, it may be possible to obtain records or other information about the procedure (including its potential variations).

Equipment: In analogy to Section 5.2.1.

5.2.6 An exchange of the presented ID document or of the person to be identified during the ID verification procedure is detected (A.6)

In principle, this topic can be considered as a special case of manipulated ID documents or manipulated biometric characteristics, as the integrity of the presented ID document and/or biometric characteristics is manipulated. If the checking entity has immediate access to the ID document during the complete ID proofing and verification procedure, an undetected exchange of the ID document can usually be ruled out. Likewise, in case of immediate visual contact with the person to be identified, an undetected exchange of the persons to be identified can usually also be ruled out.

When audio-visual transmission channels are used, the relevant attack potential can be assessed according to the guidance provided in Section 5.2.5.

5.2.7 A simultaneous manipulation of biometric characteristics (or data) of the person to be identified and the presented biometric reference data from the ID document is detected (A.7)

A.1, A.2, A.3 and A.4 cover already possible manipulations of biometric characteristics or data of the persons to be identified, as well as manipulations of the reference data from ID documents. In addition to that, A.7 considers the possibility that a detection of manipulated characteristics of the person to be identified can not necessarily rely on genuine reference data from the ID document and vice versa.

5.3 Coverage of the security objectives and threats

For the prevention and detection of the threats from Section 5.1 by the requirements from Section 5.2 the relationships from Table 7 hold.

Threat	Covered by requirements no.	Rationale
B.1	A.1, A.6	A.1 ensures that video manipulations of the transmitted biometric characteristics of the person to be identified are detected. In addition to that, A.6 ensures that transmitted biometric characteristics do not originate from more than one person without being detected.
B.2	A.2, A.6	A.2 ensures that video manipulations of the presented ID document are detected. In addition to that, A.6 ensures that transmitted ID attributes do not originate from more than one ID document without being detected.
B.3	A.3	A.3 ensures that physical manipulations of biometric characteristics of the person to be identified are detected, also in case they are recorded and transmitted through (remote) transmission channels.
B.4	A.4	A.4 ensures that physical manipulations of the presented ID document are detected, also in case the relevant information are transmitted through (remote) transmission channels.
B.5	A.5	A.5 ensures that a usage of previously recorded data is detected.

Table 7: Coverage of the security objectives and threats related to the usage of (remote) transmission channels

6 Checking of ID documents

For a specific type of ID document (or proof of identity in general) different checking procedures may be specified. With respect to the assurance level that can be attributed to a certain type of ID check, the minimum principle applies. The lowest assurance level of all authorised combinations of ID proofing and verification procedures determines the resulting assurance level for the ID check.

6.1 Genuine and non-manipulated

When checking the authenticity of an ID document, the assurance level of of this procedure (or the attack potential necessary for a successful manipulation) strongly depends on which security features are checked and how the checking is performed. Amongst others, the tools used for the checking procedures, available expertise and reference data are important factors. It must be taken into account that a document may be imitated "from the scratch", or personalised data (ID attributes) of an originally genuine document may be manipulated. It must also be taken care of that illegally "cloned" documents are detected as counterfeits.

Depending on the type of ID document and the checking procedures, physical security features (e.g., optical, tactile, mechanical features) and/or data stored on a chip with eID functionality (e.g., signed data) may be used for checking ID documents. The overall assurance level results from the maximum assurance level from a physical and an electronical checking. Generally, the checking procedures may be based on a single set of security features, i.e., limited to checking only physical security features or only electronical security features.

6.2 Validity

In addition to ensuring that an ID document is genuine and not manipulated, also its validity needs to be checked. This includes the original validity period as well as any possible extensions. Depending on the available options, it may also include repeated checks for reports of lost, stolen or revoked ID documents.

6.3 Threats

For secure checking of proofs of identities, the following threats have to be taken into account:

B1. An ID document reported as stolen, lost or revoked is used.

B2. An expired ID document is used.

B3. A counterfeited ID document is used.

B4. A document with manipulated ID attributes is used.

6.4 Requirements for assurance level assessment

For the prevention and detection of the threats from Section 6.3, the below discussed requirements for the checking of ID documents have to be taken into account. Those requirements are differentiated according the to the assurance levels. This is summarized in Table 8.

