Federal Office
for Information Security

Technical Guideline TR-03121-1

Biometrics for Public Sector Applications

Part 1: Framework

Version 4.3

Federal Office for Information Security
P.O. Box 20 03 63, 53133 Bonn, Germany

E-Mail: TRBiometrics@bsi.bund.de

Web: https://www.bsi.bund.de

Index of Contents

1 Introduction 5

1.1 Motivation and Objectives of Technical Guideline Biometrics 5

1.2 Fundamentals of this Guideline 5

1.3 Target Audience and User 6

1.4 Terminology 6

2 Structure of TR Biometrics 7

3 How to use this Technical Guideline 9

4 Application Profiles 10

5 Function Modules 11

5.1 Organisation of the Function Modules 11

5.2 Function Module Classes 11

6 Changelog 13

6.1 Changes from Version 4.2 to 4.3 13

6.1.1 Application Profiles 13

6.1.2 Function Modules 13

6.1.3 XML Schemata 13

6.2 Changes from Version 4.1 to 4.2 14

6.2.1 Application Profiles 14

6.2.2 Function Modules 14

6.2.3 XML Schemata 14

7 List of Abbreviations 15

8 Bibliography 18

List of Tables

Table 5-1: Function Module Classes.......... 12

List of Figures

Figure 2-1: Overview of the Technical Guidelines.......... 7

1 Introduction

1.1 Motivation and Objectives of Technical Guideline Biometrics

Biometric methods are used in many different areas of applications. The solutions and systems available on the market are able to serve a broad range regarding performance, security, usability and standard conformance. For public sector applications, it is necessary to define precise requirements and general conditions. Furthermore, the systems have to be defined in a way which allows for extension in future developments.

The objective of this Technical Guideline (TR Biometrics) is to offer a basis for a consistent and comparable quality of public sector applications and for building a common architecture.

This guideline has the following objectives:

- Specification of standardised quality requirements for various kinds of biometric applications,
- definition of standardised security requirements,
- support for procurement processes of the public sector,
- establishment of guidelines across applications (specification of requirements from enrolment to verification or identification),
- design of a simple and well-structured software architecture with defined interfaces to avoid proprietary systems and to establish investment security, flexibility and interoperability,
- establishment of a certification scheme for conformance testing,
- integration into the international context by adoption of established standards.

1.2 Fundamentals of this Guideline

The fundamental concepts of this guideline are:

- Modularity
  The complete guideline is built from several single guideline modules. For a single application area only the respective modules have to be taken into account. This is done in order to avoid side effects between different kinds of applications which would occur due to changes of special functions.
- Clarity
  The concept of this guideline follows a well structured framework. With this framework it is easily understandable which kind of guideline modules are valid for the respective application scenario.
- Expandability
  Modularity is the key component of expandability in the scope of this guideline. This is valid regarding new applications as well as new functional units.
- Standard conformance
  The Technical Guideline takes national and international standards and guidelines into account and deploys them for governmental applications.
- Conformance and certification
  The guideline modules are designed in such a way that requirements and conditions for single functional units are clearly separated from each other. Products for single functional units are clearly defined regarding the interfaces and the range of their functionality so that they can be tested for conformance with this guideline and certified.

- Ability to reference
  The use of functional units allows to specify precise requirements for products that are used in according application scenarios. Therefore, this guideline can be used as a reference e.g. for tenders.
- Market orientation
  The definition of functional units is related to the products that can be found on the market. Requirements of the guideline can be unambiguously assigned to the respective systems and components.

It should be noted that the content of this guideline is limited to the aspects of biometrics. Interfaces to further technologies (e.g. connection of optical or electronic document readers) are out of scope of this document.

1.3 Target Audience and User

Audience for this guideline are institutions that are dealing with projects using biometrics in public sector applications. These include:

- Agencies that are issuing identity documents or visas, e.g. passport agencies of the local authorities or missions abroad of the Federal Foreign Office.
- Public Authorities using biometric applications for identity verification of people, e.g. the German Federal Police (Polizeien des Bundes) or the Police of the Federal States (Polizeien der Länder), the German Customs Administration (Bundeszollverwaltung) or the Federal Administrative Office (Bundesverwaltungsamt).

