For Publication on the ICAO Website

Best Practice Guidelines for Optical Machine Authentication

Part 1- Recommendations

DISCLAIMER: All reasonable precautions have been taken by ICAO to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied; nor does it necessarily represent the decisions or policies of ICAO. The responsibility for the interpretation and use of the material contained or referred to in this publication lies with the reader and in no event shall ICAO be liable for damages arising from reliance upon or use of the same. This publication shall not be considered as a substitute for the government policies or decisions relating to information contained in it. This publication contains the collective views of an international group of experts, believed to be reliable and accurately reproduced at the time of printing. Nevertheless, ICAO does not assume any legal liability or responsibility for the accuracy or completeness of the views expressed by the international group of experts.

Version 1.2

February 2018

File: Best Practice Guidelines for Optical Machine Authentication

Author: Subgroup of the New Technologies Working Group (NTWG), Working group of the ICAO Technical Advisory Group on the Traveller Identification Programme (TAG/TRIP)

Release Control

Release	Date	Description
1.0	2015-11-17	Distributed at the NTWG Meeting
1.1	2016-02-29	Incorporated comments by NTWG, especially from CHE (Fedpol), FRA (AFNOR), NZL (Passport Office), GBR (Delarue), USA (DOS) and D (Bundesdruckerei)
1.1.1	2016-03-02	Incorporated comments by NLD (MOI)
	2016-03-30 to 2016-04-01	ICAO TAG/TRIP 1, ex-TAG/MRTD23: Agenda Item 2: WP 20 endorsed and approved
1.1.2	2016-05-03	Incorporated amended comments by FRA (AFNOR) and comments by BE (Foreign Affairs) and additional comments by D (Bundesdruckerei)
1.1.2.a	2016-05-24	Incorporated additional comments by FRA (AFNOR)
1.1.3	2016-11-09	Incorporated additional comments by FRA (AFNOR and Oberthur) as well as outcome discussion NTWG Seattle
1.1.4	2017-07-28	Marginal amendments inside the catalogue of generic check routines (to be consistent with BSI-TR-03135)
1.1.5	2017-11-08	Amendment of the Introduction referencing the Publication “Passport and Systematic Checks at Ports of Entry and Strategies to Combat Document Fraud among G7 Countries”
1.2	2018-02-28	Incorporated comments of JPN: amendment of the catalogue of generic check routines to include barcode features; Changed document status to Technical Report

Editorial group		
Uwe Seidel	D	NTWG, sub group leader
Ulrich Schneider	D	BKA
Evelyn Spitzwieser	D	secunet
Christophe Ndong Ntoume	D	secunet
Jörn-Marc Schmidt	D	secunet

Summary

In the field of machine assisted authentication of Machine Readable Travel Documents (MRTDs), considerable progress has been made over the last decade. Technical innovations made in the security design of MRTDs and in the development of authentication systems (readers, software, etc.) have allowed for machine-based document authentication to slowly become an integral part of several control infrastructures and processes (e.g. border control).

However, new challenges arise for experts, manufacturers and authorities involved in the field as technical improvements achieve higher security and efficiency in operational processes. Some of the main challenges are the lack of harmonization and standardization of the processes in place, and the lack of coordination between the main parties involved in those processes, both leading to system parts and components being developed independently without consideration for major implications resulting from their interaction. Furthermore, the complexity and diversity of the systems currently available on the market make it especially difficult to evaluate and/or compare them.

This first part of the Best Practice Guidelines aims to provide a set of recommendations and methods for improving the design of security documents as well as integration and operation of systems and processes involved in optical machine assisted authentication of MRTDs. To achieve this goal, this document will:

- Propose a modular definition of the following key components of a generic document inspection system:

    - the machine readable travel document (MRTD) itself with its specific security features,

    - the full page reader with its technical capabilities for optical machine authentication (e.g. resolution, illumination geometry and spectral range), and

    - the authentication software, usually based on a proprietary authentication database.

- Propose and structure the steps of the inspection process of MRTDs.

- Propose a catalogue that allows for a common generic specification of feasible check routines and processes across different inspection systems. This specification is based on a systematic description of a feature and the corresponding ability to apply a check routine. Therefore, the generic check routines are categorized via the following three parameters: illumination wavelength applied, feature property probed, and region considered.
  The application of this catalogue of generic check routines will greatly improve

ways to generically describe, measure and analyze the performance of the above mentioned key components.

- Give recommendations for all parties involved, namely security documents' designers, manufacturers of full page readers, programmers of authentication software and databases and finally the operating authorities. The following details are discussed:

  - Suitable and potentially interfering security features and their particular design from a machine vision point of view,

  - Minimum requirements for the technical specifications of full page readers to allow for successfully conducting machine authentication,

  - Requirements for authentication software, especially image acquisition, hardware-software (in)dependence, document detection and order of live-image capture,

  - Mechanisms for document identification and document verification processes,

  - Handling of multiple pages (such as ID cards) and cross document results (e.g. Passport plus Visa),

  - Exemplary GUI and process visualization, and

  - System update modalities.

- Address monitoring and logging issues, especially privacy considerations including anonymization methods.

A second part – to be published later – will focus on the methods and tools of evaluating machine authentication systems, based on the analysis and insights gained from real-life setups and operative border control systems: this Part 2 will act as guideline for evaluating optical authentication systems from planning the test setup and selecting the evaluation components to analyzing based on defined error rates.

Table Of Contents

List of Figures

List of Tables

1 Introduction

For the authentication of machine-readable travel documents (MRTDs) as part of stationary border control as well as ABC gates, the use of IT systems, which go beyond the pure extraction and checking of the documents' MRZ and also automatically inspect optical security features increases. The major improvements in technologies used in the context of machine based document authentication have contributed to the growth of the amount and diversity of the authentication systems. However, the significant increasing traveler volume still remains challenging for all actors involved in the design, production and deployment of authentication systems and MRTDs.

Authentication systems used to perform machine authentication of MRTDs include several components that are required to properly interact with each other. Furthermore, the security features of machine-readable documents need to be designed and implemented in accordance with the capabilities of the authentication systems and the insights of experienced practitioners. Even though extensive work has been done on the subject in the ICAO Technical Report "Machine Assisted Document Security Verification" [MADSV], international standardization for all components involved in the authentication process is currently not being enforced and is therefore of particular importance.

The Best Practice Guidelines are divided into two parts. The first part (this document) provides a set of recommendations for the main parties involved in the design, implementation and operation of the affected systems and key components, whereby the main goals are:

- increase the awareness for the relevant security-related questions of machine authentication, involving the main stakeholders e.g. security document producers, reading equipment manufacturers and government,
- propose a catalogue of generic check routines with a consistent terminology,
- define recommendations for security document designers, manufacturers of authentication systems, and operational level.

The second part of the Best Practice Guidelines defines a set of methods and tools for the evaluation of authentication systems and document related security features. For further details about the evaluation part of the Best Practice Guidelines, please refer to "The Best Practice Guidelines for Optical Machine Authentication Part 2" [BPGOMA_Part2].

This document is meant to support practitioners in the design, development of authentication systems. It is however important to bear in mind that the authentication system should be used to facilitate adjudication for its operator, and should not be regarded as decision maker by itself, particularly with regards to the security features that cannot be checked by the machine and can only be verified by a human operator.

The Best Practice Guidelines only deal with the optical part of the authentication of MRTDs and the scope of the recommendations provided in this document is limited to data acquired through Full Page Readers, i.e. full size images of the document. Furthermore, the Best Practice Guidelines do not distinguish between 1st, 2nd and 3rd level inspection as full page readers can be used in each of those scenarios. Altogether, mobile devices are (so far) not taken into consideration due to their limited optical capabilities with respect to different light sources (neither UV nor IR) and therefore not being able to meet the proposed requirements.

The basics and terminology required for a better understanding of this document are introduced in section 2. The issue of harmonization and standardization of check routines is addressed in section 3, where a catalogue of generic check routines will be defined. In section 4 the focus will be put on elaborated recommendations for manufacturers of authentication systems, and section 5 will highlight several approaches and methodologies related to data procession in accordance with data protection policies.

1.1 Terminology

Although the recommendations and guidelines presented in this document are non-binding for the parties directly affected by it, the present terminology has been adopted in order to provide an unambiguous description of what should be observed in order to achieve the goals defined in this document.

The present terminology should be regarded as a practical way to organize the recommendations and guidelines of this document in order of importance, and should not be mistaken with a set of restrictive requirements similar to those used in classical standards (e.g. ISO). This document is neither a standard nor defines a set of restrictive requirements and exclusively aims, as the title clearly states, to provide a set of best practice guidelines for machine authentication. Nevertheless, in order to provide the target group of this document with clear, precise and unambiguous guidance as to what is and is not in line with best practices, the present terminology is being used.

1.2 Previous work

The correlation between security features and check routines for machine assisted authentication has previously been analyzed in [MADSV] and discussed in [MADSV-DP] in which advice is given for manufacturers of MRTDs and readers. Even though similar concepts (such as feature classification) are addressed in [MADSV], the focus is directed more towards reader capabilities and the most appropriate document (security) features to get the most out of those capabilities.

The Best Practice Guidelines extend the scope of the insights collected in [MADSV] by expanding the set of recommendations to the main parties involved in the design, implementation, and most significantly, the operation of the affected systems and components. In contrast to [MADSV], the focus of the Best Practice Guidelines is more directed towards the greatest common divisor for all systems involved in the authentication process, and less towards a classification of readers' capabilities.

In addition, there has been substantial effort by ICAO to standardize security features for machine authentication (see [ICAO9303] Part 2, Chapter 3.1 "Feature types"). So far there has been only one concrete feature implemented in MRTDs that follows the requirements defined within that work: a considerable number of security documents are equipped with the so called "Structure feature" which is individual per nation and document type and can be verified by a common mechanism. As this special type of diffractive element so far unfortunately needs a very sophisticated document reader, there is currently no simple solution for machine-based detection of this element. Therefore, this document does not focus on machine inspection of proprietary security features or other dedicated security features that require special (also proprietary) hardware solutions.

Recently the publication "Passport and Systematic Checks at Ports of Entry and Strategies to Combat Document Fraud among G7 Countries" of the Migration Experts Sub-Group [G7-MESG] was circulated among the G7 countries. It summarizes answers of five countries to questionnaires sent to all G7 states and cumulates the findings. Finally recommendations are deduced, among them the following cited issues completely in line with this guideline:

- *Develop/compile best practices for MRTD inspection (usage) at the border. This includes both manual and automated border control.*
- *Promote and train border authorities to conduct thorough checks of ePassport security features at POEs ("ports of entry").* Findings indicate that the security features of ePassport are not fully utilized at POEs. […]
- *Develop and routinely update a set of minimum functionalities and operational performance tests for automated document inspection systems and passport readers.*
- *Compile a list and routinely update interoperability /technical issues with specific country passports, other non-standard travel documents and passport inspection systems and share with passport and border officials.* […]Lack of reference knowledge, as well as non-standard or unsuitable design and production of travel documents in circulation (passports and also ID cards), significantly affects the effectiveness of inspection processes and weakens confidence in the integrity of inspection systems.

- *Develop International system of document inspection standards* […]the continuous development and sophistication of the physical, optical and electronic security features of travel documents currently in circulation brings significant challenges[…]

1.3 Influence of the eletronic check on the authentication process

Although this document focuses on the optical part of the authentication of MRTDs, the electronic part has to be taken into consideration. Based on current state of technology, the interaction between a chip (eMRTD) and an RF module (full page reader) during the authentication process is highly probable and can be expected. Some of the recommendations given in this document are best understood when keeping in mind that both optical and electronic checks (if applicable) are complementary processes converging to an overall result.

In this document, two aspects of the interaction between electronic and optical checks are of particular interest: the comparison of optical and electronic data and the implications behind the check for presence of a chip if one is expected. For these two aspects, the influence of the electronic check cannot be disregarded and will be highlighted in the corresponding recommendations.

2 Definitions

In the following chapter, a consistent terminology will be introduced for further use. The process of inspection of MRTDs is described in general in section 2.1, and in detail in section 2.2. In section 1.3 the influence of the electronic part of the authentication process is being addressed.

2.1 Process of Identification and Verification of MRTDs

The authenticity verification of a travel document includes the verification of the document's optical security features. It is performed by an authentication system which consists of the following components: a full page reader, authentication software, an authentication database and optionally a reference database.

The full page reader creates full size images of the travel document to be verified under different light sources. This so-called *live data-set* (=full size images of the document) is transferred to the authentication software by the full page reader.

The authentication software usually identifies the so-called *document model* of the document using the Machine Readable Zone (MRZ) and/or additional information (e.g. document specific pattern, date of issue, specific optical features, etc.) as input. A document model covers those document series of a nation which have the same optical appearance.

In accordance to the technical guideline [BSI-TR-03135], a document model is defined by means of the country code (C), document type (T), a unique identification number (N) and the year value of first issuance (Y):

Document Model := (C, T, N, Y) [1]

The country code C has to be filled in according to the ICAO specifications in [ICAO9303] as a three-letter code.

The document type T is specified by the ICAO in [ICAO9303].

The identification number N must be a unique chronological increasing integer number starting with 1 referencing the model – or generation – of the document.

The year Y refers to the year as a 4-digit integer value in which a document of that particular model was issued for the first time. If the year is unknown, this value shall be omitted.

[1] The Best Practice Guidelines only focus on the optical part of machine-based document authentication. This means that documents that are optically identical but differ when considering electronic features, are considered to belong to the same document model.

For instance, the two British passport/document models from 2008 and 2010 currently in circulation have the following identifiers: (GBR, P, 1, 2008) and (GBR, P, 2, 2010).

There are various technical approaches for identifying the document model. MRZ acquisition is one of them (cf. section 4.3.2). If the MRZ is used but not sufficient for the unambiguous determination of the document model, additional document parameters (e.g. patterns) have to be used to help narrow down the identification results; especially when dealing with several valid document models of the same country (e.g. British passport)[2].

The authentication software sends the document model's identifier to the authentication database where the so-called *check routines* are stored. These check routines define which testing procedures have to be applied to the live data-set of this particular travel document model. A specific set of check routines, the so-called *authentication data-set*, is determined for each document model. After the receipt of the document model's identifier, the authentication database sends the corresponding data-set to the authentication software. Further details on the setup of an authentication database will be provided in section 2.2.

[2] Some countries, such as Australia, use a series' Letter to distinguish different document models or series (e.g. N-series). Even though this method might be sufficient at national level, it is not very efficient for international classification because of the lack of standardisation. Therefore, this document follows the recommendations of [BSI-TR-03135] which are considered to be more suitable for that purpose.

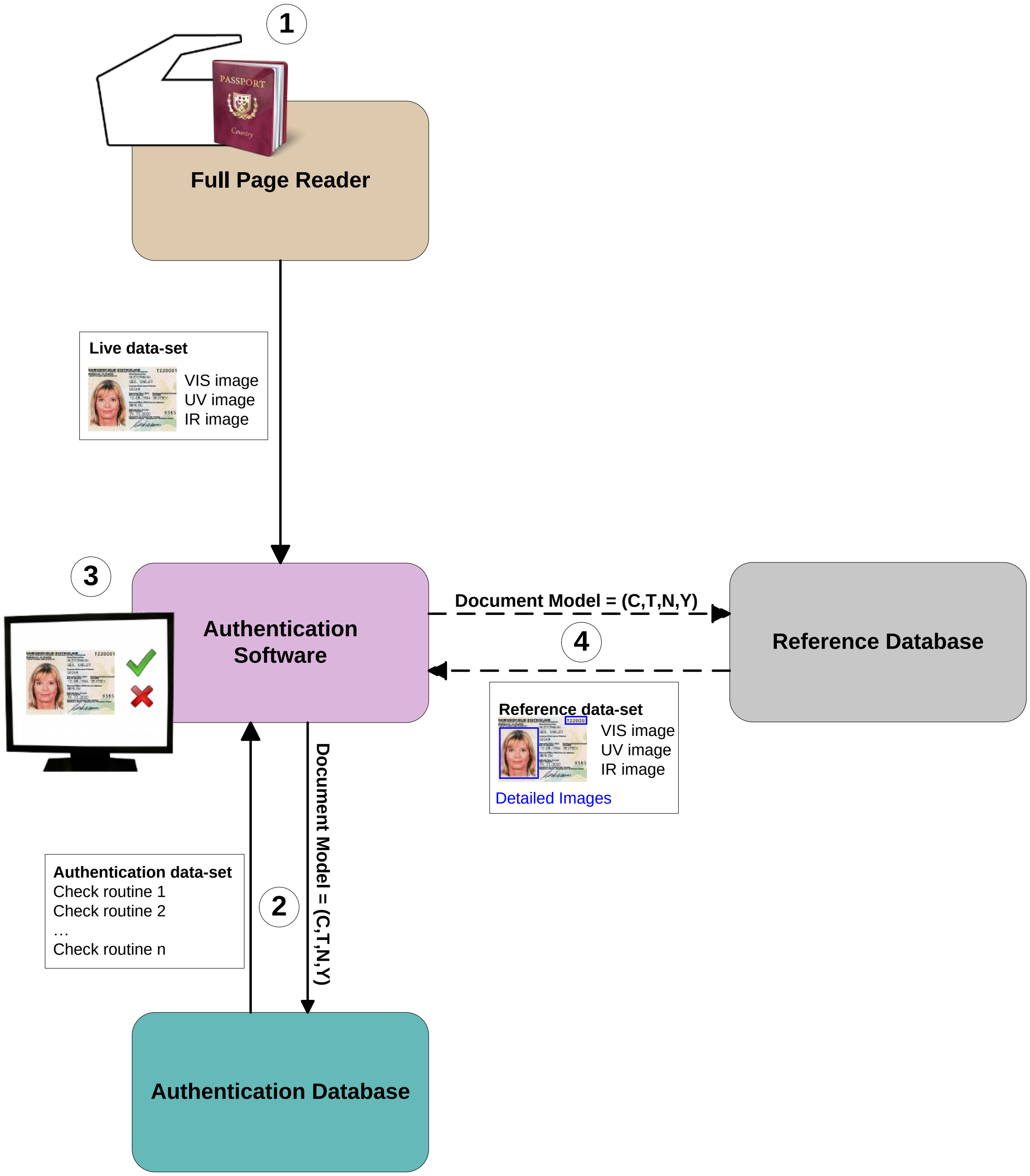


Figure 2–1: Process of document identification and verification; the numbers denote the order of the involved process steps

The verification is now performed by the authentication software. The check routines are applied to the travel document’s live data-set. This examination usually leads to a Pass- or Fail-result. A Pass-result implies that the checked document does not present any abnormalities, whereby a Fail-result means the opposite. Depending on the application scenario, the interpretation of the result (pass or fail) is the responsibility of the human operator.

