ISO/IEC JTC 1 **N 16532**

ISO/IEC JTC 1 "Information technology"
Secretariat: **ANSI**
Committee manager: **Rajchel Lisa Mrs.**

SC 37 Business Plan 2023

Document type	Related content	Document date	Expected action
General / Other		2023-09-24	**COMMENT/REPLY** by 2023-10-16

Description

This document is circulated for review and consideration at the November 2023 JTC 1 Plenary.

BUSINESS PLAN FOR ISO/IEC JTC 1/SC 37, BIOMETRICS
PERIOD COVERED: September 2022 – August 2023

SUBMITTED BY: Patrick Grother, JTC 1/SC 37 Chair

New & Current Work Items

WG 6 Cross-Jurisdictional and Societal Aspects of Biometrics	Jurisdictional and societal considerations for commercial applications
	Pictograms, Icons and Symbols for use with Biometric Systems
	Biometrics and Elderly People
	Identifying and mitigating the differential impact of demographic factors in biometric systems
	Use of biometrics for identity management in healthcare
	Biometrics and identity management for major incident response
WG 5 Biometric Testing and Reporting	Quantifying biometric system performance variation across demographic groups
	Biometric performance estimation methodologies using statistical models
	Performance testing of biometrics on mobile devices
	Machine readable test data for biometric testing and reporting - Test reports
	Evaluation methodology for user interaction influence in biometric system performance
	Use of biometrics in video surveillance systems - Performance testing and reporting
	Biometric performance testing and reporting - Principles and framework
WG 4 Technical Implementation of Biometric Systems	Face-aware capture subsystem specifications
	Use of biometrics in video surveillance systems - Design and specification
	Best practices for slap ten-print captures
	Guidance for biometric enrolment
	Biometric recognition of subjects in motion in access related systems
WG 3 Biometric Data Interchange Formats	Face image quality assessment
	Latent fingerprint image quality
	Morph attack potential
	Biometric data interchange formats - DNA data
	Extensible biometric data interchange formats (e.g. tagged binary data format based on an extensible specification in ASN.1 & a textual data format based on an XML schema)
	Finger image data
	Face image data
	Full body image data
	Gait image sequence data
	Guidelines for transition from ISO/IEC 19794-5 to ISO/IEC 39794-5
	Biometric presentation attack detection -Profile for evaluation of mobile devices
	Use of biometrics in video surveillance systems - Part 4: Ground truth and video annotation procedure
WG 2 Biometric Technical Interfaces	Common Biometric Exchange Formats Framework - Patron format specifications
	Object oriented BioAPI - C++ Implementation
	Object oriented BioAPI - Java Implementation
	Object oriented BioAPI - C# Implementation
	Common Biometric Exchange Formats Framework - Data element specification

BUSINESS PLAN FOR ISO/IEC JTC 1/SC 37, BIOMETRICS
PERIOD COVERED: September 2022 – August 2023

WG 1 Harmonized Biometric Vocabulary	Harmonized Biometric Vocabulary

1 EXECUTIVE SUMMARY

Accounting for new projects, revision of existing standards and technical reports, JTC1/SC 37 is currently responsible for twenty four projects developed with, on average, four subprojects. JTC 1/SC 37 has published, including amendments, 135 international standards including the four projects completed during this period. In addition, four new work items have been approved. ISO maintains a list of published standards and ongoing projects.

During this period, JTC1/SC 37 held its Plenary in January 2020 in New Orleans, USA co-located with its six Working Groups (WGs). These WGs then met again virtually July 2020. As part of JTC1/SC 37 business planning activities, JTC1/SC 37 and the WGs periodically develop roadmaps. The JTC1/SC37 roadmap is posted in the public information area of the Subcommittee web site. WG roadmaps are posted in the public areas of each of the WG eCommittee sites as JTC1/SC37 Standing Documents 14-1 to 14-6. Names and main responsibility for each of the WGs are detailed in Clause 2.3 “Resources”.

2 CHAIRMAN’S REMARKS

2.1 Market Requirements, Innovation

Biometric technologies used alone, or combined with other authentication technologies such as tokens, can provide higher degrees of security and can be used to overcome their weaknesses. While JTC 1/SC 37’s overall strategy has changed little since its inception, that will now change driven by two factors: First, the incorporation into some biometric products of AI- and ML-based algorithms and approaches; and, second, the current global initiatives to legally regulate particular applications of biometrics, notably those with potential to undermine democratic freedoms.

