Federal Office
for Information Security

Federal
Criminal Police Office

Federal Police

Technical Guideline BSI TR-03135

Machine Authentication of MRTDs for Public Sector Applications

Part 2: Application profiles for official document inspection systems

BSI TR-03135-2
Version 2.3.0

Federal Office for Information Security with the Federal Criminal Police Office and the Federal Police
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: tr-03135@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

Tables

1 Introduction

This profiling document is part of Technical Guideline TR-03135 Machine Authentication of MRTDs for Public Sector Applications. The Technical Guideline TR-03135 specifies and describes necessary requirements for machine assisted document checks on MRTDs in Public Sector Applications.

The technical description of the checks referenced in this document are specified in Part 1 of TR-03135, see [TR-03135-1].

1.1 Terminology

Keywords used within in this document are to be interpreted as described in [RFC2119].

1.2 Technical terms

For clarity, terms were shortened to make this Technical Guideline more readable. Abbreviations can be found in [TR-03135-1].

2 Operational scenarios

This profiling refers to operational eMRTD inspection scenarios in German Public Sector Applications. In this respect the operational application scenarios are defined in the following chapters.

2.1 Stationary application scenarios

Stationary systems are systems which are permanently installed at border crossings, at police stations or at other localities with raised focus concerning security issues (e. a. government buildings, ministries, embassies or official meeting locations) as well as temporary systems in accordingly prepared sites (e.g. for major events such as sports or music events).

2.2 Self Service application scenarios

Self Service systems are systems with which automated or semi-automated document and identity checks are performed (e. g. so-called eGates/ABC systems, automated border control systems/gates).

2.3 Partially mobile application scenarios

Partially mobile application scenarios usually take place at checkpoints, in patrol cars or vessels, but also in rail, air and shipping traffic environments. This includes, for example portable PC stations, which are the size of a notebook, or a tablet PC. These systems are often equipped with a swipe or full-page reader in order to be able to read the MRZ/CAN, but also with a RFID-chip reading module.

2.4 Fully mobile application scenarios

Fully mobile application scenarios will usually be performed in rail, air and shipping traffic as well as during general patrol duty. The systems are carried by the officer. The devices have the similar size and design as smartphones or tablet PCs.

2.5 Kiosk application scenarios

Kiosk application scenarios usually take place at border crossing points (air- or sea-ports). These systems are unengaged and unmanaged pillar styled units that can be operated by the traveller. A traveller can pre-register and pre-process before crossing the border. These systems are equipped with a full-page document reader in order to be able fully read the MRTD. This also includes reading the RFID chip of an eMRTD. In addition, such a kiosk system can capture live images of the traveler and fingerprints. An interactive electronic registration prompt guides the traveler through the process.

3 Requirements from TR-03135-1

This chapter details the requirements from [TR-03135-1] which are relevant for these application profiles.

3.1 Requirements on the document checking system

The generic requirements of a document checking system SHALL fit the requirements regarding chapters 2 and 3 of [TR-03135-1].

3.2 Requirements on document checks

3.2.1 General requirements for all scenarios

If a specific check is implemented it SHALL be performed regarding

- optical checks as specified in [TR-03135-1] chapter 4.5
- electronic checks as specified in [TR-03135-1] chapter 4.6
- combined checks as specified in [TR-03135-1] chapter 4.7
- handling of defects as specified in [TR-03135-1] chapter 4.8

The implementation SHALL support the following SSV check groups if applicable

- GRP_UV_DULLNESS: Required to facilitate UV dullness check results and groups all checks that belong to this group.
- GRP_SSV_CHECK: Required to facilitate typical pattern checks into one group.
- GRP_EVAL_CHECK: Evaluatory check group, required to perform checks that are performed and logged, but do not incorporate into a final check result.

The false negative rate per country SHOULD not exceed 2% for correctly placed, captured and identified documents.

