9868 standard development at SC37

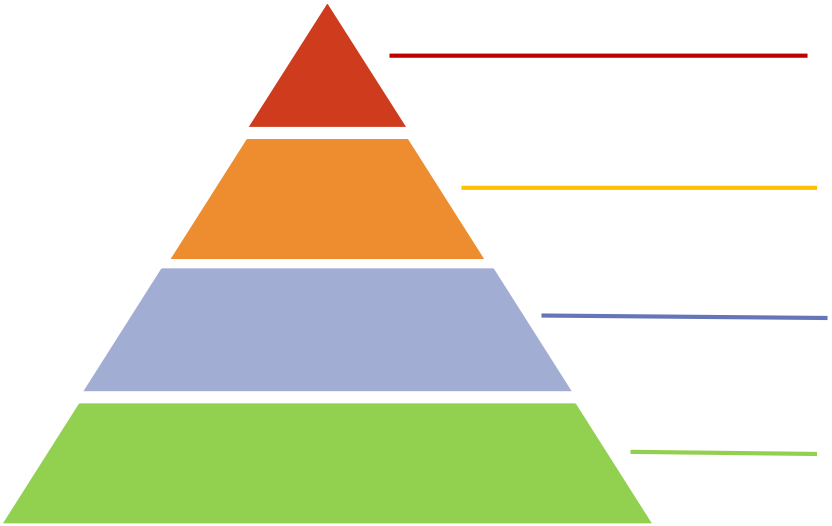
Background, development and content

Project background

Proposal, approval, assignment of work

Project background

The proposal EU regulation introduces a tiered-risk classification for AI systems



Unacceptable risk
Real-time RBI systems for law enforcement purposes in publicly accessible spaces

High risk
All RBI systems

AI with specific transparency obligations
Emotional recognition and categorisation systems

Minimal or no risk
Biometric authentication/verification
Closed set identification/ controlled environment

The regulation defines high level technical requirements to be met by high-risk system

- Remote Biometric Identification (RBI) systems are considered high risk
- Conformity assessment required for providers

Project background

› European Commission mandated JTC1 for a standard making regulation's requirements operational and implementable by operators in order to demonstrate compliance.

- Goal is to cover systems which are considered "high risk" by the proposal.

› JTC1 approved the project in November 2021

- While the project was originally proposed as a sector-specific Management System Standard (MSS), it is developed as technical standard covering specific technical aspects of biometric systems.
- Operators will refer to ISO/IEC 42001 for management system aspects.

› After approval, JTC1 assigned the project to SC37 (Biometrics) for development.

- Work started in January 2022
- Project is developed in WG5 (Biometric testing and reporting) and in joint working groups sessions
- Experts from SC27 (Information security, cybersecurity and privacy protection) and SC42 (Artificial intelligence) can also comment and contribute through liaisons

⇒Goal is to make the standard available in 2024

- Added complexity of the regulation being still under discussion at Parliament at the moment

Project background

The document will cover topics from biometric perspective

- This will not define AI concepts (for example explainability or trustworthiness) but refer to standards developed by ISO/IEC SC42 when necessary.
- SC42 experts support to align definitions and wording.

Intended as a world-reference standard

- Growing concern in the sector regarding privacy and fundamental rights protection and accurate performance.
- Need for strong guidelines and harmonised practices.

Development process

Draft and meetings

Development process

SC37 usual process for standard development

- 36 months development after approval to publish a standard
- Drafts updated every 6 months following January and July SC37 experts' meetings

Process for 9868

- 24 months development period as the goal is to finish in 2024
- The process will be faster with more drafts and intermediate meetings

→ Update of Working Drafts (WD) can be fast as no ballots required

	6 stages	Action	Balloting time
1	Proposal NP	Proposal to start a new project	• 3-month ballot by default • 2-month ballot possible • TC/SC resolution for revision & amendments
2	Preparatory WD	Expert consensus within working group	
3	Committee CD	Committee consensus	• 2-month ballot by default • 3 or 4 month vote possible • Can be skipped
4	Enquiry DIS	National consensus	• 2-month translation • 3-month ballot
5	Approval FDIS	YES or NO vote	• Skipped by default • Can be introduced • 2-month ballot
6	Publication	ISO International Standard	

