Federal Office
for Information Security

Checking report template for checking identification procedures according to TR-03147 in version 1.0.6

Version 1.0.0
December 28, 2021

Table of Contents

1 Introduction

The Technical Guideline TR-03147 [TR-03147] describes threats and requirements for procedures for (initial) identity verification of natural persons based on ID documents such as identity cards or passports. [TR-03147] makes it possible to classify different ID procedures according to their assurance level ("normal", "substantial" or "high") and thus compare them in terms of their security. In particular, [TR-03147] provides a basis for systematic and sound assessment of assurance levels of ID procedures.

Examples of such ID procedures are

- "video identification procedures",

- "photo identification procedures",

- procedures involving the direct presence of the person to be identified and an inspector, and

- procedures based on the use of the online ID function of the German identity card, the eID card for citizens of the EU and the EEA (eID card) or the electronic residence permit.

This document is the checking report template to be used for an assessment of the assurance level of an ID procedure against [TR-03147]. The requirements set out in the Technical Guideline are divided into individual, atomic checking criteria in order to support systematic verification and to document and guarantee the reproducibility of results from different inspectors in the best possible way. The overall result for each requirement of the Technical Guideline and ultimately for the entire procedure is then derived from the assessments of the individual checking criteria using the minimum principle (deviations from this are explicitly mentioned).

The checking report template is supplemented by an accompanying catalogue of requirements [AnfKat], which provides the inspector with a guideline for their assessment of each checking criterion and generally explains how the checking report template is to be used.

This checking report template contains general information on the procedure and verification in the other sections of this chapter (1.1 to 1.4), which must be provided by the inspector or the inspection company.

Chapter 2 summarises the results obtained in tabular form. If requirements from this checking report template are not relevant for a specific procedure and are therefore not checked, they are nevertheless to be listed in the checking report as not applicable.

Chapters 3 to 8 list the individual checking criteria derived from the requirements of [TR-03147]. These are to be addressed by the inspector and the associated table entries are to be completed appropriately. The structure of the checking report template as well as that of the catalogue of requirements follows the structure of the TR in order to assist in simultaneous handling of these documents as much as possible.

1.1 Overview

Assessor:	
Name of the procedure:	
Version number:	
Provider / operator of the procedure:	
Procedure category	<direct> | <indirect> | <electronic>
Assessment period:	from DD/MM/YYYY to DD/MM/YYYY
Basis for assessment:	[TR-03147] [AnfKat]

Validity period:	
Result of the assurance level assessment:	

1.2   Object of assessment

The functional principle of the procedure to be assessed as well as the context of its application are to be briefly described. At this point, the object of the assessment must also be precisely defined. It must be clearly distinguished from its surroundings, which are necessary for its operation but are not part of the assessment. The form in which the object of assessment is made available by the provider must also be explained at this point, as well as any additional materials and documentation. All objects must be clearly identifiable.

1.3   Tools

All tools used for the assessment must be clearly identified (hardware and software). If the products are non-commercial or freely available, this must be explicitly mentioned.

Ref.	Description	Manufacturer	Licence	Description of the tool

1.4   Persons and agencies involved

All persons involved in the assessment (including the contact persons of the manufacturer of a process) must be named, together with an indication of the tasks assumed.

Ref.	Name	Company	Title/function/task

2 Overview of the requirements and results

ID	Requirement	Conclusion
A1	Trustworthy ID documents Chapter 4 in [TR-03147]	
	A1.G-1	
	A1.G-2	
A1.1	Authoritative source Chapter 4.2.1 in [TR-03147]	
	A1.1-1	
	A1.1-2	
	A1.1-3	
	A1.1-4	
	A1.1-5	
	A1.1-6	
	A1.1-7	
	A1.1-8	
	A1.1-9	
	A1.1-10	
A1.2	Contains a sufficient amount of ID attributes Chapter 4.2.2 in [TR-03147]	
	A1.2-1	
	A1.2-2	
A1.3	Tamper- and forgery-proof Chapter 4.2.3 in [TR-03147]	
	A1.3-1	
	A1.3-2	
A1.4	Security features are known and effectively verifiable Chapter 4.2.4 in [TR-03147]	
	A1.4-1	
A1.5	Allows for reliable matching with the user Chapter 4.2.5 in [TR-03147]	
	A1.5-1	
	A1.5-2	
A1.6	ID attributes are current Chapter 4.2.6 in [TR-03147]	
	A1.6-1	
A1.7	Available lost, stolen or revoked reports are checked Chapter 4.2.7 in [TR-03147]	

