IDENTITY STANDARDS

BixeLab

DR TED DUNSTONE - FIRST EDITION

INTRODUCTION

The foundation of any robust, maintainable, and interoperable identification system lies in the adoption of universally accepted standards and shared interfaces. These standards encompass a wide range of protocols and guidelines, including those for data exchange, testing procedures, quality benchmarks, and best practices for the acquisition, storage, transmission, and utilization of identity information. Furthermore, they dictate the specifications for identity credentials, the structure of biometric data, and the protocols for authentication.

This primer provides an introduction to the myriad of standard methodologies, from globally recognized ISO norms to consensus-based industry protocols and standardized open frameworks. Embracing these standards facilitates the creation of interoperable components that can undergo rigorous testing and validation. This, in turn, ensures a stable operational environment conducive to a diverse ecosystem of vendors, system integrators, and open-source initiatives. Through this exploration, this book aims to both act as a reference for identity standards, and underscore the critical role that standards play in the seamless operation and future scalability of identification systems.

DATA

- **Data Protection:** Data protection standards help to ensure that biometric data if it was stolen cannot be misused. They also aid in ensuring that systems meet security and privacy standards.

- **Data Formats:**
    - *Container formats* are standards for enclosing biometric data and associated meta-data; they are typically modality agnostic.
    - *Modality formats* are standards for the wrapping of the biometric data.
- **Data integrity standards:** Data integrity standards help to ensure that biometric data is securely implemented from end-to-end.
- **Data storage standards:** There are a range of standards that are not identity specific, but relate to the storage of biographic and biometric data and data security.

HARDWARE

- **Acquisition Devices:** Acquisition devices are the hardware (and driver software) designed to collect a raw biometric from a user. Standards are to allow such devices to be interchangeable when the overall specifications and modalities are similar.
- **Tokens/Credentials**: The physical Identity tokens (such as passports) are subject to a range of standards that provide for interoperability, security and design.

SOFTWARE

- **General:** Good software design dictates that large scale systems should be as loosely coupled as possible. This necessitates having well defined and standard interfaces between the various components.

- **Biometric Specific:** Standards to both instruct the type of biometric algorithm operation required (e.g. identification, authentication, enrolment) and to specify the format of any returned result.

- **API Lock-in:** API standards can assist in preventing vendor lock-in by enabling system owners to build interoperable biometric APIs without the use of proprietary software or external resources.

WHY USE STANDARDS?

The adoption of standards is not merely a procedural formality but a foundational pillar for ensuring compatibility, security, and future-proofing in technology systems. The absence of universally accepted standards or their inconsistent adoption can lead to a myriad of operational challenges. Here are a few illustrative scenarios:

1. Hardware Interoperability Issues: Imagine devices that struggle with basic tasks such as capturing and encrypting data or fail to communicate with software from different vendors due to incompatible formats. This is where the implementation of Application Programming Interfaces (APIs) becomes crucial, as it facilitates seamless interaction between diverse hardware and software ecosystems.

2. Software Compatibility Setbacks: Consider an Automated Biometric Identification System (ABIS) shackled by proprietary algorithms. These systems produce unique templates that are impossible to replicate or understand by external systems, often accompanied by restrictive licensing agreements. The solution? Embracing open formats for storing raw biometric images, enabling any ABIS to re-template and interpret the data efficiently.

3. Data Accessibility Hurdles: When biometric data—such as images and templates—is locked away in proprietary formats, it becomes inaccessible to systems developed outside the original vendor's ecosystem. Transitioning to open standards for data storage and transmission can overcome these barriers, ensuring that biometric data remains portable and accessible across platforms.

Through these examples, we highlight the critical need for adopting and adhering to open standards, underscoring their role in fostering interoperability, enhancing security, and promoting innovation across the technological landscape.

DATA

At the heart of a secure and effective identity system lies the meticulous management, utilization, and safeguarding of identity data. This encompasses everything from the foundational representation of data to the frameworks for data sharing and the specific standards that guide these processes. As the digital landscape evolves, the importance of adhering to technical standards that provide robust advice and set stringent requirements becomes paramount. Many of these standards, especially those at the foundational level, have been established for some time and have seen widespread adoption across various platforms and systems.

This chapter aims to unravel the complex web of standards and guidelines that underpin the secure handling of identity data. By dissecting the layers from data protection protocols to container formats and beyond, we offer a comprehensive overview of the technical benchmarks essential for building a resilient identity management system. Through this exploration, we underscore the critical role these standards play in not just protecting biometric and identity data from misuse in the event of a breach but also in ensuring that systems are built to the highest security and privacy specifications.