If a live data-set cannot be assigned unambiguously to a particular document model, a subset of check routines should be performed optionally. These check routines are specified independently of the document model.

In order to support the human operator in a manual verification, the authentication software can request the so-called *reference data-set* from the reference database on the basis of the identified document model. The reference data-set contains the visible-light (white), IR and UV images of the document model and can also include more detailed pictures of document parts as well as further textual descriptions. However, this so-called reference database, also referred to as *expert database* in practice, is not a mandatory component of the actual authentication system. The process of document identification and verification is illustrated in Figure 2–1.

2.2 Detailed Setup of an Authentication Database

In the authentication database a distinct set of check routines is stored for each document model. For instance, the check routines for the German document model from 2007 differ from the routines which have to be applied to the British document model from 2008.

A check routine of a set denotes a test specification for an optical security feature's property. E.g. the check routine 1 in Figure 2–2 checks whether the photo is absorbent in visible light. In this case the photo is the optical feature, which is tested for the property of absorption under visible light (see light source 1 in check routine 1). The implementation of this check routine is carried out by an authentication algorithm provided by the authentication software (see authentication algorithm 1 in check routine 1). In this case, algorithm 1 is an authentication algorithm which checks the feature's brightness. In contrast, check routine x in Figure 2–2 checks whether or not the ink is luminescent under UV light within the area of the photo by using the "pattern check" algorithm (check algorithm n of the authentication software on Figure 2–2). This example shows clearly that an optical security feature can offer different properties under different light sources (see Figure 2–3).

In terms of the EU regulation on minimum standards for security features and biometrics in passports and travel documents [EC2252] these check routines can be reasonably split into the three categories: material, printing technique and personalization.

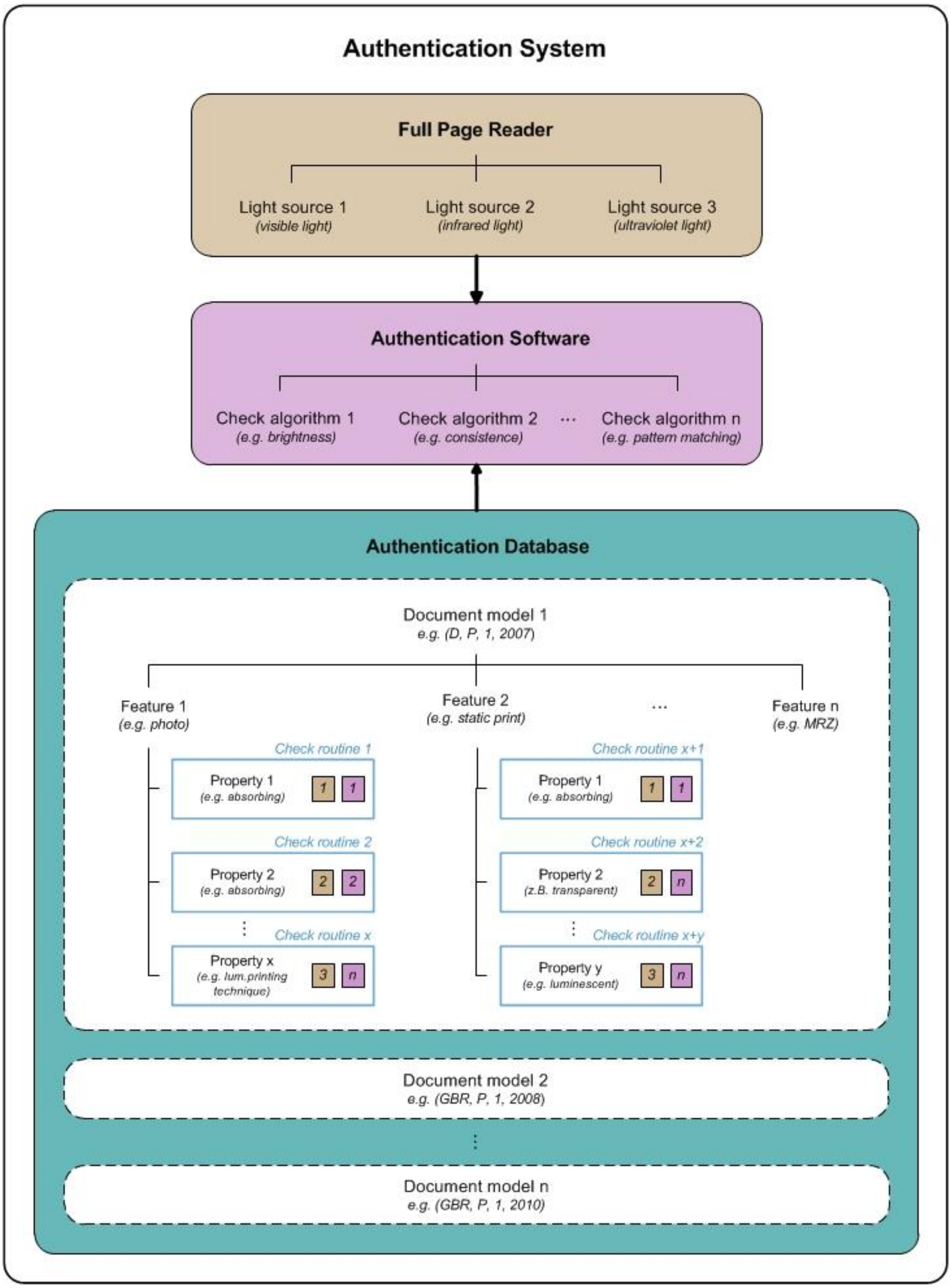


Figure 2–2: Schematic diagram of the setup of an authentication system

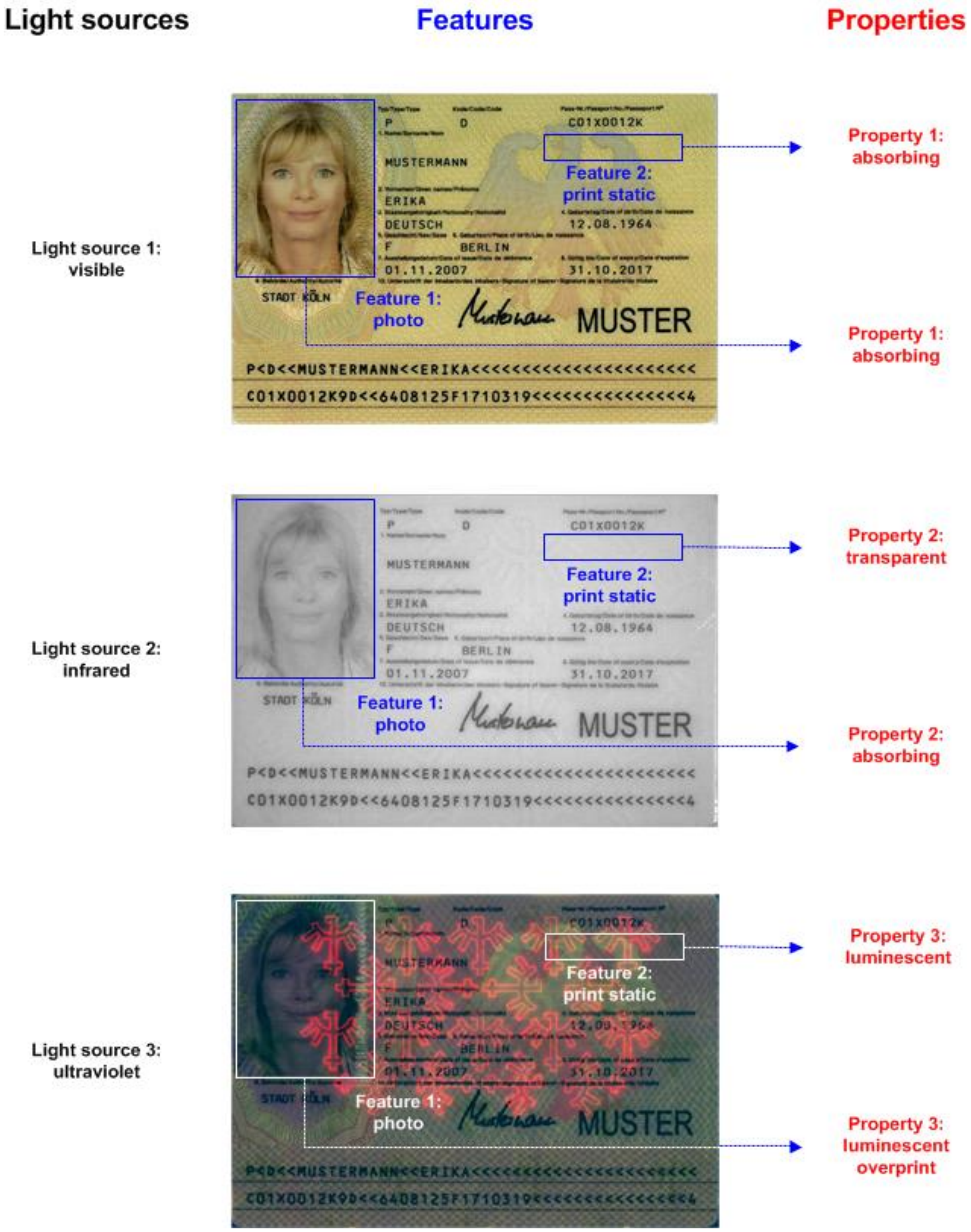


Figure 2–3: Features and properties under different light sources using the example of the German passport

3 Catalogue of Generic Check Routines

Every developer of an authentication system defines his own identifiers for the check routines. On the one hand these check routines are distinct for each document model. On the other hand the identifiers for these check routines are often not self-explanatory. Hence, the comparability of the applied check routines for the same document model for different authentication systems is in general not existent.

In order to solve this problem, it is possible to define a catalogue of feasible check routines on the basis of the spectrally selective security features in travel documents. The content of this catalogue may be extended in future versions of this guideline preserving the proposed nomenclature. The corresponding so-called *spectrally selective check routines* record different reactions occurring on a document checked under visible (VI - visible light) or extra visible (UV - ultraviolet, IR - infrared) light. Based on the three records (VI, UV, IR), the absorbent, reflective or luminescent reactions of these features can be checked. Sequentially these spectrally selective check routines will be denoted by *generic check routines* as defined in the [BSI-TR-03135].

The application of this catalogue of generic check routines would greatly improve the above mentioned situation and will allow for a better understanding of machine authentication mechanisms.

3.1 Description of Generic Check Routines

The below defined unambiguous identifiers of check routines have been defined for the optical machine authentication on the basis of the spectral reaction of security features in travel documents. They can be reasonably split into the following four categories defined in the EU regulation on minimum standards for security features and biometrics in passports and travel documents [EC2252] as well as in ICAO Doc9303 [ICAO9303]:

- Check for material (substrate) properties: Reactions of the printing substrate are verified, e.g. brightness under UV light
- Check for printing technique properties: Features, which are printed onto/into the document irrespective of personalization, are tested, e.g. form print
- Check for features that protect copying: usually diffractive or holographic elements or laminates
- Check for issuing technique (personalization) properties: Personalized features are tested, e.g. the name of the document’s holder

The optical appearance of the features of the category “copy protection” is very depending on illumination geometry. Therefore features of this category– well suited for human inspection – can be very problematic for machine authentication in general. For this reason, features of this category are not addressed by the proposed check routines.

The 48 generic check routines defined below consist of so-called *basic check routines (BR)* and *composite check routines (CR)*. Basic check routines are individual routines, which refer to one property (e.g. IR absorption) of a single feature. Composite check routines are defined as logical combinations of basic check routines. Consequently, a single feature can be tested for multiple properties such as IR absorption and transparency in visible light.

For the basic check routines, the following abbreviated definitions according to [BSI-TR-03135] are used:

Basic check routine := (XX, YY, ZZ)

XX specifies the light source for the image on which the check routine is performed:

- **IR** – Infrared light
- **UV** – Ultraviolet light
- **VI** – Visible (white) light

YY is an identifier for the optical property of the particular feature:

- **AB** – absorbent, property of ink
- **BR** – brightness, property of substrate (e.g. bright under exposure of UV light)
- **FR** – spatial frequency property of patterns (e.g. characteristics of patterns obtained after spatial frequency transformation such as spatial Fourier transformation)
- **LU** – luminescent, property of patterns (e.g. visible under exposure of UV light)
- **TL** – translucent, property of ink shining through the substrate
- **TR** – transparent, property of ink (e.g. transparent under exposure of IR light)

ZZ is an identifier[3] for the feature itself or the position in the document:

- **FI** – Fibers

[3] Within this nomenclature, document model specific properties are denoted by “static” (such as UV overprint of a coat of arms) whereas document specific (individual/personalised) properties are denoted by “dynamic” (such as UV overprint repeating the document number).

- **FU** – Full (complete) data page
- **IS** – printed feature, which already exists on the substrate (ink static)
- **MR** – Machine Readable Zone (MRZ)
- **OM** – Overprinted MRZ
- **CA** – Card Access Number (short: CAN)
- **BC** – Barcode feature
- **PD** – Personalized, “dynamic” perforation
- **PS** – Perforation showing “static” content
- **PH** – Area of the photo
- **SP** – Area of the secondary photo
- **OP** – Overprinted photo
- **TH** – Security thread
- **VZ** – Visual inspection zone (VIZ)
- **WM** – Watermark
- **ID** – any other personalized, “dynamic” feature (ink dynamic), e.g. a secondary photograph
- **AF** – any additional feature that cannot be attributed to the items specified above

If a generic check routine consists of more than one single check routine, a sequential number has to be assigned to each single check routine.

The following generic check routines result from these short-terms[4]:

Check of material properties: (12 BR + 1 CR)

- **(IR, AB, PS) →** (IR, absorbent, static perforation): Check whether the static perforation is visible under IR light.
- **(IR, AB, TH) →** (IR, absorbent, thread): Check whether the security thread is visible under IR light.

[4] Check routines based on the AF feature are not explicitly listed, because they can be combined with each of the mentioned light source and optical property.