ID	Requirement	Conclusion
	A1.7-1	
	A1.7-2	
A1.8	Regular checks of the set of permissible ID documents Chapter 4.2.8 in [TR-03147]	
	A1.8-1	
	A1.8-2	
A2	Security of the transmission channels Chapter 5 in [TR-03147]	
A2.1	Video/information manipulations of biometric data of the person to be identified are detected Chapter 5.2.1 in [TR-03147]	
	A2.1-1	
A2.2	Information-technological manipulation of information transmitted by the ID document is detected Chapter 5.2.2 in [TR-03147]	
	A2.2-1	
	A2.2-2	
A2.3	Physical manipulations of biometric characteristics of the person to be identified are detected Chapter 5.2.3 in [TR-03147]	
	A2.3-1	
A2.4	Physical manipulations of the presented ID document are detected Chapter 5.2.4 in [TR-03147]	
	A2.4-1	
A2.5	Live transmission of all data is guaranteed Chapter 5.2.5 in [TR-03147]	
	A2.5-1	
A2.6	An exchange of the presented ID document or the person to be identified during the check is detected Chapter 5.2.6 in [TR-03147]	
	A2.6-1	
A3	Checking of ID proofs Chapter 6 in [TR-03147]	
	A3.G-1	
A3.1	Type of ID document used can be determined Chapter 6.4.1 in [TR-03147]	
	A3.1-1	
A3.2	ID document is valid Chapter 6.4.2 in [TR-03147]	
	A3.2-1	

ID	Requirement	Conclusion
A3.3	Forged security features are detected Chapter 6.4.3 in [TR-03147]	
	A3.3-1	
	A3.3-2	
A3.4	Falsifications of the personalised data are detected Chapter 6.4.4 in [TR-03147]	
	A3.4-1	
	A3.4-2	
A4	Reliable match between the person to be identified and the ID document (integrity of the ID proof) Chapter 7 in [TR-03147]	
A4.1	Confidential knowledge factors are only communicated to the legitimate holder Chapter 7.2.1 in [TR-03147]	
	A4.1-1	
A4.2	Security of the authentication means used Chapter 7.2.2 in [TR-03147]	
	A4.2-1	
A4.3	The actual control of the person to be identified over the ID document is ensured Chapter 7.2.3 in [TR-03147]	
	A4.3-1	
A4.4	ID attributes to be matched are captured in sufficient quality Chapter 7.2.4 in [TR-03147]	
	A4.4-1	
	A4.4-2	
A4.5	Reliable matching of relevant biometric ID attributes between ID document and person to be identified Chapter 7.2.5 in [TR-03147]	
	A4.5-1	
A5	Correct capture of the required ID attributes Chapter 8 in [TR-03147]	
A5.1	ID attributes to be captured allow for unique identification Chapter 8.2.1 in [TR-03147]	
	A5.1-1	
A5.2	Specific expertise of the inspectors and tools to be used, if any, are available Chapter 8.2.2 in [TR-03147]	
	A5.2-1	
	A5.2-2	
A5.3	ID attributes are transferred to the capture system in full and without	

ID	Requirement	Conclusion
	errors Chapter 8.2.3 in [TR-03147]	
	A5.3-1	
	A5.3-2	
A5.4	Captured data is checked for timeliness, consistency and plausibility Chapter 8.2.4 in [TR-03147]	
	A5.4-1	
	A5.4-2	
	A5.4-3	
A6	Assuring the integrity of all process steps Chapter 9 in [TR-03147]	
A6.1	Compliance with the prescribed checking criteria is ensured Chapter 9.2.1 in [TR-03147]	
	A6.1-1	
	A6.1-2	
	A6.1-3	
	A6.1-4	
	A6.1-5	
A6.2	ISMS Chapter 9.2.2 in [TR-03147]	
	A6.2-1	
A7.G	Global attack scenarios supplementary to [TR-03147]	
	A7.G-1	

3 Trustworthy ID documents

3.1 Relevance

Security objective:	Existence Legitimacy
Examples of procedure types:	"VideoIdent" "PhotoIdent" Procedure with direct presence ("on-site" identification e.g. in a branch, including "on-site reading" of identity cards or electronic residence permits). Procedure with online identification function of identity cards or electronic residence permits

3.2 Multiple approved ID documents

CheckCrit ID	A1.G-1				
CheckCrit description;	What is the assurance level of the ID document that has been approved for the ID procedure and has the lowest assurance level?				
Reference	Chapter 4				
Checking task:	Determination of the assurance level across all ID documents according to the minimum principle.				
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

3.3 Valid ID documents

CheckCrit ID	A1.G-2				
CheckCrit description:	When using the ID procedure, does the ID document used get checked if it is valid at the time of checking?				
Reference	Chapter 4.2				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