Beside these users, this guideline also addresses vendors of biometric systems as well as integrators and application developers.

1.4 Terminology

The key words “MUST”, MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this technical guideline are to be interpreted as described in [RFC2119].

2 Structure of TR Biometrics

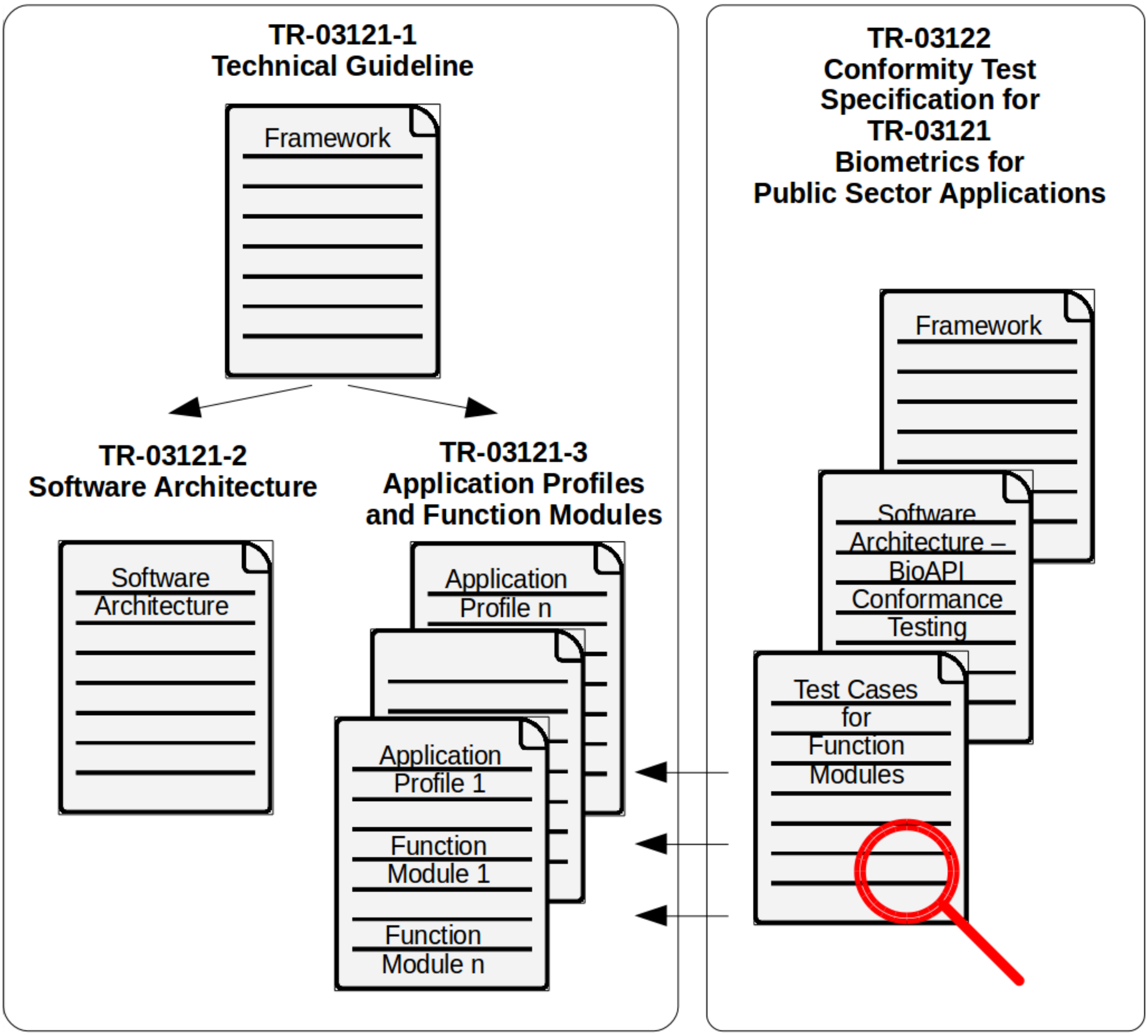
TR-03121-1
Technical Guideline
Framework
TR-03121-2
Software Architecture
Software Architecture
TR-03121-3
Application Profiles and Function Modules
Application Profile n
Application Profile 1
Function Module 1
Function Module n
TR-03122
Conformity Test Specification for TR-03121 Biometrics for Public Sector Applications
Framework
Software Architecture – BioAPI Conformance Testing
Test Cases for Function Modules