We see standards being developed to generally support trust, particularly in the following areas.

- **Bias mitigation:** The broad and rapid adoption of AI in many domains, including biometrics, has been quickly followed by a realization that it is necessary to test for bias essentially as a due diligence step in fielding ML-trained components and systems. Biometrics is particularly vulnerable to this because it universally includes the analog-to-digital conversion step of imaging or otherwise sensing signals emitted by a human being. SC 37 was quick to respond to this, particularly with the ISO/IEC TR 22116 guidance on the origins of bias in biometric systems, and then with the ISO/IEC 19795-10 standard on formally testing for bias. However, there is more work needed. This stems from the realization that not just recognition engines, but ancillary components such as quality assessment, attack detection and even (non-AI non-ML) sensors can exhibit differential effects across demographic groups.

  That supply-side concern, has a parallel demand-side analogue: There is a critical need for end-users, including government and commercial customers, to be educated on what is and isn’t important in particular workflows and parts of the lifecycle. This arises from some press coverage and advocacy that is technically incomplete, incorrect or misleading.

- **Preventing, detecting and impeding adversarial attacks**: A second driver of future SC 37 work will be adversarial activities around biometrics. The adoption of AI by industry opens additional lines of attack of dependent systems including image manipulation, dataset poisoning, and deep fakes.
- **Improved privacy and security:** The march toward reliable, efficient and vetted mathematical techniques aimed at reducing the unwanted dissemination or privacy-related personal information has continued to the point that technology is increasingly being deployed.

An extension of the scope of SC 37 may be need to properly develop of liaise with SDOs that are using biometric data for non-biometric applications. Biometrics, strictly defined, is about identity - either verification of a claim, or determination of who is present. However, there are at least two classes of application that process biometric data without addressing the "who" aspect. First, are analysis applications, such as age or gender verification typically from a face photograph, which deal only one personal attribute. Second are applications that leverage recognition technologies to bind a biometric sample to an event, or outcome, without any knowledge of who the subject is. An extension to the scope has not been proposed in recent years.

As ever, JTC 1/SC 37 initiates work as required and engages with external organizations as appropriate. This is done to meet the needs of the IT community and other customers, to promote adoption of the biometric standards, and to support the market adoption of biometric technologies. In the regulator arena, SC 37 expects to develop standards related to design, development and audit of pre- and post-deployed technologies.

The market has expanded and evolved as technical capabilities have improved, in some cases massively. This trend has been accompanied by greater adoption and greater maturity in the implementation of biometrics-based systems, particularly with respect to performance and security. Forecasts may vary, but a significant growth of the biometric marketplace is apparent such as the rising demand in many countries around the world. APAC and African markets have substantial growth. Much of the growth is occurring in non-governmental applications, the civil sector and personal authentication, with strong uptake of fingerprint and face recognition. Further growth is also expected over the next decade in emerging markets including in particular Africa, S. Asia and E. Asia.

SC 37 continues to develop international standards and technical reports keeping in mind the customer's needs and the support for the mass market adoption of these standards. JTC1/SC 37 closely monitors the development of related standard efforts (e.g., JTC1/SC 17, JTC1/SC 27, JTC1/SC 42 projects, cloud computing, personal authentication, and identity management) with the view to offering its standards to relevant committees and liaison organizations (e.g. FIDO). Through its work, JTC1/SC 37 is helping to ensure that standards-based personal recognition systems and applications based on biometric solutions are more interoperable, scalable and secure.

There is ever more interest in audit, certification and more general-purpose data afforded by enhanced and more rigorous performance tests. This applies both to security-related assessments – active attack on biometric systems – and equally to passive performance indicators needed to state capability and to assess presence of demographic imbalances in accuracy or speed. Given myriad ways to undermine informative tests, standards from SC 37 Working Groups 5 are very timely in their marketplace role.

JTC1/SC 37's long-term vision focuses on supporting the personal authentication market. As personal authentication transactions are predicted to significantly increase in government (e.g. homeland defence), enterprise (e.g. prevention of identity theft) and consumer markets (e.g., convenience, financial transactions), the need for biometrics and biometric standards to support performance testing, interoperability and data interchange is expected to significantly grow as well. As face recognition is adopted in many more applications, the need for image quality measurement standardization becomes more important.