3.4 Authoritative source

CheckCrit ID	A1.1-1				
CheckCrit description:	Are the authorities responsible for issuing the respective ID document known?				
Reference	Chapter 4.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

CheckCrit ID	A1.1-2				
CheckCrit description:	Is publicly available information on compromises (e.g. media reports on compromises of such bodies) collected via the responsible bodies?				
Reference	Chapter 4.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

CheckCrit ID	A1.1-3				
CheckCrit description:	Is information on compromises collected via the responsible bodies (e.g. media reports on compromises of such bodies) taken into account in a timely manner?				
Reference	Chapter 4.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

CheckCrit ID	A1.1-4

CheckCrit description:	Is up-to-date information on manipulations and forgeries of ID documents collected?				
Reference	Chapter 4.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A1.1-5				
CheckCrit description:	Is the information collected on tampering and forgery of ID documents taken into account in a timely manner?				
Reference	Chapter 4.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A1.1-6				
CheckCrit description:	Does the process of creating and issuing the ID document used sufficiently check the eligibility and identity of an applicant?				
Reference	Chapter 4.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A1.1-7				
CheckCrit description:	Does the ID procedure check whether the ID document used belongs to an explicitly limited set of authorised ID documents?				
Reference	Chapter 4.2.1				
Documentation:					

Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A1.1-8				
CheckCrit description:	Is the ID document an explicit ID document?				
Reference	Chapter 4.2, Table 4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A1.1-9				
CheckCrit description:	Does the ID document fulfil the domestic ID requirement?				
Reference	Chapter 4.2, Table 4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A1.1-10				
CheckCrit description:	Does the ID document have an equivalent level of security of features and their verifiability for protection against forgery and manipulation as domestic ID documents?				
Reference	Chapter 4.2, Table 4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

3.5 Contains a sufficient amount of ID attributes

CheckCrit ID	A1.2-1				
CheckCrit description:	Is there a sufficient set of ID attributes?				
Reference	Chapter 4.2.2				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

CheckCrit ID	A1.2-2				
CheckCrit description:	Is unique identification possible through the given ID attributes?				
Reference	Chapter 4.2.2				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

3.6 Tamper- and forgery-proof

CheckCrit ID	A1.3-1
CheckCrit 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 forgery?
Reference	Chapter 4.2.3
Documentation:	
Interview partner:	
Checking task:	
Analysis:	

Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A1.3-2
CheckCrit description:	What assurance level does the ID document in question have in terms of the potential for attack in order to forge or tamper with it, taking into account the category of the procedure?
Reference	Chapter 4.2.3
Documentation:	
Interview partner:	
Checking task:	
Analysis:	

Assessment:	Normal	Subst.	High	N/A	Not fulfilled

3.7 Security features are known and effectively verifiable

CheckCrit ID	A1.4-1
CheckCrit description:	Are all security features of the approved ID documents used in the ID procedure known and effectively verifiable?
Reference	Chapter 4.2.4
Documentation:	
Interview partner:	
Checking task:	
Analysis:	

Assessment:	Normal	Subst.	High	N/A	Not fulfilled

3.8 Allows for reliable matching with the user

CheckCrit ID	A1.5-1
CheckCrit description:	What is the assurance level of the knowledge-based data available on the ID document for matching with the user?
Reference	Chapter 4.2.5
Documentation:	
Interview partner:	
Checking task:	

Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

CheckCrit ID	A1.5-2				
CheckCrit description:	What is the assurance level of the biometric data available on the ID document for matching with the user?				
Reference	Chapter 4.2.5				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

3.9   ID attributes are up to date

CheckCrit ID	A1.6-1				
CheckCrit description:	Is the timeliness of the ID attributes on the ID document used sufficiently guaranteed?				
Reference	Chapter 4.2.6				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

3.10   Available lost, stolen or revoked reports are checked

CheckCrit ID	A1.7-1	
CheckCrit description:	Has the maximum validity period of the ID document been checked?	
Reference	Chapter 4.2.7	
Documentation:		
Interview partner:		
Checking task:		

Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A1.7-2
CheckCrit description:	Are lost, stolen or revoked reports for the ID document queried to determine validity?
Reference	Chapter 4.2.7
Documentation:	
Interview partner:	
Checking task:	
Analysis:	

Assessment:	Normal	Subst.	High	N/A	Not fulfilled

3.11   Regular checking of the set of permissible ID documents

CheckCrit ID	A1.8-1
CheckCrit description:	How often are the ID documents approved for the ID procedure checked in accordance with requirements A1.7-1 and A1.7-2?
Reference	Chapter 4.2, Table 4; Chapter 4.2.8
Documentation:	
Interview partner:	
Checking task:	
Analysis:	

Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A1.8-2
CheckCrit description:	Is new knowledge gained from requirements A1.8-1 taken into account when carrying out the ID procedure?
Reference	Chapter 4.2.8
Documentation:	
Interview partner:	
Checking task:	
Analysis:	

Assessment:	Normal	Subst.	High	N/A	Not fulfilled

4 Security of the transmission channels

4.1 Relevance

Security objective:	existence legitimacy
Examples of procedure types:	"VideoIdent" "PhotoIdent" Procedure with online identification function of identity cards or electronic residence permit

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

CheckCrit ID	A2.1-1				
CheckCrit 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?				
Reference	Chapter 5.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

4.3 Information manipulation of information transmitted by the ID document is detected

CheckCrit ID	A2.2-1				
CheckCrit 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?				
Reference	Chapter 5.2.2				
Checking task:	Determination of the lowest attack potential over all ID proofs according to the minimum principle and determination of the achieved assurance level.				
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

CheckCrit ID	A2.2-2				
CheckCrit 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?				
Reference	Chapter 5.2.2				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

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

CheckCrit ID	A2.3-1				
CheckCrit 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?				
Reference	Chapter 5.2.3				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

4.5 Physical manipulations of the ID document are detected

CheckCrit ID	A2.4-1	
CheckCrit 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?	
Reference	Chapter 5.2.4	
Documentation:		
Interview partner:		
Checking task:		

Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

4.6 Live transmission of all data is guaranteed

CheckCrit ID	A2.5-1				
CheckCrit description:	What assurance level does the ID procedure in question have in terms of attack potential for successfully reusing pre-recorded data?				
Reference	Chapter 5.2.5				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

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

CheckCrit ID	A2.6-1				
CheckCrit description:	What assurance level does the ID procedure in question have in terms of attack potential in order to successfully carry out an exchange of the ID document presented or of the person to be identified during the check?				
Reference	Chapter 5.2.6				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

5 Checking of ID proofs

5.1 Relevance

Security objective:	uniqueness
Examples of procedure types:	"VideoIdent" "PhotoIdent" Procedure with direct presence (e.g. PostIdent) Procedure with online identification function of identity card or electronic residence permit

5.2 Multiple ID proofs

CheckCrit ID	**A3.G-1**				
CheckCrit 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?				
Reference	Chapter 6				
Checking task:	Determination of the assurance level across all ID documents according to the minimum principle.				
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

5.3 Type of ID document used can be determined

CheckCrit ID	**A3.1-1**				
CheckCrit description:	Can the type of ID document presented for checking be established and verified?				
Reference	Chapter 6.4.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

5.4   ID document is valid

CheckCrit ID	A3.2-1				
CheckCrit description:	Can the validity of the ID document presented be established and verified?				
Reference	Chapter 6.4.2				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

5.5   Forged security features are detected

CheckCrit ID	A3.3-1				
CheckCrit description:	What are the mandatory check requirements for the ID documents that are admissible in the ID procedure?				
Reference	Chapter 6.4.3				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

CheckCrit ID	A3.3-2				
CheckCrit description:	What assurance level does the ID procedure in question have in terms of attack potential in order to successfully forge security features in it?				
Reference	Chapter 6.4.3				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

5.6   Falsifications of the personalised data are detected

CheckCrit ID	A3.4-1				
CheckCrit description:	Is a consistency check carried out on the various ID attributes?				
Reference	Chapter 6.4.4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

CheckCrit ID	A3.4-2				
CheckCrit description:	What assurance level does the ID procedure in question have in terms of attack potential in order to successfully carry out forgeries of personalised data in it?				
Reference	Chapter 6.4.4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

6 Matching of persons with ID proofs

6.1 Confidential knowledge factors are only communicated to the legitimate holder

CheckCrit ID	A4.1-1				
CheckCrit description:	What assurance level is achieved by the transmission of the confidential knowledge factor to the legitimate holder?				
Reference	Chapter 7.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

6.2 Security of the authentication means used

CheckCrit ID	A4.2-1				
CheckCrit description:	What assurance level is achieved by the authentication means used?				
Reference	Chapter 7.2.2				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

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

CheckCrit ID	A4.3-1
CheckCrit description:	Does the person to be identified have actual control of their ID document during the ID procedure?
Reference	Chapter 7.2.3

Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

6.4 ID attributes to be matched are captured in sufficient quality

CheckCrit ID	A4.4-1				
CheckCrit 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?				
Reference	Chapter 7.2.4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A4.4-2				
CheckCrit 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?				
Reference	Chapter 7.2.4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