Figure 2-1: Overview of the Technical Guidelines

The TR Biometrics consists of the following several parts which are illustrated in Figure 2-1.

- Part 1: Framework (TR-03121-1)
  - TR-03121-1 is the framework document of the guideline. It explains the concept and the relation between the different parts.
- Part 2: Software Architecture (TR-03121-2)
  - In the second part of this guideline at first the Software Architecture based on the BioAPI standard (ISO/IEC 19784-1) is defined.
- Part 3: Application Profiles and Function Modules (TR-03121-3)
  - In the third part, the different Applications Profiles with corresponding Function Modules are defined. These contain the detailed technical requirements for each of the components.

  - For practical purposes, this part is split up in different volumes to serve different user groups.

Additionally, the technical guideline BSI-TR 03122 “Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications” describes the requirements that are essential to declare conformance or to declare the absence of conformance. It consists of the following parts:

- Part 1: Framework (TR-03122-1)
- Part 2: Software Architecture – BioAPI Conformance Testing (TR-03122-2)
- Part 3: Test Cases for Function Modules (TR-03122-3).

3 How to use this Technical Guideline

This chapter gives a short overview how to read and apply this guideline step by step.

1. The user chooses the desired Application Profile. With the help of the Application Profile the user can get a deeper insight into the application, the required software architecture components and the described functionality. TR-03121-2 offers further information about the software architecture component model.
2. Based on the Application Profile, the mandatory Function Modules are identified. One profile can link to several Function Modules due to different kinds of underlying biometric characteristics or the fact that different technologies (e.g. scanners or digital cameras for the digitisation of a photo) are used.
   Function Modules are referenced by an explicit identifier, e.g. P-FP-GID. The first part identifies the Function Module (e.g. Process), the second part represents the biometric characteristic (e.g. fingerprint), and the last part denotes a further descriptor, typically the scope (e.g. German Identity Document).
   Function Modules for different biometric characteristics are divided by a comma while a choice between different technologies is denoted by a slash (e.g. AH-FP-FTR, AH-PH-FBS/AH-PH-DC).
3. On the basis of the identifier the according Function Module can be examined. Every Function Module provides detailed technical requirements and recommendations.

4 Application Profiles

Different areas in which this guideline can be used are defined in separate Application Profiles. Application Profiles can have mandatory status, e.g. through published regulations and laws or by requirements given in tenders. Besides, such Application Profiles can also be considered as Best Practices.

An Application Profile is described with the following items:

- Introduction (legal requirements)
- Process overview
- Target audience
  - Users
  - Technology suppliers
- Software Architecture Overview
- Relevant standards and conditions
- List of mandatory Function Modules

5 Function Modules

5.1 Organisation of the Function Modules

Specific technical requirements are structured in Function Modules. They contain detailed technical requirements for the respective component.

Function Modules are aligned to the products on the market and to the targets of evaluation.

Every Function Module is built of one or more sub-clauses which are assigned to unique identifiers. Within the sub-clauses requirements and recommendations are specified in detail.

5.2 Function Module Classes

Figure 2-1 gives an overview of the different Function Module classes.