3.2.2 Requirements for Stationary application scenarios

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
Optical Checks		
4.5.2	m	For all further optical checks, the document SHALL be detected and needs to be fully captured under different light sources.
4.5.3	m	Identification of the document model SHALL be performed.
4.5.4.1	m	The MRZ shall be checked for ICAO compliance.
4.5.4.2	m	Spectrally selective checks SHOULD be performed if applicable for the given document model. At least the check (UV, BR, FU) SHALL be performed.

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
		Option: If chip authenticity is guaranteed by the electronic check, the mode of spectrally selective checks can be changed to evaluatory. Additional note: The system SHALL support a blacklist, where this option can be disabled for specific countries.
Electronic Checks		
4.6.1	m	Connections to the background public key infrastructures SHALL be available.
4.6.1.1	m	Defect and Master Lists SHALL be supported.
4.6.2	m	Access and process sequences SHALL be supported.
4.6.3	m	Chip access protocols SHALL be supported.
4.6.4	m	Checking chip contents SHALL be performed.
Combined Checks		
4.7.1	m	Checking the expiration of the documents SHALL be performed.
4.7.2	m	If the document is an eMRTD / eID, “Checking the optical biographic data against the electronic biographic data” SHALL be performed.
4.7.3	o	Checks across document pages.
4.7.4	o	Checks across several documents and linking of multiple document checks in a transaction.
4.7.5	o	Comparison of personalization contents is recommended for all documents that are present in a check database.
4.7.6	o/e	Checking DG2 against the facial image from the VIZ.

Table 3.1: Requirements for Stationary application scenarios

3.2.3 Requirements for Self Service application scenarios

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
Optical Checks		
4.5.2	m	For all further optical checks, the document SHALL be detected and needs to be fully captured under different light sources.
4.5.3	m	Identification of the document model SHALL be performed.
4.5.4.1		The MRZ SHALL be checked for ICAO

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
		compliance.
4.5.4.2	m/e	Spectrally selective checks SHOULD be performed if applicable for the given document model. At least the checks (UV, BR, FU) SHALL, and one check each (IR, TR, *ZZ*) and (UV, LU, *ZZ*) SHOULD be performed. Option: If chip authenticity is guaranteed by the electronic check, the mode of spectrally selective checks can be changed to evaluatory. Additional note**:** The system SHALL support a blacklist, where this option can be disabled for specific countries.
Electronic Checks		
4.6.1	m	Connections to the background public key infrastructures SHALL be available.
4.6.1.1	m	Defect and Master Lists SHALL be supported.
4.6.2	m	Access and process sequences SHALL be supported.
4.6.3	m	Chip access protocols SHALL be supported.
4.6.4	m	Checking chip contents SHALL be performed.
Combined Checks		
4.7.1	m	Checking the expiration of the documents.
4.7.2	m	If the document is an eMRTD / eID, “Checking the optical biographic data against the electronic biographic data” SHALL be performed.
4.7.3	o	Checks across document pages.
4.7.4	o	Checks across several documents and linking of multiple document checks in a transaction.
4.7.5	o	Comparison of personalization contents is recommended for all documents that are present in a check database.
4.7.6	o	Checking DG2 against the facial image from the VIZ.

Table 3.2: Requirements for Self Service application scenarios

3.2.4 Requirements for Partially Mobile application scenarios

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
Optical Checks		
4.5.2	o	Depending on the optical reader it may be not possible to capture the full document, but parts of it like the MRZ or CAN SHOULD be captured. If possible, the presence of a document in the reader SHOULD be detected.
4.5.3	o	Depending on the optical reader, the document model SHOULD not be identified (e. g., swipe reader).
4.5.4.1	m	If a MRZ was read, the MRZ SHALL be checked for ICAO compliance.
4.5.4.2	o/e	Depending on the optical reader, spectrally selective checks SHOULD be performed if applicable for the given document model. At least the checks ~~(IR, AB, MR) and~~ (UV, BR, FU) SHALL be performed. Option: If chip authenticity is guaranteed by the electronic check, the mode of spectrally selective checks can be changed to evaluatory. Additional note: The system SHALL support a blacklist, where this option can be disabled for specific countries.
Electronic Checks		
4.6.1	m	Connections to the background public key infrastructures SHALL be available.
4.6.1.1	m	Defect and Master Lists SHALL be supported.
4.6.2	m	Access and process sequences SHALL be supported.
4.6.3	m	Chip access protocols SHALL be supported.
4.6.4	m	Checking chip contents SHALL be performed.
Combined Checks		
4.7.1	m	Checking the expiration of the documents.
4.7.2	m	If the document is an eMRTD / eID, “Checking the optical biographic data against the electronic biographic data” SHALL be performed.
4.7.3	o	Checks across document pages.
4.7.4	o	Checks across several documents and linking of multiple document checks in a transaction.