DATA PROTECTION STANDARDS

Data protection standards help to ensure that biometric data, if it was stolen, cannot be misused. They also aid in ensuring that systems meet security and privacy standards.

ISO/IEC 24745:2011 – *Information technology — Security techniques — Biometric information* protection provides guidance for the protection of biometric information and guidelines for the secure and privacy-compliant management and processing of biometric information.

ISO/IEC 19785-1:2020 – *Information technology — Common Biometric Exchange Formats Framework* defines structures and data elements for biometric information records (BIRs) and the concept of a CBEFF patron format. This standard includes method for security blocks which contains information concerning the encryption of biometric data blocks (BDBs) in a biometric information record (BIR) (3.5) and the integrity of the BIR).

IEEE P2410 – *Standard for Biometric Privacy (SBP)* provides a mechanism for supporting a formal specification for privacy and biometrics such that a conforming SBP system does not incur privacy obligations by using homomorphic encryption.

DATA FORMAT STANDARDS

Container Formats

Container formats are standards for enclosing biometric data and associated meta-data; they are typically modality agnostic. Container formats allow for the exchange of biometric data as well as associated meta data.

ISO/IEC 19785-1:2020 – *Information technology - Common Biometric Exchange Formats Framework (CBEFF)* defines structures and data elements for biometric information records (BIRs) and the concept of a CBEFF patron format.

ANSI/NIST-ITL Special Publication 500-290 -- *Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information*. To effectively exchange identity data across jurisdictional lines or between disparate systems manufactured by different manufacturers, the NIST standard defines a common data exchange commonly used by law enforcement and government.

National Information Exchange Model (NIEM) - a common vocabulary that enables efficient information exchange across diverse public and private organizations. NIEM provides consistent, reusable data terms and definitions, and repeatable processes. The Biometrics domain supports information sharing and promotes interoperability between mission-based organizations engaged in activities such as homeland security, national defence, border management, immigration benefits and global law enforcement through the joint development and alignment of XML Biometric Standards.

Modality Formats

Modality formats are standards for the wrapping of the biometric data, these are usually modality dependent. These standards help to ensure that the format of

biometric data is consistent across systems, thereby enhancing interoperability and ensuring data is stored in a form that can be migrated to new systems.

ISO/IEC 19794:2011 and **ISO/IEC 39794:2019**[1] – *Information technology — Biometric data interchange formats* provides details on data interchange formats for biometric data for various modalities (including part 5 – Face image data and part 4 – Fingerprint image data).

NIST WSQ 3.1 – *Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Specification* specifies a compression standard for fingerprint data that produces archival quality images at compression ratios of around 20:1 while maintaining image integrity.

DATA INTEGRITY

Data integrity standards help to ensure that biometric data is securely implemented from end-to-end.

ISO/IEC 24761:2019 – *Information technology — Security techniques — Authentication context for biometrics* defines the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric enrolment and verification process executed at a remote site.

FIPS 186-4 – *Digital Signature Standard (DSS)* specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory.

W3C/ETSI XAdES – *XML Advanced Electronic Signatures* defines XML formats for advanced electronic signatures, including evidence as to its validity even if the signer or verifying party later attempts to repudiate the validity of the signature.

RFC8485 - *IETF Vectors of Trust* documents a mechanism for determining transactional trust defines a mechanism for describing and signalling several aspects of a digital identity transaction and its participants.

SAML 2.0 – *Security Assertion Markup Language Specification* standard defines an XML-based framework for describing and exchanging security information between on-line business partners. This security information is expressed in the form of portable SAML assertions that applications working across security domain boundaries can trust.

DATA STORAGE

Data storage standards

There are a range of standards that are not biometric specific but relate to the storage of biometric data including:

Images

ISO/IEC 15444-1:2019 – *Information technology — JPEG 2000 image coding system — Part 1: Core coding system* defines a set of lossless (bit-preserving) and lossy compression methods for coding bi-level, continuous-tone greyscale, palletised colour, or continuous-tone colour digital still images.

ISO/IEC 15948:2004 – *Information technology — Computer graphics and image processing — Portable Network Graphics (PNG): Functional specification* specifies a datastream and an associated file format, Portable Network Graphics (PNG, pronounced "ping"), for a lossless, portable, compressed individual computer graphics image transmitted across the Internet.

