Federal Office
for Information Security

Catalogue of requirements for checking identification procedures in accordance with TR-03147 version 1.06

Version 1.0.1
December 01, 2022

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

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

Tables

1 Introduction

1.1 Structure of the checking criteria

The checking criteria in [PBV] are structured according to a fixed scheme. This includes the following points in particular:

Checking criterion ID: This involves the identification of the checking criterion by means of an ID in the form Ax.y-z with x, y and z numbered consecutively, each starting with 1, which is used both in the [PBV] and in this catalogue of requirements. Additionally, generally valid requirements in a section of this TR are marked with the letter "G", e.g. A1.G-1 as checking criterion ID for the first general checking criterion for the requirement "Trustworthy ID documents ". The form of the ID is based on the designation of the requirements in [TR-03147].

Checking criterion description: This is the description of the checking criterion, which will also be referred to again in the present catalogue of requirements. If necessary, the individual requirements specified in [TR-03147] are divided into several atomic checking criteria. The description gives an overview of the checking criterion. Additional details or explanations can be found in the respective sections of this document.

Reference: Indication of a reference to [TR-03147] that the checking criterion refers to.

Documentation: Within the scope of the checking task, the inspector shall also take into account any documentation relevant to the checking criterion. In particular, this includes manufacturer documentation (e.g. description of the process, instructions for use, interface specifications, etc.). The documents taken into account are to be indicated under this item with a reference to the relevant text passages.

Interview partner: Within the scope of checking tasks, the inspector is to have facts explained to them or shown to them. The respective interview parties are to be listed under this item.

Checking task: This is where the inspector describes the procedure for checking the respective checking criterion. The description should be comprehensive enough to allow a person not involved in the check to independently understand the procedure.

Analysis: Under this item, a justification for the chosen approach to the check as well as the assessment on the checking criterion is to be given. This is based primarily on the findings and results of the checking tasks carried out. The description of the procedure as well as the findings and results is especially intended to make the assessment reached comprehensible.

Assessment: At the end, the inspector gives an assessment of the checking criterion. The assessment follows as a direct result of the completed analysis. The assessment alternatives available for selection are, depending on the checking criterion, a combination of:

- Normal, substantial, high: Classification according to assurance levels as per [TR-03147].
- N/A (not applicable): In this case, the inspector has to give reasons for their assessment.
- Not fulfilled: The procedure does not meet the minimum requirements for the assurance level normal.

1.2 Assurance level and checking depth

In [TR-03147] the three assurance levels *normal*, *substantial* and *high* are used. The required checking tasks are derived from the respective checking criteria as well as the checking depth. For the requirements from [TR-03147] the checking criteria are described in section 3. The associated checking depth is largely determined by the highest assurance level for which compliance/achievement is checked for a procedure and affects the achievable assurance level according to Table 1:

Assurance level	Checking depth
Normal	**Document check** – All requirements are checked on the basis of the available documentation. References to the inspected document bodies are to be listed in the checking report. Examples of documentation to be checked are security concept, system description, interface definition, manuals or also work instructions. If necessary, the checking depth is to be expanded selectively (i.e. for individual requirements) to include an implementation check. This is the case in particular if, after the document check, there is a concrete suspicion that the procedure can already be compromised with an "*enhanced basic*" attack potential.
Substantial	**Implementation check** – In addition to document check, each requirement must also be checked in terms of implementation in practice. Particular attention must be paid to the correspondence between documented information and concrete implementation. Implementation check should take place in "live practice" (e.g. in the productive environment). The inspector should ask for a description of the aspects relevant to a requirement and must inspect each implementation themselves. The checking report is to list both parties to the interview as well as aspects of the procedure inspected and to describe the observations made during the checking task. If necessary, the checking depth is to be expanded selectively (i.e. for individual requirements) to include independent tests. This is the case in particular if, after the implementation check, there is a concrete suspicion that the procedure can already be compromised with an "*moderate*" attack potential.
High	**Independent tests** – In addition to document and implementation check, independent tests (including, in particular, known or developed attack scenarios) shall be conducted for the procedure. For this, the inspector is to be provided with an appropriate testing option. The checking tasks carried out are to be documented in the checking report. The method of the independent tests should be based, for example, on the Common Criteria [CC] and in particular the Evaluation Methodology [CEM].

Table 1: Checking depth of the assurance level

These classifications into a checked assurance level, which are made depending on the checking depth, are applied in principle to all checking criteria. However, there are checking criteria for which a stringent application of these classifications does not make sense in principle. Specific deviations from this general rule are defined for each of these checking criteria. For example, the decision as to whether or not an ID document fulfils the domestic ID requirement (see checking criterion A1.1-9), can be made independently of an **implementation check** and **independent tests**.

2 General terms and definitions

2.1 Definitions of terms

The following terms are defined for this catalogue of requirements and the associated checking report template [PBV]. The definitions based on [ISO-HBV] and their translations in the German version of [CB-STD]. It should be noted that other, different definitions do exist.

- **Biometric characteristic** is a biological or behavioural characteristic of an individual that is used to collect biometric data, e.g. facial topography or papillary ridge structure ("fingerprint").
- **Biometric sample** is an analogue or digital representation of a biometric characteristic, e.g. the data set of an image of a face.
- **Biometric features** consist of numbers or identifiers extracted from a biometric sample and used for comparison.
- **Biometric data** is a biometric sample or collection of biometric samples at any stage of processing (e.g. biometric features).
- **Biometric false match rate** is the probability that a biometric match is successful even though an unregistered biometric characteristic was used. An example would be a false positive event during a fingerprint check, i.e. successfully checking a fingerprint with a fingerprint sensor using a finger other than the registered finger.
- **Biometric false acceptance rate** is the probability that a biometric claim is falsely accepted by the overall checking system. It is calculated by multiplying the FMR by the number of failed attempts allowed by the overall system.

The following definition is based on Technical Guideline [TR-03107-1].

- **Authentication means** are technical means which enable the holder to authenticate an identity (i.e. a set of ID attributes) or other transmitted data. Examples of authentication means are passwords, identity cards or signature cards. If several technical means are necessary (such as chip card and PIN), then the complete authentication means is made up of several authentication factors.

Other definitions.

- **User** uses an ID document to identify themselves.

2.2 Categories of ID procedures

This document defines guidelines for assessing the assurance level achieved for the widest possible range of different ID procedures. In order to formulate the checking criteria nevertheless as clearly and specifically as possible, all ID procedures are divided into the following three categories:

a) **Direct**: ID procedures in which the user is personally present and the inspector can directly inspect the ID document used as well as the person to be checked and, if necessary, carry out further checks (e.g. read out the ID document on site such as with an "on-site read-out" of their identity card or electronic residence permit).

b) **Indirect**: ID procedures where the user is not present in person but the inspector can inspect the ID document and the person being inspected via a remote, usually audio-visual, channel.

c) **Electronically**: ID procedures based on cryptographically secured electronic authentication or other automated, non-personal checks.

These categories are referred to in some checking criteria and further explanations. Assurance levels of ID documents for different categories of ID procedures are not directly comparable. For example, it is often easier to create a counterfeit of a given visual security feature that can pass inspection via a remote visual channel than one that is directly viewed by the person inspecting it. In general, counterfeits that can pass an inspection using a method in the "indirect" category require a lower potential for attack (e.g. lower level of insider knowledge) for their creation than those that can pass inspections using a method in the "direct" category. The attack scenarios for forging electronic authentication features, in turn, differ greatly from those for forging visual or haptic features.

2.3 Assessment of attack potential

The potential of an attacker using the checked ID procedure is of repeated concern in this document. The attack potential is evaluated according to the procedure defined in Appendix B.4 of the [CEM] using the following criteria:

- The elapsed **time** necessary for the identification, preparation and execution of an attack.
- The necessary specialist **expertise** of the attacker
- The necessary **insider knowledge** (knowledge of the target of evaluation) of the attacker
- The necessary **window of opportunity** for an attack
- The necessary **equipment** for an attack

For the assessment of the work involved, the implementation of the attack must be considered first and foremost. The work involved in preparation is only taken into account in exceptional cases, when the effort required for this is extremely high compared to the implementation. This takes into account the fact that, for example, a single attack can be successfully carried out several times in a short period of time, but its preparation takes a longer period of time. Particularly in such cases, the assessed attack potential should be based on the execution and not on the preparation of the attack.

Furthermore, with regard to the **window of opportunity** criterion, [CEM] considers the window of opportunity for accessing the product under review. When checking ID procedures as opposed to products, the possibility of separating the object to be checked from its environment is not given in the same way as is usual when checking products. This means that it is not always possible to establish a "clear boundary" between the "**windows of opportunity**" criteria and the "**equipment**" criteria. For example, limited access to practical video- or branch-based procedures may be compensated for by replicating all or part of a practical procedure through the procurement of appropriate equipment. This "simulation environment" could then be used to develop and test attacks instead of the actual procedure.

The assurance level of an ID procedure results as follows from its resistance to an attack with a corresponding attack potential:

ID procedure with assurance level	Resistant Attack with	**Attack potential**
Not fulfilled		If applicable, low (basic)
Normal		Normal (enhanced basic)
Substantial		Substantial (moderate)
High		High

3 Checking instructions

3.1 Trustworthy documents

3.1.1 Multiple approved ID documents

A1.G-1

Checking criterion description: What is the assurance level of the ID document that has been approved for the ID procedure and has the lowest assurance level?

Explanation / note:

The basis for a regular ID check is the availability of at least one trustworthy ID document (as a reliable source according to the eIDAS Implementing Regulation 2015/1502 [eIDAS 2015/1502]). Insofar as the use of several ID documents is permitted in an ID procedure, the ID document permitted for an ID check with the lowest assurance level determines the overall maximum achievable assurance level for the ID procedure according to the minimum principle.

The checking criteria for the "Trustworthy ID Documents" requirement are to be applied to all ID documents approved for the ID procedure by the inspector and the overall result of the requirement is to be determined according to the minimum principle mentioned above.

For checking an ID document, the checking criterion A1.G-2 and all checking criteria with a checking criterion ID in the form A1.y-z with $1 \leq y \leq 8$ and z numbered consecutively, starting with 1, are to be applied.

3.1.2 Valid ID document

A1.G-2

Checking criterion description: When using the ID procedure, does the ID document used get checked if it is valid at the time of checking?

Explanation / note:

A valid ID document, i.e. specifically one that has not expired, is required. The minimum assurance level of "normal" can only be achieved if the ID procedure checks whether the ID document is valid at the time of the check. The ID procedure must check if the "Valid until" date has passed and, if present, if the date of issue is in the past. If necessary, equivalent checking steps are to be carried out. For example, for an expiry date, it must be checked if it has passed or been reached. In principle, ID documents without a validity period can also be used. With these, however, the assurance levels "substantial" or "high" are not achievable.

The following procedure-specific aspects are to be considered in the check (see also category of ID procedures according to explanation / note to A1.3-1):

- VideoIdent, PhotoIdent: The attributes for validity must be uniquely identifiable and readable. The person checking the ID document must have the necessary expertise (e.g. through training) to perform the check of the ID document attributes using the ID procedure. If necessary, the ID procedure can also be used for technical support, e.g. in the form of instructions.
- ID procedure with direct presence: Like VideoIdent (see above). In addition, the inspector should also carry out a haptic check of the ID document, for example.

- ID procedure with online identification function of the German ID card, eID Card for citizens of the EU and the EEA, or electronic residence permit: It must be ensured that the ID procedure can securely read out and check the attributes for validity.

The assessment of the assurance level is to be carried out as follows:

- Not fulfilled: When using the ID procedure, the ID document used is not checked to see if it is valid at the time of the check.
- Normal: When using the ID procedure, the ID document used is checked to see if it is valid at the time of the check. The check was carried out with the checking depth **document check**.
- Substantial: When using the ID procedure, the ID document used is checked to see if it is valid at the time of the check and has a validity period. The check was carried out with the checking depth **implementation check**.
- High: When using the ID procedure, the ID document used is checked to see if it is valid at the time of the check and has a validity period. The check was carried out with the checking depth **independent tests**.

3.1.3 Authoritative source

A1.1-1

Checking criterion description: Are the authorities responsible for issuing the respective ID document known?

Explanation / note: Examples of bodies responsible for issuing the respective ID document are:

- The body responsible is a government agency (e.g. for issuing an identity card or passport).
- The ID document is application-related and is issued within a legal context (e.g. for the issuance of a driving licence or public health-insurance card)
- The body responsible is a (private sector) organisation (e.g. for issuing an employee ID card).
- The body responsible is a (registered) association or a comparable organisation (e.g. for issuing a membership card).

The reputation of a body is to be verified by the inspector using the appropriate methods. This can vary from the assumption that the issuing body is sufficiently known (e.g. in the case of identity cards or passports) to a search on the internet (e.g. organisations for licensing or training for professional licences) to verify the knowledge of the responsible body. It is also possible to assume sufficient awareness for those bodies that issue application-related ID documents on a statutory basis (e.g. driving licence, health-insurance card, health professional card). In case of any doubts, the reputation should be checked by additional measures (e.g. the job is listed in a government agency's list). The reputation of private sector organisations can be checked, for example, by using the commercial register.

The assessment of the assurance level is to be carried out as follows:

- Not fulfilled: The bodies responsible for issuing the respective ID document are not known.
- Normal: The bodies responsible for issuing the respective ID document are known. The check was carried out with the checking depth **document check**.
- Substantial: The bodies responsible for issuing the respective ID document are known. The check was carried out with the checking depth **implementation check**.
- High: The bodies responsible for issuing the respective ID document are known. The check was carried out with the checking depth **independent tests.**

A1.1-2

Checking criterion description: Is publicly available information on compromises of the responsible bodies (e.g. media reports on compromises of such bodies) collected?

Explanation / note: For sovereignly issued documents that fulfil the domestic identification requirement, it can be conclusively presumed that the bodies responsible for issuing them have not been compromised.

The assessment of the assurance level is to be carried out as follows:

- Not fulfilled: Publicly available information on compromises of the responsible bodies is not collected.
- Normal: Publicly available information on compromises of the responsible bodies is collected. The check was carried out with the checking depth **document check**.
- Substantial/high: Publicly available information on compromises of the responsible bodies is collected. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth").

A1.1-3

Checking criterion description: Is collected information on compromises of the responsible bodies (e.g. media reports on compromises of such bodies) taken into account in a timely manner?

Explanation / note: See A1.1-2. Such information can be taken into account in a timely manner by modifying the ID procedure itself (e.g. by no longer allowing affected ID documents) or by a checking step in the ID procedure evaluating this additional information.

The following procedure-specific aspects are to be considered in the check:

- VideoIdent, PhotoIdent, ID procedure with direct presence (e.g. checked in a branch office): It must be ensured that the person checking the ID document has the information about compromises (or their consequences) and takes them into account correctly.
- ID procedure with online identification function, e.g. of the German ID card, eID Card for citizens of the EU and the EEA, or electronic residence permit: It must be ensured that the information on compromises (or their consequences) is taken into account in the (possibly automated) execution of the ID procedure.

The assessment of the assurance level is to be carried out as follows:

- Not fulfilled: Available information on compromises of responsible bodies is not taken into account in a timely manner.
- Normal: Available information on compromises of responsible bodies is taken into account in a timely manner. The check was carried out with the checking depth **document check**.
- Substantial/high: Available information on compromises of responsible bodies is taken into account in a timely manner. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth").

A1.1-4

Checking criterion description: Is up-to-date information on manipulations and counterfeits of ID documents collected?

Explanation / note: The assessment of the assurance level is to be carried out as follows:

- Not fulfilled: Up-to-date information on manipulations and counterfeits of ID documents is not collected.
- Normal: Up-to-date information on manipulations and counterfeits of ID documents is collected. The check was carried out with the checking depth **document check**.
- Substantial/high: Up-to-date information on manipulations and counterfeits of ID documents is collected. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

A1.1-5

Checking criterion description: Is the information collected on counterfeits and manipulation of ID documents taken into account in a timely manner?

Explanation / note: Such information can be taken into account in a timely manner by modifying the ID procedure itself (e.g. by no longer allowing affected ID documents) or by a checking step in the ID procedure considering this additional information.

A process-specific distinction is to be made as in checking criterion A1.1-3.

The assessment of the assurance level is to be carried out as follows:

- Not fulfilled: Up-to-date information on manipulations and counterfeits of ID documents is not taken into account in a timely manner.
- Normal: Up-to-date information on manipulations and counterfeits of ID documents is taken into account in a timely manner. The check was carried out with the checking depth **document check**.
- Substantial/high: Up-to-date information on manipulations and counterfeits of ID documents is taken into account in a timely manner. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

A1.1-6

Checking criterion description: Does the process of producing and issuing the ID document used sufficiently check the eligibility and identity of an applicant?

Explanation / note: The assessment of the assurance level is to be carried out as follows:

- Not fulfilled: The process of producing and issuing the ID document used does not sufficiently check the eligibility and identity of an applicant.
- Normal: The process of producing and issuing the ID document used does sufficiently check the eligibility and identity of an applicant. The check was carried out with the checking depth **document check**. Document check can be skipped if the ID document is generally recognised as trustworthy, e.g. the identity card (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).
- Substantial: The process of producing and issuing the ID document used does sufficiently check the eligibility and identity of an applicant. The check was carried out with the checking depth **implementation check**. Implementation check can be skipped if the ID document is generally recognised as trustworthy, e.g. the German identity card (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).
- High: The process of producing and issuing the ID document used does sufficiently check the eligibility and identity of an applicant. The check was carried out with the checking depth **independent tests**. Carrying out independent tests can be skipped if the ID document is generally recognised as trustworthy,

e.g. the German identity card (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth").