No.	**Requirement**	**Required for assurance level**		
		normal	**substantial**	**high**
A.1	Type of presented ID document can be determined	yes	yes	yes
A.2	ID document is valid	yes; only check of	yes; same as for	yes

No.	Requirement	Required for assurance level normal	substantial	high
		validity date	level *normal*	
A.3	Counterfeited security features are detected	yes; secure against "enhanced-basic" attack potential	yes; secure against "moderate" attack potential	yes; secure against "high" attack potential
A.4	Manipulations of personalised data are detected	yes; secure against "enhanced-basic" attack potential	yes; secure against "moderate" attack potential	yes; secure against "high" attack potential

Table 8: Requirements on checking of proofs of identity differentiated according to the assurance levels

6.4.1 Type of presented ID document can be determined (A.1)

For the security of ID verification procedures, it is mandatory that any proof of identity is only accepted if it is based on a predefined type of ID document. According to that, the exact document type must be determined and verified for each presented ID document. Based on its type, it can be decided whether the presented ID document is in principle qualified for the desired assurance level. In case of passports for instance, the exact document type is defined by the tuple (CountryCode, Document Type, ID-Number, Year of first issuance). Awareness and acceptance of the type of an ID document that is presented implies that sufficient criteria are defined for checking the authenticity of the ID document (cf. Section 4.2.4).

6.4.2 ID document is valid (A.2)

Document validity comprises checks for the document expiration date, formal status of the document w.r.t. the use case of the ID check, any applicable blacklists, including checks for any lost or stolen reports. This part of the ID verification procedure is complementary to the checks of Section 4.2.7. Furthermore, it includes any checks for the validity of the relevant ID attributes (cf. Section 4.2.6). A precondition for checking for lost or stolen reports is the technical and legal availability to access necessary background systems or blacklists.

6.4.3 Counterfeited security features are detected (A.3)

On the basis of known and effectively verifiable security features (cf. Section 4.2.4), binding inspection instructions for each admissible type of ID document (cf. Section 6.4.1) have to be defined. This includes in particular

- clear criteria under which conditions a proof of identity is accepted as authentic and unadulterated
- any additional tools (e.g. UV-, IR lamp, document scanners) to be used, whose availability and operativeness must be ensured
- documented competence of the staff in charge on checking all admitted ID documents, including competence in utilizing all relevant tools
- knowledge and awareness of existing "best practices" to detect counterfeits and manipulations
- sufficient time for each step of the inspection procedure

Based on the security features of an ID document to prevent counterfeit and manipulation (cf. Section 4.2.3), the actually performed checking procedures are the effective benchmark to evaluate the required attack potential. In other words, the actual checking procedures are the ultimate yardstick for the necessary effort for a successful counterfeiting and thus for the necessary attack potential in accordance with Section 4.2.3.

To recognize a proof of identity as falsified, the detection of a single falsified security feature is sufficient. In order to determine the actually necessary attack potential from the perspective of the ID document's security against forgery, the cumulative effort has to be evaluated in order to counterfeit all checked security features in sufficient quality for all applied checking procedures.

6.4.4 Manipulation of personalized data is detected (A.4)

This aspect comprises the detection of manipulations and falsifications of personalized data (i.e. ID attributes) or of illegitimate combinations of different ID documents. Although this can be considered as a special case of Section 6.4.3, for the manipulation of personalized ID attributes, the minimum principle applies: it is necessary that every relevant ID attribute is unaltered. That is, an attack is already successful as soon as any relevant ID attribute has been successfully manipulated.

In addition, the ID attributes should be checked for consistency. For example, the facial image, date of birth and date of issuance must match or the data from a machine readable zone (MRZ) must be consistent and match the other personalized data.

6.5 Coverage of the security objectives and threats

For the prevention and detection of the threats from Section 6.3 by the security requirements specified in Section 6.4 the relationships from Table 9 hold:

Threat	**Covered by requirements no.**	**Rationale**
B.1	A.2	A.2 ensures that ID documents reported as lost/stolen/invalid can no longer be used for a proof of identity.
B.2	A.2	A.2 ensures that expired ID documents can no longer be used for a proof of identity.
B.3	A.1, A.3	A.1 ensures that only whitelisted ID documents with known and verifiable security features are permitted. A.3 ensures that counterfeited ID documents can be detected based on well-defined criteria.
B.4	A.1, A.5	A.1 ensures that only whitelisted ID documents with known and verifiable security features are permitted. A.5 ensures that manipulated ID documents can be detected based on well-defined criteria.