- **(IR, AB, WM)** → (IR, absorbent, watermark): Check whether the watermark is visible under IR light.
- **(UV, BR, FU)** → (UV, brightness, full): Check for the brightness of the full data page under UV light.
- **(UV, BR, MR)** → (UV, brightness, MRZ): Check for the brightness in the MRZ area under UV light.
- **(UV, BR, PH)** → (UV, brightness, photo): Check for the brightness in the photo area under UV light.
- **(UV, BR, VZ)** → (UV, brightness, VIZ): Check for the brightness in the Visual Inspection Zone (VIZ) under UV-light
- **(UV, LU, FI)** → (UV, luminescent, fibers): Check for the presence of fibers which are luminescent under UV light.
- **(UV, LU, PS)** → (UV, luminescent, static perforation): Check whether traces of a static perforation are luminescent under UV light.
- **(UV, LU, TH)** → (UV, luminescent, thread): Check for the presence of a security thread which is luminescent under UV light.
- **(VI, TR, TH)** → (VI, transparent, thread): Check whether the security thread is transparent under visible light.
- **(VI, AB, PS)** → (VI, absorbent, static perforation): Check whether a static perforation is visible under visible light.
- **(IR, AB, TH)** ° (**VI, TR, TH)** → (IR, absorbent, thread) in combination with (VI, transparent, thread): Check whether a security thread, which is visible under IR light, is transparent under visible light.

Check of printing technique properties: (8 BR + 2 CR)

- **(IR, AB, IS)** → (IR, absorbent, static ink): Check whether the ink of the static print is absorbent under IR light.
- **(IR, TL, IS)** → (IR, translucent, static ink): Check whether the ink on the back of the data page (usually the title page) is translucent under IR light and can be detected on the IR image of the data page.
- **(IR, TR, IS)** → (IR, transparent, static ink): Check whether the ink of the static print is transparent under IR light.
- **(UV, LU, IS)** → (UV, luminescent, static ink): Check whether the ink of the static print is luminescent under UV light.

- **(UV, LU, OM)** → (UV, luminescent, overprinted MRZ): Check whether the ink of the static print is luminescent in the MRZ area under UV light.

- **(UV, LU, OP)** → (UV, luminescent, overprinted photo): Check whether the ink of the static print is luminescent in the area of the photo under UV light.

- **(VI, AB, IS)** → (VI, absorbent, static ink): Check whether the ink of the static print is absorbent under visible light.

- **(VI, TR, IS)** → (VI, transparent, static ink): Check whether the ink of the static print is transparent under visible light.

- **(IR, TR, IS)** ° **(IR, AB, IS)** → (IR, transparent, static ink) in combination with (IR, absorbent, static ink): Check whether parts of the static print are absorbent in IR light, whereas other parts of the same feature are transparent in IR light.

- **(IR, TR, IS)** ° **(VI, AB, IS)** → (IR, transparent, static ink) in combination with (VI, absorbent, static ink): Check whether the ink of the static print is both transparent under IR light and absorbent under visible light.

Check of personalization properties: (28 BR + 3 CR)

- **(IR, AB, ID)** → (IR, absorbent, dynamic ink): Check whether the ink of the dynamic print is absorbent under IR light.

- **(IR, AB, MR)** → (IR, absorbent, MRZ B900 check): Check whether the MRZ is visible under IR light.

- **(IR, AB, CA)** → (IR, absorbent, CAN): Check whether the CAN is visible under IR light.

- **(IR, AB, BC)** → (IR, absorbent, barcode): Check whether the barcode is visible under IR light.

- **(IR, AB, PD)** → (IR, absorbent, dynamic perforation): Check whether a dynamic perforation is visible under IR light.

- **(IR, AB, PH)** → (IR, absorbent, photo): Check whether the photo is visible under IR light.

- **(IR, FR, PH)** → (IR, frequency, photo): Check whether the pattern has the expected characteristics after spatial frequency transformation.

- **(IR, AB, SP)** → (IR, absorbent, secondary photo): Check whether the secondary photo is visible under IR light.

- **(IR, TR, SP)** → (IR, transparent, secondary photo): Check whether the secondary photo is transparent under IR light.

- **(IR, TR, ID) →** (IR, transparent, dynamic ink): Check whether the ink of the dynamic print is transparent under IR light.

- **(IR, TR, PH) →** (IR, transparent, photo): Check for the transparency of the photo under IR light.

- **(UV, FR, PH)** → (UV, frequency, photo): Check whether the pattern has the expected characteristics after spatial frequency transformation.

- **(UV, LU, SP)** → (UV, luminescent, secondary photo): Check whether the secondary photo is luminescent under UV light.

- **(UV, LU, BC)** → (UV, luminescent, barcode): Check whether the barcode is luminescent under UV light.

- **(UV, LU, ID) →** (UV, luminescent, dynamic ink): Check whether the ink of the dynamic print is luminescent under UV light.

- **(UV, LU, PD) →** (UV, luminescent, dynamic perforation): Check whether marks of a dynamic perforation are luminescent under UV light.

- **(VI, AB, ID) →** (VI, absorbent, dynamic ink): Check whether the ink of the dynamic print is visible under visible light.

- **(VI, AB, MR) →** (VI, absorbent, MRZ): Check whether the MRZ is visible under visible light.

- **(VI, AB, CA) →** (VI, absorbent, CAN): Check whether the CAN is visible under visible light.

- **(VI, AB, BC)** → (VI, absorbent, barcode): Check whether the barcode is visible under visible light.

- **(VI, TR, BC)** → (VI, transparent, barcode): Check whether the barcode is transparent under visible light.

- **(VI, AB, PD) →** (VI, absorbent, dynamic perforation): Check whether a dynamic perforation is visible under visible light.

- **(VI, AB, PH)** → (VI, absorbent, photo): Check whether the photo is visible under visible light.

- **(VI, AB, SP)** → (VI, absorbent, secondary photo): Check whether the secondary photo is visible under visible light.

- **(VI, TR, SP)** → (VI, transparent, secondary photo): Check whether the secondary photo is transparent under visible light.

- **(VI, FR, PH)** → (VI, frequency, photo): Check whether the pattern has the expected characteristics after spatial frequency transformation.

- **(VI, AB, SP)** → (VI, absorbent, secondary photo): Check whether the secondary photo is visible under visible light.

- **(VI, TR, ID)** → (VI, transparent, dynamic ink): Check whether the ink of the dynamic print is transparent under visible light.

- **(IR, TR, ID)** ° **(VI, AB, ID)** → (IR, transparent, dynamic ink) in combination with (VI, absorbent, dynamic ink): Check whether the ink of the dynamic print is transparent in IR light as well as absorbent under visible light.

- **(IR, TR, SP)** ° **(VI, AB, SP)** → (IR, transparent, secondary photo) in combination with (VI, absorbent, secondary photo): Check whether the secondary photo is transparent in IR light as well as absorbent under visible light.

- **(VI, TR, BC)** ° **(IR, AB, BC)** → (VI, transparent, barcode): Check whether the barcode is transparent under visible light as well as absorbent under IR light.

The following composite check routine is defined jointly for the two inspection classes printing and personalization:

- **(IR, TR, IS)** ° **(VI, AB, IS)** ° **(IR, AB, ID)** → (IR, transparent, static ink) in combination with (VI, absorbent, static ink) in combination with (IR, absorbent, dynamic ink): Check whether the ink of the static print is both absorbent under visible light and transparent in IR light. In addition, a dynamically printed feature is visible under IR light at the same position.

The check routines specified above are not of equal value related to their inspection significance. For instance, the result of the check routine (VI, AB, ID) is not meaningful per se. Though it gains in crucial importance for counterfeit detection when it is combined with the check routine (IR, TR, ID).

Counterfeit-specific properties or features should be incorporated by inverting the logic of check routines: e.g. a specific configuration of imitated security fibers by printing should be checked for absence of this pattern (i.e. VI, TR, IS).

The following Table 3-1 gives an overview of the classification of the generic check routine system. The three components of the routines' identifiers – feature, light source and property – are grouped in a matrix. Row, column and the cell's content describe a generic basic check routine. The assigned inspection classes are marked by the colors green (material), blue (printing technique) and yellow (personalization).

Feature		**Light source**		
		VI	**UV**	**IR**
Fibers	FI		LU	
Full data page	FU		BR	
Static printed feature	IS	{AB. TR}	LU	{AB, TR, TL}
MRZ	MR	AB	BR	AB
Overprinted MRZ	OM		LU	
CAN	CA	AB		AB
Barcode	BC	{AB, TR}	LU	AB
Personalized perforation (dynamic)	PD	AB	LU	AB
Perforation on the substrate (static)	PS	AB	LU	AB
Photo	PH	{AB, FR}	{BR, FR}	{AB, FR, TR}
Secondary Photo	SP	{AB, TR}	LU	{AB, TR}
Overprinted photo	OP		LU	
Security thread	TH	TR	LU	AB
Visual Inspection zone, VIZ	VZ		BR	
Watermark	WM			AB
Personalized dynamic feature	ID	{AB, TR}	LU	{AB, TR}
Additional feature	AF	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}	{AB,BR,LU, TL,TR}

Table 3-1: Matrix representation of the generic basic check routines

4 Recommendations for Machine Authentication of MRTDs

In the context of these Best Practice Guidelines, following key components are involved in the process of automated machine authentication: the document, the full page reader and the authentication software (incl. the authentication database, see section 2.2). However, these components are often designed/manufactured without consideration of their interdependencies especially with respect to the security-document design. In order to be able to perform an optimal machine authentication it is crucial that these components flawlessly interact with each other.

In the following sections, recommendations are given for efficient and effective design for the document itself (see section 4.1), for the full page reader (see tion 4.2), for the authentication software (see section 4.3), for the authentication database (see section 4.4) and for the reference database (see section 4.5). In section 4.6, the recommendations made in the former sections are mapped to exemplary usage scenarios in order to support operational managers in planning the operation of optical authentication systems.

When discussing recommendations for the different components, the difference of the typically involved time scales should be respected when referring to changes made:

- Inspection system software: 1 - 12 months
- Inspection system hardware: 3 - 5 years
- Security Document: 10 - 20 years (resulting from a typical issuing period of 5 – 10 years, and a validity period 5 – 10 years)

4.1 Document Designers

To design a document with optical features as secure as possible for the human inspection should not be the only goal of a document designer. The security features offered by the document should be applicable for machine authentication as well. In addition to the base design of machine readable travel documents (MRTD's) according to [ICAO9303], the following chapters summarize suitable features for machine authentication. Additionally, the following chapters will also summarize features that – even though they are of value for the human inspection – may counteract machine authentication (section 4.1.2). These features will be referred to as "potentially interfering" in the context of machine authentication.

Document designers should not be deterred from including those features in a document and should consider including those features while keeping their possible (negative) impact on the machine authentication process in mind.

4.1.1 Suitable Features for Machine Authentication

In the following, recommendations concerning suitable features for machine authentication are listed. These features have been selected because they are easy to detect on VI, IR and UV images and at the same time increase the counterfeiting effort.

A.1 **Define unambiguous identification features:** It is a common practice among certain countries to bring out successive document models within a relative short period of time in order to improve the security properties of their MRTDs. The British passport models (GBR, P, 1, 2008) and (GBR, P, 2, 2010) are good examples of successive document models. It is therefore required, during the document design process, to define features, which enable an unambiguous identification of the document model (e.g. barcode[5] with document model).

A.2 **Define features under all three light sources:** Field experience has shown that it is quite challenging for counterfeiters to properly reproduce features which appear genuine under different light sources while it is a standard feature of full page readers to capture images under these light sources. The definition of optical security features under all three light sources (VI, IR and UV) is therefore required to significantly increase the effort required to produce counterfeits.

A.3 **Define features in three categories:** Providing a balanced distribution of security features in the classes “material”, “printing technique” and “personalization” also increases the counterfeiting effort. Therefore, features must be defined in each class in compliance [EC2252].

A.4 **Define features on both sides of ID cards:** ID-1 sized ID cards are allowed to be positioned on a full page reader with both sides. Hence, document designers shall design ID-1 sized ID cards with identification and verification features on both sides in order to allow identification and verification independent of the card side.

A.5 **Define features reacting differently under different light sources:** Document features behaving differently under different light sources (see Figure 4–1), help to considerably reduce the success probability of counterfeiters in producing proper counterfeits. For machine authentication, it is therefore required to use features that can be either checked for their presence and/or ab-

[5] This example does not contradict the recommendations of [ICAO9303] (cf. section B3.6 of [ICAO9303]) which are meant for storing biometric data.

sence, depending on the corresponding light source (e.g. metameric inks, also called IR split in Figure 4–1, checkable by routine (IR, TR, IS) ° (VI, AB, IS)).

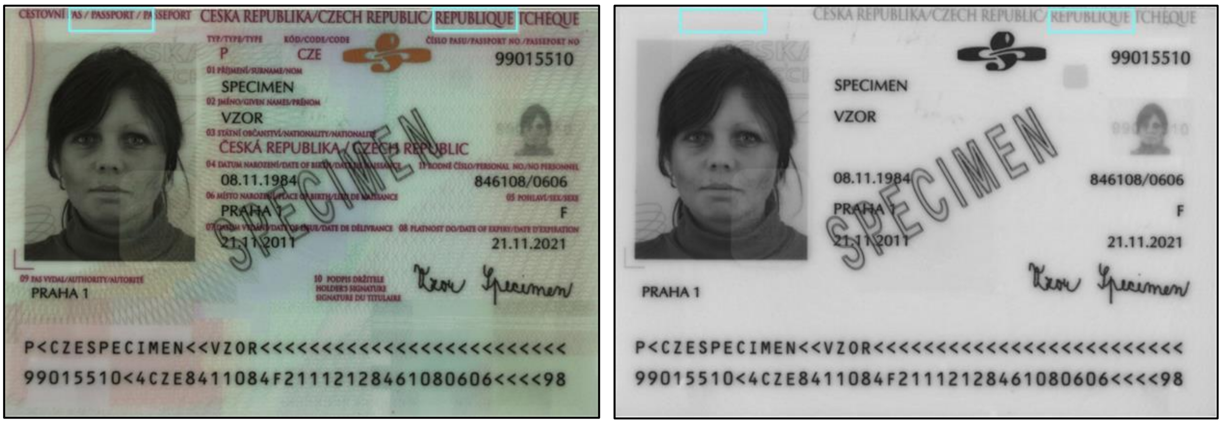

ČESKÁ REPUBLIKA/CZECH REPUBLIC/REPUBLIQUE TCHEQUE
P
CZE
99015510
SPECIMEN
VZOR
ČESKÁ REPUBLIKA/CZECH REPUBLIC
08.11.1984
846108/0606
PRAHA
F
21.11.2011
21.11.2021
PRAHA 1
SPECIMEN
P<CZESPECIMEN<<VZOR<<<<<<<<<<<<<<<<<<<<<<<<
99015510<4CZE8411084F2111212846108O606<<<<98

Figure 4–1: Passport (CZE, P, 1, 2011): IR split in title text

A.6 **Define features with different colors under UV light:** Features with different luminescent colors under UV light (see Figure 4–2) make the reproduction of that feature more complicated and are therefore recommended. At the same time, the color scheme of that feature can be checked during machine based authentication in addition to the simple presence check of that feature. Furthermore, it is recommended to use colors that differ significantly with respect to their chromaticity coordinates in order to facilitate the distinction by machines. The luminescence properties of the involved inks tend to degrade which further increases the challenge for reliable automatic detection.

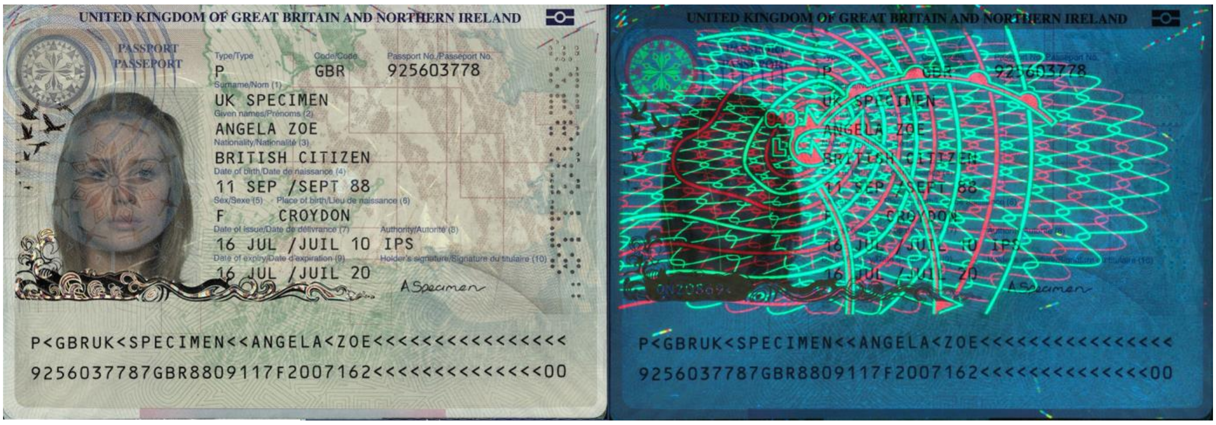

UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
PASSPORT
PASSEPORT
P
GBR
925603778
UK SPECIMEN
ANGELA ZOE
BRITISH CITIZEN
11 SEP /SEPT 88
F
CROYDON
16 JUL /JUIL 10
IPS
16 JUL /JUIL 20
P<GBRUK<SPECIMEN<<ANGELA<ZOE<<<<<<<<<<<<<<<<
9256037787GBR8809117F2007162<<<<<<<<<<<<<<00

Figure 4–2: Passport (GBR, P, 2, 2010): UV pattern with two colors[6]

A.7 **Define patterns with individual content, e.g. secondary facial image:** It is recommended to define individual patterns that can both be checked for their property and compared with already existing dynamic content on the data page. For instance, a secondary facial image can be compared with the primary facial image, and these two representations can have the same or different

[6] Source: http://edisontd.net/

spectral properties. The list of following patterns with secondary facial images is meant to illustrate this recommendation but is neither complete nor is it meant to be an explicit recommendation for these specific features:

a) Secondary facial image as smaller repetition of the facial image which is visible under visible light and transparent under IR light (checkable by (VI, AB, ID) ° (IR, TR, ID)).

b) Optically variable ink (OVI) and diffractive optically variable image devices (DOVIDs) that are personalized e.g. with laser engraving or laser ablation (see Figure 4–3). The exemplary feature depicted in Figure 4–3 shows different colors under different viewing angles in visible light (first and second picture) and a secondary facial image slightly visible under transmitted light (third picture). Under IR light, the secondary facial image can clearly be captured and compared to the facial image. The feature is checkable by the following composite check routine: (IR, AB, ID) ° (VI, AB, IS) ° (IR, TR, IS), which is a threefold combination.