Function Module class	Description
Process	The module Process describes the modality of how the different Function Modules have to be called and combined in order to achieve the objective of the Application Profile. Any deviant call of modules is specified with additional information.
Acquisition Hardware	Devices that are used for digitising physical representable biometric characteristics are called acquisition hardware. Scanners for capturing photographs, digital cameras to capture facial images, fingerprint sensors, or signature tablets can be named as examples.
Acquisition Software	Acquisition Software encapsulates all functionality regarding image processing except for biometric purposes. Therefore, this module usually contains device driver software for the Acquisition Hardware or in general software that is very close to the physical hardware. Furthermore, colour management and image enhancement mechanisms are often part of this software layer.
Biometric Image Processing	The module Biometric Image Processing provides the extraction of all relevant biometric information from the data, which is provided by the Acquisition Hardware or the Acquisition Software layer. Thus, a proprietary data block is transformed to a digital image of a biometric characteristic. In general, specific image processing for biometrics is addressed here e.g. provision of full frontal images or segmentation of fingerprints.
Quality Assurance	This module contains all kinds of mechanisms and procedures to check the quality of the biometric data or to select the best quality data out of multiple instances. Quality assurance is typically used in evaluation of an application's performance over time..
Compression	The objective of the module Compression is to keep the biometric data below a feasible size without losing too much quality for a biometric verification or identification.
Operation	Within the module Operation, the working process is specified for the respective operator.
User Interface	The User Interface modules give requirements on visualization and user interaction. This

Function Module class	Description
	encloses, among other things, functionality, quality assurance information, and veto messages.
Reference Storage	The objective of this module is to store biometric data in a way that it can be used for reference purposes later on.
Biometric Comparison	The module Biometric Comparison encloses the mechanisms and algorithms to verify or identify an identity based on a one-to-one or one-to-many biometric comparison between reference data and a current biometric sample (usually a live presented image) no matter where the reference is stored.
Logging	The module Logging contains requirements how and in which modality data has to be logged.
Coding	This module contains the procedures to code logging data as well as biometric data in defined formats. Interoperability is provided by means of standard compliant coding.
Evaluation	Methods and interfaces which are used in the scope of evaluation are the content of this module.

Table 5-1: Function Module Classes

6 Changelog

6.1 Changes from Version 4.2 to 4.3

6.1.1 Application Profiles

- TR-03121-3 Volume 4: “Documents for Asylum Seekers” updated to version 4.3

6.1.2 Function Modules

- COD-ALL-MMI: increased mmi4v1.xsd to mmi4v2.xsd
- COD-ALL-GID: increased gid-app4v1.xsd to gid-app4v2.xsd
- added COD-ALL-GENERIC to all app profiles
- PAD-FP-APP: Added requirements for self-service scenarios
- PAD-FP-APP: updated transition rule to 1.11.2019
- LOG-ALL-GID: Added requirement to log BHKZ in Location element
- LOG-ALL-AAD: Added requirement to log city or village in Location element
- COD-FP-GSAT: Added details of handling missing fingers and single finger mode in GSAT transactions
- QA-FP-APP: select best image only form images without hardware reported issue
- QA-PH-SB: bugfix: QA shall happen on cropped images
- P-FP-ROLL: repeat capture of rolled fingers up to two times because of QA rejection or hardware reported issues, removed term "slap"
- P-FP-PLAIN: removed hardware capture task and therewith the evaluation of hardware reported issues
- COM-FP-WSQ: require WSQ version 3.1
- PAD-FP-APP: Added usability requirements in terms of BPCER and BPNRR
- PAD-FP-APP: Added requirement to not display PAD information to person who's fingers are acquired
- COD-ALL-AAD: Type changes at NTR,PAA,DAA
- COD-ALL-AAD: Added missing int-i:RecordActivity in mnemonic OBU
- COD-FP-GSAT3: Added GSAT example for amputated finger
- LOG-FP-GENRIC: added: if quality values have been calculated for a finger, those should be logged
- AS-FP-ROLL: Added requirement to detect issue while rolling a finger which may affect capture quality
- UI-PH-APP: removed obsolete requirement to comment on rejection of images
- AH-FP-FTR: renamed to AH-FP-OPT, removed specificity to use FTR technology – FTR and optic direct technologies are allowed now
- Added EVA Modules for AKN profile