Representative examples of new or proposed projects are:

- Presentation attack detection on mobile devices
- Measurement and mitigation of impacts of demographics-based differentials in biometric systems
- Capture guidance, including image quality assessment, and specifications for face-aware capture systems
- Testing and evaluation of biometric acquisition on mobile devices
- Efficient, effective and economic testing

Other examples of future work:

- Relaxed face capture profiles
- Performance of de-identification schemes
- Performance of template protection schemes
- Human-in-the-loop aspects
- Use of synthetic biometric data
- Broadening of demographic testing standards
- Revision of operational testing standards
- Specifications for biometric systems that feature remote-capture
- Requirement on developers and deployers of such systems
- Improved guidance on characterizing performance in operations
- Predictive performance
- Guidance to developers for consumer applications

2.2 Accomplishments

The completion of the ISO/IEC 30107 standards, Part 1 on Framework, Part 2 on data exchange, Part 3 on testing, and particularly Part 4 on mobile devices promise substantial support to the rapidly growing segment of the biometrics marketplace that relies on unattended device interaction. The vocabulary and performance metrics aspects alone are vital to support procurements and have seen early adoption from the FIDO alliance. The Part 4 profile specifically supports FIDO and has being completed with active liaison work.

SC 37 has continued to break new ground by developing ISO/IEC 9868 (in support the draft EU regulation of AI-based high-risk biometric systems) and expediting its development by maintaining the document at working draft and thereby eliding the need for ballot review periods, SC 37 has generated ten working drafts in approximately 18 months. This expedited process is at least four times faster than our traditional cadence. We anticipate considering such a process for all new projects.

With the addition of ISO/IEC 19795-10 Quantifying biometric system performance variation across demographic groups to the program of work, market participants will be able to follow, contribute and benefit from world-class actively developed testing standards.

The ISO/IEC 19795-1 standard for biometric testing was revised in 2019-2021 and has seen considerable adoption in certification processes both in personal authentication use-cases, and in the duplicate detection steps often employed in the prior credential issuance phase.

Meeting customers' requirements, JTC1/SC 37 is completing work on the ISO/IEC 39794 series of extensible biometric data interchange formats to represent tagged binary data formats based on an extensible specification in ASN.1 and a textual data format based on an XML schema definition (both capable of holding the same information). These flagship products consolidate data elements from the prior versions 19794 version. In particular SC 37 Working Group 3 has delivered, on-time, the ISO/IEC 39794-1 (framework), -4 (fingerprint) and -5 (face) standards that International Civil Aviation Organization (ICAO) will require on all electronic passports from 2024. The progress made during this period is reflected by the number of projects that reached the next stage (many at FDIS/FDAM/DIS/DAM stage) and projects that were completed or published (as detailed above). Accounting for the documents submitted and posted in both the SC 37 document list as well as the WG document lists, over 540 documents have been posted during this period.

Three documents reached the latest stages of development (e.g. FDIS / FDAM) and they are expected to be completed and published during the next work period. ISO's website has a list of projects stages.

International and national organizations and programs have adopted or are considering adopting many of the biometric standards developed by the Subcommittee. Many of the examples have been discussed in more detail in previous reports. A significant adoption example is the International Civil Aviation Organization adopting biometric data interchange standards for several biometric modalities (for Machine Readable Travel Documents - MRTD). Recently, ICAO indicated that there are 760+ Million e-Passports in the fields, issued by more than 111 states.

Adoption of biometric-based, interoperable systems continues to depend, in part, on the timely availability of a portfolio of technically-sound biometric standards required by other standards bodies and other customers (end-users and industry). The major risk that may jeopardize this consumer adoption is the time associated with the development of these standards.

2.3 Resources

Participation in JTC1/SC 37's Programme of Work (PoW) by National Bodies and Liaison Organizations is very good. The Plenary of the Subcommittee and the meetings of its working groups continue to be well-attended. The large number of editors and co-editors that the Subcommittee relies on allows the program of work to progress in an efficient and timely manner.

Development of the JTC1/SC 37's PoW continues to be performed through the six WGs:

WG 1 – Harmonized biometric vocabulary,

WG 2 – Biometric technical interfaces,

WG 3 – Biometric data interchange formats,

WG 4 – Technical Implementation of biometric systems,

WG 5 – Biometric testing and reporting and

WG 6 – Cross-jurisdictional and societal aspects of biometrics.

The WGs establish Special Groups as needed to examine new areas of work. In addition, JTC1/SC 37 business is conducted through its Plenary and via a SC 37 Special Group (SG) on Strategy established to coordinate JTC1/SC 37 contributions to JTC 1 subgroups and to address JTC1/SC 37 strategic issues between Plenary meetings.