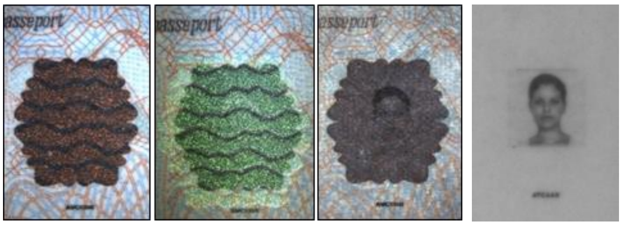


Figure 4–3: Passport (HUN, P, 1, 2006): Personalized OVI viewed under two different angles, under transmitted light and under IR light

c) Personalized laser engraving that reacts in an opposite (“negative”) manner (see Figure 4–4). The exemplary feature depicted in Figure 4–4 can be captured in visible light, where it shows a negative secondary facial image under two different angles.

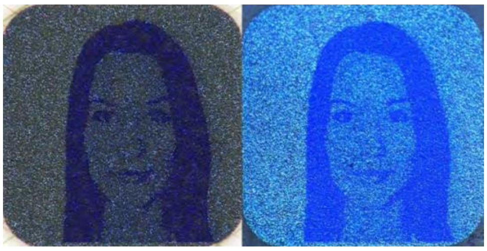


Figure 4–4: Passport (LVA, P, 1, 2015): “Negative” personalization through laser engraving under different viewing angles in visible light

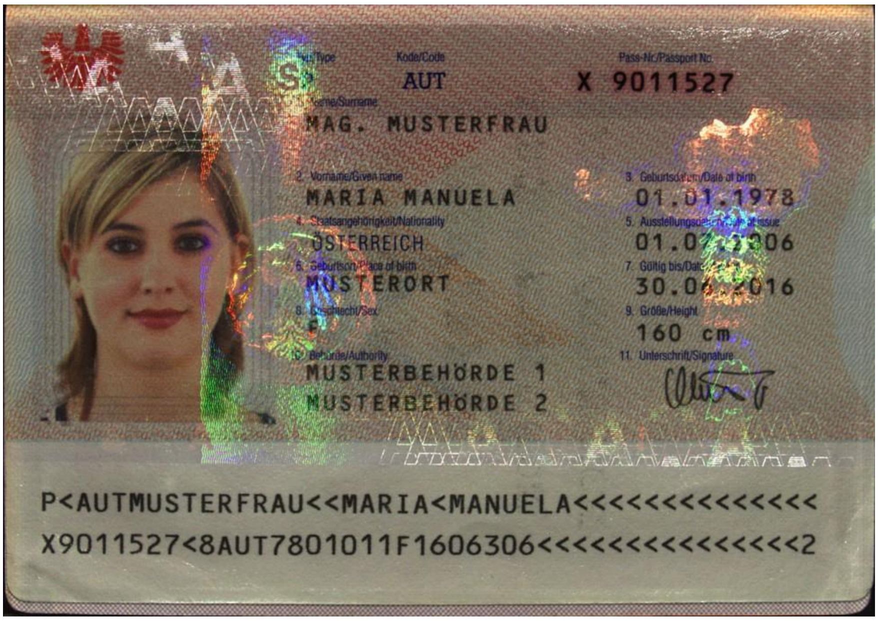
A.8 **Define features that remain stable over the validity period of the MRTD:** Some features tend to wear out over time. Colors of UV patterns, for instance, may fade over the validity period of the MRTD. Overlay glues can make UV patterns considerably lose their sharpness over time, leading to possible inaccurate check results for the feature. It is therefore recommended to define features that remain as stable as possible over of the validity period of the MRTD.

A.9 **Define a utopian document holder for specimen documents:** In order to establish a standardized way to identify specimen documents, it is recommended to set the nationality of the document holder to "UTO" for sample documents.

4.1.2 Potentially interfering features for Machine Authentication

This section deals with features that can possibly interfere with machine authentication (within the context mentioned at the beginning of section 4.1):

- **Overlapping features:** Overlapping features which are defined without considering their interdependency may negatively interact under the influence of a light source. The diffractive effects of a DOVID may interfere with the acquisition of the data page (see Figure 4–5).



Typ/Type P Kode/Code AUT Pass-Nr./Passport No. X 9011527

Name/Surname MAG. MUSTERFRAU

2. Vorname/Given name MARIA MANUELA

3. Geburtsdatum/Date of birth 01.01.1978

4. Staatsangehörigkeit/Nationality ÖSTERREICH

5. Ausstellungsdatum/Date of issue 01.07.2006

6. Geburtsort/Place of birth MUSTERORT

7. Gültig bis/Date of expiry 30.06.2016

8. Geschlecht/Sex F

9. Größe/Height 160 cm

10. Behörde/Authority MUSTERBEHÖRDE 1 MUSTERBEHÖRDE 2

11. Unterschrift/Signature

```
P<AUTMUSTERFRAU<<MARIA<MANUELA<<<<<<<<<<<<<<
X9011527<8AUT7801011F1606306<<<<<<<<<<<<<<<2
```

Figure 4–5: Passport (AUT, P, 1, 2006): Hologram security laminate with optically distorting influence

- **Features near the upper edge of the document:** Field experience has shown that optical features close to the document upper edge (e.g. in case of an involved booklet) can interfere with machine authentication and may lead to cutting of the captured area. A partial capture of that feature might lead to errors.

- **Features only visible in high resolution:** Based on current state of technology, most of the current full page readers used in authentication systems support a maximal nominal resolution of 400 ppi providing real optical resolutions that are even below this value. Features which are only visible in high resolution of more than 400 ppi (e.g. microtext, Guilloches) will remain undetectable for most of the full page readers currently available on the market (see ure 4–6). However, these features may be verifiable by full page readers in the near future having 600 ppi or more.

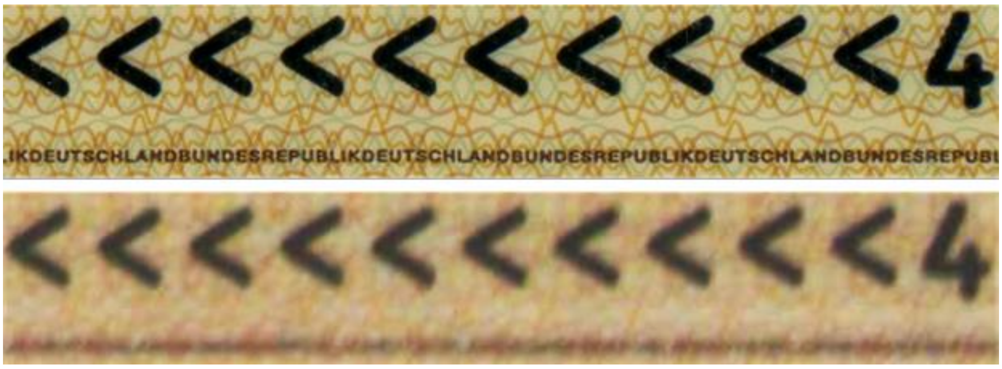

<<<<<<<<<<4
IKDEUTSCHLANDBUNDESREPUBLIKDEUTSCHLANDBUNDESREPUBLIKDEUTSCHLANDBUNDESREPUBI
<<<<<<<<<<4

Figure 4–6: Passport (D, P, 1, 2007): Comparison between a high-resolution image of the microtext (1000 ppi) and an image of the same microtext taken from a full page reader (nominal 400 ppi)

- **Features for which the appearance depends on individual handling:** Some features are potentially not suited for machine authentication because they can considerably change the appearance of the document: depending on how the page is placed on the document reader, the content of the live image is more or less different. In the following, two of such features are mentioned exemplarily:

a) Window feature: Depending on how data page and cover are placed on the document reader, it is possible to see the content of the cover through the window, the reader housing, the fingertip or the content of the window is empty (see Figure 4–7) leading to incident light.

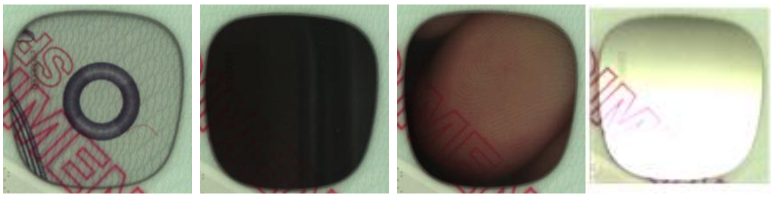
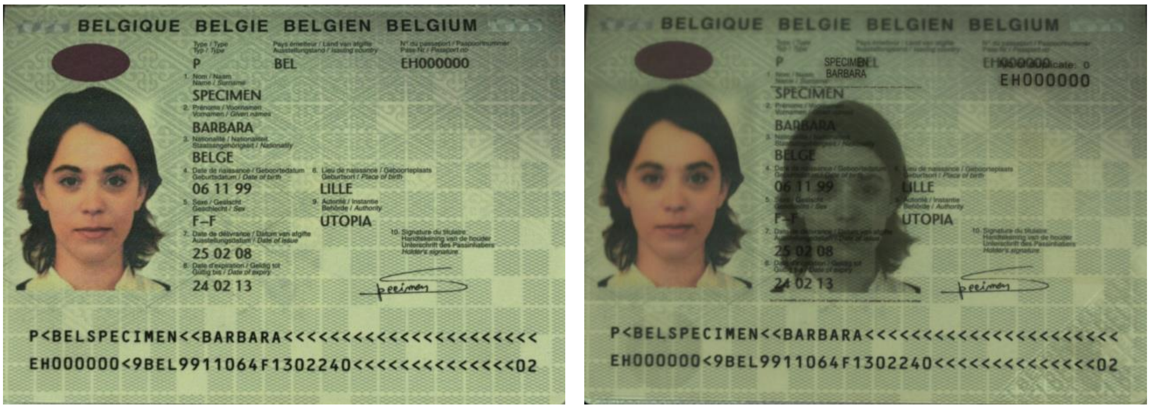


Figure 4–7: Passport (SWE, P, 1, 2012): Window feature with variable content; from left to right: inner front cover; reader housing; fingertip; glare induced by incident light

A single-sided window on ID-1 sized ID cards, i.e. a window feature that can be seen only from the front, is more suitable for machine authentication because the content of the window does not vary in the extent of Figure 4–7 and does not obstruct the checking process on the back of the card.

b) Transparent full page overlay sheet: These sheets can lead to different results depending on their presence (or absence) during the image capture process (see Figure 4–8).



BELGIQUE BELGIE BELGIEN BELGIUM

P BEL EH000000

SPECIMEN

BARBARA

BELGE

06 11 99 LILLE

F–F UTOPIA

25 02 08

24 02 13

P<BELSPECIMEN<<BARBARA<<<<<<<<<<<<<<<<<<<<<

EH000000<9BEL9911064F1302240<<<<<<<<<<<<<<02

Figure 4–8: Passport (BEL, P, 1, 2008); left: plain data page; right: data page with an overlay of the transparent sheet for visual inspection

The difficulties related to the use of these features can be overcome by proper training of the operator (in the case of human assisted document inspection) or user guidance (e.g. for automated border control).

- **Additional visa pages:** Passports that can be amended with additional visa page inserts can become too massive for ordinary full page reader geometries.

4.2 Manufacturer of Full Page Readers

The reliability of an authentication process not only depends on the set of functionalities provided by the full page reader used in the process; a practical and easy handling of the deployed full page reader also has a direct impact on the quality of the images delivered to the authentication software (see Section 4.3), and therefore automatically influences the overall result of the authentication process. The generic recommendations given in this section should be taken into consideration in the design process of full page readers:

B.1 **Assure proper wavelengths of light spectrum:** Image recording using proper wavelengths is a prerequisite for the appropriate analysis of optical features/properties. For example, a feature which is supposed to be transparent under IR light might become visible on an IR image if the capture is done with an inappropriate wavelength of the corresponding light spectrum. This might lead to faulty live data-sets, and therefore to a wrong interpretation of the optical check results. Following wave lengths for the corresponding light spectrums are required for recording images of live data-sets:

- VI: spectral range of 400 – 700 nm

- IR: a wavelength within the range of 850 – 950 nm[7]
- UV: 365 nm

Even though some passport readers support shorter UV wavelengths (e.g. 254 and 313 nm), this technology is still not widely spread yet and is not considered further in this document.

B.2 **Assure minimum resolution:** The quality of the live data-sets delivered to the authentication software, measured in pixel per inch (short: ppi), has a direct impact on the accuracy of the authentication process. Field experience has shown that live data-sets shall have a minimum resolution of 385 ppi [FRONTEX-ABC], although many properties of security printing would profit from an aquisition resolution of 600 ppi or higher.

B.3 **Deliver standard image formats:** Live data-sets shall be delivered in the most widely used/supported formats. As an example, the following formats can be used: BMP, JPG (incl. JPG2000) and PNG.

B.4 **Capture up to ID-3 size:** The full page reader should allow the verification of MRTDs of all sizes specified in [ICAO9303]. The capture area should therefore be suitable for documents up to ID-3 size. Although this document focuses on full page readers, one should keep in mind that there are application scenarios that do not require the verification of MRTDs of all sizes but only require the full page reader to scan documents of a specific size (e.g. mobile devices).

B.5 **Assure capturing of all areas with the same quality**: The full page reader shall be able to capture the whole data page with constant image quality. This can for example be provided by a homogeneous illumination of the capture surface.

B.6 **Assure short response time and constant intensity**: The light source used for the capture shall have a short response time and shall provide constant light intensity because any deterioration of the light during the authentication process might lead to the generation of unsuitable live data-sets.

B.7 **Assure constant image quality**: The light sources of full page readers of the same type might emit light differently due to production-related deviations. In addition, these light sources conditions of a full page reader may change their intensity over time. The full page reader shall therefore implement functionalities that help to compensate for deviations thus providing a constant image quality over time and regardless of the individual device being used. In the following, two examples are given in order to illustrate how this recommendation can be fulfilled:

[7] This value was derived from the recommendations defined in [ICAO9303] Part 3.

a) The manufacturer provides functionalities to perform color management and additional calibration (e.g. by means of a calibration card) and customize the settings of the full page reader (e.g. brightness, exposure time).

b) The manufacturer provides in-built sensors allowing for the automatic compensation of deviations.

B.8 **Allow setting of UV light exposure by authentication software**: Different document models often require different UV light exposure in order to illuminate the document optimally. In this case, the UV light exposure information is stored in the authentication database. Therefore, the full page reader shall allow the setting of the UV light exposure via the authentication software through forwarding of UV settings stored in the authentication database (cf. section 4.4.2, item D.8.).

B.9 **Allow capturing of multiple UV images**: The full page reader should support multiple images capturing with different exposure setting, e.g. for a combination of UV features showing a high contrast in luminescence (e.g. high dynamic range).

B.10 **Allow glare-free images**: Reflections may appear on the captured image and often cover biographical data or security features of the data page. Therefore, the images delivered by the full page reader should contain as little glare as possible. This can be realized by capturing multiple visible (white) light images from different angles or by using diffuse illumination.

B.11 **Provide mechanism to press the document flat onto the capture area**: As stated previously, the user-friendliness of the full page reader directly influences the efficiency and the speed of the authentication process. The full page reader should therefore provide mechanisms to mechanically press the document flat onto the window in order to allow proper captures of the document pages.