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

CheckCrit ID	A4.5-1				
CheckCrit description:	Which assurance level is achieved by the employed biometric matching procedure?				
Reference	Chapter 7.2.5				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

7 Correct capture of the required ID attributes

7.1 Relevance

Security objective:	uniqueness
Examples of procedure types:	"VideoIdent" "PhotoIdent" Procedure with direct presence (e.g. PostIdent) Procedure with online identification function of identity card or electronic residence permit

7.2 ID attributes to be captured allow for unique identification

CheckCrit ID	**A5.1-1**				
CheckCrit description:	Is unique identification possible with the captured ID attributes?				
Reference	Chapter 8.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

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

CheckCrit ID	**A5.2-1**				
CheckCrit description:	Is there proof of competence for the personnel involved in the interpretation and capture of ID attributes for all ID proofs?				
Reference	Chapter 8.2.2				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

CheckCrit ID	A5.2-2				
CheckCrit description:	Are the intended tools always available for the ID attribute capture process?				
Reference	Chapter 8.2.2				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

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

CheckCrit ID	A5.3-1				
CheckCrit 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)?				
Reference	Chapter 8.2.3				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A5.3-2				
CheckCrit description:	Is the capture system technically capable of capturing all relevant ID attributes completely and accurately?				
Reference	Chapter 8.2.3				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

7.5 Captured data is checked for timeliness, consistency and plausibility

CheckCrit ID	A5.4-1				
CheckCrit description:	Is a check of the ID attributes for consistency and plausibility carried out?				
Reference	Chapter 8.2.4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A5.4-2				
CheckCrit description:	Is the ID check aborted for open mandatory fields during capture?				
Reference	Chapter 8.2.4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A5.4-3				
CheckCrit description:	What is the assurance level of the ID attribute check for timeliness, consistency and plausibility when capturing these attributes?				
Reference	Chapter 8.2.4				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

8 Ensuring the integrity of the processes

8.1 Relevance

Security objective:	The requirement "Ensuring the integrity of the processes" defines cross-organisational security measures and ensures the implementation of the necessary requirements to achieve all security objectives, i.e. existence, legitimacy and uniqueness.
Examples of procedure types:	"VideoIdent" "PhotoIdent" Procedure with direct presence (e.g. PostIdent) Procedure with online identification function of identity card or electronic residence permit

8.2 Compliance with the prescribed checking criteria is ensured

CheckCrit ID	**A6.1-1**				
CheckCrit description:	Is compliance with the ID checking criteria ensured by technical and organisational measures or a combination thereof?				
Reference	Chapter 9.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	**A6.1-2**				
CheckCrit description:	Are the security features to be checked for each ID document defined?				
Reference	Chapter 9.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	**A6.1-3**

CheckCrit description:	What is the assurance level for updating the definitions of the security features to be checked?				
Reference	Chapter 9.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A6.1-4				
CheckCrit description:	What is the assurance level of the expertise and trustworthiness of the personnel assigned to manually performed checking steps?				
Reference	Chapter 9.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

CheckCrit ID	A6.1-5				
CheckCrit 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?				
Reference	Chapter 9.2.1				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	Normal	Subst.	High	N/A	Not fulfilled

8.3   ISMS

CheckCrit ID	A6.2-1
CheckCrit	Is an ISMS according to ISO / IEC 27001 and ISO / IEC 27002 or equivalent

description:	implemented for the generic assurance of the processes' integrity, which covers all IT components and IT processes used for identity verification or storage or transmission of data captured in the process?				
Reference	Chapter 9.2.2				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

9 Overarching attack scenarios against ID procedures

9.1 Relevance

Security objective:	existence legitimacy uniqueness
Examples of procedure types:	"VideoIdent" "PhotoIdent" Procedure with direct presence (e.g. PostIdent) Procedure with online identification function of identity card or electronic residence permit

9.2 Global attack scenarios

CheckCrit ID	A7.G-1				
CheckCrit description:	What is the minimum assurance level for the entire ID procedure resulting from the assessment of the attack potential of global attack scenarios?				
Reference	supplementary to [TR-03147]				
Documentation:					
Interview partner:					
Checking task:					
Analysis:					
Assessment:	**Normal**	**Subst.**	**High**	**N/A**	**Not fulfilled**

Bibliography

TR-03147   Federal Office for Information Security: Technical Guideline TR-03147 Assurance Level
                Assessment of Procedures for Identity Verification of Natural Persons, Version 1.0.6

AnfKat   Federal Office for Information Security: Catalogue of requirements for checking
                identification procedures in accordance with TR-03147 version 1.06