ISO/IEC 10918:1994 – *Information technology — Digital compression and coding of continuous-tone still images* specifies processes for converting source image data to compressed image data, processes for converting compressed image data to reconstructed image data, coded representations for compressed image data, and gives guidance on how to implement these processes in practice.

DATA SECURITY

ISO/IEC 9594-8:2020 – *Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks* addresses some of the security requirements in the areas of authentication and other security services through the provision of a set of frameworks upon which public-key certificate and attribute certificate services can be based.

ITU-T X.509 – Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks defines frameworks for public-key infrastructure (PKI) and privilege management infrastructure (PMI).

RFC 8017 – *Public-Key Cryptography Standards (PKCS)* provides recommendations for the implementation of public-key cryptography based on the RSA algorithm.

NIST FIPS 140-3 – *Security Requirements for Cryptographic Modules* provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments related to the secure design, implementation and operation of a cryptographic module.

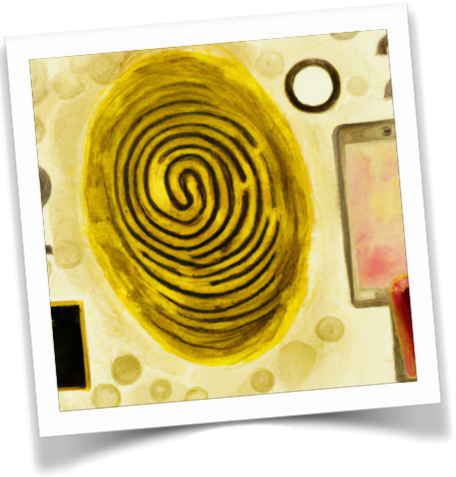
METADATA

NIST IR 8112 – *Attribute Metadata* contains a metadata schema for attributes that may be asserted about an individual during an online transaction. The schema can be used by relying parties to enrich access control policies, as well as during run-time evaluation of an individual's ability to access protected resources.

HARDWARE

In the intricate ecosystem of identity verification, hardware plays a pivotal role in ensuring secure, efficient, and reliable collection of biometric data. The standards governing this hardware lay the groundwork for systems that are both flexible and robust, enabling seamless integration and operation across various platforms and vendors. These standards are crucial not only for ensuring the hardware's performance meets rigorous expectations but also for fostering an environment where devices are capable of interoperating without friction.

This chapter explores the breadth of standards that underpin the hardware components of identity systems, from acquisition devices that gather raw biometric inputs to the tokens and credentials that serve as physical vessels of digital identity. Each standard serves as a testament to the industry's commitment to creating a secure, interoperable, and scalable ecosystem that can adapt to the evolving demands of identity verification.



ACQUISITION DEVICES

Acquisition devices are the hardware (and driver software) designed to collect a raw biometric from a user. Standards are to allow such devices to be interchangeable when the overall specifications and modality are similar.

Acquisition Device Standards

ISO/IEC 19784-1:2018: *Information technology — Biometric application programming interface — Part 1: BioAPI specification:* defines the Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that support the provision of that biometric system using components from multiple vendors.

ISO/IEC 17839 – *Information technology — Biometric System-on-Card* establishes functional architecture of Biometric System on-card. This standard also describes the sensor types in a biometric system-on-card and outlines minimum requirements with respect to biometric accuracy criteria, interfaces, and power supply options.

ISO/IEC 29164:2011 – *Embedded BioAPI standard hardware interface* provides a common interface for all biometric systems where BioAPI cannot be implemented.

ISO/IEC 29141:2009 – *Tenprint capture using BioAPI* outlines the requirements for the use of ISO/IEC 19784-1 for the purpose of performing a tenprint capture operation. It specifies a biometric data block format that is used to interact with a BioAPI framework to support an application requiring to perform a tenprint capture.

NIST Special Publication 500-288: *Specification for WS-Biometric Devices (WS-BD)* provides a command-and-control protocol for biometric devices.

FBI Appendix F (Electronic Biometric Transmission Specification (EBTS)): has stringent image quality conditions, focusing on the human fingerprint comparison and facilitating large scale machine one-to-many matching operation. Devices certified to Appendix F specifications also are considered to have met PIV specifications.

PIV-071006: A lower-level standard designed to support one-to-one fingerprint verification.

Tokens/Credentials

The physical identity tokens (such as passports) are subject to a range of standards that provide for interoperability, security and design. In particular, for the issuance of a national ID to allow access to critical government services, guidelines covering management, technical, and security should be prescriptively described and followed.

Token/Credential Standards

ISO/IEC 7501 – *Passports, machine readable travel documents and visas* Is intended for use in all applications relating to machine readable passport, travel documents and visas.