B.12 **Allow single-handed operation**: Additionally, single-handed operation of the reader should be possible and the reading process should be symmetric such that it can be operated by right- and left-handed users.

B.13 **Provide interactive user guidance**: Interactive user guidance not only increases the comfort of users operating the document reader, it also helps to significantly reduce the duration of the whole authentication process. User guidance is crucial especially for ABC-gates typically following a self-service approach: In contrast to stationary document control, the document authentication hardware is used by document holders themselves. Therefore, the document reader should be able to provide interactive user guidance. This can be realized by, for example, delivering a live-stream of the document placed on the capture surface indicating the progress of the image capture (e.g. scanner metaphor). In this way, the user gets a direct feedback and can notice much faster if the document is placed correctly on the document reader or not.

B.14 **Provide hardware with a high degree of robustness**: Depending on the deployment scenario, full page readers are subject to various external conditions (incorrect handling, humidity, etc.). Over time, these external conditions can more or less damage key components (e.g. scratches on the capture surface) of the full page reader, thus accelerating wear or even breakage of the device. It is therefore recommended to equip the full page reader with robust hardware components.

4.3 Manufacturer of the Authentication Software

The following proposals are exemplarily based on the technical guideline [BSI-TR-03135] by the Federal Office for Information Security (BSI) as it currently provides the only public sector solution within this area. It is highly recommended to implement the authentication software in accordance with this guideline. The subsequent recommendations should rather be understood as an extension of [BSI-TR-03135].

Please consider the following technical recommendations for the authentication software:

C.1 **Enable processing of pre-recorded images:** The authentication software shall also work without hardware and must be able to process pre-recorded images (minimum requirements for the images are given in section 4.2, items B.1, B.2 and B.3). This functionality is especially important for automated evaluation processes. It is however necessary to prevent the authentication software from processing pre-recorded images during productive operation, as this can be used as a potential attack vector. Therefore, the usage of the interface used to process pre-recorded images must be restricted to specific configurations (e.g. evaluation setup).

C.2 **Enable processing of images from different hardware sources:** The software shall be able to process images taken from at least two different full page readers without degradation of verification results. The manufacturer of the authentication software shall therefore provide a specification describing the properties of the images delivered to the authentication software (color space, contrast, etc.).

C.3 **Abstract GUI from authentication software and hardware**: The optical authentication process of an MRTD is most of the time accompanied by the electronic check of this MRTD and a biometric verification with the document holder’s face and maybe also the fingerprint. In addition, background checks, e.g. to SIS, have to be performed. Therefore, it is recommended to use an abstraction layer between the GUI and the concrete software and hardware components needed for document, biometric and background checks. In this way, the GUI is independent from these components. Furthermore, the mentioned components can be easily switched without changing the GUI.

In the following sections, the recommendations for manufacturers of authentication software products are structured in accordance with the steps executed during the process of authentication: The document must be detected (cf. section 4.3.1), identified (cf. section 4.3.2) and subsequently verified (cf. section 4.3.3). Furthermore, the whole process must be visualized (cf. section 4.3.4) and documented by using appropriate logging mechanisms (cf. section 4.3.5).

4.3.1 Document detection

For the detection of documents placed on the reader's surface, the following recommendations are given:

C.4 **Detect document automatically and manually**: The authentication software shall provide mechanisms for automatic and manual triggering of document detection. Manual triggering is especially crucial if automatic document detection does not operate properly.

C.5 **Compensate rotation and crop captured data page accordingly**: Image capturing is started automatically after the complete personal data page has been placed on the capture surface. The authentication software shall be able to compensate potential rotation and realign the image automatically. Additionally, the authentication shall crop the captured data page accordingly for further processing.

C.6 **Detect document based on optical presence**: The presence of a document shall be detected only by using its optical properties. The detection process shall still be carried out optically even if an expected chip is absent or malfunctioning (cf. section 1.3).

4.3.2 Identification

A prerequisite for document verification is the correct identification of the document model. For the identification of a live data-set, the following recommendations are given:

C.7 **Identify the document model:** As previously mentioned, the verification of a document presupposes a correct identification of its document. Therefore, it is required to identify to document model, regardless of the methods applied as long as the method applied guarantees a correct identification of the document model. The most common methods used for document model identification are MRZ (incl. pattern analysis) or pattern analysis only.

C.8 **Allow fast identification via MRZ:** If the MRZ is used as primary input for document model identification, the authentication software should implement methods and routines allowing for a fast identification process. In the following, two examples are given in order to illustrate how this recommendation can be fulfilled:

a) Begin with the capture of the IR image in order to extract the MRZ and derive the document model.

b) Because generating images in full resolution can be time-consuming, a fast IR-image capture for an early MRZ analysis can be run with a lower resolution than the minimum recommended for the IR image used for identification purposes.

C.9 **Provide fallback if MRZ is not readable under IR light:** An unambiguous identification of the document model should be possible by all means, as long as the document allows it. Even if the MRZ is not readable under IR light (not ICAO-compliant), the document has to be identified correctly. The software manufacturer therefore must support fallback solutions like performing OCR in the VI image for MRZ analysis if the MRZ is not printed using IR absorbent ink.

C.10 **Provide an unambiguous document model:** The software manufacturer must provide an unambiguous link to the document model in order to allow access to the authentication data-set of this document model in the authentication database.

C.11 **Enable partial identification:** The authentication software should enable partial identification to be configured in order to considerably reduce false identification and non-identification rates. Nevertheless, the assessment of partial identification requires human interaction and specific knowledge on MRTDs to select the correct document model manually and therefore does not suit every scenario, e.g. ABC gates.

C.12 **Enable manual identification:** The system should allow for a completely manual choice of the document model – instead of the automatic process and/or by overruling the machine’s choice – for cases in which the system’s automatic identification process fails. Furthermore, the system should only allow for manual identification if partial identification cannot be performed. Naturally, manual identification requires human interaction, specific knowledge on MRTDs and therefore does not suit every scenario (e.g. is not practical for ABC).

C.13 **Identify ID cards on both sides:** ID-1 sized documents are special in the sense that the MRZ is not on the personal data page (showing the facial image). However, ID-1 sized ID cards are allowed to be positioned on a full page reader with both sides. Therefore, ID-1 sized documents should be identifiable on either side of the document (cf. recommendation A.4 in section 4.1.1).

C.14 **Identify specimen documents:** The authentication software should also identify sample or specimen-documents as such and inform the operator accordingly without interrupting the authentication process (cf. tion A.9 in Section 4.1.1).

Recommendations for the visualization of the identification procedure in the graphic user interface can be found in section 4.3.4.

4.3.3 Verification

In the following, recommendations for verifying documents are given:

C.15 **Perform minimum number of spectrally selective checks:** Spectrally selective check routines must be performed in order to check the absorbent, reflective or luminescent reactions of the live data-set. Even if a document could not be identified, following mandatory checks must be performed:

a) (IR, AB, MR): this check routine also known as B900 test can be performed without selection of a document model, and

b) (UV, BR, FU): with certain restrictions on accuracy, this check routine can also be performed on non-identified live-datasets.

If the document model could be identified, the following spectrally selective checks complementary to the above mentioned (i.e. checking the optically opposite property) shall be performed additionally:

a) (IR, TR, *ZZ*): at least one check which investigates the complementary property "transparent under IR light" compared to (IR, AB, MR) shall be performed.

b) (UV, LU, *ZZ*): at least one check which investigates the complementary property "luminescent under UV light" compared to (UV, BR, FU) shall be performed.

C.16 **Perform MRZ consistency check:** Besides the minimum number of spectrally selective checks, plausibility checks (e.g. errors in MRZ, ICAO-3-Letter-Code) must be performed with all documents in order to guarantee minimal security also in case of non-identification.

C.17 **Perform checks in all categories**: The authentication software shall perform check routines in all three categories (material, printing technique and issuing technique) and cover all three light source images (cf. recommendation A.3 for document designers in section 4.1.1).

C.18 **Verify chip presence**: If the existence of an RF chip is expected for a particular document model, which is not working or seems not existent, this must clearly raise a warning in addition to the optical results (cf. section 1.3).

C.19 **Check dynamic patterns**: It is recommended to provide algorithms which compare individual respectively dynamic patterns (e.g. photo, signature). For instance, the facial image could be compared with a secondary facial image located on the data page (see Figure 4–9 and recommendation A.7 for document designer in section 4.1.1).

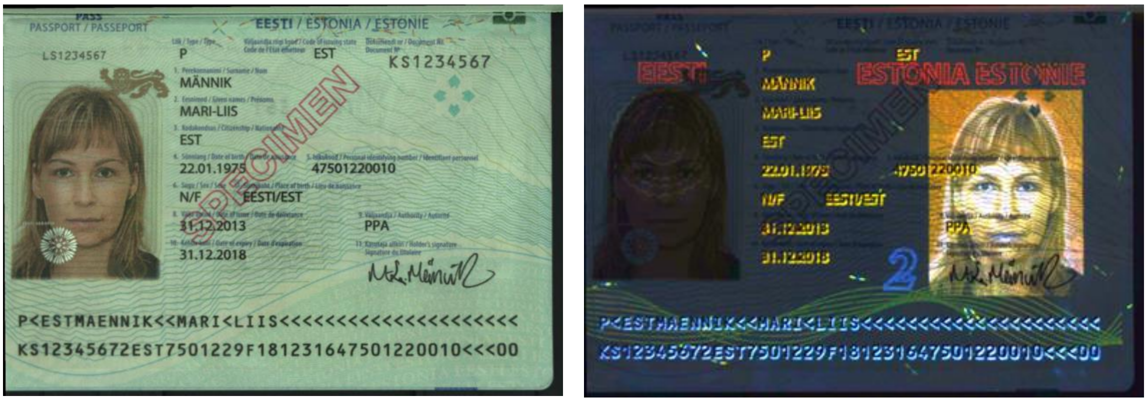
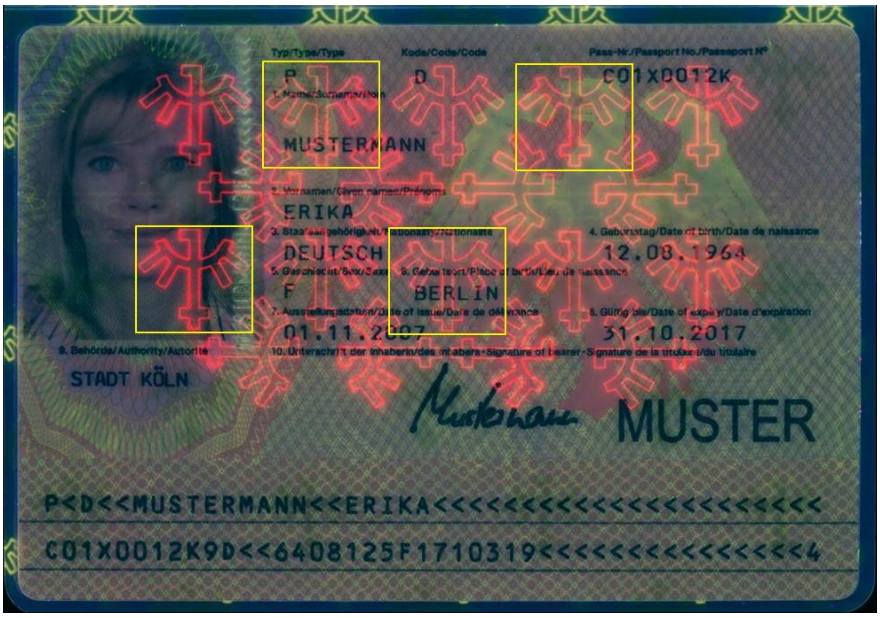


Figure 4–9: Passport (EST, P, 1, 2013): Verify the facial image in the visible light image against the one printed with UV-luminescent ink

C.20 **Combine check routines if necessary**: Some features can be checked by different check routines. For example, features behaving differently under different light sources serve as input for separate check routines (cf. recommendation A.5 for document designers in section 4.1.1). It is therefore recommended to combine the results of such check routines logically or to combine the check scores by a decision function. For instance, a composite check routine could still output a pass-decision, even if the score of one basic check routine is slightly below its threshold.

C.21 **Perform redundant check routines on multiple positions:** For features which appear more than once on the document, the corresponding check routine should be also performed on multiple positions on the live data-set. For example, for the document model (D, P, 1, 2007) in Figure 4–10, the UV eagle-pattern can be checked on multiple positions. A check routine performed on multiple positions is called a redundant check routine.



Typ/Type/Type
P
Kode/Code/Code
D
Pass-Nr./Passport No./Passport N°
C01X0012K

1. Name/Surname/Nom
MUSTERMANN

2. Vornamen/Given names/Prénoms
ERIKA

3. Staatsangehörigkeit/Nationality/Nationalité
DEUTSCH

4. Geburtstag/Date of birth/Date de naissance
12.08.1964

5. Geschlecht/Sex/Sexe
F

6. Geburtsort/Place of birth/Lieu de naissance
BERLIN

7. Ausstellungsdatum/Date of issue/Date de délivrance
01.11.2007

8. Gültig bis/Date of expiry/Date d'expiration
31.10.2017

9. Behörde/Authority/Autorité
STADT KÖLN

10. Unterschrift der Inhaberin/des Inhabers · Signature of bearer · Signature de la titulaire/du titulaire
Mustermann

MUSTER

P<D<<MUSTERMANN<<ERIKA<<<<<<<<<<<<<<<<<<<<<<
C01X0012K9D<<6408125F1710319<<<<<<<<<<<<<<<4

Figure 4–10: Redundant pattern verification

In addition to multiple appearance of a feature, some features are statistically more subject to falsification than others. In many cases, counterfeiters for example change the date of expiry or substitute the facial image. It is therefore recommended to perform check routines, which are able to detect attacks on these “sensitive” features, redundantly.

C.22 **Perform redundant check routines on multiple UV colors:** Execution of redundant check routines is also recommended for UV features which appear in multiple colors on the document (cf. recommendation A.6 and Figure 4–2 for document designers in section 4.1.1).

C.23 **Link and check both pages of an ID card:** A second page scan shall be linked automatically to the previous scan if both are from the same ID document. In addition, it is recommended to verify both sides of ID-1 sized documents in order to get an overall verification result for both sides, and maximize the number of optical features used for the authentication of the document (cf. recommendation A.4 for document designers in section 4.1.1).

C.24 **Allow multiple pages cross checking of personal data:** Personal data of the document’s holder should be identical, regardless of the page on which they are. For instance, personal data on the data page of a passport are supposed to be identical to personal data on potentially existing visa. It is therefore recommended to perform multiple sides cross checks if e.g. personalized contents are expected to be identical / redundant.

C.25 **Perform check routines dependent on significance:** It is not always necessary or meaningful to perform a whole set of check routines just because it is technically possible to apply them on the live data-set. A more efficient approach would be to assess the relevance of the checks in correlation with the verification process. Some check routines are more susceptible to deliver helpful results than others, and deliver information leading to a more accurate analysis of the verification results. Therefore:

a) The checks should be conducted by their order of relevance/significance and the results immediately shown in the graphical user interface (see Visualization in section 4.3.4), and

b) The results of the checks should be combinable by decision functions different from only performing a simple logical AND-combination (i.e. using weighted check results). Decision functions have to be logged in the XML catalogue (cf. recommendation C.46 for Logging in section 4.3.5).

C.26 **Consider feature deviation**: Security features may change over time because of wear and tear of the MRTD, e.g. some UV colors may degrade. However, these features have to be checked with constant reliability during the MRTD validity period. Therefore, tolerances of check routines should be considered.

C.27 **Detect generic attacks:** In addition to the pure verification of document feature properties, the authentication software should provide tools for the detection of traces of generic attacks such as “paper damage”, “cut marks”, “photo substitution” or “laminate wrinkles” if the illumination conditions allow for it. The scheme for generic check routines can also be applied to checks detecting forgeries.

Recommendations for the visualization of the verification procedure in the graphic user interface can be found in the next section.