A1.1-7

Checking criterion description: Does the ID procedure check whether the ID document used belongs to an explicitly limited set of authorised ID documents?

Explanation / note: For example, if a specific ID procedure requires an official photo ID from a specific state list as permissible ID document, it is necessary to check during the ID procedure if the ID document used is included in such a allowlist.

A distinction is to be made in terms of procedure as follows:

- VideoIdent, PhotoIdent, ID procedure with direct presence (e.g. PostIdent): It must be ensured that the person checking the ID document is informed about the permitted set of ID documents and applies this information correctly.
- Electronic procedures such as procedures with the online identification function of the German ID card, eID Card for citizens of the EU and the EEA, or electronic residence permit: Due to the mutual authentication with the establishment of a secure channel between the identity card and the reading agency on the basis of the existing security mechanisms (e.g. terminal authentication) and the key management used for this purpose, it can be reasonably assumed that only the online identification function of the German ID card, eID Card for citizens of the EU and the EEA, or electronic residence permit products are supported by this ID procedure. Similar considerations should be made for electronic procedures based on other ID documents.

The assessment of the assurance level is to be carried out as follows:

- Not fulfilled: No explicitly limited set of authorised ID documents is specified for the ID procedure, or the ID procedure does not check whether the ID document used belongs to an explicitly limited set of authorised ID documents.
- Normal: The ID procedure checks whether the ID document used belongs to an explicitly limited set of authorised ID documents. The check was carried out with the checking depth **document check**.
- Substantial/high: The ID procedure checks whether the ID document used belongs to an explicitly limited set of authorised ID documents. Carrying out an implementation check can be skipped (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth").

A1.1-8

Checking criterion description: Is the ID document an explicit ID document?

Explanation / note: An ID document is an explicit ID document if it has been issued for the purpose of proving the identity of the holder. For example, identity cards and passports are explicit ID documents.

In contrast, the purpose of a driving licence is to prove that the specified holder has a driving licence. With restrictions (e.g. photo may be older), a driving licence also enables identification, but it is not an explicit ID document. (e.g. during roadside checks, an identity card is also required in addition to the driving licence). In other words, a driving licence issued in Germany is an ID document in the sense of this TR, but not an explicit ID document.

If an explicit ID document in turn has additional applications such as a driving licence, health care card or bank card, this has no effect on the assessment and the ID document remains an explicit ID document.

The assessment of the assurance level is to be carried out as follows:

- Not fulfilled: It is not possible to say whether it is an explicit ID document or not.

- Normal: The type of the ID document is known and the ID document is **not** an explicit ID document (e.g. driving licence).
- Substantial/high: The assurance level is not further differentiated at this point. The ID document is an explicit ID document. The check was carried out with the checking depth **document check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth").

A1.1-9

Checking criterion description: Does the ID document fulfil the domestic ID requirement?

Explanation / note: Definition of the domestic ID requirement according to [TR-03147], Table 4 (footnote 8): According to the legal system of the respective country on the basis of which ID proof is required or according to the legal arrangement that has been explicitly agreed in the case of private law contracts. ID documents such as identity cards and passports fulfil the national ID requirement in Germany (Law on Identity Cards and Electronic Proof of Identity (Gesetz über Personalausweise und den elektronischen Identitätsnachweis, § 1; see e.g. http://www.juraforum.de/lexikon/ausweispflicht).

The assessment of the assurance level is to be carried out as follows:

- N/A: It is an explicit identity document, but does not fulfil the domestic ID requirements.
- Normal/substantial: The assurance level is not further differentiated at this point. The ID requirement is not fulfilled (in the case of a non-explicit ID document). The check was carried out with the checking depth **document check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth").
- High: The domestic ID requirement is fulfilled. The check was carried out with the checking depth **document check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth").

A1.1-10

Checking criterion description: Does the ID document have at least an equivalent level of security features and their verifiability for protection against counterfeits and manipulation as domestic ID documents?

Explanation / note: ***The ID document does not fulfil the domestic ID requirement;*** The inspector's assessment that the ID document has at least a comparable level of security to an ID document that fulfils the domestic ID requirement must be adequately substantiated.

An electronic residence permit can be assumed to have a comparable level of security to the German identity card.

The assessment of the assurance level is to be carried out as follows:

- N/A: It is an explicit identity document that fulfils the domestic ID requirements.
- Not fulfilled: It is not possible to make a conclusion as to whether the security level of features and their verifiability are at least equivalent.
- Normal/substantial: The ID document does not have a security level of features and their verifiability that is at least equivalent to domestic ID documents to protect against counterfeit and manipulation. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **document check**.
- High: The ID document does have a security level of features and their verifiability that is at least equivalent to domestic ID documents to protect against counterfeit and manipulation. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth").

3.1.4 Contains a sufficient set of ID attributes

A1.2-1

Checking criterion description: Is there a sufficient set of ID attributes?

Explanation / note: The set of ID attributes required depends on the respective application. The ID attributes are to be indicated in the checking report.

- Not fulfilled: The set of ID attributes required in the application for ID proof cannot be specified or it cannot be determined from each approved document.
- Normal/substantial/high: The set of ID attributes required in the application for ID proof can be specified. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **document check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

A1.2-2

Checking criterion description: Is unique identification possible through the given ID attributes?

Explanation / note: Only relevant if required for the application being checked.

- N/A: Unique identification by the ID attributes is not required for the application.
- Not fulfilled: No unique identification is provided by the ID attributes, although this is required for the application. The check was carried out with the checking depth **document check**.
- Normal/substantial/high: Unique identification is provided by the ID attributes. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **document check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

3.1.5 Tamper-proof

This point checks the assurance level that the used ID document has against manipulations and counterfeits. The current state of research and technology is decisive for the assessment. The assessment is carried out according to [CEM], see section 2.3. In terms of a "make or buy" decision, the simplest or most cost-effective acquisition and implementation of an attack from an attacker's point of view is to be evaluated.

The category of the ID procedure is decisive for the assessment of the assurance level of the protection against counterfeit or manipulation of the ID document under consideration. The tamper and counterfeit resistance of an ID document that does not meet A1.3-1 is not an absolute criterion, but depends on which category (direct, indirect or electronic) the checked ID procedure falls into. This means in particular the way in which ID proofs are checked for potential counterfeits or falsification.

A1.3-1

Checking criterion description: Is the ID document in question a German identity card, an EU residence permit or an EU or EFTA passport and does it thus correspond to the assurance level "high" with regard to the security against tampering and counterfeit?

Explanation / note: For the aforementioned ID documents, an assurance level of "high" is generally assumed with regard to the security against counterfeit and manipulation. If, despite this, there is strong evidence that this assumption does not apply to any of the above ID documents, these reasons are to be elaborated in the analysis, and A1.3-1 is to be rated ***N/A***. If A1.3-1 is applicable, assessment A1.3-2 is not applicable.

Note that for identity documents and passports from countries not belonging to the EU or EFTA, A1.3-1 is not applicable and thus an assessment according to A1.3-2 is necessary.

A1.3-2

Checking criterion description: What assurance level does the ID document in question have in terms of the potential for attack in order to counterfeit or manipulate it, taking into account the category of the procedure?

Explanation/note: In this case, an assessment as described in section 2.3 is to be carried out.

N/A: Only possible if A1.3-1 has been rated "high".

Expertise

For ID procedures in the "direct" and "indirect" categories, the relevant expertise is to be expected mainly in the area of physical reproduction/manipulation of an ID document, including the necessary knowledge about the function or mode of action, production and implementation of the security features used.

Counterfeits that can pass a check using a method in the "indirect" category generally require a lower level of expertise for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, expertise in the areas of cryptography and IT security is important, among other things.

- *Layperson*: The ID document can be counterfeited or manipulated by an interested layperson without special knowledge. This would include, for example, the use of a photocopier or a standard commercial printer, the use of image editing software, or manually overwriting or pasting over data and security features.
- *Proficient*: Counterfeit or manipulation of the ID document requires special knowledge that goes well beyond that of an interested layperson. Knowledge about the processing of special plastics, types of paper or other substrates or materials, as well as unusual inks and colours are worth mentioning here. Knowledge of how to counterfeit individual security features, such as holograms, can also be included here.
- *Expert*: Counterfeit or manipulation of the ID document requires expert knowledge, for example for the operation of customized machines (lasers, special printing machines) necessary for the production or manipulation of the ID document.
- *Multiple experts*: Counterfeit or manipulation of the ID document requires multiple expert skills that do not complement each other or complement each other only slightly, for example for the operation of several customized machines that are necessary for the production of the ID document.

Insider knowledge

For ID procedures in the "direct" and "indirect" categories, knowledge about the process parameters of production machines used in the production of specific ID documents as well as material properties and compositions (e.g. of plastics, paper, melting fibres, printing ink, bindings) are examples of relevant insider knowledge.

Counterfeits that can pass a check using a method in the "indirect" category generally require a lower level of insider knowledge for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, insider knowledge of the hardware and software used is typically relevant here.

- *Public*: The necessary knowledge is freely available and/or can be researched with little effort by an interested layperson (e.g. on the internet), e.g. dimensions, font sizes and types of imprint s. This may also apply to security features that have not been officially disclosed, if there is no guarantee that such features will not become public through unofficial channels.
- *Restricted*: The necessary knowledge is only available to a defined and restricted group of people. Examples include the way in which special types of paper or other substrates are used, as well as unusual inks and colours in printing processes, or the detailed, basic functioning of individual security features.
- *Sensitive*: The necessary knowledge is only known to the group of people entrusted with the direct production of the original documents, such as the exact composition of a material used or the exact operating parameters of a specially manufactured machine used.
- *Critical*: The necessary knowledge is only known to the group of people entrusted with the direct development or production of the original documents, such as the exact composition of several materials used or the exact operating parameters of several specially manufactured machines used.

Windows of opportunity

For ID procedures in the "direct" and "indirect" categories, examples of windows of opportunity are access to system components used in the procedure (including required production and personalisation machines) or access to required raw and auxiliary materials or pre-produced blank documents.

Counterfeits that can pass a check using a method in the "indirect" category generally require less restrictive windows of opportunity for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, favourable windows of opportunity in the event of software attacks are, for example, access to possibly stolen cryptographic key material or to the source code of the software used. Favourable windows of opportunity in hardware attacks are, for example, the access to personalised and non-personalised smart card samples or other hardware based secure elements.

- *Unnecessary/unlimited access*: No special windows of opportunity are necessary to counterfeit or manipulate the ID document, i.e. this is easily possible in normal premises, for example. Access to required raw and auxiliary materials or blank documents is not subject to any special restrictions.
- *Easy*: Restrictive windows of opportunity are necessary to counterfeit or manipulate the ID document. Access to required raw and auxiliary materials or blank documents is only possible for a restricted group of people.
- *Moderate*: Highly restrictive windows of opportunity are necessary to counterfeit or manipulate the ID document, for example, access to machines used to produce the original documents, or lots and/or highly skilled personnel with insider knowledge. Access to required original raw and auxiliary materials or blank documents is only possible for a restricted group of people, and their disclosure to unauthorised persons is punishable by law.
- *Difficult*: Multiple highly restrictive windows of opportunity are necessary, for example access to machines used to produce the original documents and at the same time access to matching blank documents.

Equipment

For ID procedures in the "direct" and "indirect" categories, printing and other production and personalisation machines are to be mentioned here.

Counterfeits that can pass a check using a method in the "indirect" category generally require less sophisticated equipment for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, hardware interfaces to the ID document, measurement and IT technology (standard PCs, possibly with special additional hardware, oscilloscopes, spectrum analysers, etc.) are examples of necessary equipment.

- *Standard*: The equipment necessary for counterfeiting or tampering can be special, but is available at short notice from specialised dealers at a manageable cost, e.g. standard electronic components, standard PCs and standard software, stamps, tools such as knives, scalpels, special erasers, chemical substances freely available to everyone, such as various adhesives and solvents.
- *Specialised*: The equipment necessary for counterfeiting or tampering is only available from specialised suppliers at an increased cost, e.g. optical and electronic measurement technology such as oscilloscopes, spectrometers, special PC hardware and software or chemical substances that are not freely available, such as hydrofluoric acid.
- *Bespoke*: The equipment necessary for counterfeiting or tampering is highly specialised, and includes at least one possibly adapted, often bespoke device, such as a special printing machine, a laser for optical personalisation or a machine for inserting a kinetic image (optically variable device, OVD) into the ID document.
- *Multiple bespoke*: The equipment necessary for counterfeiting or tampering is highly specialised in several ways, and consists of several possibly adapted, often bespoke devices, such as a special printing machine in combination with a tuned laser for optical personalisation.

It should be noted at this point that assurance levels of ID documents for different categories of ID procedures according to section 2.2 are not directly comparable with each other. This applies even if it is the same ID document. For example, an ID document may meet the assurance level "high" for an ID procedure based on a personal check ("direct" category) due to numerous security features that are difficult to counterfeit (e.g. kinetic images, guilloches, special printing ink), but only the assurance level "normal" for a procedure based on electronic identification ("electronic" category) due to an implementation error of the cryptographic functionality. Deviations from this procedure are possible; these are then to be detailed in the analysis.

Additional information on ID procedures of the category "indirect", such as an identification procedure by means of video transmission, can be found in the Appendix (section 4).

3.1.6 Security features are known and effectively verifiable

The assurance level to be assigned to the security features of the ID document used in terms of their reputation and verifiability is to be determined here. Only those security features that are actually checked in the ID procedure are to be considered.

A1.4-1

Checking criterion description: Are all security features of the approved ID documents used in the ID procedure known and effectively verifiable?

Explanation/note: Provide a list of all security features considered by the ID procedure for all authorised ID documents, along with any necessary equipment or other requirements to effectively check said security features. The respective assurance level within this subset of assurance features is based on the results from section 3.1.5 „Tamper-proof“.

- Not fulfilled: A security feature used by the ID procedure is not known or cannot be effectively verified.
- Normal/substantial/high: The assurance level is based on the results from section 3.1.5.

Additional information on ID procedures of the category "indirect", such as an identification procedure by means of video transmission, can be found in the Appendix (section 4).

3.1.7 Allows for reliable matching with the user

This assesses how reliably the ID document under consideration can in principle be assigned to its rightful owner. This is usually done by matching knowledge-based or biometric data, depending on the ID document used. The assurance levels of A1.5-1 and A1.5-2 are determined by the maximum probability that an unauthorised user could successfully misidentify themselves using the ID document.

A1.5-1

Checking criterion description: What is the assurance level of the knowledge-based data available on the ID document for matching with the user?

Knowledge-based matching procedures are commonly used for electronic ID procedures, and are based on the input of a knowledge feature (in most cases a PIN), with a retry counter that ensures that the total number of consecutive incorrect input attempts is limited.

For the assessment of the assurance level, the following requirements for the assurance levels are taken as a basis for knowledge-based procedures:

- Normal: The probability of guessing the knowledge feature in the maximum number of attempts is at most 3×10^{-4} (three out of ten thousand), and the knowledge feature used (usually a PIN) is secret according to the usage provision. The check was carried out with the checking depth **document check**.
- Substantial: The probability of guessing the knowledge feature in the maximum number of attempts is at most 3×10^{-5} (three out of a hundred thousand), and the knowledge feature used (usually a PIN) is secret and freely selectable by the rightful holder according to the usage provision. The check was carried out with the checking depth **implementation check**.
- High: The probability of guessing the knowledge feature in the maximum number of attempts is at most 3×10^{-6} (three out of a million), and the knowledge feature used (usually a PIN) is secret and freely selectable by the rightful holder according to the usage provision. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

The knowledge-based data of the checked ID document and procedures for matching with the user are to be described in the analysis and the assignment of the corresponding assurance level is to be made understandable.

If the ID document does not provide knowledge-based data or if it is not used in the procedure under consideration, A1.5-2 is to be rated "N/A".

A1.5-2

Checking criterion description: What is the assurance level of the biometric data available on the ID document for matching with the user?

Biometric reference data for matching with the user can be used with all categories of ID procedures. The most common matching procedure is visual inspection of a photograph in direct and indirect ID procedures. However, it is also possible to match electronically stored biometric data, such as fingerprints, iris characteristics or electronic photo data.

The following assurance level requirements apply to biometrics:

- Normal: The false acceptance rate of the biometric method is not significantly worse than 3 x 10^{-4} (three out of ten thousand). A photograph of the user allows the recognition of the essential facial features of the rightful holder. The check was carried out with the checking depth **document check**.
- Substantial/high: The false acceptance rate of the biometric method is not significantly worse than 3 x 10^{-5} (three out of a hundred thousand). The photograph of the user at least meets the requirements of identity cards in terms of reproduced resolution and photographic image quality. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).
- The biometric reference data of the checked ID document for matching with the user is to be described in the analysis and the determined assurance level is to be described in an understandable way.