Table 9: Coverage of the security objectives and threats for the checking of ID documents

7 Comparison of persons with ID document data

Frequently, a person provides a proof of identity by presenting her ID document, and the ID verification is done by comparing data from that ID document with biometric characteristics (e.g. facial image) of the person. A possible threat in such situations is the usage of a valid ID document by an illegitimate person (identity theft). To counter such threats it needs to be ensured that only the legitimate owner of an ID document can use it for successful proofs of identity[16]. Multi factor authentication requires that more than a single factor (like ownership of an ID document) needs to be proofed for a successful ID verification procedure.

Following [ISO/IEC 19790], authentication factors can be classified into the following categories:

1. Something you know (e.g., a PIN) – "knowledge"
2. Something you have (here: an ID document) – "possession"
3. Something you are (such as a biometric characteristic, e.g. facial image or fingerprint; behaviour patterns e.g., signature, dynamics of key strokes) – "inherent factors"

The number and type of required authentication factors depends on the specific type of ID verification procedure and the required assurance level.

For the verification of the legitimate ownership of a presented ID document, as many authentication factors as possible should be checked. Furthermore, complementary authentication factors should be checked, i.e. authentication factors from different categories. It can be expected that for a legitimate owner, each checked authentication factor usually results in a positive match. Thus, for a positive overall result of the ID verification procedure, it is required that the result of each verified authentication factor is a positive match.

The guidance given in this section assumes the ID verification is based on a multi-factor authentication. That is, authentication factors from at least two different categories are verified: Basis is the proof of possession of a suitable ID document together with the verification of at least one additional factor from the category "knowledge" and/or "inherent factors".

7.1 Threats

To ensure the secure verification of the legitimate ownership of a presented ID document, the following threats have to be taken into account:

B1. A confidential knowledge factor that must only be known by the legitimate owner of an ID document is compromised.

B2. An ID document (or, more generally, any proof of identity) is used by another person (instead of the legitimate person).

B3. Biometric characteristics (including behavioural patterns) of a different person are imitated (e.g. presentation attacks).

ID verification procedures that do not check knowledge based or inherent factors can ignore the respective threats.

7.2 Requirements for assurance level assessment

A secure verification of the legitimate ownership of a presented ID document requires some kind of interaction with the person to be identified. For the prevention and detection of the threats from Section 7.1,

16 In this section and throughout the document, only proofs of identity that are based on previously issued ID documents are considered.

the below discussed requirements for the checking of ID documents have to be taken into account. Those requirements are differentiated according the to the assurance levels. This is summarized in Table 10.

No.	Requirement	Required for assurance level		
		normal	**substantial**	**high**
A.1	Confidential knowledge based factors are communicated exclusively to the legitimate person	yes	yes; same as for level *normal* plus separate transmission path	yes; same as for level *substantial* plus explicit activation
A.2	Security of the used authentication factors	one factor	two factors, secure against “moderate” attack potential	two factors, secure against “high” attack potential
A.3	The actual power of control of the person to be identified over the ID document is ensured	-	yes	yes
A.4	The comparison of ID attributes is based on data of sufficient quality (e.g. resolution)	yes; appropriate for the max. permitted FMR; secure against targeted attacks with “enhanced-basic” attack potential	yes; appropriate for the max. permitted FMR; secure against targeted attacks with “moderate” attack potential	yes; appropriate for the max. permitted FMR; secure against targeted attacks with “high” attack potential
A.5	Trustworthy comparison of relevant biometric ID attributes (between ID document and from the person to be identified)			

Table 10: Requirements for the comparison of the person to be identified and data from the ID document (proof of identity) for the different assurance levels.

7.2.1 Confidential knowledge based factors are communicated exclusively to the legitimate person (A.1)

When transmitting confidential knowledge based factors that are linked to an ID document, it must be ensured that this information is only disclosed to the legitimate owner. Besides a tamper proof transmission, also a tamper evident transmission may be sufficient in case it is ensured that any illegitimate access to the information is detected and thwarted in due time. The requirements on the issuance of authentication means from [TR-03107-1] apply.

For assurance levels *substantial* and *high*, the delivery of a knowledge based factor must be separated from the delivery of all other authentication factors. For assurance level *high*, an activation of knowledge based factors prior to their first usage is required.