4.3.4 Visualization

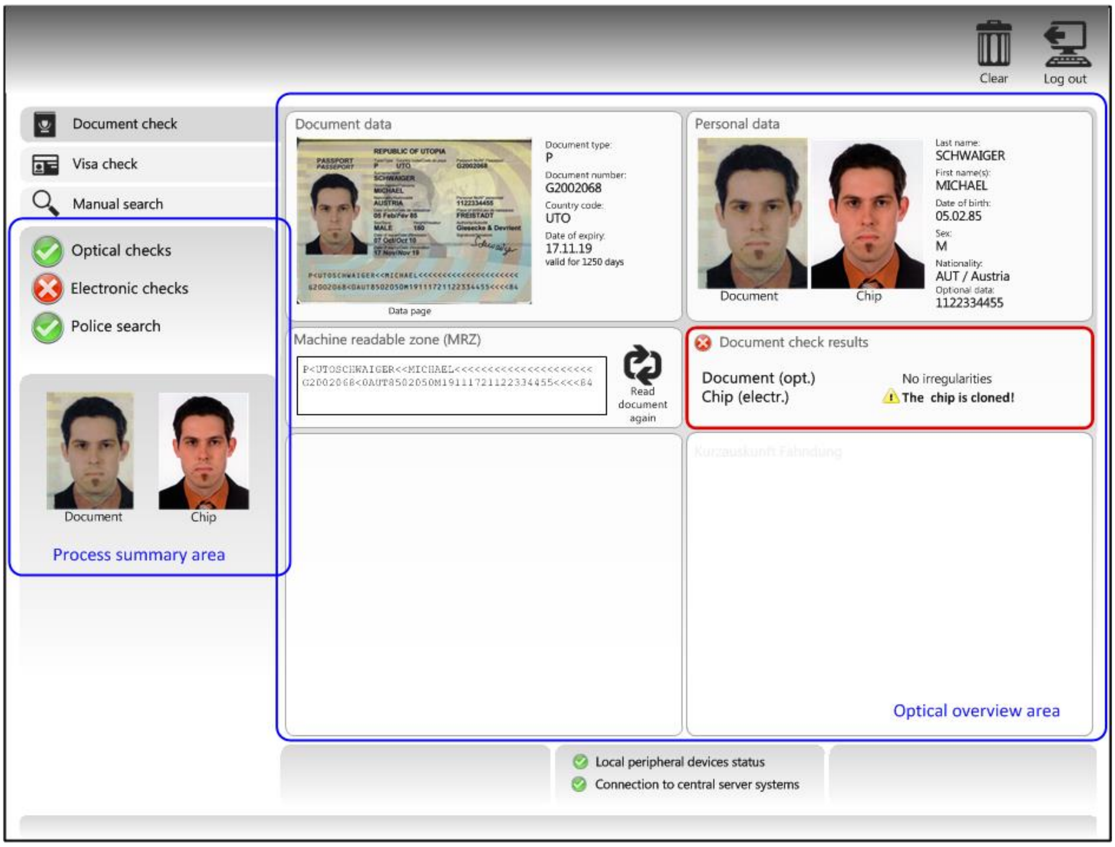
Visualization of the authentication results is the process by which the user of the authentication system is provided with visual feedback and information about the results of the authentication process. The visualization should be realized in the form of a graphic user interface (short: GUI).

The GUI for the visualization of optical check results should provide the user only with the most relevant information in order to be able to determine irregularities at first sight. In the following, this information is divided into the so-called “process summary area” (see C.29), the so-called “optical overview area” (see C.30) and more detailed information is shown in the so-called “optical details area” (see C.35).

Recommendations for choosing eligible information and displaying it in a compact and minimalistic way are made in the following:

C.28 **Display all document checks in one GUI**: The GUI may be an integral part of the delivered authentication software or be delivered and operated in a separate abstraction layer. Independent from this, it is recommended to display all types of performed checks (electronic, biometric, optical and background) in one GUI. This considerably reduces the effort of the system's operator and facilitates the assessment of the check results due to a better overview of the process. Furthermore, special focus should be placed on occurring anomalies or irregularities (cf. recommendations C.41– C.45).

C.29 **Always show *process summary area*:** This area should show the overall result of the optical authentication and must be displayed to the user on the start page (see Figure 4–11 for exemplary stationary border control GUI). This area should always be visible to the user, independent of further selected details on specific verification results. The process summary area should show one overall result of the optical authentication with a traffic light symbol. Furthermore, the area should display a cropped facial image of the data page next to the facial image stored on the chip, if present.



Document type: P
Document number: G2002068
Country code: UTO
Date of expiry: 17.11.19
valid for 1250 days

Last name: SCHWAIGER
First name(s): MICHAEL
Date of birth: 05.02.85
Sex: M
Nationality: AUT / Austria
Optional data: 1122334455

```
P<UTOSCHWAIGER<<MICHAEL<<<<<<<<<<<<<<<<<<<<<
G2002068<0AUT8502050M1911172112233445<<<<84
```

Document check results

Document (opt.)	No irregularities
Chip (electr.)	⚠ The chip is cloned!

Figure 4–11: Exemplary start page for stationary border control GUI

C.30 **Display *optical overview area* on start page:** This area shows an overview of the optical check routines and should be displayed to the operator on the start page.

a) This area should contain the following information (see Figure 4–11):

- The VI (visible light) image of the document per default. The operator staff should be able to change the default image to IR or UV, depending on the specific requirements.
- The personal data of the document holder contained in the MRZ: last name, first name, date of birth, sex, nationality and optional data.
- The document data: document type, document number, issuer country, date of expiry and optional data.
- The extracted MRZ to allow comparison of the extracted MRZ with the MRZ printed on the document.
- A button to allow the manual triggering of the document reading process.
- A cropped facial image of the data page next to the facial image stored on the chip (if present, cf. section 1.3) to allow easy detection of photo substitution.

b) It is also recommended to display following information in the optical overview area:

- The age of the document holder as well as the remaining validity period. This information can be recognized easier and faster by the operator than the dates contained in the MRZ.

C.31 **Select more details via one click:** From the optical overview area, the operator should click only once to get access to an additional page containing more details of the optical verification: the *optical details area* (see C.35) For instance, in the exemplary GUI in Figure 4–11, more details can be retrieved by clicking on the area “Document data”.

C.32 **Show results with traffic lights**: As specified in [BSI-TR-03135], the results of the optical check processes should be displayed using a traffic light system (e.g. red/green/yellow/grey lights). In addition to the color, the traffic lights should contain unambiguous symbols indicating the verification results (e.g. check, cross). This is especially important for users with red-green color blindness. Furthermore, the representation scheme should be the same for all areas of the GUI (e.g. negative results are all displayed with the same symbol and color).

C.33 **Provide result mapping according to TR-03135**: The traffic light system should provide a consistent mapping to the following verification results: **successful**, **failed**, **undetermined** and **not supported/not performed** defined in [BSI-TR-03135]. Table 4-1 gives an overview of the mapping used in this document. This mapping is based on [BSI-TR-03135] and should be used for practical implementations of the GUI.

Verification result	Traffic light color
Successful	green
Failed	red
Undetermined	yellow
Not supported/not performed	grey
Aborted	black

Table 4-1: Traffic light system mapping

C.34 **Provide minimalistic result mapping**: Alternatively, a minimalistic mapping consisting only of the colors green and red may be used for the traffic light system. As displayed in Table 4-2, the color green can be used to display a positive verification result, whereby the color red can be used to display any other verification result.

Verification result	Traffic light color
Successful	green
Failed	red
Undetermined	
Not supported/not performed	grey
Aborted	

Table 4-2: Minimalistic traffic light system mapping

A further reduction of the mapping would be to display the last four verifications in Table 4-2results with red.

C.35 **Display details in a dedicated *optical details area*:** The details area is only available via user click and contains detailed information about the different processes and results of the optical authentication. It is meant to provide the user with the information needed to perform further analysis if required.

a) The optical details area should contain the following information (see example in Figure 4–12):

- The VI, the IR and the UV image of the document. The three images should be presented next to each other.

- The proprietary document model identifier of the manufacturer of the authentication software, if the document model identifier proposed in tion 2.1 cannot be displayed in generic form.

- A list of selected check routines, showing their results via traffic lights: In the context of border control, the border control guard should only be confronted with the most important verification information in a human readable form. Therefore, the results of the generic check routines are summarized in three categories, described by easy and understandable terms

  - MRZ IR readability: The corresponding traffic light shows the result of the generic check routine (IR, AB, MR).

  - UV brightness: The corresponding traffic light shows the combined result of the generic check routines (UV, BR, FU), (UV, BR, VZ), (UV, BR, PH) and (UV, BR, MR).

  - Pattern check: The corresponding traffic light shows the combined result of the remaining generic check routines which have been performed for this document (see section 3).

- In addition, the results of the following mandatory checks according to [BSI-TR-03135] should be visualized using traffic lights:

  - MRZ consistency

  - Date of expiry

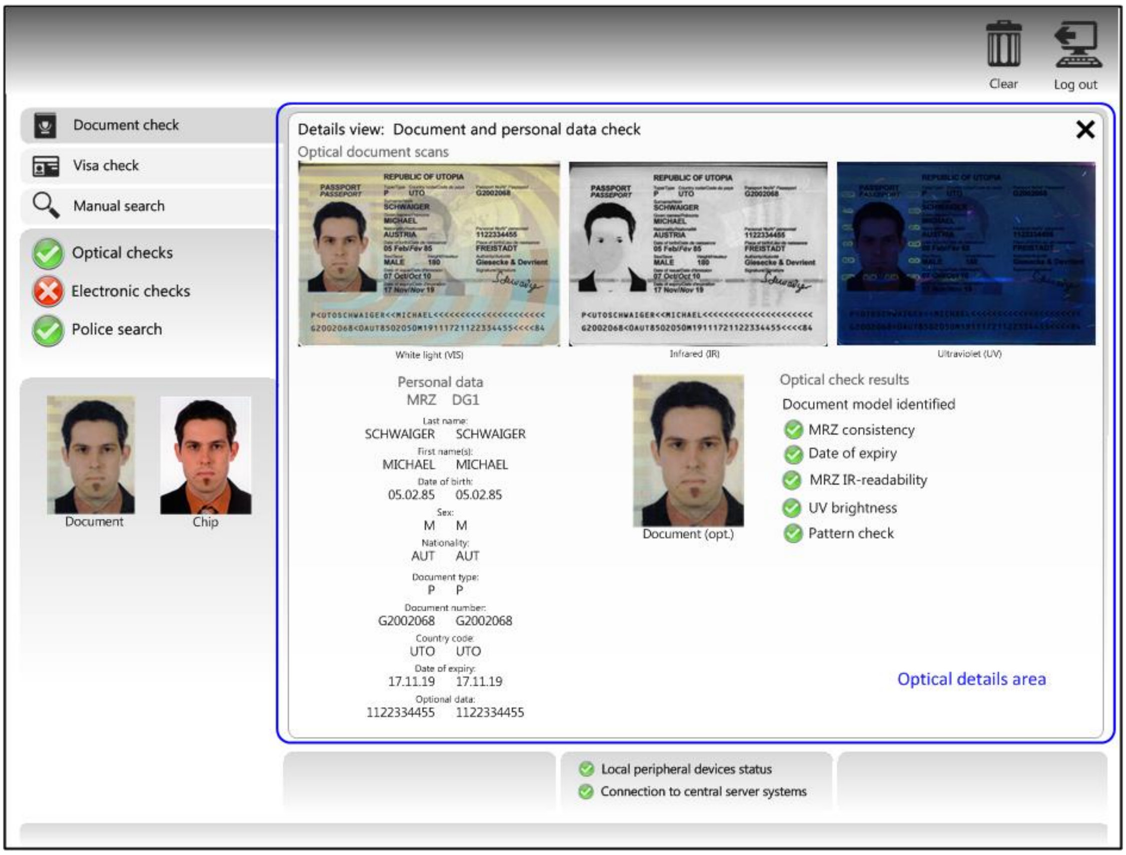
- The extracted MRZ.

- During the authentication process, the data elements extracted from the optically read MRZ are compared with the MRZ elements stored on the chip (if available). The data elements of the optical MRZ should be displayed with the result(s) of this comparison. The result(s) should be displayed with the same traffic light system used throughout the GUI.

b) It is also recommended to display the following information in the optical details area:

- The identified document model in human readable form, e.g. D 2007. Using the standard document model identifier of [BSI-TR-03135] could probably cause more confusion than clarity amongst the users of the GUI. The representation of the document model identifier in the GUI should therefore be specified on the basis of common agreement with the operator of the authentication system.

- Both the data elements extracted from the optically read MRZ and the ones extracted from chip should be displayed next to each other (cf. section 1.3).



Details view: Document and personal data check

Optical document scans

White light (VIS)

Infrared (IR)

Ultraviolet (UV)

Personal data

	MRZ	DG1
Last name:	SCHWAIGER	SCHWAIGER
First name(s):	MICHAEL	MICHAEL
Date of birth:	05.02.85	05.02.85
Sex:	M	M
Nationality:	AUT	AUT
Document type:	P	P
Document number:	G2002068	G2002068
Country code:	UTO	UTO
Date of expiry:	17.11.19	17.11.19
Optional data:	1122334455	1122334455

Document (opt.)

Optical check results

Document model identified

- ✓ MRZ consistency
- ✓ Date of expiry
- ✓ MRZ IR-readability
- ✓ UV brightness
- ✓ Pattern check

Optical details area

- ✓ Local peripheral devices status
- ✓ Connection to central server systems

Figure 4–12: Exemplary view for the optical details area

C.36 **Guide users during document reading**: During the reading process, the user should be given a hint to not remove the document before the reading process is complete (cf. recommendation B.13 in section 4.2). For example, this hint can be realized as a process indicator displayed during the reading process. This hint can be placed upon the process summary area.

C.37 **Display information from central databases:** If the authentication process requires queries to a background database system, the optical details page may show the information retrieved from this system if it is correlated to optical authentication, e.g. the facial image retrieved from the central visa information system (C-VIS).

C.38 **Provide homogenous layout for MRTDs**: The layout of the GUI should be the same for all types of machine readable documents (e.g. passports, national ID cards, resident permits, etc.). For instance, the optical authentication information obtained from both sides of an ID-1 card should be displayed analogous to the visualization of the passport verification (one process summary area, one optical overview area and one optical details area).

C.39 **Guide operators through multi-page verification:** The verification of both sides of an ID-1 sized document demands an interactive guidance of the user. For a card put on the capture surface, the user should get a hint that the presentation of the second page could be the next step.

C.40 **Allow comparison of passport and visa/eRP content:**

a) Guide operators through multi-page verification: During the verification of a passport, the user should be warned that the passport holder requires a visa/eRP in order to cross the border. This can, for example, be realized with a prompt on the overview page. This prompt should be an indication for the user, that the presentation of the visa/eRP to the full page reader is a possible next step.

b) Keep passport information available: During optical visa/eRP authentication, the overview and details areas showing the passport authentication results must still be available to be able to switch to them if desired.

c) Allow comparison in process summary area: Besides the optically captured facial image from the data page, the facial image on the visa/eRP should be displayed (see example in Figure 4–13). In addition, the chip image of the passport holder (if available, cf. section 1.3) and the image retrieved from a visa information query system (e.g. the European VIS) or from the eRP chip should be displayed (see C.37).

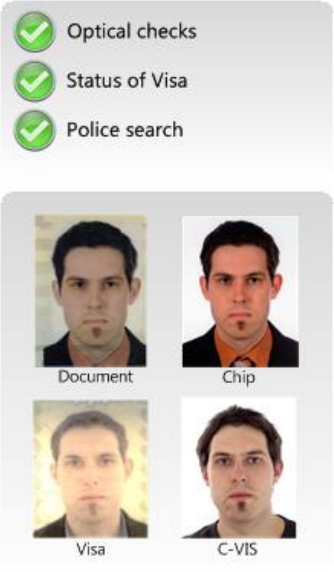


Figure 4–13: Exemplary view for the comparison of passport and visa

d) Allow comparison in visa optical details area: During the authentication process, the data elements Last Name, First Name, Date of birth, Sex and Nationality extracted from the optical MRZ of the visa are compared with these MRZ elements on the data page of the passport and/or the chip (cf.

tion 1.3). The data elements of the visa MRZ should be displayed with the result(s) of this comparison. The result(s) should be displayed with the same traffic light system used in the rest of the GUI. The age of the document holder as well as the remaining validity period of the visa should also be displayed in this area, because this information can be recognized easier and faster by the operator than the dates contained in the MRZ.