If the ID document does not provide biometric reference data, A1.5-2 is to be assessed as "N/A".

3.1.8 ID attributes are up to date

A1.6-1

Checking criterion description: Is the timeliness of the ID attributes on the ID document used sufficiently guaranteed?

Explanation / note: It must be assessed to what extent it may be assumed that all ID attributes on the ID document used are sufficiently up-to-date. Taking the maximum validity period into account is only of very limited significance. Rather, the administrative processes and regulations associated with ID documents and the updating of ID attributes must be taken into account. For example, ID attributes may be provided with information on the date they were captured or last updated. For example, a photograph for use in an identity card must not be more than one year old at the time of application.

- Normal: The timeliness of the ID attributes is not guaranteed.
- Substantial/high: The timeliness of the ID attributes is guaranteed. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

3.1.9 Available lost, stolen or revoked reports are checked

A1.7-1

Checking criterion description: Has the maximum validity period of the ID document been checked?

Explanation / note: The specified maximum period of validity of the ID document must be checked. If this cannot be read directly from the ID document, it must be provided for in the ID procedure.

- N/A: No maximum validity period is set for the ID document and therefore it cannot be checked.
- Normal/substantial: A maximum validity period is set for the ID document and can be checked. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **document check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).
- High: A maximum validity period is set for the ID document and can be checked. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

A1.7-2

Checking criterion description: Are lost, stolen or revoked reports for the ID document queried to determine validity?

Explanation / note: An essential prerequisite for the verifiability of lost, stolen or revoked reports is the implementation of a system for recording and querying lost, stolen or revoked reports. Given this prerequisite, the ID procedure continues to determine whether a query of lost, stolen or revoked reports can also be carried out. Even for the assurance levels "substantial" and "high", a query of lost, stolen or revoked reports is only obligatory if it can be implemented within the framework of the ID procedure.

- N/A: No system for recording and querying lost, stolen or revoked reports is implemented for the ID document.

Or: It is not possible to check lost, stolen or revoked reports in the ID procedure. An explanation is to be provided for this.

- Normal: A system for recording and querying lost, stolen or revoked reports is implemented for the ID document. However, despite its feasibility, lost, stolen or revoked reports are not checked in the ID procedure. The check was carried out with the checking depth **document check**.
- Substantial/high: A system for recording and querying lost, stolen or revoked reports is implemented for the ID document and available lost, stolen or revoked reports are checked in the ID procedure. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

3.1.10 Regular checking of the set of permissible ID documents

A1.8-1

Checking criterion description: How often are the ID documents approved for the ID procedure checked in accordance with requirement A1.7-1 and A1.7-2?

Explanation / note: The set of admissible ID documents must be checked and updated at regular intervals. These include, for example, the legality of identity documents, which could lapse, or their security, which could be compromised. The time interval of the check is to be indicated. The check can be done, for example, by consulting suitable sources.

- Not fulfilled: No regular check is carried out.
- Normal: A check of the admissible ID documents is carried out at least annually. A check of the criterion was carried out with the checking depth **document check**.
- Substantial: A check of the admissible ID documents is carried out at least quarterly. A check of the criterion was carried out with the checking depth **implementation check**.
- High: A check of the admissible ID documents is carried out at least monthly. A check of the criterion was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

A1.8-2

Checking criterion description: Is new knowledge gained from requirements A1.8-1 taken into account when carrying out the ID procedure?

Explanation / note: During regular ID document checks, new findings (such as counterfeits and forgeries that have become known) must be taken into account in the ID procedure process. For example, a previously approved ID document must have its approval for the ID procedure withdrawn as soon as it is deemed no longer sufficiently trustworthy due to a successful attack. The sources of information used to obtain these findings are to be indicated.

- Not fulfilled: New findings are not taken into account in the regular check.
- Normal: New findings are taken into account in the regular check. The check was carried out with the checking depth **document check**.
- Substantial: New findings are taken into account in the regular check. The check was carried out with the checking depth **implementation check**.
- High: New findings are taken into account in the regular check. The check was carried out with the checking depth **independent test**.

3.2 Security of the transmission channels

According to [TR-03147], depending on the channel under consideration, additional Technical Guidelines of the BSI must be taken into account or can be used as an additional basis for an assessment of the procedure. For details, please refer to the following guidelines:

- [TR-03116-4] for securing the transport channel using TLS,
- [TR-03107-1] and [TR-03116-4] for securing the transport layer and the security of dedicated eID applications and
- [TR-03127] , [TR-03124-1] and [TR-03130] for the eID function of the German identity card and electronic residence permit.

The classification of the ID procedure into the category indirect or electronic significantly determines the assessment of the assurance level with regard to the security of the transmission channels. In the case of an indirect procedure, a secured transmission channel (without a dedicated eID procedure) is used. Attention must be paid to both the reduced quality or reduced information content and the risk of digital signal manipulation during transmission. The electronic procedures category includes dedicated eID procedures.

3.2.1 Video/information manipulations of biometric data of the person to be identified are detected

In this case, the assurance level of the transmission channel in the ID procedure is defined, which is to be assigned to the prevention and detection of video tampering with biometric data (e.g. the image of the face of a person to be identified is changed or exchanged). The current state of research and technology is decisive for the assessment. The assessment is carried out according to [CEM], see section 2.3.

These assessments depend on the attack potential required to carry out a successful attack. With regard to the prevention and detection of this type of video tampering, according to [TR-03147], section 5.2.1, the following aspects, among others, have an impact on the potential for attack to be considered for the assessment:

- Based on the state-of-the-art research and technology, it is necessary to assess the attack potential which is sufficient to achieve a false acceptance rate above the permissible maximum.
- For the assessment of the work involved in the attack, the implementation must be considered first and foremost. The work involved in preparation is only taken into account in exceptional cases, see section 2.3.

A2.1-1

Checking criterion description: What assurance level does the ID procedure in question have in terms of attack potential in order to successfully carry out video/information tampering with biometric data?

Explanation/note: In this case, an assessment as described in section 2.3 is to be carried out.

N/A: Only possible with direct or electronic ID procedures.

Expertise

- *Layperson*: The attacker has basic knowledge of installing and operating software and possibly hardware, e.g. for video manipulations.
- *Proficient*: The attacker requires in-depth knowledge in the area in question, e.g. about the use of video editing software or the unnoticed injection of a manipulated data stream for use in the ID procedure software.
- *Expert*: The attacker requires expert knowledge of the latest research and technology beyond the use of available video editing software.
- *Multiple experts*: The attacker requires expert knowledge of the latest research and technology in several areas, e.g. in the field of real-time video processing and at the same time in the field of software reverse engineering in order to be able to manipulate the software of the ID procedure during runtime.

Insider knowledge

- *Public*: The necessary information is publicly available, e.g. on the internet.
- *Restricted*: The necessary information is held by the manufacturer and is only passed on to third parties, for example, under a non-disclosure agreement.
- *Sensitive*: The necessary information is only accessible to specific teams and employees of the manufacturer on a limited basis.
- *Critical*: The necessary information is only accessible to a very limited and explicitly authorised group of people.

Windows of opportunity

- *Unnecessary/unlimited access*: A simple video recording of any person is required.
- *Easy*: A simple video recording of a specific person is required.
- *Moderate*: A high-quality video recording of a specific person, suitable for professional post-production, is required.
- *Difficult*: Several different, high-quality biometric samples of a specific person suitable for professional post-processing are required, e.g. a video recording of the head, face, and a suitable sample of a fingerprint.

Equipment

- *Standard*: Equipment is available directly from specialist retailers, e.g. PCs, cameras, standard software, adapters.

- *Specialised*: Although the equipment is available directly from specialist retailers, it has been expertly customised, e.g. arrays of graphics cards, expert integration and configuration of multiple software components.
- *Bespoke*: The equipment is state-of-the-art in research and technology, is difficult to obtain commercially and often consists of bespoke items, e.g. multi-camera setups with custom-built computer/camera hardware to capture and manipulate a scene in three dimensions in real time.
- *Multiple bespoke*: The equipment is state-of-the-art in research and technology across several different fields, is difficult to obtain commercially and often consists of bespoke items, e.g. multi-camera setups with custom-built computer/camera hardware to capture and manipulate a scene in three dimensions in real time and hardware to manipulate network traffic.

It should be noted at this point that assurance levels for different categories of ID procedures are not directly comparable, even though the same ID document is used in these procedures. A video identification procedure, for example, can only reach the assurance level "normal" as a result of the possibility of video manipulation (e.g. the face of a person to be identified can be manipulated), whereas a procedure based on electronic identification ("electronic" category) can only reach the assurance level "high". The same ID document can be used in both cases.

Deviations from this procedure are possible; these are then to be detailed in the analysis.

3.2.2 Manipulation of information transmitted from the ID document is detected

This involves the detection of video manipulation of optically personalised data on an ID document as well as general manipulation of data stored electronically on the ID document. The assessment is carried out according to [CEM], see section 2.3.

These assessments for checking criteria A2.2-1 and A2.2-2 depend on the attack potential necessary to carry out a successful attack or on the attack potential that the ID procedure under consideration is able to counter. With regard to preventing and detecting such manipulations, according to [TR-03147], section 5.2.2, special consideration is to be given to whether the false acceptance rate is above the maximum permissible for the assurance level under consideration.

A2.2-1

Checking criterion description: What is the assurance level of the ID proof used for the ID procedure for which the lowest attack potential is sufficient to compromise?

Explanation / note: Insofar as the use of different ID proofs is permitted in an ID procedure, according to the minimum principle, the ID proof permissible for an ID check with the lowest required attack potential determines the overall attack potential necessary to achieve a false acceptance rate above the permissible maximum. The checking criteria for the requirement „Manipulation of information transmitted from the ID document is detected“ addressed in this section is to be applied to all ID proofs accepted for the ID procedure by the inspector and the overall result of the requirement is to be determined according to the minimum principle mentioned above. In other words, the necessary attack potential is determined by the lowest attack potential achieved for an ID proof. This also determines the assurance level achieved across all ID proofs taken into account.

Additional information on ID procedures of the category "indirect", such as an identification procedure by means of video transmission, can be found in the Appendix (section 4).

A2.2-2

Checking criterion description: What assurance level does the ID procedure in question have in terms of attack potential in order to successfully carry out information manipulation of information transmitted by the ID document?

Explanation/note: In this case, an assessment as described in section 2.3 is to be carried out.

N/A: Only possible with direct or electronic ID procedures.

Expertise

- *Layperson*: The attacker has basic knowledge of installing and operating software, e.g. for video tampering.
- *Proficient*: The attacker requires in-depth knowledge in the area in question, e.g. about the use of video editing software or the unnoticed injection of a manipulated data stream in the software used in the ID procedure.
- *Expert*: The attacker requires expert knowledge of the latest research and technology beyond the use of already available video editing software.
- *Multiple experts*: The attacker requires expert knowledge of the latest research and technology in several areas, e.g. in the field of real-time video processing and at the same time in the field of software reverse engineering in order to be able to manipulate the software of the ID procedure during runtime.

Insider knowledge

- *Public*: The necessary information is publicly available, e.g. on the internet.
- *Restricted*: The necessary information is held by the manufacturer and is only passed on to third parties, for example, under a non-disclosure agreement.
- *Sensitive*: The necessary information is only accessible to specific teams and employees of the manufacturer on a limited basis.
- *Critical*: The necessary information is only accessible to a very limited and explicitly authorised group of people.

Windows of opportunity

In general, the opportunities for the manipulation of information transmitted by the ID document are to be considered here. The following section looks at this manipulation using the example of a video recording, among others.

- *Unnecessary/unlimited access*: A simple biometric sample (e.g. video recording) of any person is required.
- *Easy*: A simple biometric sample (e.g. video recording) of a specific person is required.
- *Moderate*: A high-quality biometric sample (e.g. video recording) of a specific person, suitable for professional post-processing, is required.
- *Difficult*: Several different, high-quality biometric samples of a specific person suitable for professional post-processing are required, e.g. a video recording of the head, face, and a valid sample of a fingerprint.

Equipment

- *Standard*: Equipment is available directly from specialist retailers, e.g. PCs, cameras, standard software, adapters.
- *Specialised*: Although the equipment is available directly from specialist retailers, it has been expertly customised, e.g. arrays of graphics cards, expert integration and configuration of multiple software components.
- *Bespoke*: The equipment is state-of-the-art in research and technology, is difficult to obtain commercially and often consists of bespoke items, e.g. multi-camera setups with custom-built computer hardware to capture and manipulate a scene in three dimensions in real time.
- *Multiple bespoke*: The equipment is state-of-the-art in research and technology across several different fields, is difficult to obtain commercially and often consists of bespoke items, e.g. multi-camera setups with custom-built computer hardware to capture and manipulate a scene in three dimensions in real time and hardware to manipulate network traffic.

It should be noted at this point that assurance levels of ID documents for different categories of ID procedures are not directly comparable with each other. This applies even if it is the same ID document. For example, an ID document can reach the assurance level "high" for an ID procedure in the "indirect" category due to numerous very high-quality security features (e.g. kinetic images, guilloches, special printing ink), because IT manipulation proves too costly, but only the assurance level "normal" for a procedure based on electronic identification (category "electronic") due to a known implementation error of the cryptographic functionality.

Deviations from this procedure are possible; these are then to be detailed in the analysis.

Additional information on ID procedures of the category "indirect", such as an identification procedure by means of video transmission, can be found in the Appendix (section 4).

3.2.3 Physical manipulations of biometric characteristics of the person to be identified are detected

In this context, all types of "presentation attacks" (the person to be identified appears with manipulated characteristics) are specifically considered. In particular, the way in which the biometric characteristics are captured in the procedure plays an important role in assessing the required attack potential. The assessment is carried out according to [CEM], see section 2.3.

It should be noted that the checks required here must be carried out independently of the ID document used, in order to also exclude simultaneous manipulation of biometric characteristics and ID documents.

A2.3-1

Checking criterion description: What assurance level does the ID procedure in question have in terms of attack potential in order to successfully carry out a physical manipulation of biometric characteristics of the person to be identified?

Explanation/note: In this case, an assessment as described in section 2.3 is to be carried out.

N/A: Only possible with direct or electronic ID procedures.

Expertise

- *Layperson*: Successful manipulation of the biometric characteristics requires specialist lay knowledge, e.g. on how to replicate fake fingerprints, which are not recognised as such by simple fingerprint sensors.
- *Proficient*: Successful manipulation of the biometric characteristics requires relevant specialised knowledge, e.g. make-up artist training.

- *Expert*: Successful manipulation of biometric characteristics requires state-of-the-art knowledge, e.g. on how to produce fake fingerprints that are not recognised as such by liveness detection.
- *Multiple experts*: Successful manipulation of biometric characteristics requires state-of-the-art knowledge in several areas, e.g. on the replication of multiple biometric characteristics.

Insider knowledge

- *Public*: The necessary information is publicly available, e.g. on the internet.
- *Restricted*: The necessary information is held by the manufacturer and is only passed on to third parties, for example, under a non-disclosure agreement.
- *Sensitive*: The necessary information is only accessible to specific teams and employees of the manufacturer on a limited basis.
- *Critical*: The necessary information is only accessible to a very limited and explicitly authorised group of people.

Windows of opportunities

- *Unnecessary/unlimited access*: A biometric characteristic (e.g. a fingerprint) of any person is required.
- *Easy*: A biometric characteristic (e.g. a fingerprint) of a specific person is required.
- *Moderate*: A biometric characteristic of a specific person is needed, which is particularly complex to obtain, e.g. the exact 3D profile of the target's face.
- *Difficult*: Several independent biometric characteristics of a specific person are required, which are particularly complex to obtain, e.g. the exact 3D profile of the face and the iris pattern of the target person.

Equipment

- *Standard*: Equipment is directly available in specialised shops, e.g. ready-made masks, material for making simple fingerprints.
- *Specialised*: Although the equipment is directly available in specialised shops, it must be further processed by experts, e.g. make-up artist supplies, special make-up, special brushes, latex as the basic material of masks or fake fingerprints.
- *Bespoke*: The equipment is state-of-the-art, commercially difficult to obtain and consists mainly of bespoke items, e.g. custom-made contact lenses with a specific iris pattern.
- *Multiple bespoke*: The equipment is state-of-the-art in several different fields, is difficult to obtain commercially and often consists of bespoke items, e.g. custom-made contact lenses with a specific iris pattern, and a fake fingerprint that is not recognised by a fingerprint sensor with liveness detection.

It should be noted at this point that assurance levels for different categories of ID procedures are not directly comparable (see section 2.2), even though the same ID document is used in these procedures. For example, a video identification procedure using a specific ID document may achieve a different assurance level than an electronic procedure using the same ID document.

Deviations from this procedure are possible; these are then to be detailed in the analysis.

3.2.4 Physical manipulations of the ID document are detected

This section is closely related to the requirements in section 3.1.5. In particular, it is to be noted that limitations in the detectability of manipulations may result from the actually available checking possibilities in a procedure. The assessment is carried out according to [CEM], see section 2.3.

It should be noted that the checks required here must be carried out independently of the specific biometric characteristic under consideration, in order to also exclude simultaneous manipulation of biometric characteristics and ID documents.

A2.4-1

Checking criterion description: What assurance level does the ID procedure in question have in terms of attack potential in order to successfully carry out a physical manipulation of the ID document in it?