6.1.3 XML Schemata

- add the possibility to reference FingerCaptureAttempts from FingerQuality using new ref attribute
- add the possibility to reference FaceCapture from FaceQuality using new ref attribute
- Remove type.face.and.finger.enrolment: Note that the elements FingerprintCaptureAllowed and FingerprintExcludedOption have changed their namespace

6.2 Changes from Version 4.1 to 4.2

6.2.1 Application Profiles

- TR-03121-3 Volume 2: “Enrolment Scenarios for Identity Documents” updated to version 4.2

6.2.2 Function Modules

- FM P-FP-PLAIN
  - updated workflows to handle hardware reported errors
- FM QA-FP-APP:
  - clarification and updates regarding selection of best fingers in capture workflows
- P-FP-PLAIN:
  - clarification and updates regarding selection of best fingers in capture workflows

6.2.3 XML Schemata

7 List of Abbreviations

Abbreviation	Description
AAD	Arrival Attestation Document
ACQ	Acquisition
AD	Acquisition Device
AFIS	Automated Fingerprint Identification System
AH	Acquisition Hardware
ANSI	American National Standards Institute
AP	Application Profile
APP	Application
AS	Acquisition Software
BEA	Biometric Evaluation Authority
BioAPI	Biometric Application Programming Interface
BioSFPI	Biometric Sensor Function Provider Interface
BioSPI	BioAPI Service Provider Interface
BIP	Biometric Image Processing
BMS	Biometric Matching System
BMP	Windows Bitmap version 3
BPCER	Bona fide presentation classification error rate
BFNRR	Bona fide presentation non-response rate
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
BFP	Biometric Function Provider
BSFP	Biometric Sensor Function Provider
BSP	Biometric Service Provider
CMP	Biometric Comparison
COD	Coding
COM	Compression

Abbreviation	Description
CRM	Cross-matching
CTS	Conformance test suite
DC	Digital camera
DET	Detection error trade-off
eID	Electronic identity document
ePass	Electronic passport
EU	European Union
EVA	Evaluation
FAR	False accept rate
FBS	Flat bed scanner
FM	Function Module
FMR	False match rate
FNMR	False non-match rate
FOM	Freedom of Movement
FP	Fingerprint
FRR	False reject rate
FTR	Frustrated total reflection
GID	German Identity Document
ICAO	International Civil Aviation Organization
ID	Identity
IUT	Instance under test
JPG	JPEG
JP2	JPEG 2000
LOG	Logging
MF	Multi finger
MMI	Multimodal Identification
NCA	National Central Authority

Abbreviation	Description
NIST	National Institute of Standards and Technology
O	Operation
P	Process
PG	Photo Guideline ("Fotomustertafel”)
PH	Photo
PNG	Portable Network Graphics
PT	Photo Template ("Lichtbildschablone”)
QA	Quality Assurance
REF	Reference Storage
SB	Software based
SDK	Software Development Kit
SF	Single finger
STANAG	NATO Standardization Agreement
TC	Test Case
TR	Technische Richtlinie (Technical Guideline)
UI	User Interface
VAPP	Visa Application
VBIC	Visa Basic Identity Check
VEIC	Visa Extended Identity Check
VIC	Visa Identity Check
VID	Verification Identity Document
VIS	Visa Information System
WSQ	Wavelet Scalar Quantisation
WSQR	Wavelet Scalar Quantisation for reference storage

8 Bibliography

[ANSI_NIST] ANSI/NIST-ITL 1-2000, American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, available at: http://www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf

[CBEFF] ISO/IEC 19785-1:2006 "Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification"

[EAC] Technical Guideline BSI TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents, Version 2.10, 2012

[EBTS/F] FBI Electronic Biometric Transmission Specification Version 8, Appendix F, September 2007.