Development process

- **A first Working Draft (WD1) was proposed in January**
  - Mostly an empty table of content with calls for contributions
- **Currently at WD6 after WG5 experts meetings in March, April, May, September and November**
  - Still a few sections to complete/update, but content is becoming mature
- **Next expert work session in January during a SC37 joint meeting**

⇒**May move to CD stage after that, with ballot time of two months**

Title and scope

A moving project title

⟩ Original title was:

Remote Biometric Identification systems - Design, development and audit

⟩ This title made reference to European Commission draft (April 2021) regulation's definition of high risk RBI system :

- 'remote biometric identification system' means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;

⇒Experts consensus was that "remote" was unclear

⟩ Since WD3 :

Biometric identification systems involving passive capture subjects

Scope

Current scope of the document

This standard establishes recommendations and requirements for the design, development and maintenance of biometric identification systems involving passive capture subjects including pre and post deployment evaluation.
While the emphasis is on surveillance systems, other types of biometric identification systems involving passive capture subjects are in scope, regardless of biometric modality or sensing technology.

Biometric verification systems, opt-in identification systems and identification systems involving active capture subjects are not in scope of this document.

This document does not define specific services, platforms or tools.

Scope

Current scope of the document

This standard establishes recommendations and requirements for the design, development and maintenance of biometric identification systems involving passive capture subjects including pre and post deployment evaluation.
While the emphasis is on surveillance systems, other types of biometric identification systems involving passive capture subjects are in scope, regardless of biometric modality or sensing technology.

Biometric verification systems, opt-in identification systems and identification systems involving active capture subjects are not in scope of this document.

This document does not define specific services, platforms or tools.

Scope

Current scope of the document

This standard establishes recommendations and requirements for the design, development and maintenance of biometric identification systems involving passive capture subjects including pre and post deployment evaluation.
While the emphasis is on surveillance systems, other types of biometric identification systems involving passive capture subjects are in scope, regardless of biometric modality or sensing technology.

Biometric verification systems, opt-in identification systems and identification systems involving active capture subjects are not in scope of this document.

This document does not define specific services, platforms or tools.

Scope

Current scope of the document

This standard establishes recommendations and requirements for the design, development and maintenance of biometric identification systems involving passive capture subjects including pre and post deployment evaluation.

While the emphasis is on surveillance systems, other types of biometric identification systems involving passive capture subjects are in scope, regardless of biometric modality or sensing technology.

Biometric verification systems, opt-in identification systems and identification systems involving active capture subjects are not in scope of this document.

This document does not define specific services, platforms or tools.

Scope

Current scope of the document

This standard establishes recommendations and requirements for the design, development and maintenance of biometric identification systems involving passive capture subjects including pre and post deployment evaluation.
While the emphasis is on surveillance systems, other types of biometric identification systems involving passive capture subjects are in scope, regardless of biometric modality or sensing technology.

Biometric verification systems, opt-in identification systems and identification systems involving active capture subjects are not in scope of this document.

This document does not define specific services, platforms or tools.

Scope

Current scope of the document

This standard establishes recommendations and requirements for the design, development and maintenance of biometric identification systems involving passive capture subjects including pre and post deployment evaluation.
While the emphasis is on surveillance systems, other types of biometric identification systems involving passive capture subjects are in scope, regardless of biometric modality or sensing technology.

Biometric verification systems, opt-in identification systems and identification systems involving active capture subjects are not in scope of this document.

This document does not define specific services, platforms or tools.

⇒Topics to be covered:

- Data management, appropriateness of training
- Human oversight, provision of information to operators
- Privacy measures, cybersecurity
- Accuracy and demographic differential evaluation

Technical clauses

Current content and contribution needed

Table of content

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviated terms
5 Scenarios and use of biometric systems involving passive capture subjects
6 Consideration of risk arising from passive biometric identification systems
7 Design and development practice
- 7.1 Algorithms
- 7.2 Sensors
- 7.3 Integration of System Components and User Processes

8 Technical capabilities of the system
- 8.1 Performance
- 8.2 Adaptation
- 8.3 Security and integrity
- 8.4 Privacy measures
- 8.5 Biometric data management
- 8.6 Support for human-initiation and human-review
- 8.7 Support for oversight
- 8.8 Support for testing during operation