Explanation/note: In this case, an assessment as described in section 2.3 is to be carried out.

N/A: Only possible with direct or electronic ID procedures.

Expertise

For ID procedures in the "indirect" category, the relevant expertise is to be expected mainly in the field of physical reproduction of an ID document, including the necessary knowledge about the functioning, production and integration of the security features used.

Counterfeits that can pass a check using a method in the "indirect" category generally require a lower level of expertise for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, expertise in the areas of cryptography and IT security is important, among other things.

Examples of the classification are:

- *Layperson*: Successful manipulation of the ID document for a particular transmission channel requires specialist lay knowledge, e.g. knowledge of the verifiability of printed security features such as guilloche by visual inspection.
- *Proficient*: Successful manipulation of the ID document for a particular transmission channel requires relevant specialised knowledge, e.g. determining the effective transmission quality of a camera image, depending on resolution, compression and signal/noise ratio.
- *Expert*: Successful manipulation of the ID document for a particular transmission channel requires state-of-the-art knowledge, e.g. detailed knowledge of the possibilities and limitations of current automated pattern recognition algorithms.
- *Multiple experts*: Successful manipulation of the ID document for a particular transmission channel requires state-of-the-art knowledge in several areas, e.g. detailed knowledge of the possibilities and limitations of current automated image recognition algorithms, and detailed knowledge of the manipulation of holographic security features.

Insider knowledge

For ID procedures in the "indirect" category, knowledge about the process parameters of production machines as well as material properties and compositions (e.g. of paper, printing ink, bindings) are examples of relevant insider knowledge.

Counterfeits that can pass a check using a method in the "indirect" category generally require a lower level of insider knowledge for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, insider knowledge of hardware and software development is usually particularly relevant here.

Examples of the classification are:

- *Public*: The necessary information is publicly available, e.g. on the internet.
- *Restricted*: The necessary information is held by the manufacturer and is only passed on to third parties, for example, under a non-disclosure agreement.
- *Sensitive*: The necessary information is only accessible to specific teams and employees of the manufacturer on a limited basis.
- *Critical*: The necessary information is only accessible to a very limited and explicitly authorised group of people.

Windows of opportunity

For ID procedures in the "indirect" category, examples of windows of opportunity are access to required original production and personalisation machines or access to required raw and auxiliary materials or pre-produced (blank) documents.

Counterfeits that can pass a check using a method in the "indirect" category generally require less favourable windows of opportunity for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, favourable windows of opportunity in the event of software attacks are, for example, access to possibly stolen cryptographic key material or to the source code of the software used. Favourable windows of opportunity in hardware attacks are, for example, access to personalised and non-personalised smart card samples that can be used for identification in the procedure (see section 2.3).

Examples of the classification are:

- *Unnecessary/unlimited access*: An ID document of any person is required.
- *Easy*: An ID document of a specific person is required.
- *Moderate*: An ID document of a specific person is required, which is particularly complex to obtain.
- *Difficult*: An ID document and a biometric sample of a specific person are required, e.g. the exact 3D profile of the face and a sovereign ID document of the person. An additional example is the need for an original blank document.

Equipment

For ID procedures in the "indirect" category, printing and other production machines are to be mentioned here.

Counterfeits that can pass a check using a method in the "indirect" category generally require less sophisticated equipment for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, hardware interfaces to the ID document, measurement and IT technology (standard PCs, possibly with special additional hardware, oscilloscopes, spectrum analysers, etc.) are examples of necessary equipment.

Examples of the classification are:

- *Standard*: Equipment is available directly from specialist retailers, e.g. glue, transparent adhesive tape, film, printers, also laminating machines.
- *Specialised*: Although the equipment is freely available, it must be expertly processed, e.g. special types of paper, plastic card blanks.
- *Bespoke*: Equipment is difficult to obtain commercially and often consists of bespoke items, e.g. lasers for surface processing, wire bonders, electron microscopes, focused ion beam equipment or the use of cleanrooms.
- *Multiple bespoke*: Several necessary pieces of equipment are difficult to obtain commercially and often consist of bespoke items, e.g. lasers for surface treatment or optically variable elements.

It should be noted at this point that assurance levels of ID documents for different categories of ID procedures are not directly comparable with each other (see section 2.2). This applies even if it is the same ID document. For example, an ID document can reach the assurance level "high" for an ID procedure in the "indirect" category due to numerous very high-quality security features (e.g. kinetic images, guilloches, special printing ink), but only the assurance level "normal" for a procedure based on electronic identification (category "electronic") due to a known implementation error of the cryptographic functionality.

Deviations from this procedure are possible; these are then to be detailed in the analysis.

Additional information on ID procedures of the category "indirect", such as an identification procedure by means of video transmission, can be found in the Appendix (section 4).

3.2.5 Live transmission of all data is guaranteed

In this context, attacks with recorded data (e.g. specially prepared for import or stored in a previous process for reimport) and their countermeasures (e.g. random values or dynamic processes) must be taken into account. The assessment is carried out according to [CEM], see section 2.3.

A2.5-1

Checking criterion description: What assurance level does the ID procedure in question have in terms of attack potential in order to successfully reuse recorded data in it?

Explanation/note: In this case, an assessment as described in section 2.3 is to be carried out.

N/A: Only possible with direct or electronic ID procedures.

Expertise

Examples of the classification are:

- *Layperson*: The attacker has basic knowledge of installing and operating software, e.g. for video tampering.
- *Proficient*: The attacker requires in-depth knowledge in the area in question, e.g. about the use of video editing software or the unnoticed injection of a previously recorded data stream for use in the ID procedure software.
- *Expert*: The attacker requires expert state-of-the-art knowledge beyond the use of available video editing software, e.g. combining pre-recorded video footage with live video footage at the same time in a data stream.
- *Multiple experts*: The attacker requires expert state-of-the-art knowledge in several areas, e.g. combining pre-recorded video footage with live video footage at the same time in a data stream and at the same

time knowledge in software reverse engineering to be able to manipulate the software of the ID procedure during runtime.

Insider knowledge

The availability of information used in the planning, production and use of pre-produced material is to be assessed. Moreover, insider knowledge to circumvent protective mechanisms that prevent the import of pre-produced data must be taken into account.

Examples of the classification are:

- *Public*: The necessary information is publicly available, e.g. on the internet.
- *Restricted*: The necessary information is held by the manufacturer and is only passed on to third parties, for example, under a non-disclosure agreement.
- *Sensitive*: The necessary information is only accessible to specific teams and employees of the manufacturer on a limited basis.
- *Critical*: The necessary information is only accessible to a very limited and explicitly authorised group of people.

Windows of opportunity

For the preparation of an attack, it may be necessary to know the procedure of a (successful) ID check as precisely as possible. It is therefore necessary to assess what level of detail of records or other information about possible variants and sequences is required to carry out a successful attack.

Examples of the classification are:

- *Unnecessary/unlimited access*: The process of the ID procedure must be known in principle, e.g. which category (direct, indirect, electronic) is involved, which ID documents are permitted.
- *Easy*: The main features of the ID procedure and its variants must be known, e.g. which security features are checked.
- *Moderate*: The process of the ID procedure and its variants must be known in detail, e.g. which security features are checked and how they are checked.
- *Difficult*: The process of the ID procedure must be fully known, e.g. the exact process of decision-making for all possible cases and variants including the time schedule is known. The exact instructions to the inspector are known.

Equipment

Examples of the classification are:

- *Standard*: Equipment is available directly from specialist retailers, e.g. PCs, cameras, standard software, adapters.
- *Specialised*: Although the equipment is available directly from specialist retailers, it has been expertly customised, e.g. arrays of graphics cards, expert integration and configuration of multiple software components.
- *Bespoke*: The equipment is state-of-the-art in research and technology, is difficult to obtain commercially and often consists of bespoke items, e.g. multi-camera setups with custom-built computer hardware to capture and manipulate a scene in three dimensions in real time.

- *Multiple bespoke*: The equipment is state-of-the-art in research and technology across several different fields, is difficult to obtain commercially and often consists of bespoke items, e.g. multi-camera setups with custom-built computer hardware to capture and manipulate a scene in three dimensions in real time and hardware to manipulate network traffic.

It should be noted at this point that assurance levels for different categories of ID procedures are not directly comparable, even though the same ID document is used. A video identification procedure, for example, can only reach the assurance level "normal" due to the possibility of introducing pre-produced material, but a procedure based on electronic identification ("electronic" category) can reach the assurance level "high". The same ID document can be used in both cases.

Deviations from this procedure are possible; these are then to be detailed in the analysis.

3.2.6 An exchange of the presented ID document or the person to be identified during the check is detected

As a kind of special case, this section is closely related to the requirements on physical manipulations of biometric characteristics of the person to be identified (section 3.2.3) or on the ID document (section 3.2.4). The assessment is carried out according to [CEM], see section 2.3.

A2.6-1

Checking criterion description: What assurance level does the ID procedure in question have in terms of attack potential in order to carry out an undetected exchange of the ID document presented or of the person to be identified during the check?

Explanation/note: In this case, an assessment as described in section 2.3 is to be carried out.

N/A: Only possible with direct or electronic ID procedures.

Expertise

For ID procedures in the "indirect" category, the relevant expertise is to be expected mainly in the field of the necessary knowledge about the functioning, production and integration of the security features used insofar as an exchange of the presented document is under consideration. The instructions in sections 3.2.3 and 3.2.5 can be used if the person to be identified is exchanged during the check. For ID procedures in the "electronic" category, expertise in the areas of cryptography and IT security is important, among other things.

Examples of classification in the use of audiovisual transmission channels in ID procedures in the "indirect" category are:

- *Layperson*: The attacker has basic knowledge of installing and operating software, e.g. for video tampering.
- *Proficent*: The attacker requires in-depth knowledge in the area in question, e.g. about the use of video editing software or the unnoticed injection of a manipulated data stream for use in the ID procedure software.
- *Expert*: The attacker requires expert knowledge of the latest research and technology beyond the use of available video editing software.
- *Multiple experts*: The attacker requires expert knowledge of the latest research and technology in several areas, e.g. in the field of real-time video processing and at the same time in the field of software reverse engineering in order to be able to manipulate the software of the ID procedure during runtime.

Insider knowledge

For ID procedures in the "indirect" category, knowledge about the process parameters of production machines as well as material properties and compositions (e.g. of paper, printing ink, bindings) are examples of relevant insider knowledge insofar as an exchange of the presented document is under consideration. The instructions in sections 3.2.3 and 3.2.5 can be used if the person to be identified is exchanged during the check. For ID procedures in the "electronic" category, insider knowledge of hardware and software development is usually particularly relevant.

Examples of classification in the use of audiovisual transmission channels in ID procedures in the "indirect" category are:

- *Public*: The necessary information is publicly available, e.g. on the internet.
- *Restricted*: The necessary information is held by the manufacturer and is only passed on to third parties, for example, under a non-disclosure agreement.
- *Sensitive*: The necessary information is only accessible to specific teams and employees of the manufacturer on a limited basis.
- *Critical*: The necessary information is only accessible to a very limited and explicitly authorised group of people.

Windows of opportunity

For ID procedures in the "indirect" category, examples of windows of opportunity are access to required original production and personalisation machines or access to required raw and auxiliary materials or pre-produced blank documents insofar as an exchange of the presented document is under consideration. An alternative is the possibility of exchanging the ID document by means of a (manipulated) ID document of another person. The instructions in sections 3.2.3 and 3.2.5 can be used if the person to be identified is exchanged during the check. For ID procedures in the "electronic" category, favourable windows of opportunity in the event of software attacks are, for example, access to possibly stolen cryptographic key material or to the source code of the software used.

Examples of classification in the use of audiovisual transmission channels in ID procedures in the "indirect" category are given below. This involves assessing what level of detail of records or other information about possible variants and sequences is required to carry out a successful attack by exchanging the person or ID document.

- *Unnecessary/unlimited access*: The process of the ID procedure is known in principle, e.g. which category (direct, indirect, electronic) is involved, which ID documents are permitted.
- *Easy*: The main features of the ID procedure is known, e.g. which security features there are.
- *Moderate:* The process of the ID procedure is known in detail, e.g. which security features are checked.
- *Difficult*: The process of the ID procedure is fully known, e.g. the exact process of decision-making for all possible cases including the time schedule is known. The exact instructions to the inspector are known.

Equipment

For ID procedures in the "indirect" category, for example, techniques that do not reveal manipulation of the ID document used for exchange via the communication channel are to be considered, provided that an exchange of the presented document is under consideration. The instructions in sections 3.2.3 and 3.2.5 can be used if the person to be identified is exchanged during the check. For ID procedures in the "electronic" category, for example, the exchange of the ID card used is to be considered. In this case, such an exchange could also be made by redirecting the communication path via another card reader to another ID card.

Examples of classification in the use of audiovisual transmission channels in ID procedures in the "indirect" category are:

- *Standard*: Equipment is available directly from specialist retailers, e.g. PCs, cameras, standard software, adapters.
- *Specialised*: Although the equipment is available directly from specialist retailers, it has been expertly customised, e.g. arrays of graphics cards, expert integration and configuration of multiple software components.
- *Bespoke*: The equipment is state-of-the-art in research and technology, is difficult to obtain commercially and often consists of bespoke items, e.g. multi-camera setups with custom-built computer hardware to capture and manipulate a scene in three dimensions in real time.
- *Multiple bespoke*: The equipment is state-of-the-art in research and technology across several different fields, is difficult to obtain commercially and often consists of bespoke items, e.g. multi-camera setups with custom-built computer hardware to capture and manipulate a scene in three dimensions in real time and hardware to manipulate network traffic.

It should be noted at this point that assurance levels for different categories of ID procedures are not directly comparable, even though the same ID document is used. For example, an ID document can reach the assurance level "high" for an ID procedure in the "indirect" category due to numerous very high-quality security features (e.g. kinetic images, guilloches, special printing ink), because an exchange of the ID document during the check also counters attacks with the attack potential "high", but only the assurance level "normal" for a procedure based on electronic identification (category "electronic") due to a known implementation error of the cryptographic functionality.

Deviations from this procedure are possible; these are then to be detailed in the analysis.

3.2.7 Simultaneous manipulation of biometric characteristics of the person to be identified and corresponding reference data on the ID document is detected

According to [TR-03147], section 5.2.7 an additional requirement is that the simultaneous manipulation of the biometric feature of the person to be identified and corresponding reference data on the ID document is detected. This is covered by checking the requirements in sections 3.2.3 and 3.2.4 and is therefore not a separate point in [PBV].

3.3 Checking of ID proofs

The following requirements for the ID procedure refer to the checking methods defined for an ID proof, whereby validity is to be checked in addition to authenticity. The minimum principle is to be applied across all relevant combinations of ID proof and permitted checking method. In principle, a physical or digital security feature is sufficient for a check. Generally, however, checking several, preferably complementary, features increases the effort required for a successful attack.

Due to the widespread use of document checking devices at border controls, extensive operational experience is available on their suitability. With the intended use of suitable document checking device, it is possible to achieve the assurance level "high" for this partial aspect of identity verification. Taking photographs of the document under constant and controlled conditions provides a defined data base for image processing and document check algorithms. For example, it is also possible to check for alterations to the photograph by checking corresponding security features in these areas. The document checking devices can also use hidden security features, i.e. those that are not visible in white light, to assess authenticity. Nevertheless, not all common types of security features can be checked with document checking devices: holographic features, for example, cannot yet be verified in terms of content. Tactile features can also not be checked by means of a document checking device and accordingly cannot be used for the assessment.

Nevertheless, manual inspection of these features is possible on site. On the other hand, there is now a steadily growing number of identity documents worldwide that contain security features specially developed for checking using document checking devices. The integration of such features into identity documents has also been included in the [ICAO9303] standard for the design of travel documents.

When using document checking devices for checking identity documents, the relevant recommendations from [TR-03135-1] and [TR-03135-2] should be taken into account. The minimum requirements for checking at assurance level "substantial" or "high" are, in particular, the following steps:

- Automated creation of photographic images under defined lighting conditions and spectra. Additional use of light spectra that are not available for manual visual inspection in white light without technical aids.
- Identification of the presented document (i.e. issuing country and document type) using a suitable reference database.
- Performing the optical checks individually specified in the reference database for the respective document, e.g. brightness or pattern tests on the basis of the images taken by matching them with the information from a suitable reference database.
- If available, read out and check the electronic chip in the document (incl. the digital signature and the associated certificates).

Unless the document checking device performs a suitable cryptographic check of the authenticity and integrity of the document, it must be taken into account that checking on the basis of optical security features does not provide a clear-cut result in some cases, even when using document checking devices. In such cases, manual assessment can sometimes be carried out by persons with suitable training and sufficient experience as a secondary control authority on the basis of the data recorded by the document checking device. Insofar as the document is not physically available or the necessary technical aids are not available, however, a clear check result is not possible in some cases. In such cases, the identity document must not not be assessed as authentic and genuine with regard to assurance level "substantial" or "high".

3.3.1 Multiple ID proofs

A3.G-1

Checking criterion description: What is the assurance level of the ID proof used for the ID procedure for which the lowest attack potential is sufficient to compromise the ID procedure?