[EC_767_2008] Regulation (EC) No. 767|2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)

[EC_296_2008] Regulation (EC) No 296/2008 of the European Parliament and of the Council of 11 March 2008 amending Regulation (EC) No 562/2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), as regards the implementing powers conferred on the Commission

[EC_2252/2004] Regulation (EC) No 2252/2004 of the European Parliament and of the Council of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

[EC_648_2006] Commission Decision of 22 September 2006 laying down the technical specifications on the standards for biometric features related to the development of the Visa Information System

[GSAT3] German Standard for AFIS transactions. XML schema files version 3.01_4.

[ICAO_9303] ICAO Document 9303, Machine Readable Travel Documents, 7th edition, 2016

[ISO_19784-1] ISO/IEC 19784-1:2006 “Information technology – Biometric application programming interface – Part 1: BioAPI specification”

[ISO_19784-4] ISO/IEC 19784-4:2011: “Information technology – Biometric application programming interface – Part 4: Biometric sensor function provider interface”

[ISO_FACE] ISO/IEC 19794-5:2005 “Information technology - Biometric data interchange formats – Part 5: Face image data”

[ISO_FINGER] ISO/IEC 19794-4:2005 “Information technology - Biometric data interchange formats – Part 4: Finger image data”

[ISO_IRIS] ISO/IEC 19794-6:2011 “Information technology” - Biometric data interchange formats - Part 6: Iris image data

[ISO_IRIS_QA] ISO/IEC 29794-6:2015 “Information technology” - Biometric sample quality - Part 6: Iris image data

[ISO_PAD_1] ISO/IEC 30107-1: Information technology – Biometric presentation attack detection – Part 1: Framework

[ISO_PAD_3] ISO/IEC 30107-3: Information technology – Biometric presentation attack detection – Part 3: Testing and reporting

[ISO_10918-1] ISO/IEC 10918-1:1994: “Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines”

[ISO_15444] ISO/IEC 15444-1:2004 “Information technology – JPEG 2000 image coding system: Core coding system”

[ISO_15948] ISO/IEC 15948:2004 “Information technology – Computer graphics and image processing – Portable Network Graphics (PNG): Functional specification”

[ISO_19785-3] ISO/IEC 19785-3:2007 “Information technology – Common Biometric Exchange Formats Framework – Part 3: Patron format specification”

[ISO_24709-1] ISO/IEC 24709-1: 2007 “Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 1: Methods and procedures”

[ISO_24709-2] ISO/IEC 24709-2: 2007 “Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 2: Test assertions for biometric service providers”

[ISO_24722] ISO/IEC TR 24722:2015: “Information technology – Biometrics – Multimodal and other multibiometric fusion”

[NBIS] http://fingerprint.nist.gov/NBIS/index.html

[NFIS] http://fingerprint.nist.gov/NFIS/index.html

[NFIQ2.0] http://www.nist.gov/itl/iad/ig/development_nfiq_2.cfm, Source code from Apr 28, 2016.

[PhotoGuide] Photo guideline ("Fotomustertafel")

[RFC2119] RFC 2119: Key words for use in RFCs to Indicate Requirement Levels.

[STANAG4715] NATO STANAG 4715: “Biometric Data, Interchange, Watchlist and Reporting”, 2013

[TR03146] BSI TR-03146 Elektronische Bildübermittlung zur Beantragung hoheitlicher Dokumente (E-Bild hD) ,Version 1.0

[Template] Photo template ("Lichtbildschablone")

[UN REGIO] Standard Country or Area Codes for statistical Use, United Nations Department Of Economic and Social Affairs Statistics Division, 1999

[VIS-ANSI_NIST] VIS-ANSI/NIST, European Commission Directorate-General Justice, Freedom and Security – Visa Information System – NIST Description, Version 1.23, 2009