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
4.7.5	o	Comparison of personalization contents is recommended for all documents that are present in a check database.
4.7.6	o	Checking DG2 against the facial image from the VIZ.

Table 3.3: Requirements for Partially Mobile application scenarios

3.2.5 Requirements for Fully Mobile application scenarios

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
Optical Checks		
4.5.2	m	Depending on the optical reader it may be not possible to capture the full document, but parts of it like the MRZ or CAN SHOULD be captured (e. g., swipe reader, integrated camera). Also presence of a document in the reader SHOULD be detected.
4.5.3	o	Depending on the optical reader, the document model SHOULD not be identified (e. g., swipe reader, integrated camera).
4.5.4.1	o	If a MRZ was read, the MRZ SHALL be checked for ICAO compliance.
4.5.4.2	o/e	Depending on capabilities the optical reader, spectrally selective checks SHOULD be performed if applicable for the given document model. At least the checks (UV, BR, FU) SHOULD be performed. Option: If chip authenticity is guaranteed by the electronic check, the mode of spectrally selective checks can be changed to evaluatory. Additional note: The system SHALL support a blacklist, where this option can be disabled for specific countries.
Electronic Checks		
4.6.1	m	Connections to the background public key infrastructures SHALL be available.
4.6.1.1	m	Defect and Master Lists SHALL be supported.
4.6.2	m	Access and process sequences SHALL be supported.
4.6.3	m	Chip access protocols SHALL be supported.
4.6.4	m	Checking chip contents SHALL be performed.
Combined Checks		

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
4.7.1	m	Checking the expiration of the documents.
4.7.2	m	If the document is an eMRTD / eID, “Checking the optical biographic data against the electronic biographic data” SHALL be performed.
4.7.3	o	Checks across document pages.
4.7.4	o	Checks across several documents and linking of multiple document checks in a transaction.
4.7.5	o	Comparison of personalization contents is recommended for all documents that are present in a check database.
4.7.6	o	Checking DG2 against the facial image from the VIZ.

Table 3.4: Requirements for Fully Mobile application scenarios

3.2.6 Requirements for kiosk application scenarios

Such systems are unengaged and unmanaged kiosk styled units that can be operated by the traveller. The advantage is, that the traveller can pre-register and pre-process before crossing the border. Such systems are often equipped with a full-page reader in order to fully read the MRTD, but this scenario also includes reading the RFID chip, if present. In addition, a kiosk system SHOULD also capture and process the live face and optionally the fingerprint images of the traveller.

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
Optical Checks		
4.5.2	m	For all further checking steps the model SHALL be identified.
4.5.3	m	MRZ consistency check shall always be possible, regardless of the used technology.
4.5.4.1	m	If a MRZ was read, the MRZ SHALL be checked for ICAO compliance.
4.5.4.2	o/e	Depending on capabilities the optical reader, spectrally selective checks SHOULD be performed if applicable for the given document model. At least the checks (UV, BR, FU) SHOULD be performed. Option: If chip authenticity is guaranteed by the electronic check, the mode of spectrally selective checks can be changed to evaluatory. Additional note: The system SHALL support a blacklist, where this option can be disabled for specific countries.
Electronic Checks Remark: Only valid and performed, if the provided document contains a chip (e. a. is an eMRTD)		