In the following, recommendations for displaying errors are made:

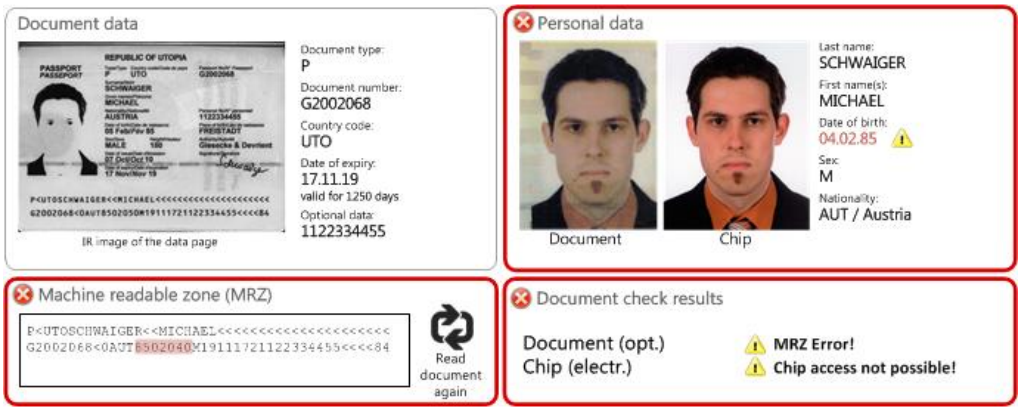
C.41 **Highlight only irregularities**: It is required to make use of color highlighting only to signalize irregularities in the authentication process (e.g. example for check failure in Figure 4–11). This approach considerably helps the user in recognizing the most relevant information delivered by the GUI at first sight.

C.42 **Display errors in process summary area:** If a document is not authentic, the traffic light for the optical authentication must show a negative overall result. If the document model could not be identified, the traffic light for the overall optical authentication result should show a warning.

C.43 **Display errors in optical overview area:** If errors occur because of optical irregularities, they should be displayed in the following way:

a) <u>Irregularity of spectrally selective property</u>: If an error occurs because of a spectrally selective check routine, the image in the corresponding light spectrum should be displayed in the optical document data area instead of the standard VI image (e.g. if (UV, BR, FU) fails, the UV image should be displayed). In addition, the optical overview area should be surrounded by a red frame.

b) <u>MRZ not consistent:</u> If an error occurs because of the MRZ consistency check, the corresponding part of the extracted MRZ including the check sum should be highlighted in red. In addition, the corresponding inconsistent personal data and the area containing the personal data should be highlighted in red (e.g. see Figure 4–14). The operator should be able to manually correct the MRZ and trigger another reading process manually via a button.



Document data

Document type:
P
Document number:
G2002068
Country code:
UTO
Date of expiry:
17.11.19
valid for 1250 days
Optional data:
1122334455

IR image of the data page

Personal data

Last name:
SCHWAIGER
First name(s):
MICHAEL
Date of birth:
04.02.85
Sex:
M
Nationality:
AUT / Austria

Machine readable zone (MRZ)

```
P<UTOSCHWAIGER<<MICHAEL<<<<<<<<<<<<<<<<<<<<<
G2002D68<0AUT8502040M1911172112233445S<<<<84
```

Document check results

Document (opt.) MRZ Error!
Chip (electr.) Chip access not possible!

Figure 4–14: Exemplary view for error visualization: MRZ consistency

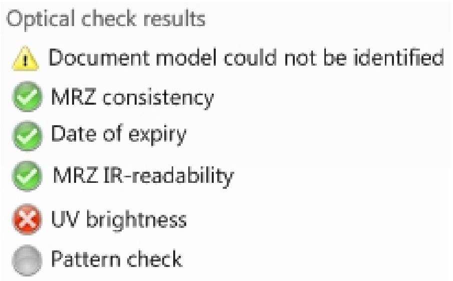
c) Document expired: If the document is expired, the date of expiry should be highlighted red.

d) Chip not detected: If an electronic chip is expected in the identified document model but it cannot be detected (cf. section 1.3), a warning should be displayed. The warning symbol should clearly be distinguishable from the traffic light symbols used to display the check results (e.g. yellow triangular warning sign).

C.44 **Display errors in optical details area:** If errors occur because of optical irregularities, they should be displayed in the following way:

a) Document not identified: If the document model could not be identified, a warning symbol should be displayed as result of the document model identification. The warning symbol should be clearly distinguishable from the traffic light symbols used to display the check results (e.g. yellow triangular warning sign, see Figure 4–15). A warning text should be displayed next to the warning symbol, e.g. “Document model could not be identified”.

b) Negative verification check: For every verification check displayed in the details page (see Figure 4–15), a negative check result should lead to a red traffic light. The respective features of the failed spectrally selective check should be highlighted on the corresponding image, e.g. by showing a red rectangle surrounding the searching area of the feature (e.g. the MRZ of the IR image due to a negative MRZ IR readability).



Optical check results

⚠ Document model could not be identified

✓ MRZ consistency

✓ Date of expiry

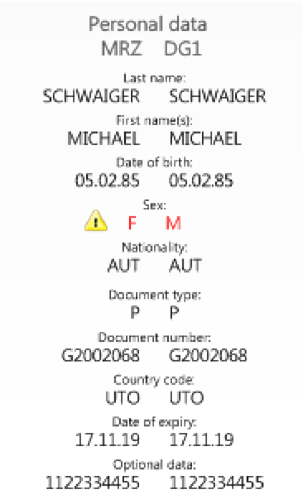
✓ MRZ IR-readability

✗ UV brightness

● Pattern check

Figure 4–15: Exemplary for view error visualization: Document model and negative verification check

c) Inconsistent chip information: For every MRZ data which is not the same for the optical data page and the chip (cf. section 1.3), the inconsistent pair of information should be displayed in red (with a warning symbol, see Figure 4–16).



Personal data

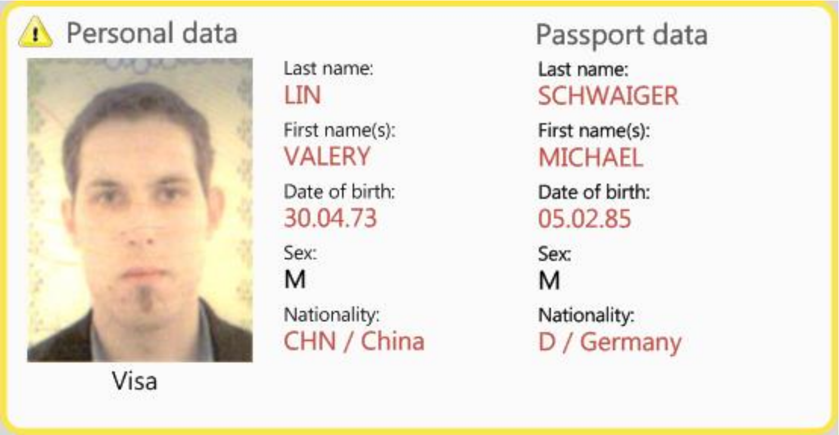
	MRZ	DG1
Last name:	SCHWAIGER	SCHWAIGER
First name(s):	MICHAEL	MICHAEL
Date of birth:	05.02.85	05.02.85
Sex: ⚠	F	M
Nationality:	AUT	AUT
Document type:	P	P
Document number:	G2002068	G2002068
Country code:	UTO	UTO
Date of expiry:	17.11.19	17.11.19
Optional data:	1122334455	1122334455

Figure 4–16: Exemplary view for error visualization: MRZ data

d) Inconsistent overall check digit: Errors related to the overall check digit (cf. [ICAO9303]) could be an indication for a manipulation of the check digits, e.g. insertion of incorrect check digits in the MRZ in order to prevent the execution of access control mechanisms (e.g. BAC). For every failed check on the optical MRZ, the captured check digit of the corresponding MRZ element should be displayed next to the expected check digit.

C.45 **Display errors of passport and visa/eRP comparison:** If at least one of the comparable MRZ data is not the same for the passport and the visa/eRP, this inconsistency should be displayed in the following way:

a) Visa/eRP overview area: The comparable MRZ data (Last Name, First Name, Date of Birth, Sex, and Nationality) of the passport must be displayed in the visa/eRP overview page next to the MRZ data of the visa/eRP. Every inconsistent pair of information should be displayed in red with a warning symbol (see example in Figure 4–17).



⚠ Personal data

Last name: LIN

First name(s): VALERY

Date of birth: 30.04.73

Sex: M

Nationality: CHN / China

Visa

Passport data

Last name: SCHWAIGER

First name(s): MICHAEL

Date of birth: 05.02.85

Sex: M

Nationality: D / Germany

Figure 4–17: Exemplary view for the comparison of the visa and the passport data

- Visa/eRP details area: For every MRZ data which is not the same for the visa/eRP and the passport, the inconsistent pair of information should be displayed in red (with a warning symbol).

4.3.5 Logging

For the logging of the optical machine authentication process, the following recommendations are applicable:

C.46 **Log XMLs according to TR-03135:** Logging must be realized according to the XML schemes defined in [BSI-TR-03135] which contain, besides the detailed optical results, also the results of the electronic and combined (optical and electronic) verification of a document. For instance, this allows to:

- Log the generic check routine identifier of a proprietary check routine (see section 3).
- Put check routines in silent mode, i.e. the routine is executed and its results are logged, but the check result is not taken into account in the overall result of the authentication process. This is of particular importance if new check routines, algorithms or thresholds are evaluated.

Further information on the spectrally selective checks might be required by the operator for evaluation purposes and to update the underlying database to guarantee consistent and high quality authentication results over time. This information is the same for all documents of a specific document model, for example the decision function, textual explanations on the check routines, the image section from the reference database etc. Therefore, the manufacturer must supply this XML catalogue in machine readable form according to the defined XML scheme in [BSI-TR-03135] which summarizes all necessary information on the spectrally selective verification checks. Due to the format, the catalogue can be integrated into the evaluation of the results.

C.47 **Allow logging of optional image data:** The XML schemes defined in [BSI-TR-03135] allow but not directly regulate the storage of the processed live data-set as well as cropped images displaying the search area of check routines. The authentication software must be able to store the mentioned image data in the XML data strucutre. Recommendations for the operational manager for storing image data in compliance with the prevailing data protection regulations are made in section 5.

C.48 **Provide anonymization capabilities:** The software should provide capabilities to anonymize the live data-set directly after the authentication in order to be allowed to permanently store the images for further inspection. Please refer to section 5.1 for recommendations for anonymization.

4.4 Manufacturer of the Authentication Database

As described in section 2.1 and 2.2, the authentication database contains distinct sets of check routines for different document models. It directly interacts with the authentication software to which it delivers the set of check routines corresponding to the identified document model. Because of new established document models and permanently arising counterfeits, a well-maintained, flexible authentication database is crucial. In the following sections, the recommendations for the database are summarized concerning the updating process (see section 4.4.1) and the configurability of the database (see section 4.4.2).

4.4.1 Update

The following recommendations are given for manufacturers of authentication databases regarding the update process:

D.1 **Exchange information about new document models or counterfeits**: The manufacturer of the authentication database shall establish a dedicated communication channel with the operational manager for secure transfer of datasets with information on new document models that should be inserted in the database. The manufacturer shall exchange information about new document models with the operational manager by using one of the following method:

a) Exchange via original sample: In this case, an original sample of the new document model or the counterfeit must be provided for definition and upload of the corresponding set of check routines in the database. The established communication channel and associated processes must take into account national legislation on data protection (cf. section 5).

b) Exchange via capture software: In this case, capture software has to be provided to the operational manager in order to generate a suitable live data-set of new document models or counterfeits. This data-set must at least contain one VI, UV and IR image. Ideally, several images of one light spectrum should be generated by this capture software (analogous to high dynamic range photography). The data-set is transferred to the manufacturer for definition of a corresponding set of check routines to be included in the next edition of the database. The manufacturer must recommend a list of suitable capture devices for this purpose.

D.2 **Update database regularly**: The authentication database shall enable regularly scheduled updates (minimum every 3 months). The authentication database shall also enable ad hoc updates on special (urgent) request:

a) If the manufacturer obtained new information about genuine documents or counterfeits and updated the document database based on this information in cooperation with the operational manager (see D.1 a), or

b) If the operator generated a live data-set with the capture software (genuine document or counterfeit) and sent it to the manufacturer (see D.1 b).

D.3 **Provide incremental updates**: By default, the manufacturer of the authentication database must supply the operator with full version updates. Incremental updates should also be distributed in order to save time and bandwidth.

D.4 **Provide sufficient documentation on changes**: At update delivery, the manufacturer of the authentication database must provide sufficient documentation about the changes made in the database.

4.4.2 Database content and configurability

In this section a list of recommendation for manufacturers of authentication databases regarding the content and configurability of the database are given:

D.5 **Provide reduced content scales:** The authentication database should be available with different scales and therefore customizable for different scenarios. For instance, commercial scenarios are much limited in scope and the type of checked documents is generally very specific (e.g. driver license). It is therefore recommended to provide authentication databases that specifically address the needs of commercial scenarios via reduced content scales. By providing a database with reduced scales, the manufacturer ensures that it remains cost efficient and easy to integrate in different setups.

D.6 **Allocate checks with significance levels**: Checks should be allocated with a significance level to allow the authentication software to perform the checks in order of significance (see recommendation C.25 a) for manufacturer of authentication software in section 4.3).

D.7 **Provide different operational modes**: Different usage scenarios require different levels of security concerning the acceptance or rejection of a document: Stationary border control, for instance, relies on high security, whereas commercial scenarios focus in general more on high convenience for the document's holder. Therefore, the authentication database should provide at minimum two different operational modes for high security and for high convenience.

D.8 **Provide document model specific UV light exposure information**: As mentioned in section 4.2, different document models often require different UV light exposure. For example, certain document models require a longer UV illumination in order to properly check specific features under UV light. Therefore, the authentication database should contain information about the UV exposure settings required for corresponding document models, so that the authentication software can automatically configure the full page reader accordingly (cf. section 4.2, item B.8).

D.9 **Support server-based setup**: It is recommended to supply an authentication database that can also be operated in a server-based setup. In this case, different authentication software would be able to access a single authentication database. Additionally, two or more authentication databases could be operated as a cluster being accessible for several authentication software products.

4.5 Manufacturer of the Reference Database

Even though the reference database is not directly a part of the authentication system (see Section 2.1) it can be used as a complementary source of information if the authenticity of a document cannot be clearly determined on basis of the machine authentication. In this case, the reference database is able to support the operator with detailed information on the corresponding document model, e.g. with high quality images of features, textual explanations and information on common counterfeits (aimed for 2nd-line / back-office inspection). An example for a reference database provided by the European Union is the so-called FADO system (False and Authentic Documents Online). The publicly available counterpart of the FADO is the so-called PRADO[8] (Public Register of Authentic Documents Online).

In case of its usage, there are some practical implications that need to be considered by the manufacturer of the reference database. This section addresses these implications in the form of recommendations:

E.1 **Provide automatic output:** The reference database shall receive and process an unambiguous link to a document model as input from the identification process. It should also provide a reference data-set corresponding to the link as output.

E.2 **Allow manual selection of data set**: In addition to the automatic selection of a reference data-set, an operator shall also be able to manually search for and choose a specific data set via a GUI.

E.3 **Provide extensive information on authentic documents**: The reference database shall contain information on authentic documents and may be accompanied by linked descriptions of typical forgeries. Specific properties of the reference document models shall be described in detail and every content shall have a textual description.

In this context it is worth mentioning that a commercial database such as the Keesing Database “DocumentChecker”[9] can also be taken into consideration. In order to increase the usage of commercial databases, the mechanisms described in recommendation D.1 can be used.

[8] http://prado.consilium.europa.eu/en/homeindex.html.
[9] http://www.documentchecker.com

4.6 Operational Manager

The so-called *operational manager* is the organization responsible for the administration and the management of all processes related to the operation of the authentication infrastructure. Operators are members of the operational manager's staff who directly interacts with the authentication system.

The concrete realization of the planned operation depends on the inspection scenario. Exemplary scenarios are:

- **Stationary border control** (in short SBC): In this case, governmental customers for stationary border control assume the role of the operational manager (e.g. border police). Usually for this setup, operators are very familiar with optical document verification. The inspection scope is immense due to the high number and diversity of the checked documents. Furthermore, the system requires an extensive interaction and assessment of the operators who directly interact with both the system and the document's holder.

- **Automated border control via ABC gates** (in short ABC): For this scenario, governmental customers for ABC gates also assume the role of the operational manager which often more focus on fast than on extensive document authentication. The operators in this case are also well trained border guards and usually supervise a set on ABC-gates valuing a minimalistic visualization. In contrast to stationary border control, the system is used by travelers and therefore needs extensive user guidance, which is out of scope of this paper.

- **Document authentication for commercial purposes** (in short CP): In this case, commercial customers assume the role of the operational manager (e. g in banks). Contrary to the previous mentioned scenarios, the operators are usually not familiar with optical document verification and the inspection scope is generally smaller than for border control.

The capabilities of the components acquired must be in line with the needs of the operational manager and the requirements of the deployment scenario. In this section, the recommendations for the manufacturers of full page readers (see tion 4.2), of authentication software (see section 4.3), of authentication databases (see section 4.4) and of reference databases (see section 4.5) are mapped to the usage scenarios. Recommendations for monitoring in compliance with data protection regulations are made in chapter 5.

For each scenario, the following table summarizes the reasonable usage of the recommendations for the manufacturer of full page readers.

