Federal Office
for Information Security

BSI Technical Guideline TR-03135-2

Machine Authentication of MRTDs for Public Sector Applications

Part 2: Application profiles for official document inspection systems

Version 2.5

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
E-Mail: tr-03135@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1. Changelog

The following tables present the changes introduced between the latest versions of this Technical Guideline. The changelog lists the changes grouped per part of this Technical Guideline, per element (section, table, figure) and type of change, refer to [KeepAChangelog]:

- *Added* for new features
- *Changed* for changes in existing functionality
- *Deprecated* for soon-to-be removed features
- *Removed* for now removed features
- *Fixed* for any bug fixes
- *Security* in case of vulnerabilities

1.1. Changelog 2.5 Part 2

Element Name	Type of Change	Change Description
Chapter Requirements from TR-03135-1	Added	Digital seal checks as general requirement
Chapter Requirements from TR-03135-1	Added	Digital seal checks requirements for all application scenarios
Chapter Requirements from TR-03135-1	Added	Extended data nodes for digital seal checks
Chapter Requirements from TR-03135-1	Added	Standard logging profile with evaluation extensions for digital seals
Chapter Requirements from TR-03135-1	Added	Asylum registration application scenarios

Table 1.1 Changelog BSI TR-03135, Part 2

2. 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 Machine Readable Travel Documents (MRTDs) in Public Sector Applications.

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

2.1. Terminology

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

2.2. Technical terms

For clarity and better reading, terms are abbreviated. The ▸glossary contains the list of the used abbreviations.

3. Operational Scenarios

This profiling refers to operational Electronic Machine Readable Travel Document (eMRTD) inspection scenarios in German Public Sector Applications. In this respect the operational application scenarios are defined in the following chapters.

3.1. 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).

3.2. 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/Automated Border Control (ABC) systems, automated border control systems/gates).

3.3. 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 Machine Readable Zone (MRZ)/Card Access Number (CAN), but also with a radio-frequency identification (RFID)-chip reading module.

3.4. 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.

3.5. 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.

3.6. Asylum registration application scenarios

Asylum registration application scenarios take place when a human seeking asylum is registered.

4. Requirements from TR-03135-1

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

4.1. Requirements on the document checking system

The generic requirements of a document checking system SHALL fit the requirements regarding chapter 4 and 5 in [BSI TR-03135-1].

4.2. Requirements on document checks

4.2.1. General requirements for all scenarios

If a specific check is implemented it SHALL be performed regarding

- optical checks as specified in [BSI TR-03135-1], chapter 5.5
- electronic checks as specified in [BSI TR-03135-1], chapter 5.6
- combined checks as specified in [BSI TR-03135-1], chapter 5.7
- handling of defects as specified in [BSI TR-03135-1], chapter 5.8
- digital seal checks as specified in [BSI TR-03135-1], chapter 5.9

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.

4.2.2. Overview of the requirements for the application scenarios

An overview of the requirements for the different application scenarios is given in ▸Table 4.1

Ref. [BSI TR-03135-1	**Stationary**	**Self Service**	**Partially Mobile**	**Fully Mobile**	**Kiosk**
Optical Checks					
5.5.2	m	m	o	m	m
5.5.3	m	m	o	o	m
5.5.4.1	m	m	m	o	m
5.5.4.2	m	m/e	o/e	o/e	o/e
Electronic Checks					

Ref. [BSI TR-03135-1	**Stationary**	**Self Service**	**Partially Mobile**	**Fully Mobile**	**Kiosk**
5.6.1	m	m	m	m	m
5.6.1.1	m	m	m	m	m
5.6.2	m	m	m	m	m
5.6.3	m	m	m	m	m
5.6.4	m	m	m	m	m
Combined Checks					
5.7.1	m	m	m	m	m
5.7.2	m	m	m	m	o
5.7.3	o	o	o	o	o
5.7.4	o	o	o	o	o
5.7.5	o	o	o	o	o
5.7.6	o/e	o	o	o	m/e
Digital Seal Checks					
5.9.1	m	m	m	m	m

Table 4.1 Requirements for application scenarios - Overview

4.2.3. Requirements for Stationary application scenarios

The requirements for Stationary application scenarios are given in ▸Table 4.2 (Optical checks), ▸Table 4.3 (Electronic Checks), ▸Table 4.4 (Combined Checks) and ▸Table 4.5 (Digital Seal Checks).

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.5.2	m	For all further optical checks, the document SHALL be detected and needs to be fully captured under different light sources.
5.5.3	m	Identification of the document model SHALL be performed.
5.5.4.1	m	The MRZ shall be checked for International Civil Aviation Organization (ICAO) compliance.
5.5.4.2	m	Spectrally selective checks SHOULD be performed if applicable for the given document model. At least the check (UV, BR, FU) SHALL be performed. 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.