ISO/IEC 7810 – *ID cards physical characteristics* specifies physical dimensions, resistance to bending; chemicals; temperature and humidity; and toxicity. This standard also includes test methods for resistance to heat.

ISO/IEC 7816 – *Integrated circuit ID cards* specifies characteristics of integrated circuit cards with contacts. Part 1 of this standard can be applied to identification cards of ID-1 card type.

ISO/IEC 14443 – *Cards and security devices for personal ID* describes the physical characteristics of proximity cards (PICCs).

ISO/IEC 18004 – *QR symbology specification* defines the specifications for the symbology known as QR Code. It describes QR code characteristics, data character encoding methods, symbol formats, dimensional characteristics, error correction rules, reference decoding algorithm, production quality requirements, and user selectable application parameters.

ISO/IEC 24727 – *ID cards integrated circuit card programming interfaces* is the first international standard to address the need for creation of a layered framework for smart cards providing identification, authentication, and digital signature services.

ISO/IEC 24787 – *Identification cards — On-card biometric comparison* states architectures of biometric comparison using ICC, on-card biometric comparison, work-sharing and security policies around on-card biometric comparison.

ISO/IEC TR 30125 – *Biometrics used with mobile devices* provides guidance for developing a consistent and secure method of biometric personalisation and authentication in a mobile environment for systems.

ISO/IEC CD 27553 (under development) – Security Requirements for Authentication Using Biometrics on Mobile Devices.

ICAO 9303 – *Machine Readable Travel Documents standards* is a technical standard for machine readable passports, official travel documents, emergency travel documents, visas, and electronic documents.

ISO/IEC TR 30117 – *Guide to Standards and Applications for the Integration of Biometrics and Integrated Circuit Cards* summarises how the international standards, recommendations, and technical reports dealing with identification cards, biometrics, and/or information security related to each other in the context of the use of biometrics in conjunction with integrated circuit cards.

Issuance Device Frameworks

FIDO/FIDO2 – Protocol to allow password-less authentication through local device. The FIDO Alliance has published three sets of specifications for simpler, stronger user authentication: FIDO Universal Second Factor (FIDO U2F), FIDO Universal Authentication Framework (FIDO UAF) and the Client to Authenticator Protocols (CTAP).

SOFTWARE

For identity verification systems, software can acts as the central nervous system, orchestrating the intricate dance between security, functionality, and user interaction. From the high-level security frameworks that guard against unauthorized access, to the nuanced layers of testing, analysis, and end-user interfaces, software standards play a critical role in shaping systems that are not only robust and reliable but also universally accessible and interoperable.

This chapter discusses the diverse array of software standards that serve as the building blocks for modern identity verification systems. An overview of the general standards that guide system-wide interactions, such as OAuth 2.0 and OpenID Connect, illuminates the pathways through which systems can securely manage access and authenticate users. These protocols, can underpin the architecture of secure web services, enable a more streamlined and secure exchange of information across the digital ecosystem.

We also explore the specific standards that pertain to the unique challenges and requirements of biometric data processing within financial services and other sensitive applications. Standards like ISO/IEC 19092:2008 exemplify the industry's efforts to harness biometrics in a manner that enhances security without compromising flexibility or vendor neutrality.

GENERAL

The **OAuth 2.0 Authorisation Framework** enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol for verifying the identity of - and obtaining basic profile information about - the End-User. This builds on the RFS 6749 OAuth 2.0 framework to provide a secure identity layer that allows the client to request and receive information about authenticated sessions and end-users.

BIOMETRIC SPECIFIC

> **ISO/IEC 19092:2008** – *Financial services – Biometrics – Security framework* describes the security framework for using biometrics and could be useful for authentication of individuals in financial services. This standard can help to prevent vendor lock-in where third-party financial services create solutions that interface with the identity system using biometric credentials.

API

API standards can assist in preventing vendor lock-in by enabling system owners to build interoperable biometric APIs without the use of proprietary software or external resources.

API STANDARDS AND SPECIFICATIONS

ISO/IEC 24708:2008 – *Information technology — Biometrics — BioAPI Interworking Protocol* specifies the syntax, semantics, and encodings of a set of messages (BIP messages) that enable a BioAPI-conforming application (see ISO/IEC 19784-1) to request biometric operations in BioAPI-conforming biometric service providers (BSPs) across node or process boundaries, and to be notified of events originating in those remote BSPs.