Manufacturer of Full Page Readers				
No.	**Short description**	**Usage scenario**		
		SBC	**ABC**	**CP**
B.1	Assure proper wavelengths of light spectrum	X	X	X
B.2	Assure minimum resolution	X	X	X
B.3	Deliver standard image formats	X	X	X
B.4	Capture up to ID-3 size	X	X	X
B.5	Assure capturing of all areas with the same quality	X	X	X
B.6	Assure short response time and constant intensity	X	X	X
B.7	Assure constant image quality	X	X	
B.8	Allow setting of UV light exposure by authentication software	X	X	
B.9	Allow capturing of multiple UV images	X		
B.10	Allow glare-free images	X	X	
B.11	Provide mechanism to press the document flat onto the capture area	X	X	X
B.12	Allow single-handed operation	X	X	X
B.13	Provide interactive user guidance		X	X[10]
B.14	Provide hardware with a high degree of robustness	X	X	X

Table 4-3: Recommendations for full page readers classified by inspection scenarios

For each scenario, the following table summarizes the reasonable usage of the recommendations for the manufacturer of authentication software products.

Manufacturer of Authentication Software				
No.	**Short description**	**Usage scenario**		
		SBC	**ABC**	**CP**
C.1	Enable processing of pre-recorded images[11]	X		
C.2	Enable processing of images from different hardware sources	X	X	X

[10] The way user guidance is realized highly depends on the commercial use case.

[11] This recommendation is important for evaluation of authentication software products.

C.3	Abstract GUI from authentication software and hardware	X	X	X
Document detection				
C.4	Detect document automatically and manually	X	X[12]	
C.5	Compensate rotation and crop captured data page accordingly	X	X	X
C.6	Detect document based on optical presence	X	X	X
Identification				
C.7	Identify the document model	X	X	X
C.8	Allow fast identification via MRZ	X	X	X
C.9	Provide fallback if MRZ is not readable under IR light	X	X	X
C.10	Provide an unambiguous document model	X	X	X
C.11	Enable partial identification	X		
C.12	Enable manual identification	X		
C.13	Identify ID cards on both sides	X	X	X
C.14	Identify specimen documents	X	X	X
Verification				
C.15	Perform minimum number of spectrally selective checks	X	X	X
C.16	Perform MRZ consistency check	X	X	X
C.17	Perform checks in all categories	X	X	X
C.18	Verify chip presence	X	X	X
C.19	Check dynamic patterns	X	X	X
C.20	Combine check routines if necessary	X	X	X
C.21	Perform redundant check routines on multiple positions	X		X
C.22	Perform redundant check routines on multiple UV colors	X		
C.23	Link and check both pages	X	X	X

[12] Manual document detection is not applicable in the automated border control scenario.

C.24	Allow multiple pages cross checking of personal data	X	X	X
C.25	Perform check routines dependent on significance	X	X	X
C.26	Consider feature deviation	X	X	X
C.27	Detect generic attacks	X	X	X
Visualization				
C.28	Display all document checks in one GUI	X	X	X
C.29	Always show *process summary area*	X	X	X
C.30	Display *optical overview area* on start page	X		
C.31	Select more details via one click	X	X	
C.32	Show results with traffic lights	X	X	X
C.33	Provide result mapping according to TR-03135	X	X	X
C.34	Provide minimalistic result mapping	X	X	X
C.35	Display details in a dedicated *optical details area*	X		
C.36	Guide users during document reading	X	X	X
C.37	Display information from central databases	X		
C.38	Provide homogenous layout for MRTDs	X		X
C.39	Guide operators through multi-page verification	X		
C.40	Allow comparison of passport and visa/eRP content	X		
C.41	Highlight only irregularities	X	X	X
C.42	Display errors in process summary area	X	X	X
C.43	Display *optical overview area* on start page	X		
C.44	Display errors in optical details area	X		
C.45	Display errors of passport and visa/eRP comparison	X		
Logging				

C.46	Log XMLs according to TR-03135	X	X	X
C.47	Allow logging of optional image data	X	X	X
C.48	Provide anonymization capabilities	X	X	X

Table 4-4: Recommendations for authentication software classified by inspection scenarios

For each scenario, the following table summarizes the reasonable usage of the recommendations for the manufacturer of authentication databases.

Manufacturer of Authentication Database				
No.	**Short description**	**Usage scenario**		
		SBC	**ABC**	**CP**
D.1	Exchange information about new document models or counterfeits	X	X	
D.2	Update database regularly	X	X	X
D.3	Provide incremental updates	X	X	X
D.4	Provide sufficient documentation on changes	X	X	X
D.5	Provide reduced content scales			X
D.6	Allocate checks with significance levels	X	X	X
D.7	Provide different operational modes	X	X	X
D.8	Provide document model specific UV light exposure information	X	X	X
D.9	Support server-based setup	X	X	X

Table 4-5: Recommendations for authentication databases classified by inspection scenarios

For each scenario, the following table summarizes the reasonable usage of the recommendations for the manufacturer of reference databases.

Manufacturer of Reference Database				
No.	**Short description**	**Usage scenario**		
		SBC	**ABC**	**CP**
E.1	Provide automatic output	X		

E.2	Allow manual selection of data set	X		X[13]
E.3	Provide extensive information on authentic documents	X		X[13]

Table 4-6: Recommendations for reference databases classified by inspection scenarios

[13] Considering CP, it is important to adjust the level of knowledge, depending on the use case.

5 Monitoring in Compliance with Data Protection

An optical authentication process may lead to an unexpected result due to one of the following reasons:

- A counterfeit has been detected.
- A counterfeit has been classified as authentic.
- An authentic document has been classified as counterfeit.
- A handling error of the full page reader occurred, e.g. the document has been removed from the reader during authentication.
- The document model could not been identified.

In these cases, it is crucial for the operational manager to be able to analyze the reason for the wrong decision. For this, the information gained in the authentication procedure - maybe including personal information - has to be logged and analyzed. This directly raises data protection issues, because personal data is not allowed to be stored, even encrypted, without the consent of the document's holder or a determined reason. The following recommendations can be made for the operational manager:

F.1 **Log authentication reporting**: Reporting information of the authentication procedure without personal data (e.g. identified document model, authentication results, check routine results etc.) must be logged according to [BSI-TR-03135]. The live data-set, the MRZ and the VIZ are therefore excluded from logging. Reporting information does not underlie any time restriction and can be used for statistical analyses.

F.2 **Set up feedback loop to manufacturer**: Regular feedback from the operation can be used to optimize the authentication software. Therefore, the reporting information clarified in F.1 should be forwarded to the manufacturer of the authentication software regularly.

F.3 **Store unaltered live data-set if eligible**: Analysis of errors can be done at its best on the same live data-set which has been provided for authentication. It is therefore recommended to store unaltered live data-sets in the XML scheme defined by [BSI-TR-03135] if this can be done with eligible effort and consent to data privacy concerns. The following logging possibilities including images exist:

a) Store live data-set with consent of document holder: If the scenario allows for it, the live data-set used for authentication can be stored, if the consent of the document holder has been collected first in written form.

This way is only conceivable for scenarios allowing a communication with the document holder such as pilots and not for permanent operation. Furthermore, the live data-sets have to be deleted irretrievably after a contractually defined time period.

b) Store live data-set in case of error: Personal data is allowed to be stored for a contractually defined time period, if a determined reason for the storage exists, e.g. if an error occurred during authentication. If the scenario allows for it, this time period can be used for error analysis on the unaltered live data-set, which have to be deleted irretrievably afterwards.

c) Log privacy friendly regions: To avoid data privacy concerns and at the same time preserve rough analysis possibilities, only “privacy friendly” cropped images displaying the search area of check routines can be logged. These ROIs must not contain the whole facial image, the MRZ or the VIZ and can be stored for all authentication processes with no time restriction in the XML scheme defined by [BSI-TR-03135].

F.4 **Anonymize images if eligible:** Another proposition to avoid data privacy concerns but store the complete live data-set with no time restriction is to anonymize the personal data on the live data-set. Via this, the areas containing personal data are difficult to analyze whereat non-personal-related parts of the document remain fully analyzable. Therefore, it is recommended to store anonymized live data-sets in the XML scheme defined by [BSI-TR-03135] if this can be done with eligible effort. Recommendations for the application of anonymization can be found in section 5.1. An anonymization can be applied in two ways:

a) Anonymize automatically after authentication**:** The authentication software should anonymize and log the live data-set automatically after authentication. Since it needs to be known which exact document model specific parts shall be anonymized, only identified document models can be anonymized automatically. If the scenario allows it, non-identified document images can be manually anonymized later on by the operational manager (see next recommendation) or deleted otherwise.

b) Anonymize manually**:** If the anonymization cannot be performed automatically because of an occurred error or non-identification, a staff member of the operational manager may anonymize manually in a contractually defined time frame after the authentication process. If the live data-set cannot be anonymized manually in this time frame, the image has to be deleted.

F.5 **Clarify data privacy concerns**: The data privacy concerns mentioned in recommendations F.1 to F.4 must be clarified by the operational manager, e.g. via a data privacy concept. Recommendations for storing the live data-set made in F.3 and F.4 can be combined, e.g. store privacy friendly regions (cf. F.3 c) as well as automatically anonymize and store the live data-sets (cf. F.4 a).

5.1 Recommendations for Anonymization

An anonymization of a live data-set can either be done automatically by the authentication software if the live data-set could be identified or manually by operational manager staff. In the following, recommendations for the operation of the anonymization are made:

F.6 **Generate non-recoverable anonymized templates:** Generation of anonymized "templates" must be a one-way-function, i.e. it must almost impossible to recover the personal data out of the template.

F.7 **Anonymize facial image and signature with homogeneous areas:** The central part of the primary facial image, a complete secondary facial image as well as the complete area of the signature must be anonymized. It is not recommended to use "blackbox anonymization", i.e. to anonymize personal data with a black box. Instead, areas containing personal data shall be substituted with homogeneous areas filled with a color derived from the corresponding image content, as displayed in Figure 5–1. Using this method, the negative influence of the filling on check routines involving this area is limited to a minimum.

F.8 **Anonymize single characters of personal data:** Characters shall be substituted individually (one by one), e.g. via boxes or alternative characters as displayed in Figure 5–1. The following individual information must be anonymized on the data page:

- Document number: five chars starting at position four
- Card Access Number
- Primary and Secondary Identifier (Name, Forename)
- Place and Date of Birth
- Nationality
- Color of eyes
- Height
- Religious name or pseudonym
- Address

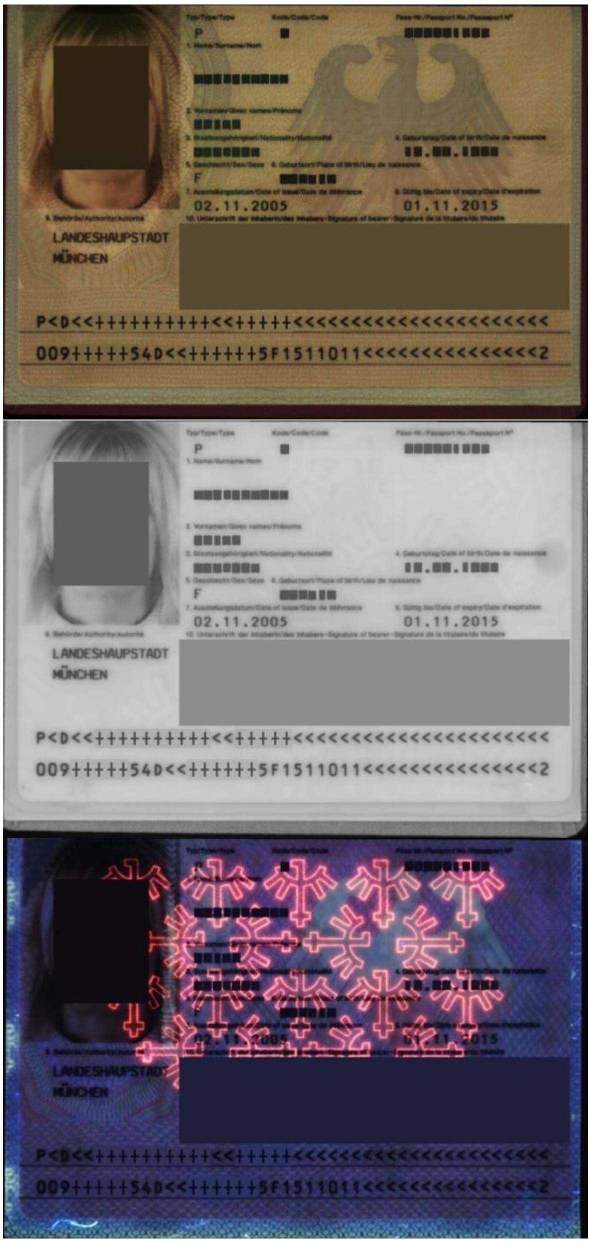

P
02.11.2005
01.11.2015
LANDESHAUPTSTADT
MÜNCHEN
P<D<<++++++++++<<+++++<<<<<<<<<<<<<<<<<<<<<<
009+++++54D<<++++++5F1511011<<<<<<<<<<<<<<<2

Figure 5–1: Anonymized sample live data-set of the data page of a German Passport

6 Glossary

ABC-Gate: Automated Border Control Gate for electronic machine readable travel documents.

Authentication database: In this database the authentication algorithms for the implementation of the check routines are stored for each document model.

Authentication data-set: A specific set of check routines for a document model within the authentication database.

Check algorithm: Software components which enable the specific implementation of check routines (e.g. search for patterns).

Check routine: Testing procedure for a feature’s specific property (e.g. examination for the presence of the photo in IR-light).

Authentication software: The authentication software receives the live data-set from the full page reader. It provides several authentication algorithms in order to apply the check routines to the live data-set.

Authentication system: An authentication system describes the combination of a full page reader, authentication software incl. authentication database and optionally the expert reference database.

Document model: Covers the document series of a nation, which have the same optical appearance (e.g. (D, P, 1, 2005), (D, P, 2, 2007) and (D, P, 3, 2010). One nation can have multiple valid document models in circulation at a given time (e.g. (GBR, P, 1, 2008) and (GBR, P, 2, 2010).

DOVID (Diffractive optically variable image device): Feature with diffractive optically variable effects, e.g. holographic effects.

Feature: An element of the document which is suitable for the proof of authenticity (e.g. IR-absorbent photo).

Live data-set: The visual-, IR-, and UV-picture of the document under test to be verified with the reader system. These pictures are used for the document’s inspection.

MRTD: Machine-Readable Travel Document (see [ICAO9303]).

eMRTD: electronic Machine Readable Travel Document.

MRZ: Machine-readable zone (see [ICAO9303]).

Operational manager: Organization responsible for the administration and the management of all processes related to the operation of the authentication infrastructure. The operational manager establishes and maintains communication channels with the vendors/manufacturers of the products used in the final authentication system.

Reference data-set: The visual-, IR-, and UV-pictures of a reference document define the check routines for the corresponding document model.

Reference document-set: The set of documents, whose reference data-sets are used to define the check routines.

Threshold: The comparison of the result value of a check routine to a corresponding threshold leads to a Passed-/Failed-decision.

Operator: A person who directly interacts with the authentication system (e.g. manual interaction with the document reader) in the context of a document check.

OVI: Optically variable ink.

Verification: A verification describes the application of a check routine to a live data-set of a document model. The result of a verification is mostly provided by a numeric result value.

VIS: Visa Information System of the European Union.

VIZ: Visual inspection zone of the data page on a MRTD (see [ICAO9303]).

7 Bibliography

[BPGOMA_Part2] BKA, secunet, „Best Practice Guidelines for optical machine authentication, Part 2” (“in preparation”)

[BSI-TR-03135] BSI, Machine Authentication for Public Sector Applications, TR-03135,“ 2017.
url: https://www.bsi.bund.de/tr03135/

[EC2252] Council Regulation (EC) No 2252/2004 of 13 December 2004: “Standards for security features and biometrics in passports and travel documents issued by Member States”

[FRONTEX-ABC] FRONTEX: Best Practice Technical Guidelines for Automated Border Control (ABC) Systems, 2012

[ICAO9303] International Civil Aviation Organization (ICAO): Doc 9303 – Machine Readable Travel Documents, Seventh Edition, 2015.
url: http://www.icao.int/mrtd

[G7-MESG] G7 Migration Experts Sub-Group (MESG): Passport and Systematic Checks at Ports of Entry and Strategies to Combat Document Fraud among G7 Countries (2017, Draft)

[MADSV] ICAO, Machine Assisted Document Security Verification, Technical Report, 2011

[MADSV-DP] ICAO, Machine Assisted Document Security Verification, Discussion Paper, 2009