Table 4.2 Requirements for Stationary application scenarios - Optical Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.6.1	m	Connections to the background public key infrastructures SHALL be available.
5.6.1.1	m	Defect and Master Lists SHALL be supported.
5.6.2	m	Access and process sequences SHALL be supported.

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.6.3	m	Chip access protocols SHALL be supported.
5.6.4	m	Checking chip contents SHALL be performed.

Table 4.3 Requirements for Stationary application scenarios - Electronic Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.7.1	m	Checking the expiration of the documents SHALL be performed.
5.7.2	m	If the document is an eMRTD / Electronic Identity Document (eID), “Checking the optical biographic data against the electronic biographic data” SHALL be performed.
5.7.3	o	Checks across document pages.
5.7.4	o	Checks across several documents and linking of multiple document checks in a transaction.
5.7.5	o	Comparison of personalization contents is recommended for all documents that are present in a check database.
5.7.6	o/e	Checking DG2 against the facial image from the Visual Zone (VIZ).

Table 4.4 Requirements for Stationary application scenarios - Combined Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.9.1	m	Digital seal checks SHALL be performed.

Table 4.5 Requirements for Stationary application scenarios - Digital Seal Checks

4.2.4. Requirements for Self Service application scenarios

The requirements for Self Service application scenarios are given ▸Table 4.6 (Optical checks), ▸Table 4.7 (Electronic Checks), ▸Table 4.8 (Combined Checks) and ▸Table 4.9 (Digital Seal Checks).

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.5.2	m	For all further optical checks, the document SHALL be detected and needs to be fully captured under different light sources.
5.5.3	m	Identification of the document model SHALL be performed.
5.5.4.1	m	The MRZ shall be checked for ICAO compliance.
5.5.4.2	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 MAY be changed to evaluatory. Additional note: The system SHALL support a blacklist, where this option can be disabled for specific countries.

Table 4.6 Requirements for Self Service application scenarios - Optical Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.6.1	m	Connections to the background public key infrastructures SHALL be available.
5.6.1.1	m	Defect and Master Lists SHALL be supported.
5.6.2	m	Access and process sequences SHALL be supported.
5.6.3	m	Chip access protocols SHALL be supported.
5.6.4	m	Checking chip contents SHALL be performed.

Table 4.7 Requirements for Self Service application scenarios - Electronic Checks

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

Table 4.8 Requirements for Self Service application scenarios - Combined Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.9.1	m	Digital seal checks SHALL be performed.

Table 4.9 Requirements for Self Service application scenarios - Digital Seal Checks

4.2.5. Requirements for Partially Mobile application scenarios

The requirements for Fully Mobile application scenarios are given in ▸Table 4.10 (Optical checks), ▸Table 4.11 (Electronic Checks), ▸Table 4.12 (Combined Checks) and ▸Table 4.13 (Digital Seal Checks)

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.5.2	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.
5.5.3	o	Depending on the optical reader, the document model SHOULD not be identified (e. g., swipe reader).
5.5.4.1	m	If a MRZ was read, the MRZ SHALL bechecked for ICAO compliance.

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.5.4.2	o/e	Depending on the optical reader, spectrally selective checks SHOULD be performed if applicable for the given document model. At least the checks (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.

Table 4.10 Requirements for Partially Mobile application scenarios - Optical Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.6.1	m	Connections to the background public key infrastructures SHALL be available.
5.6.1.1	m	Defect and Master Lists SHALL be supported.
5.6.2	m	Access and process sequences SHALL be supported.
5.6.3	m	Chip access protocols SHALL be supported.
5.6.4	m	Checking chip contents SHALL be performed.

Table 4.11 Requirements for Partially Mobile application scenarios - Electronic Checks

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

Table 4.12 Requirements for Partially Mobile application scenarios - Combined Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.9.1	m	Digital seal checks SHALL be performed.

Table 4.13 Requirements for Partially Mobile application scenarios - Digital Seal Checks

4.2.6. Requirements for Fully Mobile application scenarios

The requirements for Fully Mobile application scenarios are given in ▸Table 4.14 (Optical checks), ▸Table 4.15 (Electronic Checks), ▸Table 4.16 (Combined Checks) and ▸Table 4.17 (Digital Seal Checks)

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.5.2	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.
5.5.3	o	Depending on the optical reader, the document model SHOULD not be identified (e. g., swipe reader, integrated camera).
5.5.4.1	o	If a MRZ was read, the MRZ SHALL bechecked for ICAO compliance.
5.5.4.2	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.

Table 4.14 Requirements for Fully Mobile application scenarios

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.6.1	m	Connections to the background public key infrastructures SHALL be available.
5.6.1.1	m	Defect and Master Lists SHALL be supported.
5.6.2	m	Access and process sequences SHALL be supported.
5.6.3	m	Chip access protocols SHALL be supported.
5.6.4	m	Checking chip contents SHALL be performed.