ISO/IEC 19784-1:2018 – *Information technology — Biometric application programming interface* defines the Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that support the provision of that biometric system using components from multiple vendors.

OSIA – *Open Standards for ID APIs* was developed with the aim to develop a set of standard interfaces to allow connectivity between all components of an identity management ecosystem. OSIA defines a set of interfaces and standardised data formats to allow multiple identity ecosystem components to connect while ensuring continual interaction through pre-defined services.

KEY STANDARDS LIST

Some key technological standards are detailed below:

- **ISO/IEC 24745:2011** – Information technology — Security techniques
- **ISO/IEC 19785-1:2020** – Information technology - Common Biometric Exchange Formats Framework
- **ANSI/NIST-ITL Special Publication 500-290** -- Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information.
- **ISO/IEC 39794:2019** – Information technology — Biometric data interchange formats
- **NIST WSQ 3.1** – Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Specification
- **FIPS 186-4** – Digital Signature Standard (DSS)
- **RFC8485** - IETF Vectors of Trust
- **SAML 2.0** – Security Assertion Markup Language Specification

Certifications:

- **ISO/IEC 19795:2006** - Information technology — Biometric performance testing and reporting
- **ISO/IEC 30107:2016** - Information technology — Biometric presentation attack detection

- **ISO/IEC 29197:2015** - Information technology — Evaluation methodology for environmental influence in biometric system performance

- **FBI Appendix F** – Certification of fingerprint acquisition quality

ANNEX A - LIST OF STANDARDS

Frameworks

eIDAS – electronic IDentification and trust Services (Europe)

TDIF – Trusted Digital Identity Framework (Australia)

NDI – Singapore National Digital Identity Framework

Pan Canadian Trust Framework

ISO18013-5 - Vaccination Passport

ICAO DTC - Digital Travel Credential

Security and Privacy Standards

ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems

ISO/IEC 29100:2011 – Information technology — Security techniques — Privacy framework

ISO/IEC 29180:2012 – Information technology — Telecommunications and information exchange between systems — Security framework for ubiquitous sensor networks

ISO/IEC 29184:2020 – Information technology — Online privacy notices and consent

Procurement Guidance Standards

ISO/IEC TR 29194:2015 – Information Technology — Biometrics — Guide on designing accessible and inclusive biometric systems24714 – Guidelines for biometric system lifecycles

ISO/IEC 29115:2013 – Information technology — Security techniques — Entity authentication assurance framework

IEEE P2859 – Standard for Biometric Multi-modal Fusion: This document establishes a technical framework for a biometric multi-modal fusion system, describes business processes, and specifies the functional requirements, performance requirements, and security requirements of a biometric multi-modal fusion system.

ISO/IEC TR 29156:2015 – Information technology — Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics:

Open-Source Software

MOSIP – Modular Open-Source Identity Platform

OpenCRVS – Civil Registration and Vital Statistics Initiative

Open API Specification

OSIA – Open Standards for ID APIs

TESTING STANDARDS

ENROLMENT AND REGISTRATION SYSTEM TESTING STANDARDS

ISO/IEC 24709:2017 - Information technology — Conformance testing for the biometric application programming interface (BioAPI)

ISO/IEC 29109:2009 - Information technology — Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794

ISO/IEC 18584:2015 - Information technology — Identification cards — Conformance test requirements for on-card biometric comparison applications

ISO/IEC 19792:2009 - Information technology — Security techniques — Security evaluation of biometrics

ISO/IEC 5152 - Biometric performance estimation methodologies using statistical model **(under development)**

FIDO Biometric Requirements

EU Biometrics Evaluation and Testing (BEAT)

ISO/IEC 30107:2016 - Information technology — Biometric presentation attack detection

ISO/IEC 22116.2 - Information technology — A study of the differential impact of demographic factors in biometric recognition system performance **(under development)**

ISO/IEC 29197:2015 - Information technology — Evaluation methodology for environmental influence in biometric system performance

ISO/IEC 29189:2015 - Information technology — Biometrics — Evaluation of examiner assisted biometric applications

ISO/IEC 19795:2006 - Information technology — Biometric performance testing and reporting

ISO/IEC 29120:2015 - Information technology — Machine readable test data for biometric testing and reporting

ISO/IEC 21472 - Information technology — Scenario evaluation methodology for user interaction influence in biometric system performance **(under development)**

Android Biometric Requirements

TECHNOLOGY STANDARDS

DATA COLLECTION STANDARDS

ISO/IEC 15417:2007 – Information technology — Automatic identification and data capture techniques — Code 128 bar code symbology specification