Explanation / note: Insofar as the use of different ID proofs is permitted in an ID procedure, according to the minimum principle, the ID proof permissible for an ID check with the lowest required attack potential determines the overall attack potential necessary. The checking criteria for the requirements under "Checking of ID proofs" shall be applied by the inspector for all ID proofs approved for the ID procedure and the overall result of the requirement is to be determined in accordance with the minimum principle. In other words, the attack potential is determined according to the minimum principle over all permitted ID proofs.

Insofar as it is possible to identify those ID documents with the evidently lowest assurance level, it is sufficient to consider them. Moreover, checking a new generation of an ID document whose security is obviously at least equivalent in all respects to the previous version can be based on the checking of the previous generation. This presupposes in addition that both generations are currently permitted in circulation and in the procedure.

For checking an ID proof, all checking criteria with a checking criterion ID in the form A3.x-y with x and y numbered consecutively, starting with 1, are to be applied.

3.3.2 Type of ID document used can be determined

A3.1-1

Checking criterion description: Can the type of ID document presented for checking be established and verified?

Explanation / note: For example, the type of passport is defined by the tuple (CountryCode, Document Type, ID-Number, Year of first issuance). ID proofs may only be based on an ID document defined as admissible. Therefore, all ID documents accepted in the procedure are to be listed together with the identifiers. For each ID document, it must also be checked and also listed which assurance level can be achieved. For this purpose, sufficiently reliable criteria for an authenticity check and reliable matching with the holder must be defined. These correspond with the information in section 3.1.6 „Security features are known and effectively verifiable“.

- Not fulfilled: The type of ID document cannot be determined or is not checked.
- Normal: The type of ID document can be determined and checked. The check was carried out with the checking depth **document check**.
- Substantial/high: The type of ID document can be determined and checked. The assurance level is not further differentiated at this point. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

3.3.3 ID-Document is valid

A3.2-1

Checking criterion description: Can the validity period of the ID document presented be established and verified?

Explanation / note: The validity of the ID document includes the maximum period of validity and the lost, stolen or revoked report status. In addition to checking the validity date, it is therefore also necessary to request a lost, stolen or revoked report and thus to check whether the ID attributes are up to date. This corresponds with the information in section 3.1.9 „Available lost, stolen or revoked reports are checked“ and section 3.1.8 „ID attributes are up to date“. For checking the lost, stolen or revoked report status, availability and access to corresponding background systems or revocation lists is necessary.

- Not fulfilled: The validity of the ID document cannot be determined or is not checked.
- Normal: The validity date of the ID document is checked. The check was carried out with the checking depth **document check**.
- Substantial: The validity date of the ID document is checked. The check was carried out with the checking depth **implementation check**.
- High: Both validity date and lost, stolen or revoked report status are checked. For checking the lost, stolen or revoked report status, the availability and access to corresponding background systems or revocation lists is required.

3.3.4 Counterfeited security features are detected

This section is closely related to the requirements in section 3.1.5 „Tamper-proof“ and based on this, the actual ID checks performed are the effective measure of the relevant counterfeiting effort or the necessary attack potential. As even one detected counterfeit of a security feature is sufficient for the ID check, the cumulative effort must be assessed to determine the actual necessary attack potential. The assessment is carried out according to [CEM], see section 2.3.

The following assessment of the assurance level of the security features of the ID document under consideration with regard to their awareness and verifiability depends significantly on the category of the ID procedure.

A3.3-1

Checking criterion description: What are the mandatory check requirements for the ID documents that are admissible in the ID procedure?

Explanation / note: The mandatory check requirements for the detection of counterfeited documents (in particular counterfeited security features) correspond to the information in section 3.1.6 „Security features are known and effectively verifiable“ and must be defined and documented for all ID documents authorised in the ID procedure. These include in particular:

- Clear criteria for when ID proof is recognised as authentic and unaltered,
- Tools to be used if necessary, the availability and functionality of which must be ensured,
- Evidence of the ID inspectors' expertise in handling all admissible ID documents and the respective tools to be used,
- Knowledge and consideration of existing and documented "best practices" for the detection of counterfeits and manipulations,
- Sufficient time for all steps of the check.
- The check requirements are to be recorded in the checking report.
- Not fulfilled: Check requirements are not or insufficiently defined and documented.
- Normal/substantial/high: Mandatory check requirements are defined for the ID documents permitted in the ID procedure. In this requirement, the assurance level is not further differentiated. The check was carried out with the checking depth **document check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

Additional information on ID procedures of the category "indirect", such as an identification procedure by means of video transmission, can be found in the Appendix (section 4).

A3.3-2

Checking criterion description: What assurance level does the ID procedure in question have in terms of the potential for attack in order to successfully counterfeit security features in it?

Explanation/note: In this case, an assessment as described in section 2.3 is to be carried out.

Expertise

For ID procedures in the "direct" and "indirect" categories, the relevant expertise is to be expected mainly in the area of physical reproduction of an ID document, including the necessary knowledge about the functioning, production and implementation of the security features used.

Counterfeits that can pass a check using a method in the "indirect" category generally require a lower level of expertise for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, expertise in the areas of cryptography and IT security is important, among other things.

- *Layperson*: All security features of the ID document to be checked can be counterfeited or manipulated by an interested layperson without special knowledge. This would include, for example, the use of a photocopier or a standard commercial printer, the use of image editing software, or manually overwriting or pasting over data and security features.
- *Proficient*: Counterfeit or manipulation of all the security features of the ID document to be checked requires special knowledge that goes well beyond that of an interested layperson. Knowledge about the processing of special types of paper or other substrates, as well as unusual inks and colours are worth mentioning here. Knowledge of how to counterfeit individual security features, such as holograms, can also be included here.
- *Expert*: Counterfeit or manipulation of all the security features of the ID document to be checked requires expert knowledge, for example for the operation of customized machines (lasers, special printing machines) necessary for the counterfeit of the security features and the production of the ID document.
- *Multiple experts*: Counterfeit or manipulation of all the security features of the ID document to be checked requires multiple expert skills that do not complement each other or complement each other only slightly, for example for the operation of several specially made machines that are necessary for the counterfeit of the security features and the production of the ID document.

Insider Knowledge

For ID procedures in the "direct" and "indirect" categories, knowledge about the process parameters of production machines as well as material properties and compositions (e.g. of paper, printing ink, bindings) are examples of relevant insider knowledge.

Counterfeits that can pass a check using a method in the "indirect" category generally require a lower level of insider knowledge for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, insider knowledge of hardware and software development is usually particularly relevant here.

- *Public*: The necessary knowledge relating to the security features to be checked is freely available and/or can be researched with little effort by an interested layperson (e.g. on the internet), e.g. dimensions, font sizes and types of imprints. Knowledge of the security features used on an ID document is not restricted inside knowledge, but is always to be considered as public knowledge. This may also apply to security features that have not been officially disclosed, if there is no guarantee that such features will not become public through unofficial channels.
- *Restricted*: The necessary knowledge related to the security features to be checked is only available to a restricted group of people. Examples include the way in which special types of paper or other substrates are used, as well as unusual inks and colours in printing processes, or the detailed, basic functioning of individual security features.
- *Sensitive*: The necessary knowledge relating to the security features to be checked is only known to the group of persons entrusted with the direct production of the original documents, such as the exact composition of a material used or the exact operating parameters of a specially manufactured machine used.

- *Critical*: The necessary knowledge relating to the security features to be checked is only known to the group of persons entrusted with the direct production of the original documents, such as the exact composition of several materials used or the exact operating parameters of several specially manufactured machines used.

Windows of opportunity

For ID procedures of the "direct" and "indirect" categories, examples of relevant windows of opportunity are access to required original production and personalisation machines or access to raw and auxiliary materials used (in the production chain) or pre-produced blank documents.

Counterfeits that can pass a check using a method in the "indirect" category generally require less favourable windows of opportunity for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, favourable windows of opportunity in the event of software attacks are, for example, access to possibly stolen cryptographic key material or to the source code of the software used. Favourable windows of opportunity in hardware attacks are, for example, access to personalised and non-personalised smart card samples that can be used for identification in the procedure.

- *Unnecessary/unlimited access*: No special windows of opportunity are necessary to counterfeit or manipulate the security features of the ID document to be checked; this is easily possible in normal premises, for example. Access to the required original raw and auxiliary materials for the counterfeit of these security features or blank documents is not subject to any special restrictions.
- *Easy*: Restrictive windows of opportunity are necessary to counterfeit or manipulate the security features of the ID document to be checked. Access to the required original raw and auxiliary materials for forging these security features or even to blank documents is only possible for a restricted group of people.
- *Moderate*: Highly restrictive windows of opportunity are necessary to counterfeit or manipulate the security features of the ID document to be checked, for example, access to machines used to produce the original documents, or lots and/or highly skilled personnel with insider knowledge. Access to the required raw and auxiliary materials for forging these security features or even to blank documents is only possible for a restricted group of persons, and their unauthorised possession is punishable.
- *Difficult*: Multiple highly restrictive windows of opportunity are necessary to counterfeit or manipulate the security features of the ID document to be checked, for example on machines used to produce the original documents and at the same time access to suitable blank documents.

Equipment

For ID procedures in the "direct" and "indirect" categories, printing and other production machines are to be mentioned here. Additionally, necessary raw and auxiliary materials (in any processing stage) may also be relevant.

Counterfeits that can pass a check using a method in the "indirect" category generally require less sophisticated equipment for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, hardware interfaces to the ID document, measurement and IT technology (standard PCs, possibly with special additional hardware, oscilloscopes, spectrum analysers, etc.) are examples of necessary equipment.

- *Standard*: The equipment necessary for counterfeiting or manipulating the security features to be checked can be special, but is available at short notice from specialised dealers at a manageable cost, e.g. standard electronic components, standard PCs and standard software, stamps, tools such as knives, scalpels, special erasers, chemical substances freely available to everyone, such as various adhesives and solvents. An example of additional materials are hologram foils, insofar as they are freely available and at low cost.

- *Specialised*: The equipment necessary for counterfeiting or manipulating the security features to be checked is only available from specialised suppliers at an increased cost, e.g. optical and electronic measurement technology such as oscilloscopes, spectrometers, special PC hardware and software or chemical substances that are not freely available, such as hydrofluoric acid.
- *Bespoke*: The equipment necessary for counterfeiting or manipulating the security features to be checked is highly specialised, and includes at least one possibly adapted, often bespoke device, such as a special printing machine, a laser for optical personalisation or a machine for inserting a kinetic image into the ID document.
- *Multiple bespoke*: The equipment necessary for counterfeiting or manipulating the security features to be checked is highly specialised in several ways, and consists of several possibly adapted, often bespoke devices, such as a special printing machine and a laser for optical personalisation.

It should be noted at this point that assurance levels of ID documents for different categories of ID procedures are not directly comparable with each other (see section 2.2). This applies even if it is the same ID document. For example, an ID document can reach the assurance level "high" for an ID procedure based on a personal check ("direct" category) due to numerous very high-quality security features (e.g. kinetic images, guilloches, special printing ink), but only the assurance level "normal" for a procedure based on electronic identification (category "electronic") due to a known implementation error of the cryptographic functionality.

Deviations from this procedure are possible; these are then to be detailed in the analysis.

Additional information on ID procedures of the category "indirect", such as an identification procedure by means of video transmission, can be found in the Appendix (section 4).

3.3.5 Falsifications of the personalised data is detected

This is a special case of section 3.5.3, in which the minimum principle is applied to the detection of counterfeits or falsification of the ID attributes or combinations of different ID proofs with regard to the determination of the necessary attack potential. For a secure determination of the ID attributes, all recorded and required ID attributes must be unaltered. The assessment is carried out according to [CEM], see section 2.3.

The following assessment of the assurance level of the security features of the ID document under consideration with regard to their awareness and verifiability depends significantly on the category of the ID procedure. The awareness and verifiability of security features of an ID document depends on which category (direct, indirect or electronic) the ID procedure falls into.

A3.4-1

Checking criterion description: Is a consistency check carried out on the various ID attributes?

Explanation / note: In a consistency check, for example, the facial image, date of birth and date of issue must match, or the data from a Machine Readable Zone (MRZ) of an ID document must be consistent and match the other personalised data.

- Not fulfilled: No consistency check or only an incomplete consistency check is carried out.
- Normal: A consistency check is carried out. The check was carried out with the checking depth **document check**.

- Substantial: A consistency check is carried out. The check was carried out with the checking depth **implementation check**.
- High: A consistency check is carried out. The check was carried out with the checking depth **independent tests**.

A3.4-2

Checking criterion description: What assurance level does the ID procedure in question have in terms of attack potential in order to successfully carry out manipulations of personalised data in it?

Explanation/note: In this case, an assessment as described in section 2.3 is to be carried out.

Expertise

For ID procedures in the "direct" and "indirect" categories, the relevant expertise is to be expected mainly in the area of physical reproduction or manipulation of an ID document, including the necessary knowledge about the functioning, production and implementation of the security features used.

Counterfeits that can pass a check using a method in the "indirect" category generally require a lower level of expertise for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, expertise in the areas of cryptography and IT security is important, among other things.

For a secure determination of the ID attributes, it is necessary that each of the collected and required ID attributes are unaltered. An attack is already considered successful as soon as a relevant set of ID attributes has been successfully manipulated. The necessary attack potential must therefore be determined taking into account all ID attributes according to the minimum principle.

- *Layperson*: The personalised ID attributes can be counterfeited or manipulated by an interested layperson without special knowledge. This would include, for example, the use of a photocopier or a standard commercial printer, the use of image editing software, or manually overwriting or pasting over data.
- *Proficient*: Counterfeit or manipulation of the personalised ID attributes requires special knowledge that goes well beyond that of an interested layperson. Knowledge about the processing of special types of paper or other substrates, as well as unusual inks and colours are worth mentioning here. Knowledge of individual security features that are directly related to ID attributes, such as counterfeiting holograms in connection with passport photos, are also to be classified here.
- *Expert*: Counterfeit or manipulation of personalised ID attributes requires expert knowledge, for example for the operation of specially made machines (lasers, special printing machines). For the counterfeit of security features that are directly related to ID attributes, knowledge is necessary for the production of the ID document.
- *Multiple experts*: Counterfeit or manipulation of the personalised ID attributes requires multiple expert skills that do not complement each other or complement each other only slightly, for example for the operation of several specially made machines that are necessary. For the counterfeit of security features that are directly related to ID attributes, knowledge is necessary for the production of the ID document.

Insider knowledge

For ID procedures in the "direct" and "indirect" categories, knowledge about the process parameters of production machines as well as material properties and compositions (e.g. of paper, printing ink, bindings) are examples of relevant insider knowledge.

Counterfeits that can pass a check using a method in the "indirect" category generally require a lower level of insider knowledge for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, insider knowledge of the hardware and software development of the ID documents or procedures under consideration is usually relevant here.

For a secure determination of the ID attributes, it is necessary that each of the collected and required ID attributes are unaltered. An attack is already considered successful as soon as a relevant set of ID attributes has been successfully manipulated. The necessary attack potential must therefore be determined according to the minimum principle.

- *Public*: The necessary knowledge to counterfeit or manipulate ID attributes is freely available and/or can be researched with little effort by an interested layperson (e.g. on the internet), e.g. dimensions, font sizes and types of imprints. Knowledge of the ID attributes used on an ID document is not restricted inside knowledge, but is always to be treated as public knowledge.
- *Restricted*: The necessary knowledge to counterfeit or manipulate ID attributes is only available to a restricted group of people. Examples include the way in which special types of paper or other substrates are used, as well as unusual inks and colours in printing processes.
- *Sensitive*: The necessary knowledge to counterfeit or manipulate ID attributes is only known to the group of people entrusted with the direct production of the original documents, such as the exact composition of a material used or the exact operating parameters of a specially manufactured machine used.
- *Critical*: The necessary knowledge to counterfeit or manipulate ID attributes is only known to the group of people entrusted with the direct production of the original documents, such as the exact composition of several materials used or the exact operating parameters of several highly customised machines used.

Windows of opportunity

For ID procedures in the "direct" and "indirect" categories, examples of windows of opportunity are access to required original production and personalisation machines or access to required original raw and auxiliary materials or pre-produced blank documents.

Counterfeits that can pass a check using a method in the "indirect" category generally require less favourable windows of opportunity for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, favourable windows of opportunity in the event of software attacks are, for example, access to possibly stolen cryptographic key material or to the source code of the software used. Favourable windows of opportunity in hardware attacks are, for example, access to personalised and non-personalised smart card samples that can be used for identification in the procedure.

For a secure determination of the ID attributes, it is necessary that each of the collected and required ID attributes are unaltered. An attack is already considered successful as soon as a relevant set of ID attributes has been successfully manipulated. The necessary attack potential must therefore be determined according to the minimum principle.

- *Unnecessary/unlimited access*: No special windows of opportunity are necessary to counterfeit or manipulate ID attributes; this is easily possible in normal premises, for example. Access to required raw and auxiliary materials or blank documents is not subject to any special restrictions.
- *Easy*: Restrictive windows of opportunity are necessary to counterfeit or manipulate the ID attributes. Access to the required raw and auxiliary materials or even to blank documents is only possible for a restricted group of people.
- *Moderate*: Highly restrictive windows of opportunity are necessary to counterfeit or manipulate ID attributes, for example, access to machines used to produce the original documents, or lots and/or highly skilled personnel with insider knowledge. Access to the required raw and auxiliary materials or even to blank documents is only possible for a restricted group of persons, and their unauthorised possession is punishable.