Table 4.15 Requirements for Fully Mobile application scenarios - Electronic Checks

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

Table 4.16 Requirements for Fully Mobile application scenarios - Combined Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.9.1	m	Digital seal checks SHALL be performed.

Table 4.17 Requirements for Fully Mobile application scenarios - Digital Seal Checks

4.2.7. 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.

The requirements for Kiosk application scenarios are given in ▸Table 4.18 (Optical checks), ▸Table 4.19 (Electronic Checks), ▸Table 4.20 (Combined Checks) and ▸Table 4.21 (Digital Seal Checks).

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.5.2	m	For all further checking steps the model SHALL be identified.
5.5.3	m	MRZ consistency check shall always be possible, regardless of the used technology.
5.5.4.1	m	If a MRZ was read, the MRZ SHALL bechecked for ICAO compliance.
5.5.4.2	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.

Table 4.18 Requirements for Kiosk application scenarios - Optical Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.6.1	m	Connections to the background public key infrastructures SHALL be available.
5.6.1.1	m	Defect and Master Lists SHALL be supported.
5.6.2	m	Access and process sequences SHALL be supported.
5.6.3	m	Chip access protocols SHALL be supported.
5.6.4	m	Checking chip contents SHALL be performed.

Table 4.19 Requirements for Kiosk application scenarios - Electronic Checks

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

Table 4.20 Requirements for Kiosk application scenarios - Combined Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
5.9.1	m	Digital seal checks SHALL be performed.

Table 4.21 Requirements for Kiosk application scenarios - Digital Seal Checks

4.2.8. Requirements for asylum registration application scenarios

A document inspection system needs a recent Master list to perform electronic checks on electronic MRTDs and recent Signer Lists to perform checks on digital seals (see [BSI TR-03135-1] section 5.6.1).

There are two use cases for retrieving a new list of the type Master List or Signer List.

- Automatic Retrieval and Deployment (see [BSI TR-03135-1] section 5.6.1.1 for the RECOMMENDED implementation)

  If the list can be automatically retrieved and deployed by the document inspection system, it MUST retrieve and deploy the most recent list at least once every three workdays. It is recommended to check for updates daily and to deploy them immediately.

- Manual Retrieval and/or Deployment

  If the list has to be retrieved and/or deployed manually, the administrator of the document inspection system MUST retrieve and deploy the most recent list at least once every four calendar weeks.

In this scenario the schema element `//dc:UsedLists` MUST be present and populated in every generated log. The hash algorithm SHA256 MUST be used to calculate the hash of the list signer certificate.

Checking requirements for asylum registration application scenarios are given in ▸Table 4.22 (Optical checks), ▸Table 4.23 (Electronic Checks), ▸Table 4.24 (Combined Checks) and ▸Table 4.25 (Digital Seal Checks).

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
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 bechecked 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.

Table 4.22 Requirements for initial registration application scenarios - Optical Checks

Ref. [BSI 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.

Table 4.23 Requirements for initial registration application scenarios - Electronic Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
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 4.24 Requirements for initial registration application scenarios - Combined Checks

Ref. [BSI TR-03135-1]	**Obligation (m/o/e)**	**Notes**
4.9.1	m	Digital seal checks SHALL be performed.

Table 4.25 Requirements for initial registration application scenarios - Digital Seal Checks

4.3. Requirements on operational monitoring

The document check system SHALL implement the logging schema according to [BSI TR-03135-1], chapter 6.

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 4.26.

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/*
Digital Seal Check	//dcs:Data/dcs:Content
Biometric Check	//dc:Image

Table 4.26 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.

4.3.1. Basic logging profile

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

4.3.2. 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.

4.3.3. 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.

4.3.4. Standard logging profile with electronic evaluation extensions

Standard logging with electronic 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.

4.3.5. Standard logging profile with digital seal evaluation extensions

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

4.3.6. Full logging profile

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

4.4. Requirements on data transmission

The document check system SHALL implement the transmission and log specification according to [BSI 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.

5. Conformity

In order to conform to this Technical Guideline, an Inspection System and Inspection Application SHALL completely implement and meet all requirements from ▸Chapter 4 for the used scenario.

List of Abbreviations

Abbreviation	Description
ABC	Automated Border Control
CAN	Card Access Number
eID	Electronic Identity Document
eMRTD	Electronic Machine Readable Travel Document
ICAO	International Civil Aviation Organization
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
RFID	radio-frequency identification
VIZ	Visual Zone
XML	Extensible Markup Language

Bibliography

[BSI TR-03135-1] *BSI TR-03135-1, Technical Guideline Machine Authentication of MRTDs for Public Sector Applications. Part 1: Overview and Functional Requirements, Version 2.5.*

[KeepAChangelog] *Keep a Changelog – https://keepachangelog.com/en/1.0.0/.*

[RFC2119] *Request For Comments Editor (RFC), Bradner, Scott: Key words for use in RFCs to indicate requirement levels, RFC 2119, 1997.*