In order to foster increased expert WG participation, SC37 anticipates increased press outreach in future, both at the SC and WG levels, leveraging resources within and outside ISO, IEC and JTC 1.

2.4 Cooperation

At the current time, JTC1/SC 37 has 30 Participating Countries ("P" members), 23 "O" (observer) members and 20 liaison relationships, as detailed and listed on the ISO site.

Representative examples of close cooperation activities with SC 37 Liaison organizations follows. The technologies addressed by JTC1/SC 17 and JTC 1/SC 37 are, for some applications, complementary in nature. The potential contributions that JTC1/SC 37 can make to JTC1/SC 17 through this liaison activity are substantial, particularly in the specification of use of biometric data within their projects. JTC1/SC 37 periodically forwards to JTC1/SC 17 relevant drafts. Exchange of information between JTC1/SC 37 and JTC 1/SC 27 on Identity Management, Privacy Technologies and Biometrics is ongoing. At the January 2023 Plenary meeting, JTC1/SC 37 approved a Category A Liaison relationship with the Fast Identity Online (FIDO) Alliance, and this continues to be very active in mid 2023.

SC 37 added the European Union's Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU-LISA) organization as a liaison in September 2020. In addition, SC 37 benefits from the European Commission's category A liaison with JTC 1. Liaisons from and to JTC 1/SC 37 are listed within the Committee webpage.

2.5 Competition

In the several years, several biometric technology standards have been developed in IEEE. The IEEE standards disclose the committee members notionally involved in the development. The standards could reasonably have been developed by SC 37. While the reasons that they were not are unknown, the driving factors might include commercially driven pursuit of lower consensus requirements and development timelines.

3 Program of Work

As of August 2021, including amendments, there are 131 published international standards for biometrics. These standards, as well as a significant number of ongoing and proposed projects, aim at supporting a wide range of systems and applications that provide accurate and reliable verification and identification of individuals. Clause 2.3 "Resources" lists the main responsibility of each of the JTC 1/SC 37 WGs.

Completed standards:

- ISO/IEC 19795-1:2021 — Biometric performance testing and reporting — Part 1: Principles and framework
- ISO/IEC 30137-4:2021 — Use of biometrics in video surveillance systems — Part 4: Ground truth and video annotation procedure

- ISO/IEC TR 22116:2021 — A study of the differential impact of demographic factors in biometric recognition system performance
- ISO/IEC 39794-9:2021 — Extensible biometric data interchange formats — Part 9: Vascular image data
- ISO/IEC 39794-16:2021 — Extensible biometric data interchange formats — Part 16: Full body image data
- ISO/IEC 39794-17:2021 — Extensible biometric data interchange formats — Part 17: Gait image sequence data
- ISO/IEC 39794-1:2019 — Information technology — Extensible biometric data interchange formats — Part 1: Framework
- ISO/IEC 39794-4:2019 — Information technology — Extensible biometric data interchange formats — Part 4: Fingerprint image data
- ISO/IEC 39794-5:2019 — Information technology — Extensible biometric data interchange formats — Part 5: Face image data
- ISO/IEC 24779-5:2020 — Information technology — Cross-jurisdictional and societal aspects of implementation of biometric technologies — Pictograms, icons and symbols for use with biometric systems — Part 5: Face applications
- ISO/IEC 30107-4:2020 — Information technology — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices
- ISO/IEC TS 19795-9:2019 — Information technology — Biometric performance testing and reporting — Part 9: Testing on mobile devices
- ISO/IEC TR 49794 — Guidelines for transition from ISO/IEC 19794 to 39794 — Part 5: Face image data
- ISO/IEC 30107 — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices

Ongoing work and deliverables including revised versions of published standards under development are maintained on ISO's SC37 committee page. Additional representative examples of new or proposed projects are:

- ISO/IEC 5152 — Biometric performance estimation methodologies using statistical model
- ISO/IEC 9868 — Remote biometric identification systems — Design, development, and audit
- ISO/IEC 19794 — Biometric data interchange formats — Part 14: DNA data
- ISO/IEC TR 22604 — Biometric recognition of subjects in motion in access related systems
- ISO/IEC 30107 — Biometric presentation attack detection — Part 3: Testing and reporting
- ISO/IEC 24358 — Face-aware capture subsystem specifications
- ISO/IEC 29794-1 — Biometric quality assessment and evaluation
- ISO/IEC 29794-5 — Face image quality assessment
- ISO/IEC 19795-10 — Quantifying biometric system performance variation across demographic groups