- *Difficult*: Multiple highly restrictive windows of opportunity are necessary to counterfeit or manipulate ID attributes, for example on machines used to produce the original documents and at the same time access to corresponding blank documents.

Equipment

For ID procedures in the "direct" and "indirect" categories, printing and other production machines are to be mentioned here.

Counterfeits that can pass a check using a method in the "indirect" category generally require less sophisticated equipment for their production than those that can pass inspections using a method in the "direct" category.

For ID procedures in the "electronic" category, hardware interfaces to the ID document, measurement and IT technology (standard PCs, possibly with special additional hardware, oscilloscopes, spectrum analysers, etc.) are examples of necessary equipment.

For a secure determination of the ID attributes, it is necessary that each of the collected and required ID attributes are unaltered. An attack is already considered successful as soon as a relevant set of ID attributes has been successfully manipulated. The necessary attack potential must therefore be determined according to the minimum principle.

- *Standard*: The equipment necessary for counterfeiting or manipulating ID attributes can be special, but is available at short notice from specialised dealers at a manageable cost, e.g. standard electronic components, standard PCs and standard software, stamps, tools such as knives, scalpels, special erasers, chemical substances freely available to everyone, such as various adhesives and solvents.
- *Specialised*: The equipment necessary for counterfeiting or manipulation of ID attributes is only available from specialised suppliers at an increased cost, e.g. optical and electronic measurement technology such as oscilloscopes, spectrometers, special PC hardware and software or chemical substances that are not freely available, such as hydrofluoric acid.
- *Bespoke*: The equipment necessary for counterfeiting or manipulating ID attributes is highly specialised, and includes at least one possibly adapted, often bespoke device, such as a special printing machine or a laser for optical personalisation.
- *Multiple bespoke*: The equipment necessary for counterfeiting or manipulating ID attributes is highly specialised in several ways, and consists of several possibly adapted, often bespoke devices, such as a special printing machine and a laser for optical personalisation.

It should be noted at this point that assurance levels of ID documents for different categories of ID procedures are not directly comparable with each other (see section 2.2). This applies even if it is the same ID document. For example, an ID document can reach the assurance level "high" for an ID procedure based on a personal check ("direct" category) due to numerous very high-quality security features (e.g. kinetic images, guilloches, special printing ink), but only the assurance level "normal" for a procedure based on electronic identification (category "electronic") due to a known implementation error of the cryptographic functionality.

Deviations from this procedure are possible; these are then to be detailed in the analysis.

3.4 Matching of persons with ID proofs

This evaluates the ID attribute match between the person to be identified and the ID document. The concrete evaluation criteria differ depending on the attribute class (possession, knowledge, biometrics), but the common benchmark is the maximum accepted false acceptance rate (see [TR-03147], section 2.3).

3.4.1 Confidential knowledge factors are only communicated to the legitimate holder

A4.1-1

Checking criterion description: What assurance level is achieved by the transmission of the confidential knowledge factor to the legitimate holder?

Explanation/note: The knowledge factor must be transmitted via confidential channels to the legitimate holder. The following conditions apply for reaching the assurance level "normal**"**:

1) Access by unauthorised third parties is effectively prevented ("tamper proof"), or
2) Access by unauthorised third parties is detected in a timely and secure manner ("tamper evident")

An example of the fulfilment of condition 1) is the personal transfer of the knowledge factor by the issuing body. Condition 2) can be fulfilled, for example, by sending a letter by post that clearly indicates unauthorised knowledge ("PIN letter").

For the assurance level **"**substantial**"** to be reached, the knowledge factor must be transferred separately from other ID proof factors (e.g. possession).

To reach the assurance level **"**high**"**, the knowledge factor has to be additionally activated by the owner. An example of this is the activation process for the eID function of an identity card, where a PIN for activation is sent to the legitimate holder. This is used exclusively as authorisation to set another, self-selected PIN when or after the ID document is issued.

If no knowledge factor is used by the ID procedure under consideration, A4.1-1 is to be rated **"N/A"**.

3.4.2 Security of the authentication means used

A4.2-1

Checking criterion description: What assurance level is achieved by the authentication means used?

Explanation/note: All authentication means are classified into one of the categories "possession", "knowledge" and "biometrics".

In order to achieve the assurance level **"normal"** at a minimum, an authentication means that cannot be compromised by an attacker with the attack potential "enhanced basic" is sufficient. The following requirements must also be met:

- **Possession:** The authentication means cannot be copied by a corresponding attacker.
- **Knowledge:** The probability of guessing the knowledge-based authentication means in the maximum available attempts cannot exceed 3 x 10^{-4} (three out of ten thousand). This corresponds to the probability of guessing an unknown four-digit PIN in three attempts. In addition, the inspector shall be guided by the requirements of measure M 2.11 from “IT Grundschutz”. The requirement to change the password at regular intervals is explicitly waived. However, the general possibility to change the password must be given to the user.
- **Biometrics**: The expected false acceptance rate of the authentication means must not be significantly worse than 3 x 10^{-4} (three out of ten thousand). The authentication means must not be used as the sole factor in indirect and electronic ID procedures.

To reach the assurance level **"substantial"**, two independent factors from two different categories mentioned above have to be used. Both must resist an attacker with the attack potential "moderate". In addition, the following requirements must be met:

- **Possession:** The authentication means cannot be copied by a corresponding attacker.
- **Knowledge:** The probability of guessing the knowledge-based authentication means in the maximum available attempts cannot exceed 3 x 10^{-5} (three out of one hundred thousand). This corresponds to the probability of guessing an unknown five-digit PIN in three attempts. If the "knowledge" factor is used together with the "possession" factor, both security factors must be linked, for example when using a PIN to unlock a chip card.
- **Biometrics:** The "false acceptance rate" of the authentication means must not be significantly worse than 3 x 10^{-5} (three out of one hundred thousand).

In order to reach the assurance level **"high"**, the two factors must resist an attacker with attack potential "high". In addition, the following requirements must be met:

- **Possession:** The authentication means cannot be copied by a corresponding attacker.
- **Knowledge:** The probability of guessing the knowledge-based authentication means in the maximum available attempts cannot exceed 3 x 10^{-6} (three out of one million). This corresponds to the probability of guessing an unknown six-digit PIN in three attempts.
- **Biometrics**: The "false acceptance rate" of the authentication means must not be significantly worse than 3 x 10^{-6} (three out of one million).

If several authentication means are used in an ID procedure, the assurance level must first be determined for each individual authentication means. Criterion A4.2-1 is then to be assessed according to the lowest of these individual assurance levels. This assessment is to be outlined in the analysis.

3.4.3 The actual control of the person to be identified over the ID document is ensured

A4.3-1

Checking criterion description: Does the person to be identified have actual control of their ID document during the ID procedure?

Explanation/note: For the assurance levels "substantial" and "high" this criterion has to be fulfilled, for the assurance level "normal" this is not necessary.

The check was carried out with the checking depth **implementation check**.

For example, criterion A4.3-1 is met if the person to be identified presents the ID document in person and independently. Also if, for example, a PIN (knowledge factor) is checked on a chip card itself (possession factor), A4.3-1 is considered to be fulfilled.

3.4.4 ID attributes to be matched are captured in sufficient quality

A distinction is made in the following requirements between the enrolment and the capture process in the ID procedure, because when a person is enrolled in the biometric system for the first time, the captured ID attributes are used to generate the associated reference data. In particular, low quality in enrolment has a negative impact on FMR in subsequent capture processes, even though the quality of capture in the ID procedure itself is sufficiently good.

A4.4-1

Checking criterion description: What is the assurance level in the quality of the capture of the biometric or behavioural ID attributes to be matched at enrolment (initial registration of a person in the biometric system), where the capture of the ID attributes for the generation of the reference data takes place?

Explanation/note: The amount of data and thus the possible quality of capturing biometric ID attributes is limited in principle. This usually results in a false acceptance rate for the corresponding feature when subsequently matched with the ID document holders. This false acceptance rate results in the assurance level of criterion A4.4-1 according to the quantitative specifications from criterion A4.2-1.

The quality of the capture is to be checked here during enrolment. In other words, check the system used to capture the ID attributes to generate the reference data.

The quantification of the false acceptance rate in the analysis should be based on statistical evaluations, or at least made plausible.

A4.4-2

Checking criterion description: What is the assurance level in the quality of the capture of the biometric or behavioural ID attributes to be matched in the capture process where the ID attributes are captured as part of the ID procedure?

Explanation/note: The amount of data and thus the possible quality of capturing biometric ID attributes is limited in principle. This usually results in a false acceptance rate for the corresponding feature when subsequently matched with the ID document holders. This false acceptance rate results in the assurance level of criterion A4.4-1 according to the quantitative specifications from criterion A4.2-1.

The quality of the capture is to be checked here during the capture process. In other words, the system used to capture the ID attributes in the ID procedure is to be checked.

The quantification of the false acceptance rate in the analysis should be based on statistical data, or at least made plausible.

3.4.5 Reliable matching of relevant biometric ID attributes between ID document and person to be identified

A4.5-1

Checking criterion description: What assurance level do the biometric methods used by the ID procedure achieve?

Explanation/note: The assurance level of criterion A4.5-1 is determined by the expected false acceptance rate according to the quantitative specifications of criterion A4.2-1, as well as the protection of the matching process of the ID procedure against attackers with corresponding attack potential, also according to the specifications of criterion A4.2-1.

In the case of different biometric procedures as well as in the case of different achieved assurance levels due to the associated false acceptance rate and protection against attacks, the lowest achieved assurance level shall be decisive for the assessment of criterion A4.5-1.

If no biometric ID attributes are used in the ID procedure, then criterion A4.5-1 is to be assessed as **"N/A"**.

3.5 Correct capture of the required ID attributes

The following requirements primarily cover the internal quality aspect. Additional ID attributes can also be used which are not relevant for the actual ID check process (e.g. e-mail address, telephone number, IBAN, ...).

3.5.1 ID attributes to be captured allow for unique identification

A5.1-1

Checking criterion description: Is unique identification possible with the captured ID attributes?

Explanation / note: If unique identification is required within the scope of the application, then the capture system must prevent a new identity from being created even though an entry with identical ID attributes already exists.

Within the relevant context, a unique representation of each registered person is often required. This can be a strict requirement, i.e. each identity, defined by the tuple of all ID attributes collected, must be unique or, in a weakened form, the combination of ID attributes should most likely ensure uniqueness. Depending on the application, the ID attributes should also uniquely identify the referenced person outside the respective application context.

While the patterns of biometric characteristics, which are usually unchangeable (e.g. fingerprints, vein patterns, iris patterns) or at least change only very slowly (e.g. facial image), are well suited for distinguishing between different persons and for matching persons and ID proofs, they are often not very suitable for a "meaningful" description of a unique identity. A suitable set of ID attributes for globally unique identification is, for example, "Commission Implementing Regulation (EU) 2015/1501, Annex 'Requirements concerning the minimum set of person identification data uniquely representing a natural or legal person'".

- N/A: The application does not require uniqueness
- Not fulfilled: The application requires uniqueness, but this is not guaranteed or only insufficiently guaranteed.
- Normal: Unique identification is possible with the captured ID attributes. The check was carried out with the checking depth **document check**.
- Substantial/high: Unique identification is possible with the captured ID attributes. In this requirement, the assurance level is not further differentiated. The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

3.5.2 Specific expertise of the inspectors and tools to be used, if any, are available

A5.2-1

Checking criterion description: Is there proof of competence for the personnel involved in the interpretation and capture of ID attributes for all ID proofs?

Explanation / note: Personnel relevant to this requirement include, in particular, ID inspectors as well as those involved in the interpretation and capturing of ID attributes.

- Normal: There are no specific requirements for achieving the assurance level "normal" according to [TR-03147], section 8.2.2. For example, proof of expertise is not available for all persons or ID proofs involved in the interpretation and capture of ID attributes. It is also possible that the proof is only "insufficient". The check was carried out with the checking depth **document check**.

- Substantial/high: Sufficient proof of competence is available for the personnel involved in the interpretation and capture of the ID attributes. This includes all ID attributes in question. This requirement does not distinguish between "substantial" and "high". The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

A5.2-2

Checking criterion description: Are the intended tools always available for the ID attribute capture process?

Explanation / note: Designated tools must always be available for capturing processes. A description of the guarantee for this is to be provided. For the assurance levels **"**substantial**"** and **"**high**"** this criterion has to be fulfilled, for the assurance level **"**normal**"** this is not necessary.

- Substantial/high: Designated tools are always available. This requirement does not distinguish between "substantial" and "high". The check was carried out with the checking depth **implementation check** (in contrast to the standard procedure according to section 1.2 „Assurance level and checking depth“).

3.5.3 ID attributes are transferred to the capture system in full and without errors

A5.3-1

Checking criterion description: What measures are in place to ensure the complete and error-free transfer of ID attributes into the capture system (system for capturing ID attributes)?

Explanation / note: In order to avoid accidental errors when capturing ID attributes, in particular spelling or typing errors, the data can, for example, be entered several times or the captured data can be checked and confirmed by a second person (possibly also by the person to be identified themselves).

- Not fulfilled: The capture system is not technically capable of capturing the ID attributes completely or accurately.
- Normal: The capture system is technically suitable for recording the ID attributes completely and without errors. The check was carried out with the checking depth **document check**.
- Substantial: The capture system is technically suitable for recording the ID attributes completely and without errors. The check was carried out with the checking depth **implementation check**.
- High: The capture system is technically suitable for recording the ID attributes completely and without errors. The check was carried out with the checking depth **independent tests**.

A5.3-2

Checking criterion description: Is the capture system technically capable of capturing all relevant ID attributes completely and accurately?

Explanation / note: The system for capturing the ID attributes must be able to record and manage them completely and in an accurate form. The checking criterion assesses whether the capture system is technically suitable to capture all relevant attributes completely and accurately. In contrast, the checking criterion assesses the extent to which an error-free transfer of data into the capture system is supported by technical and organisational measures.

- Not fulfilled: The capture system cannot fully or accurately capture the ID attributes.
- Normal: The capture system can fully and accurately capture the ID attributes. The check was carried out with the checking depth **document check**.

- Substantial: The capture system can fully and accurately capture the ID attributes. The check was carried out with the checking depth **implementation check**.
- High: The capture system can fully and accurately capture the ID attributes. The check was carried out with the checking depth **independent tests**.

3.5.4 Captured data is checked for timeliness, consistency and plausibility

A5.4-1

Checking criterion description: Is a check of the ID attributes for consistency and plausibility carried out?

Explanation / note: Consistency and plausibility checks can include, for example, checking the address given or the plausibility of the date of birth (possibly in connection with available biometric data). For the assurance levels "substantial" and "high" this criterion has to be fulfilled, for the assurance level "normal" this is not necessary.

- Substantial: A comprehensive consistency and plausibility check is carried out. The check was carried out with the checking depth **implementation check**.
- High: A comprehensive consistency and plausibility check is carried out. The check was carried out with the checking depth **independent tests**.

A5.4-2

Checking criterion description: Is the ID check aborted for open mandatory fields during capture?

Explanation / note: The ID check shall not be evaluated as successful if not all predefined mandatory fields for the ID attributes can be captured. For the assurance levels "substantial" and "high" this criterion has to be fulfilled, for the assurance level "normal" this is not necessary.

- Substantial: The ID check is aborted for open mandatory fields during capture. The check was carried out with the checking depth **implementation check**.
- High: The ID check is aborted for open mandatory fields during capture. The check was carried out with the checking depth **independent tests**.

A5.4-3

Checking criterion description: What is the assurance level of the ID attribute check for timeliness, consistency and plausibility when capturing these attributes?

Explanation / note: To the extent possible, the ID attributes are to be checked for timeliness at the time of capture. This corresponds with the information in section 3.1.8 „ID attributes are up to date“. For the assurance levels "substantial" and "high" this criterion has to be fulfilled, for the assurance level "normal" this is not necessary.

- N/A: A check for timeliness is not possible.
- Substantial: The ID attributes are checked for timeliness at the time of capture. The check was carried out with the checking depth **implementation check**.
- High: The ID attributes are checked for timeliness at the time of capture. The check was carried out with the checking depth **independent tests**.

3.6 Ensuring the integrity of the processes

In accordance with [TR-03147] this section considers the overarching cross-sectional task of ensuring organisational compliance with the defined measures throughout. Moreover, requirements are defined that are intended to protect against intentional manipulation by internal and external perpetrators and that are not based on manipulated or misused ID proofs. The technical and organisational measures necessary for this must be appropriate to the respective assurance level of the ID checks.

3.6.1 Compliance with the prescribed checking criteria is ensured

A6.1-1

Checking criterion description: Is compliance with the ID checking criteria ensured by technical and organisational measures or a combination thereof?

Explanation / note: Examples of technical and organisational measures are:

- Implementation of access controls to buildings, and if necessary, rooms and properties.
- Realisation of access controls to technical systems.
- Application of appropriate access controls and definition of access rights.
- Definition of roles, their authorisations and determination of mutually exclusive roles as well as appropriate assignment to operating persons.
- Logging and archiving procedures.