Knowledge based factors must be kept secret throughout their entire lifetime (validity period). Awareness about and acceptance of this requirement needs to be confirmed by the owner of the ID document.

ID verifications can also be done without knowledge based factors, for instance if the security is based on the authentication factors possession and inherent (biometric) factors.

7.2.2 Security of the employed authentication means (A.2)

The requirements from [TR-03107-1] (specifically Section 3.3.1) apply. For a knowledge based factor, this implies in particular that it is exclusively stored on the ID document, can not be read out directly and can be verified only together with the ID document[17]. The only possible exception is the tamper proof or tamper

17 This does not exclude the possibility for the legitimate owner to change a confidential knowledge based factor. The possibility to change a knowledge based factor as well as knowledge of the factor, however, must only be

evident transmission of an (initial) knowledge based factor to the legitimate owner (cf. A.1). Chip cards are frequently used for the confidential storage of a knowledge based factor. In this case or if a similar technology is used, [JILAPS] is normative for determining the required attack potential for a compromise of the hardware.

7.2.3 The actual power of control of the person to be identified over the ID document is ensured (A.3)

This requirement can be met for instance by physically presenting the ID document. In any case the authenticity of the presented ID document must be checked in compliance with the aspired assurance level.

7.2.4 The comparison of ID attributes is based on data of sufficient quality (A.4)

Biometric ID attributes to be compared and matched must be available with a sufficient quality, both from the ID document as well as from the person to be identified. The quality of the data must allow a reliable one-to-one matching of person and ID document.

The quality criteria depend on the specific procedures that are used for the matching process. The matching can be done by personnel or machine. The decisive factor is that the maximum permitted false match rate is not exceeded.

See also Sections 4.2.3, 5.2.4, and 6.4.4 for the minimum quality required to detected forgeries on the ID document (or proof of identity) itself.

See Section 5.2.3 for relevant factors to detect presentation attacks. Checks on known cheating attempts need to be implemented, in particular, state-of-the-art liveness detection needs to be applied on presented biometric characteristics.

7.2.5 Trustworthy comparison of relevant biometric ID attributes (A.5)

The FMR is the relevant benchmark for the reliability of a comparison (matching). For the determination of the FMR, targeted manipulation attempts must be taken into consideration. Manipulation attempts are only to be considered if their required attack potential is within the relevant limit for the targeted assurance level. The analysis of the FMR should be corroborated by sound statistical data. As a minimum requirement, the FMR to be expected must be quantified and made plausible.

Ideally, several different biometric ID attributes should be compared and matched for a trustworthy comparison. For example, fingerprints together with the facial image. Particularly in the case of personnel comparisons, sufficient time is required for the comparison, in addition to the trustworthiness and expertise of the staff.

ID verifications can also be done without biometric (inherent) factors, for instance if the security is based on the authentication factors “possession” and “knowledge”.

7.3 Coverage of the security objectives and threats

For the prevention and detection of the threats from Section 7.1 by the security requirements specified in Section 7.2 the relationships from from Table 11 hold.

possible for the legitimate owner of the associated ID document.

Threat	Covered by requirements no.	Rationale
B.1	A.1, A.2	A.1 enforces measures to minimize the risk of a compromise of knowledge based factors. A.2 enforces additionally, that a (potentially compromised) knowledge based factor can be used only together with the ID document. Unlike knowledge based factors, a compromised (e.g., lost or stolen) possession based factor can be recognised in a timely manner to take appropriate actions.
B.2	A.3	A.3 ensures that the illegitimate usage of an ID document (proof of identity) is detected.
B.3	A.4, A.5	A.4 ensures that ID attribute data from the ID document and the person to be identified are captured in sufficient quality (for the purpose of a reliable comparison). A.5 ensures that ID attributes that had been captured are matched with a dependable method.

Table 11: Coverage of the security objectives and threats for the comparison of persons with ID document data

8 Correct registration of the required ID attributes

The focus of this section is on the quality management of the data capture processes to prevent accidental errors, that is errors that are not caused by malicious manipulations by internal or external attackers. That is, the focus is on (internal) quality aspects instead of security measures for the detection and prevention of targeted attacks.

Note: this section is mainly related to [eIDAS LoA] Section 2.1.1 “Application and Registration” instead of 2.1.2 “Identity proofing and verification”.