Ref. [TR-03135-1]	Obligation (m/o/e)	Notes
4.6.1	m	Connections to the background public key infrastructures SHALL be available.
4.6.1.1	m	Defect and Master Lists SHALL be supported.
4.6.2	m	Access and process sequences SHALL be supported.
4.6.3	m	Chip access protocols SHALL be supported.
4.6.4	m	Checking chip contents SHALL be performed.
Combined Checks		
4.7.1	m	Checking the expiration of the documents.
4.7.2	o	If the document is an eMRTD / eID, “Checking the optical biographic data against the electronic biographic data” SHALL be performed.
4.7.3	o	Checks across document pages.
4.7.4	o	Checks across several documents and linking of multiple document checks in a transaction.
4.7.5	o	Comparison of personalization contents is recommended for all documents that are present in a check database.
4.7.6	m/e	Checking DG2 against the facial image from the VIZ

Table 3.5: Requirements for kiosk application scenarios

3.3 Requirements on operational monitoring

The document check system SHALL implement the logging schema according to [TR-03135-1], chapter 5.

This document defines the following levels of logging configurations:

1. Basic logging profile
2. Standard logging profile
3. Standard logging profile with optical evaluation extensions
4. Standard logging profile with electronic evaluation extensions
5. Full logging profile

The set of extended data nodes is defined for the corresponding checks in table 3.6.

Type of failed check	Extended data nodes (XPath expression)

Optical Check	//dco:BasicCheckResult/dco:ScannedArea
	//dco:ScannedImages
	//dc:DocumentDetails

Electronic Check	//dce:ChipFiles //dce:Trace
Combined Check	//dcc:Mismatch/*
Biometric Check	//dc:Image

Table 3.6: Set of extended data nodes for different check types

The document check system SHALL implement all defined logging configurations. Setting the actual logging configuration SHALL be configurable by the application.

3.3.1 Basic logging profile

Basic logging SHALL contain all non-person related data from a check, including all check results. All data items from the XML schema SHALL be filled, with the exception of the set of extended data nodes.

3.3.2 Standard logging profile

Standard logging SHALL contain all available information from Basic logging profile and SHALL provide additional information on the specific **failed** and **undetermined** check(s).

For electronic check errors, the optical document data SHALL be included to allow for cross-comparison of optical and electronic document data.

Depending on the type of error, the relevant sets of extended data nodes detailing the error SHALL be present in the log. Note that extended data nodes are not present if the corresponding check was aborted. If the integrity check of a data group failed, then the extended data nodes of the optical check SHALL also be included.

3.3.3 Standard logging profile with optical evaluation extensions

Standard logging with optical evaluation extensions SHALL contain all information from Standard logging and SHALL contain all extended data nodes for the optical check regardless of the optical check result.

3.3.4 Standard logging profile with electronic evaluation extensions

Standard logging with optical evaluation extensions SHALL contain all information from Standard logging and SHALL contain all extended data nodes for the electronic check regardless of the electronic check result.

3.3.5 Full logging profile

Full logging SHALL contain all available information including all extended nodes, regardless of the check results.

3.4 Requirements on data transmission

The document check system SHALL implement the transmission and log specification according to [TR-03135-1], chapter 6. This requirement is REQUIRED for Stationary, Self Service, and Kiosk application scenarios and RECOMMENDED for Partially Mobile and Fully Mobile application scenarios. Logging data SHOULD be temporarily kept local, if transmission fails and retransmitted if the connection is available, possibility to manually transfer logs is RECOMMENDED.

4 Conformity

In order to conform to this Technical Guideline, an Inspection System and Inspection Application SHALL completely implement and meet all requirements from chapters 3 for the used scenario.

Reference Documentation

[TR-03135-1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Technische Richtlinie TR-03135, Machine Authentication of MRTDs for Public Sector Applications Part 1: Overview and Functional Requirements, 2016, Version 2.1.0.

Keywords and Abbreviations

For Keywords and Abbreviations see [TR-03135-1].