ISO/IEC 15438:2015 – Information technology — Automatic identification and data capture techniques — PDF417 bar code symbology specification

ISO/IEC 29196:2018 - Information technology — Guidance for biometric enrolment

ISO/IEC 29794:2016 - Information technology — Biometric sample quality

NIST SP 800-63-3 – Digital Identity Guidelines

Data Protection Standards

ISO/IEC 19785:2020 - Information technology — Common Biometric Exchange Formats Framework

ISO/IEC 24745:2011 - Information technology — Security techniques — Biometric information protection

ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

NIST FIPS 180-4 – Secure Hash Standard (SHS)

DATA FORMATTING STANDARDS

ISO/IEC 39794:2019 - Information technology — Extensible biometric data interchange formats (superseding ISO/IEC 19794:2011 - Information technology — Biometric data interchange formats)

ISO/IEC 30108:2015 Information technology — Biometric Identity Assurance Services

ITU-T Recommendation X.509 – Public-key and attribute certificate frameworks

Data Integrity Standards

ISO/IEC 24761:2019 - Information technology — Security techniques — Authentication context for biometrics

NIST FIPS 186-4 – Digital Signature Standard (DSS)

NIST MINEX – Minutiae Interoperability Exchange

W3C/ETSI XAdES – XML Advanced Electronic Signatures

Data Interoperability

IETF Vectors of Trust

NIST IR 8112 – Attribute Metadata

DATA STORAGE STANDARDS

ISO/IEC 15444:2019 - Information technology — JPEG 2000 image coding system

ISO/IEC 15948:2004 - Information technology — Computer graphics and image processing — Portable Network Graphics (PNG): Functional specification

ISO/IEC 19785:2020 - Information technology — Common Biometric Exchange Formats Framework

ISO/IEC 10918:1994 - Information technology — Digital compression and coding of continuous-tone still images

NIST FIPS 140-3 – Security Requirements for Cryptographic Modules

RFC 3447 – Public-Key Cryptography Standards

NIST WSQ – Wavelet Scalar Quantization Gray-Scale Fingerprint Image Compression Specification

COMPONENT STANDARDS

API Standards

ISO/IEC 24708:2008 - Information technology — Biometrics — BioAPI Interworking Protocol

ISO/IEC 9594-8:2020 - Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks

ISO/IEC 19784-1:2018 - Information technology — Biometric application programming interface

ISO/IEC 19785-1:2020 - Information technology — Common Biometric Exchange Formats Framework

HARDWARE INTERFACE STANDARDS

ISO/IEC 29164:2011 - Information technology — Biometrics — Embedded BioAPI

ISO/IEC 29141:2009 - Information technology — Biometrics — Tenprint capture using biometric application programming interface (BioAPI)

ISO/IEC 24787:2018 - Information technology — Identification cards — On-card biometric comparison

ISO/IEC TR 30125:2016 - Information technology — Biometrics used with mobile devices

ISO/IEC TR 30117:2021 - Information technology — Guide to on-card biometric comparison standards and applications

ISO/IEC CD 27553 - Information technology — Security techniques — Security requirements for authentication using biometrics on mobile devices

ISO/IEC 29794:2016 - Information technology — Biometric sample quality

ISO/IEC 24761 - Information technology — Security techniques — Authentication context for biometrics

ISO/IEC 17839:2014 - Information technology — Biometric System-on-Card

NIST SP 800-63-3 – Digital Identity Guidelines

FIDO UAF – Universal Authentication Framework

SOFTWARE STANDARDS

ISO 19092:2008 - Financial services — Biometrics — Security framework

NIST FIPS 186-4 – Digital Signature Standard

W3C/ETSI XAdES – Advanced Electronic Signatures

RFC 6749 – OAuth 2.0 Authorization Framework

BSR INCITS 420-200x – Information Technology - Biometric Profile - Interoperability and Data Interchange - Point-of-Sale Biometrics-Based Verification and Identification

OpenID Connect 1.0

SAML 2.0 – Security Assertion Markup Language

BIOMETRIC STANDARDS

Developing identification systems that are well designed, easy to maintain, and interoperable requires as its basis the utilisation of standards that have been approved at the international level and the use of common interfaces. This document examines a variety of standard approaches, ranging from those that have been ratified internationally by ISO to those that have been agreed upon by the industry to those that have been standardised and made open. The implementation of these standards has led to the production of interoperable systems, which in turn has provided a stable environment for both open-source solution providers and commercial vendors and integrators.

About the authors

About BixeLab