Within the context of specific applications, additional ID attributes may be defined and registered (e.g. e-mail address, phone number, IBAN, ...) which have not been recorded as part of the ID verification procedure. Unlike (externally) verified ID attributes, those ID attributes generated or registered later can be reliably used only within the application context for a unique identification.

8.1 Threats

For the correct registration of – possibly unique – ID attributes, the following threats have to be taken into account:

B1. The set of ID attributes does not ensure uniqueness (if needed).

B2. The set of ID attributes does not allow a legally required identification (e.g. due to anti money laundering regulations), in particular if pseudonyms are used (if needed).

B3. Transcription- and transmission errors during registration of the ID attributes, in particular

1. Typos / spelling mistakes;

2. Transcription errors or ambiguities, for instance if some characters are not natively supported in the registration system due to limited functionality; truncation errors if the complete length of a string can not be registered for some ID attributes;
3. Incorrect assignment of ID attributes (e.g. mix-up of first- and surname).

B4. Registration of incomplete or outdated ID attributes.

The relevance of these threats is strongly application dependent. For instance, in case of a sole age verification, neither an explicit nor a unique identification is relevant.

8.2 Requirements for assurance level assessment

Depending on the aspired assurance level, different requirements for capturing the (if needed unique) ID attributes have to be taken into account. This is summarized in Table 12.

No.	Requirement	Required for assurance level		
		normal	**substantial**	**high**
A.1	ID attributes to be registered allow a unique identification	yes, if application requires a unique identification	yes, if application requires a unique identification	yes, if application requires a unique identification
A.2	Specific expertise of the inspectors and relevant tools are available	--	yes	yes
A.3	ID attributes are registered completely and error free	yes	yes	yes
A.4	Registered data is checked for consistency and plausibility	--	yes	yes

Table 12: Requirements for the registration of unique ID attributes for the different assurance levels.

8.2.1 ID attributes to be registered allow a unique identification (A.1)

Depending on the application context, a unique representation of each registered person may be needed. This may be a strict requirement (i.e. for each each entity, defined by the tuple of all registered ID attributes, the uniqueness must be guaranteed) or, in a weaker form, the tuple of ID attributes must most likely ensure uniqueness but not necessarily provide an absolute guarantee.

Depending on the overall context, it may be necessary that a registered person can be uniquely identified by her real name and official ID attributes (e.g. due to legal requirements like anti money laundering regulations).

Biometric characteristics that are usually invariable over time or change only slowly (like finger prints, vein patterns, iris patterns, facial images) qualify in principle to distinguish between different persons as well as for the comparison of persons with ID document data. They are, however, rarely suitable as easily “human readable” ID attributes. In “Commission Implementing Regulation (EU) 2015/1501, Annex 'Requirements concerning the minimum set of person identification data uniquely representing a natural or legal person'”, a possible set of ID attributes for a global, unique identification is proposed.

If unique identities are required, the registration system shall prevent that a new entity can be registered if an entry with identical ID attributes does already exist.

8.2.2 Specific expertise of the inspectors and relevant tools are available (A.2)

The staff in charge with ID verification or interpretation and registration of the ID attributes must have demonstrated expertise for all types of admissible ID documents, if the targeted assurance level is *substantial* or *high*. For assurance level *substantial* or *high* it is also required that all tools that are possibly relevant for the ID proofing and verification procedure are available and fully functional.

8.2.3 ID attributes are registered completely and error free (A.3)

Exemplary measures to prevent accidental errors like typos in the registration of ID attributes could be the multiple entry (cross check) of data, possibly by different persons or different mechanisms. The system for the registration of ID attributes needs to be technically suitable to record all relevant data completely and without any ambiguities.

8.2.4 Registered data is checked for consistency and plausibility (A.4)

Checks for consistency and plausibility can include, for example, the verification of the address or consistency checks of the date of birth and available biometric data. The ID verification procedure shall be aborted if not all mandatory ID attributes can be recorded. Wherever possible, ID attributes shall be checked for being up-to-date (cf. also Section 4.2.6).

8.3 Coverage of the security objectives and threats

For the prevention and detection of the threats from Section 8.1 by the security requirements specified in Section 8.2 the relationships from Table 13 hold.