The measures may include requirements that all successful ID-checks have to be transparently documented.

The assurance level assessment is based on the opportunities for an inside or outside perpetrator to carry out a successful attack that was not detected in time without tampering with or abusing an ID proof. The assessment can be carried out on the basis of the technical organisational measures in accordance with the requirements for an ISMS, see also A6.2-1. Likewise, the information in section 2.3 on the criteria expertise, insider knowledge, windows of opportunity and equipment can be applied for the assessment.

A6.1-2

Checking criterion description: Are the security features to be checked for each ID document defined?

Explanation / note: Based on the definition of security features according to the requirement "Trustworthy ID Documents". With the definition of the security features to be checked for each ID document, their verification must also be determined. It is **not** necessary to check whether the security features to be checked include all the security features of an ID document.

- Not fulfilled: The security features to be checked for each ID document and their verification are not sufficiently defined.
- Normal: The security features to be checked for each ID document are clearly defined. The specifications for verification are indicated at least by examples.
- Substantial/high: The security features to be checked for each ID document are clearly defined. The verification specifications establish well-defined criteria for all security features regarding when the check of a security feature can be considered successful or when it has to be rejected.

A6.1-3

Checking criterion description: What is the assurance level for updating the definitions of the security features to be checked?

Explanation / note: At regular intervals, the definition of security features to be checked must be verified and, if necessary, updated. The time interval of the check is to be indicated.

- Not fulfilled: No check is carried out, or a regular check is carried out with a cycle that exceeds three years.
- Normal: A check is carried out on an ad hoc basis, but at least every three years.
- Substantial: A check is carried out on an ad hoc basis, but at least annually.
- High: A check is carried out on an ad hoc basis, but at least every 6 months.

A6.1-4

Checking criterion description: What is the assurance level of the expertise and trustworthiness of the personnel assigned to manually performed checking steps?

Explanation / note: The appropriate expertise and trustworthiness of the personnel employed must be ensured when conducting an ID procedure. The following classifications are made:

- Not fulfilled: The criterion for the assurance level normal is not met.
- Normal: The assigned personnel have written documentation or work instructions and at least one introductory training session has taken place.
- Substantial: The assigned personnel have written documentation or work instructions and an introductory training as well as recurrent trainings take place, which are to be carried out on an ad hoc basis, but at least once a year. Proof of the trustworthiness of the staff employed is provided in the form of a criminal record or equivalent.
- High: The assigned personnel have written documentation or work instructions and an introductory training as well as recurrent trainings take place, which must be carried out as required, but at least every six months and when the need arises. As proof of the trustworthiness of the staff employed, a criminal record and proof of creditworthiness (e.g. "Schufa information") or equivalent proof is available.

A6.1-5

Checking criterion description: What is the overall assurance level of the ID procedure in question with regard to whether compliance with the required checking criteria is ensured, taking into account points A6.1-1 to A6.1-4?

Explanation / note: The overall assurance level is determined by the lowest assurance level assigned in checking criteria A6.1-1 to A6.1-4.

3.6.2 ISMS

A6.2-1

Checking criterion description: Is an ISMS according to ISO / IEC 27001 [ISO 27001] or equivalent implemented for the generic assurance of the integrity of the processes, which covers all IT components and IT processes used for identity verification or storage or transmission of data collected in this process?

Explanation / note: It must be checked whether an ISMS that meets the requirements has been defined and whether the specifications contained therein are also complied with. Appropriate sampling is to be selected, if necessary, to ensure compliance. Moreover, it must be checked whether the ISMS is complete, in the sense that all IT components and all IT processes are captured that are also used for identity verification or storage or transmission of data captured in this way.

The assessment of the assurance level is based on the following information:

- Not fulfilled: The criterion for the assurance level "normal" is not met.
- Normal:
  - The ISMS meets the requirements of the cited standards or is equivalent to them, and
  - all IT components and IT processes used for identity verification or the storage or transmission of data collected in the process are captured.
- Substantial:
  - The ISMS meets the requirements of the cited standards or is equivalent to them, and
  - all IT components and IT processes used for identity verification or the storage or transmission of data collected in the process are captured and
  - the effectiveness of the defined and implemented security measures correspond to the assurance level "substantial".
- High:
  - The ISMS meets the requirements of the cited standards or is equivalent to them, and
  - all IT components and IT processes used for identity verification or the storage or transmission of data collected in the process are captured and
  - the effectiveness of the defined and implemented security measures correspond to the assurance level "high".

3.7 Global attack scenarios

A7.G-1

Checking criterion description: What is the minimum assurance level for the entire ID procedure resulting from the assessment of the attack potential of global attack scenarios?

Explanation / note:

In the previous sections, attack scenarios for different aspects of the ID procedure were considered and the corresponding attack potential or assurance level was determined. This initially only provides an assessment for a specific area or aspect of the ID procedure. This allows for a basic classification of the assurance level. In addition to these partial considerations, "global" attack scenarios are developed for the ID procedure in its entirety, i.e. including several or even all processes and system components. The findings and assessments that are already available for the partial aspects can be used as a basis. For example, components with the lowest assurance level in the partial considerations can be given special focus in the development of a global attack scenario.

For each global attack scenario developed, the attack potential is determined according to Appendix B.4 of the [CEM] and according to section 2.3 the assurance level. The attack scenario is to be described and the assessment documented.

The result for this checking criterion is the minimum of all assurance levels established for the global attack scenarios.

It should be noted that the findings from the consideration of the global attack scenarios may also have repercussions on the partial considerations in the preceding sections.

4 Appendix: Video-based Examination of Identity Documents

***Acknowledgement**: The results on video-based examination of physical documents presented in this text are from a study conducted at the German Federal Criminal Police Office (Bundeskriminalamt, BKA), KT54 – Questioned Documents, ID-Systems.*

In the case of ID procedures in the "indirect" category, such as video-based identification, the effective verifiability of optical security features of sovereign ID documents, and thus also the achievable level of assurance of the ID procedure, can vary considerably. This appendix describes the possibilities and limitations of detecting counterfeit or falsified ID documents using a video transmission. Additional attack vectors, relevant for the evaluation of an overall level of assurance for a video-based identification procedure, like the comparison of the ID document with the person to be identified or digital manipulations, are out-of-scope of this appendix.

Amongst others, the following factors have a particular relevance for an effective verifiability of optical security features of ID documents:

- Recording conditions (light sources, illumination and viewing geometry) in the proximity of the ID document to be checked.
- Properties of the device used in the identification (resolution, photosensitivity, lens and camera quality).
- Optical focusing of the camera of the video or photo recordings.
- Availability of reference material of authentic documents for comparison with the ID document presented for identification.
- Video bandwidth for the transmission of the live stream (and thus the effectively available resolution).
- Time available for inspection.

Due to inherent technical limitations, not all security features integrated inside an ID document can be checked by video transmission. For this reason, this appendix is limited to the security features that can be inspected within the visible light spectrum and are therefore in principle accessible for inspection by video transmission. These security features are:

1. Copy protection:
   - Diffractive optically variable image devices (also called "DOVID" or "hologram"):
   - Secondary facial image of the holder
   - 3D hologram
   - Kinematic structures
   - Asymmetric effects
   - 3D lens or relief effects
   - Achromatic structures
   - Zero-order structures
   - Retroreflective elements
2. Personalization technique:
   - Variable Laser Image
   - Integration technique and typeface of biographical data
   - Laser engraving, tactile elements

3. Material:
   - Windows
   - Security thread inside plastic card ID documents
   - Embossing
   - Optically variable ink (OVI)
4. Security printing:
   - Microprint
   - Guilloche/ fine line pattern
   - Rainbow colouring

Since checks for authenticity are always based on a comparison between reference material and the document in question, both the reference material and the photographs or video recordings must be of sufficient resolution and quality. The reference material must meet the following requirements:

- Adequate description of the security features present in the document. This should include the different DOVID effects as well as naming the positions of the existing security features.
- Sufficient number of shots/images at different tilt angles to obtain a complete picture of the dynamic effects contained in the DOVID.
- Sufficiently high resolution of the images to reliably detect relevant, static details such as microprinting, nuances of motifs and relative positions of individual image elements to each other.

4.1 Copy protection

4.1.1 Diffractive optically variable image devices (DOVIDs)

Basically, diffractive optically variable image devices (DOVIDs) can be utilized in ID documents in various forms. Besides different feature types, which can be ascribed to the specific properties of the implemented optical diffraction grating, further distinctions can be made with regard to the implementation and integration of DOVIDs into the document. Essentially, the distinctions between metallized and transparent DOVIDs are relevant here.

- Metallized DOVIDs: These include DOVID structures that have a thin, opaque metal layer as a basis and thus exhibit very intense colour effects.
- Transparent DOVIDs: Due to a lacking metal layer, they are transparent under certain tilt angles and allow the underlying printed structures to be seen. The intensity of the effects observed is typically somewhat lower compared to metallized DOVIDs. The Identigram in German ID documents is a specific form of a transparent DOVID, since here only a single colour can be observed for each design element.

In the following, general properties and characteristics of DOVIDs are discussed, which in principle have to be considered for all effects and feature types as well as all implementation types. Subsequently, the individual effects are discussed in more detail.

4.1.1.1 General properties (independent of the particular element/feature)

The essential general characteristics of DOVIDs are:

- In the case of the frequently present chromatic effects, the motifs pass through the visible spectral range (i.e. rainbow colours) when the document is tilted, with the exception of the Identigram (German ID documents). Here, the strongest intensity of the reconstruction is showing exactly one single colour (green, red or blue, depending on the motif).

- The motifs are observed in the 1st diffraction order (i.e. not in direct reflection of the light source).
- The DOVID shows a discrete on/off behaviour, i.e. motifs can be faded in and out by tilting the document.
- Partially-metallized DOVIDs: The de-metallized areas are often designed as a stand-alone (non-reconstructive) motif that can be checked for consistency using appropriate reference material.

The motifs are observable in the 1st diffraction order, which means that the ID document must be tilted slightly relative to the angles for direct reflection of the light source in the ID document. When using a diffuse light source, it is inherently not possible to verify with certainty that it is indeed the 1st diffraction order, since there is no information about the direction of the incident light. However, the use of a device-internal light source in video-based identification can in principle create defined conditions that allow the inspection of this property.

The on/off behaviour as well as the check for reconstruction in the 1st diffraction order can generally be evaluated best by means of video recordings, since here the appearance or disappearance of the features can be observed directly. However, at least the on/off behaviour can also be visualized by taking at least two different photos with suitable illumination and viewing configurations.

Metallized DOVIDs are characterized by a high reconstruction intensity, which is why the effects are observable under most illumination conditions. In the case of partially-metallized DOVIDs, in addition to the DOVID effects themselves described in the following sections, (detailed) reference checks of the motif of the de-metallized area can also be done. In order to be able to perform such a reference check properly, high-resolution and well-focused photo recordings as well as sufficiently detailed reference images of the de-metallized areas are indispensable.

Checking transparent DOVIDs under diffuse illumination conditions may be difficult or impossible due to low reconstruction intensity.

In contrast to other types of DOVID, the diffraction conditions of the Identigram allow only a single colour for each of its design elements, i.e., the secondary facial image of the holder, for example appears exclusively in green colour. In practice, however – depending on the configuration of illumination and viewing angle, factors such as distance as well as divergence and intensity of the light source, especially for point light sources such as spotlights and device-internal light sources – also rainbow colours instead of a single colour can sometimes be observed for genuine documents. Due to high intensities of the incident light, the diffraction image can also be strongly over-illuminated and make it difficult to recognize a defined colour. Therefore, proper verification for this characteristic of the Identigram requires sufficient expertise with regard to how to check this feature.

4.1.1.2 Identigram: Secondary facial image

The secondary facial image of the holder inside the Identigram represents a special characteristic among the diffractive structures, since holographic security features usually contain only generic but no personalised information of the document holder. The reconstruction intensity of the secondary facial image has its highest intensity within the green spectral range.

By integrating the secondary facial image directly besides the primary facial image of the document holder, a comparison of the two images on the ID document is possible. For this purpose, the light source must be far enough away from the ID document, or the light source must be sufficiently extended, in order to be able to compare a simultaneous reconstruction of the complete image instead of only a limited area. Especially when using only the internal light source of a smartphone or webcam, the verification of the matching can be strongly hampered due to the sometimes very small reconstruction area. In addition, the secondary facial image may be so strongly over-illuminated by an intense light source so that details of this feature that are crucial for detecting counterfeits cannot be recognized.

4.1.1.3 Identigram: 3D hologram (representing the German ‘federal eagle’ symbol)

The Identigram contains a holographic representation of a 3D model of the “federal eagle” (German: Bundesadler), which can be observed in red as the most intensive colour. The hologram of the federal eagle appears as floating slightly above the document.

With the exception of diffuse lighting conditions, the 3D effect of the motif is well recognizable, particularly in video recordings. Detailed motif matching requires both sufficiently detailed reference material and high-resolution and focused snapshots or photo recordings of the federal eagle motif during the inspection process.

4.1.1.4 Kinematic structures

These are DOVID structures that show dynamic motifs when passing through different tilt angles. The following forms can be found on numerous ID documents:

- "Pump" effects (e.g. enlargement/shrinking of a letter or motif during tilting)
- Transformations (e.g. transition of a letter to a geometric form (e.g. hexagon) with typically 4 to 10 intermediate stages)
- "Movements" of a motif from one position on the document to another
- Sequence of different motifs at defined tilt angles relative to a stationary light source

For proper authenticity checks of kinematic DOVID motifs, knowledge of the motifs present on a genuine document is absolutely essential. On one hand, this comprises the reconstruction sequence along a specific tilting direction, and on the other hand, the motif details with regard to contour behaviour, filled areas, lettering, and relative positions of the individual DOVID motifs to each other. Therefore, the verifiability of the kinematic features is decisively determined by the availability and proper usage of adequately detailed reference material. Directional light sources, such as spotlights or device-internal light sources, are therefore well suited for verifying these features – in particular the dynamic properties – whereas diffuse lighting conditions hamper the verification of kinematic structures. In addition, well-focused, high-resolution photo recordings are required for detailed matching of the motifs; the resolution of video recordings is usually insufficient for this aspect.

4.1.1.5 Asymmetric effects

These are DOVID structures that show different motifs when rotated 180° within the plane of the document. In the above effects considered so far, an identical motif can be observed with this type of rotation. Due to the technologically high threshold for the production of asymmetrical effects, these effects provide a highly informative value with regard to the authenticity of the document if properly examined.

For the proper verification of this effect – assuming a single light source in the room – the ID document must first be placed so that one of the expected DOVID motifs of the asymmetric effect is visible. Then the ID document is rotated by 180°. In doing so, it is essential to maintain the relative position between the camera and the light source. It is therefore recommended to place the ID document on a solid surface and rotate it by 180°. The feature is then verified by checking for the presence of the motif expected at a rotation by 180°. This change can be implemented for example as a contrast reversal; alternatively, completely different motifs can be visible for each configuration. In this case, a proper check must consider not only the presence of the motif to be expected in each case, but also the absence of the motif not to be expected.

The presence of several light sources in the room can seriously affect the verifiability of this feature. Under the least favourable arrangement of light sources, the reconstructions of the expected motifs of both configurations (rotation 0° and 180°) may overlap and be visible simultaneously. This may suggest that the feature is symmetrical, which would be indicative of a mismatch. Therefore, checking this feature requires sufficient experience of the examiner and knowledge of the number and positions of light sources in space relative to the document. In addition, this effect and the expected motifs are often not described in reference databases.

4.1.1.6 3D-lens or relief effect

3D-lens or relief effects are planar DOVID elements that, however, show a three-dimensional depth or elevation. On one hand, this can be applied to motifs; on the other hand, it can be used to achieve Fresnel lens structures that create the effect of a magnifying glass integrated inside the document. Due to the technologically high threshold for their production, these effects provide a high informative value with regard to the authenticity of the document if properly examined.

3D-lens or relief effects are characterized by the fact that they are usually observable under almost all illumination and viewing geometries (possibly with the exception of diffuse illumination described above). Therefore, no discrete on/off behaviour is to be expected, but merely a continuous change of the observable local intensity distribution during the movement or tilting of the document. In addition, the presence of multiple light sources in the room can improve the visibility of the effect. Due to this property, features with these effects are in principle also easy to verify using a video-stream, since a very precise motion sequence is not required. However, to be able to exclude the possibility that it is a static imitation, the check in the video-based identification procedure should be carried out on the basis of a video or at least two photographs taken at different viewing angles, which are checked for different local intensity distributions and a corresponding 3D-lens or relief effect.

4.1.1.7 Achromatic effects

Achromatic features, in contrast to chromatic effects (rainbow colours), are characterized by colourless light/dark contrasts as well as a larger angular reconstruction range and are also detectable under diffuse illumination conditions. To detect simple counterfeits, the on/off behaviour of the DOVID should always be verified.

Achromatic features provide an enhanced security value in the field of DOVID features, since these features cannot be imitated using easily accessible means. The information on which motifs can be expected to be colourless is often not explicitly listed in the reference databases. However, this knowledge is required for a proper verification of the authenticity of these features.