Threat	**Covered by requirements no.**	**Rationale**
B.1	A.1	A.1 ensures that the ID attributes to be registered allow a unique identification.
B.2	A.1	A.1 ensures that the true identity (in contrast to a unique pseudonym) of the person to be identified can be established.
B.3	A.2, A.3, A.4	A.2 ensures that the staff has the required expertise and the availability of relevant tools. A.3 and A.4 ensure that all steps are executed with the necessary diligence.
B.4	A.4	A.4 ensures that all required ID attributes are recorded based on the latest available data.

Table 13: Coverage of the security objectives and threats for the correct registration of ID attributes

9 Safeguarding process integrity

The requirements defined in Sections 4 to 7 are the basis for secure ID proofing and verification procedures. On top of that, compliance to all defined requirements must be ensured as a cross sectional task. This section specifies requirements for the protection from malicious manipulations by internal or external attackers that are not based on manipulated proofs of identity. Those organisational safeguards must be adequate to the (highest) assurance level for which ID checks are executed.

Aspects related to service availability or required data protection measures are out of scope of this Technical Guideline.

9.1 Threats

B1. Checks required for the ID proofing and verification procedure are not properly executed.

B2. Unauthorized / illegitimate creation of datasets related to ID verification procedures by internal or external attackers.

B3. Unauthorized / illegitimate manipulation (or deletion) or stored ID attributes or related data by internal or external attackers.

Besides these immediate threats to the security and integrity of the processes, also indirect risks like manipulated tools or corrupt staff must be taken into account.

9.2 Requirements for assurance level assessment

9.2.1 Compliance to the defined checking procedures is ensured (A.1)

Compliance to the ID checking procedures can be ensured through technical measures, organisational measures or combinations of both. The measures may include the requirement for traceable documentation of all checks that have been performed.

The basis of this requirement is the set of checks that have to be done for each ID document, according to the requirements from Section 4. This includes the requirement for updates of the set of checks that have to be done.

For manually executed checks, the expertise and the trustworthiness of the staff needs to be ensured.

9.2.2 ISMS (A.2)

As a general safeguard for the integrity of all IT based process, an ISMS according to ISO/IEC 27001:2013 and ISO/IEC 27002:2013 or equivalent must be implemented. The ISMS must cover all IT components and processes that are directly or indirectly used for the ID verification, storage or transmission of captured ID attributes and related data.

9.3 Coverage of the security objectives and threats

For the prevention and detection of the threats from Section 9.1 by the security requirements specified in Section 9.2 the relationships from Table 14 hold.

Threat	Covered by requirements no.	Rationale
B.1	A.1	A.1 ensures the compliance to all stipulated checking criteria.

Threat	Covered by requirements no.	Rationale
B.2	A.2	A.2 provides safeguards against unauthorized/illegitimate creation of data sets by internal or external attackers.
B.3	A.2	A.2 provides safeguards against unauthorized/illegitimate deletion or manipulation of records by internal or external attackers.

Table 14: Coverage of the security objectives and threats for safeguarding process integrity

Bibliography

TR-03107-1	BSI: Technische Richtlinie TR-03107 Elektronische Identitäten und Vertrauensdienste im E-Government; Teil 1: Vertrauensdienste und Mechanismen
eIDAS LoA	: COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) 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
CC1	: Common Criteria for Information Technology Security Evaluation
CEM	: Common Methodology for Information Technology Security Evaluation
TR-03121-3	BSI: Technische Richtlinie TR-03121 Technical Guideline Biometrics for Public Sector Applications
eIDAS	: 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
JILSS	: Joint Interpretation Library Minimum Site Security Requirements
RAND	Wolfgang Killmann, Werner Schindler: A proposal for: Functionality classes for random number generators
De-Mail-G	: De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), das durch Artikel 2 Absatz 3 des Gesetzes vom 22.Dezember 2011 (BGBl. I S. 3044) geändert worden ist
TR-03116-4	BSI: Technische Richtlinie TR-03116, Kryptographische Vorgaben für Projekte derBundesregierung
TR-03127	BSI: Technische Richtlinie TR-03127 eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control
TR-03124-1	BSI: Technische Richtlinie TR-03124 eID-Client
TR-03130	BSI: Technische Richtlinie TR-03130 eID-Server
ISO/IEC 19790	: Information technology -- Security techniques -- Security requirements for cryptographic modules
JILAPS	: Joint Interpretation Library Application of Attack Potential to Smartcards