4.1.1.8 Zero-order structures

Zero-order structures are high-quality security features that offer significant added security value compared to standard 1st diffraction order effects (especially chromatic effects). They are characterized by a well-defined and discrete colour change when the document is rotated 90° in the plane of the document. Usually, this colour change is from red to green (and vice versa) – however, if the combination of viewing and illumination geometry is changed accordingly, changes from blue to a gold-like hue can also be detected in the same structures defined for red-green changes. The colour transition is discrete, i.e. no passing of rainbow colours can be observed when the tilt angle is varied. Moreover, the behaviour of the element is symmetric, i.e. the same colour change can also be observed when rotating by -90°.

Zero-order structures are utilized in transparent DOVIDs and exhibit a sharp on/off behaviour when the document is rotated. In contrast to most holographic features discussed so far, zero-order structures are best checked near the angle of direct reflection (0th diffraction order) of the light source. It should be noted, however, that the device-internal light source needs to be switched off for this check, as this may restrict the verifiability of the feature to such an extent that a reliable statement on authenticity is no longer possible.

4.1.2 Retro-reflective features

Retro-reflective features require quasi-coaxial illumination conditions for a successful inspection, i.e. the light source must be in close proximity to the observer or camera. Usually, light/dark contrasts are observed, although there are now also so-called retro-chromic features that show corresponding colour reflections under quasi-coaxial conditions.

In general, retro-reflective features can be reliably inspected using a mobile device with internal light source switched on if the camera sensor and light source are installed directly next to each other. If a webcam is used, the feature is usually only faintly visible and cannot be reliably inspected. The same also applies to inspecting for motif matching with corresponding reference material. However, due to its low prevalence, this feature only offers a possible benefit for the verification for a relatively small number of types of ID documents.

4.2 Personalization technique

4.2.1 Variable laser images (e.g. MLI, CLI)

Variable laser images are features which, through an integrated lens strip structure, make visible or highlight two different motifs or personalised information (e.g. coat of arms, secondary facial image of the holder, date of birth or expiry) introduced by laser engraving at different tilt angles. Therefore, the personalised information in the variable laser image should be compared with the other personalised information and with the motifs described in the reference material. It is also possible to check the typeface used. If the variable laser image contains a secondary facial image of the holder, a detailed comparison should be made with the primary facial image, since slight differences in details often indicate a falsified document. In particular, for ID documents where the variable laser image is on a different page/side than the primary facial image, a comparison should be made using an image capture of the primary facial image.

As a further indication for the authenticity of the document, the correspondence of the lens structure can be checked, using suitable reference material. This includes matching tilt directions for motif changes as well as the properties of the lens structure itself (width of the individual lens strips) and the contour of the lens strip structure, which can also be implemented as a motif. However, some of these properties can only be reliably checked at correspondingly high resolutions and magnifications.

Using the internal light source of a mobile device can help to check for the presence of a lens structure (increased baseline brightness relative to adjacent background print) and thus detect counterfeited documents without a lens structure. For this purpose, the orientation of the document relative to the direction of incidence of the light source can increase the detectability of the lens structure if the lenses are oriented in parallel to the projection of the direction of incidence of light within the plane of the document.

Additional verification approaches are possible, but require appropriately detailed reference material, knowledgeable personnel, sufficient time for detailed inspection, and sufficient image/video quality to evaluate detailed aspects.

4.2.2 Integration technique and typeface of biographical data

The determination of the printing/integration process of the textual individual information of the document holder (name, date of birth, etc.) is an essential part of the checking of ID documents for authenticity and is carried out on the basis of the (microscopic) examination of the deposition characteristics of the print transfer process.

Recognizing deposition characteristics usually requires photo recordings with high magnifications of the corresponding areas in the ID document. This requires photos using the zoom function and optimal focusing of high-end mobile device cameras. In particular, the second aspect of optimal camera focus cannot be controlled within the setting of a video-based identification process and may additionally be influenced by the lighting conditions. Deposition characteristics are therefore generally not suitable for checking by video stream transmission.

As a further criterion, the typeface used in the document can also be checked. This requires appropriately detailed reference material and, if possible, the presence of identical characters in the reference material and the document in question. While the typeface can be a relevant criterion in the evaluation of centrally issued documents, it should be noted, however, that in the case of decentrally issued documents, deviations can also occur in practice.

4.2.3 Laser engraving, tactile

The tactile laser engraving process provides additional verification criteria compared to the standard laser engraving process. In addition to the blackening of the card material, this process also produces a raised tactile structure on the surface at the same position. In case that the personalization in counterfeits was produced using simpler printing processes, such as ink or laser printing without additional imitation of the tactility, deviations can in principle also be straightforwardly detected by video transmissions on the basis of the optical inspection of tactile laser engraving elements using appropriate illumination and viewing geometry. A prerequisite for this, however, is knowledge of which entries in the real document are made using tactile laser engraving. For ID documents that include tactile entries, the non-tactile laser engraving process is also used in other areas, so that a direct comparison between different entries on the same document is possible.

4.3 Material

4.3.1 Windows

With this security feature, the card body has a defined transparent area (window) so that it is possible to see through the document. Usually, additional security features are embedded inside this window.

The intuitive inspection criterion of the window is the check for transparency. By moving a finger behind the window or moving the document in front of a static, high-contrast background, it is easy to see whether the window area is actually transparent through the entire card body. The best way to do this is to check by video recording. Appropriate reference material should be consulted prior to the check, as only parts of the window feature may be transparent.

Since this criterion does not constitute a high effort threshold for counterfeits, the contour of the window should also be checked for conformity with reference material. The transition between the card body and the window area can also be checked for deviations from the reference material, as authentic documents often have seamless transitions here, while counterfeits often show sharp contours around the window area due to subsequent integration into the card body.

The window itself can also contain other security features such as variable laser image elements, or it can overlap or be interlinked with neighbouring features (e.g. background printing or holographic features). As production of these features is technologically more demanding, the inspection of these features within the window is more meaningful with regard to the authenticity check of the document than the inspection of the respective individual elements alone.

4.3.2 Security thread in solid plastic cards

With this security feature, a security thread is inserted in a defined area of the card body. The security thread can also be personalised with individual information. The first criterion that can be used for checking is the course of the security thread within the card body. Since the security thread is embedded in the card body material, it always ends exactly with the edge of the card. Since the thread is frequently imitated on top of the surface of the card body, this is often not the case with counterfeits.

In the case of a personalised security thread, the type of personalization of the security thread and its appearance (including typeface) can also be compared with information from the reference material. In addition, the content of the personalization can be compared with the personalised data in other areas of the document. It should be noted, however, that checking these characteristics using a video channel may be limited or even impossible due to the limited resolution. Furthermore, data matching with entries on another page or reverse side of the document requires matching between video (or a "snapshot" of it) and a previously created recording of the corresponding document page.

Suitable reference material allows also checking the motif design of the thread. However, the design of the security thread is often not the focus of the reference databases, which means that reference information required for a detailed pattern matching may be missing. By inspecting the edge in the cross-section of the card composite, it can be check additionally whether the security thread is inserted internally into the card composite or whether it lies on top of the surface of the composite. Due to the narrow edge of the card body, however, focusing the camera on the edge of the card may be difficult, which, depending on the camera and the user's knowledge of how to use it, can be a hurdle to properly verify this feature. In addition, other security features such as DOVID effects may be integrated into the security thread, which can also be checked according to the criteria described in section 4.1.

4.3.3 Embossing

For this security feature, the material of the ID document is pressed together under high pressure, e.g. between two metal plates, and a motif is imprinted onto the card surface which, after the embossing process, can also be detected as raised and/or depressed structures relative to surrounding card body. Depending on the design, additional effects or features such as variable laser images can be integrated.

For the inspection of embossed features on solid plastic cards, the document must be tilted relative to the camera so that the light source is reflected by the surface of the plastic card. The intensity of the light source is also important for good perceptibility of the embossing. The light intensity should not be too high in order to prevent over-illumination of the card body surface in relation to the embossed motif. For a reliable verification, in addition to checking for the mere presence of raised/depressed structures, a comparison of the details of the embossed motifs with corresponding reference material is necessary. Depending on the embossing motif, this may require a high-resolution image (e.g. due to microprinting) and a suitable light source (extended, medium intensity) – in addition to sufficiently detailed reference material. Even if the verification could be possible in principle, these requirements cannot be assumed to always be met in the video-based identification procedure due to the individual and uncontrolled room lighting.

4.3.4 Optically variable ink (OVI)

With this particular type of ink, the visible colour changes depending on the illumination and viewing angle of the document. Typical for most optically variable inks are pigments that appear metallic and shiny. With the exception of diffuse lighting conditions, these pigments can usually be detected by video transmission. However, before checking this feature, the presence of these pigments must be confirmed using reference material. The main characteristic of optically variable ink is its continuous change in colour when the document is tilted, with a specific colour transition between two target colours defined for each pigment. However, the colour shift depends not only on the tilting angle of the document, but also on the arrangement of the light source(s) relative to the document as well as on the viewing angle relative to the incidence of light. The use of several light sources in the room is conducive to the verifiability of the feature. Therefore, the device's internal light source should also be switched on for the inspection of optically variable colours, as this can have a complementary effect to the other light sources in the room and make the intended colours of the OVI easier to observe. However, an inspection based on the device's internal light source alone can only show one of the two target colours. Depending on the arrangement of the other light sources in the room, it may still be necessary to move the document while simultaneously changing the camera position for a successful inspection, but this is only possible indirectly via instructions to the cardholder in the context of a video-based identification procedure. Due to this complexity, the verification of the OVI should only have a confirmatory character for authenticity and should not be regarded as a definite criterion for an evaluation.

Another prerequisite for proper verification of the OVI feature is that the colours to be expected are described in the available reference material. The same applies for the verification of the correspondence between the motif introduced by means of OVI and sufficiently detailed reference material. To do such a check properly, it may be necessary to take a high-resolution photo using a zoom function.

4.4 Security printing

The features of security printing described here are typically introduced by means of spot colours. This means that they cannot be reproduced by means of ordinary four-color halftone printing, which results in a higher barrier for imitations.

The differences between security printing and conventional four-color halftone printing processes can mainly be observed using a microscope by checking for continuous lines compared to halftone printing and for spot colours compared to conventional four-color printing. Accordingly, a check of this feature requires high-resolution images to achieve a corresponding sharpness of detail, which in practice can only be realized by means of high-resolution photographs. A prior confirmation of the printing process used by means of suitable reference material is required when checking this feature, since genuine ID documents that are printed using the halftone printing processes do also exist.

An examination with regard to the deposition characteristics of the print transfer process used is not possible due to the limited resolution and magnification capabilities of even high-end mobile device cameras – as already discussed in section 4.2.2 on integration technique of biographical data.

4.4.1 Microprint

Microprint incorporates text of a very small font size inside the document in the form of positive or negative background printing. Microprint is often integrated into elements that appear like simple lines to the naked eye. Proper integration requires correspondingly high-resolution printing processes.

Due to the small size, correspondingly high-resolution images are required to check microprinting, which is usually only possible using photographs, but not video recordings. Such a detailed examination of the microprinting is also quite time-consuming. It should also be noted that, despite available high-end mobile device cameras (high resolution, zoom function), microprinting may still appear illegible due to inaccurate camera focus in a video-based identification process. Therefore, the detection of a legible microprint can at most have an affirmatory indication for authenticity, but the detection of an illegible one does not directly constitute proof of a counterfeited document.

It can therefore be assumed that, in practice it only is possible in very few cases to make a reliable statement regarding the authenticity of this feature using a video-based identification procedure.

4.4.2 Guilloche/fine line pattern

Continuous guilloche/fine line patterns are typical elements of security printing realized in spot colours that can be found in the background printing of ID documents. The motif details of the line or guilloche patterns can be checked for consistency using correspondingly detailed reference material. However, the extent to which such a check can actually provide well-founded findings also depends on the size of the motifs themselves. In most cases, very high resolution is required for this, which cannot be achieved even with high-resolution photos of high-end mobile device cameras. It should also be noted that such a detailed examination of these background print patterns is quite time-consuming.

Due to the high demands on resolution, magnification (zoom function) and, in particular, focusing for a sound inspection of guilloche/fine line patterns in the background print, it can be assumed that in practice a reliable statement regarding the authenticity of this feature is only possible in very few cases using a video-based identification procedure.

4.4.3 Rainbow colouring

Rainbow colouring refers to a continuous colour transition between two printing inks in the background printing, i.e. no discrete change from one colour to the other. Both targeted colours are located in the same ink fountain of the printing unit. Typically, a continuous line or guilloche pattern is printed in the area with rainbow colouring to make this feature easier to check.

First of all, it is already possible to observe macroscopically whether a colour change in the background print was implemented in a discrete manner or continuously. In principle, this does not require a high resolution. However, in order to be able to reliably determine whether the colour change is implemented using rainbow colouring instead of using halftone printing, high magnification and resolution are required to be able to check for any imitations. The findings and issues with respect to resolution and focus described for the security feature of guilloches/ fine line patterns in section 1.4.2 must also be considered here. In addition, the position and width of the colour transition and more specifically the respective ink zones can generally be checked. However, it should be noted that the production-related variances with regard to position and width of the rainbow colouring zones can be quite high in practice, which is why no high significance should be attributed to this check. Therefore, the feature cannot be recommended for video-based identification procedures.

4.5 Conclusion

In principle, many of the above-described features can be checked via video transmission. However, for an assurance level assessment of a video-based identification procedure, further practically relevant attack vectors must be considered in addition to the document verification described here, such as manipulation of the transmitted videos or photos. Here, the term "video transmission" or "video-based identification" explicitly also includes the taking and uploading individual photographs. For several of the security features discussed here, high resolution and/or magnification of the images of a feature are required, which even with high-end mobile device cameras can only be realized by means of photographs, but not by means of video recordings. This holds all the more since, in the case of live video transmissions, the bandwidth available for the transmission and the associated compression may also have a significant influence on the image quality and thus on the details of security features that can still be recognized. In contrast, the limitation due to bandwidth does not apply for uploading photographs.

Another problem for checking some security features by means of video transmission is the focusing of the camera, as this may further restrict the recognisability of motif details and feature characteristics, so that proper checking of features may no longer be possible. However, the camera focus cannot be controlled by the video-based identification procedure itself, but depends on the camera used and the user's ability and knowledge of how to use it.

Another important aspect is the availability of suitable reference material. To protect against misuse of the images and information, publicly available reference databases often do not disclose high-resolution detailed images, but only provide images of lower resolution and fewer details. As a result, the publicly available reference information often does not describe all necessary details of the security features discussed for their proper inspection. For DOVID structures in particular, frequently non-specific images on the reconstruction properties at different tilt angles are presented without neither distinguishing between the different effects described here nor specifically naming or depicting the different effects.

One challenge when inspecting ID documents via video transmission is also the lighting conditions for filming or photographing. For a proper inspection, some of the security features require defined conditions in terms of both illumination and movement of the document. For other security features, at least the knowledge of the positions of the light sources in the room is necessary for a proper assessment of the observations in the video stream.

In addition to evaluating the authenticity of security features, a proper authenticity evaluation must also consider the attack scenario of falsifications, i.e. manipulated genuine documents. Since many of the genuine security features remain unaffected by such a manipulation of the ID document, it must also be specifically checked for traces of a possible manipulation. Security features that contain individual (personalised) information are particularly suitable for this purpose, as these data can be compared with other parts of the ID document that contain the same information. In addition, indications of falsification can be obtained on the basis of local changes, artefacts or attenuated or even missing security features – especially in areas of relevant personalised data.

Overall, these various aspects demonstrate the complexity of evaluating security features using video transmissions, which places high demands on expertise, knowledge and experience of the examiner. In addition, authenticity checks require sufficient time for the examiner to carry out the specific, necessary checks with the required level of detail in order to detect successfully counterfeit or falsified ID documents.

Reference Documentation

PBV Bundesamt für Sicherheit in der Informationstechnik: Prüfberichtsvorlage zur Prüfung von Identifikationsverfahren gemäß TR-03147 in Version 1.0.6

TR-03147 Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen, Version 1.0.6

CC Common Criteria: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012

CEM Common Criteria: Common Methodology for Information Technology Security Evaluation

ISO-HBV International Organization for Standardization: ISO/IEC 2382-37:2017 Information technology -- Vocabulary -- Part 37: Biometrics

CB-STD Christoph Busch: Harmonized Biometric Vocabulary; https://christoph-busch.de/standards.html

TR-03107-1 BSI: Technische Richtlinie TR-03107 Elektronische Identitäten und Vertrauensdienste im E-Government; Teil 1: Vertrauensdienste und Mechanismen

eIDAS 2015/1502 EU Kommission: Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

TR-03116-4 BSI: Technische Richtlinie TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung

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

ICAO9303 ICAO: International Civil Aviation Organization (ICAO): Doc9303 – Machine ReadableTravel Documents, Parts 1 – 13

TR-03135-1 BSI: Technische Richtlinie TR-03135-1 Machine Authentication of MRTDs for Public Sector Applications Part 1: Overview and Functional Requirements

TR-03135-2 BSI: Technische Richtlinie TR-03135-2 Machine Authentication of MRTDs for Public Sector Applications Part 2: Application profiles for official document inspection systems

ISO 27001 DIN ISO/IEC 27001:2015-03: Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014)