9 Operational practice
- 9.1 Resources
- 9.2 Competence
- 9.3 Operational planning and control
- 9.4 Transparency
  - 9.4.1 Public awareness
  - 9.4.2 Provision Documented information
  - 9.4.3 Communication
- 9.5 Performance evaluation
  - 9.5.1 Monitoring, measurement, analysis and evaluation
  - 9.5.2 Management review
  - 9.5.3 Internal audit
  - 9.5.4 External audit
  - 9.5.5 Nonconformity and corrective action
- 9.6 Improvement
  - 9.6.1 Threshold management
  - 9.6.2 Continual improvement
  - 9.6.3 Upgrades

Annex A: Use Case Profiles
Annex B: Sample Audit Report

Table of content

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviated terms
5 Scenarios and use of biometric systems involving passive capture subjects
6 Consideration of risk arising from passive biometric identification systems
7 Design and development practice
- 7.1 Algorithms
- 7.2 Sensors
- 7.3 Integration of System Components and User Processes

8 Technical capabilities of the system
- 8.1 Performance
- 8.2 Adaptation
- 8.3 Security and integrity
- 8.4 Privacy measures
- 8.5 Biometric data management
- 8.6 Support for human-initiation and human-review
- 8.7 Support for oversight
- 8.8 Support for testing during operation

9 Operational practice
- 9.1 Resources
- 9.2 Competence
- 9.3 Operational planning and control
- 9.4 Transparency
  - 9.4.1 Public awareness
  - 9.4.2 Provision Documented information
  - 9.4.3 Communication
- 9.5 Performance evaluation
  - 9.5.1 Monitoring, measurement, analysis and evaluation
  - 9.5.2 Management review
  - 9.5.3 Internal audit
  - 9.5.4 External audit
  - 9.5.5 Nonconformity and corrective action
- 9.6 Improvement
  - 9.6.1 Threshold management
  - 9.6.2 Continual improvement
  - 9.6.3 Upgrades

Annex A: Use Case Profiles
Annex B: Sample Audit Report

Table of content

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviated terms
5 Scenarios and use of biometric systems involving passive capture subjects
6 Consideration of risk arising from passive biometric identification systems
7 Design and development practice
- 7.1 Algorithms
- 7.2 Sensors
- 7.3 Integration of System Components and User Processes

8 Technical capabilities of the system
- 8.1 Performance
- 8.2 Adaptation
- 8.3 Security and integrity
- 8.4 Privacy measures
- 8.5 Biometric data management
- 8.6 Support for human-initiation and human-review
- 8.7 Support for oversight
- 8.8 Support for testing during operation

9 Operational practice
- 9.1 Resources
- 9.2 Competence
- 9.3 Operational planning and control
- 9.4 Transparency
  - 9.4.1 Public awareness
  - 9.4.2 Provision Documented information
  - 9.4.3 Communication
- 9.5 Performance evaluation
  - 9.5.1 Monitoring, measurement, analysis and evaluation
  - 9.5.2 Management review
  - 9.5.3 Internal audit
  - 9.5.4 External audit
  - 9.5.5 Nonconformity and corrective action
- 9.6 Improvement
  - 9.6.1 Threshold management
  - 9.6.2 Continual improvement
  - 9.6.3 Upgrades

Annex A: Use Case Profiles
Annex B: Sample Audit Report

Terms and definitions

passive biometric identification system
PBI system

biometric identification system where biometric data capture does not require any conscious action of biometric presentation by the capture subject

Note 1 to entry : PBI systems can implement watchlist identification (3.6) as opposed to opt-in identification (3.5)

opt-in identification

biometric identification system where enrolled subjects have consented to be enrolled in and identified by the system

watchlist identification

biometric identification for which the biometric enrolment database consists of a set of identifiers of interest

Table of content

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviated terms
5 Scenarios and use of biometric systems involving passive capture subjects
6 Consideration of risk arising from passive biometric identification systems
7 Design and development practice
- 7.1 Algorithms
- 7.2 Sensors
- 7.3 Integration of System Components and User Processes

8 Technical capabilities of the system
- 8.1 Performance
- 8.2 Adaptation
- 8.3 Security and integrity
- 8.4 Privacy measures
- 8.5 Biometric data management
- 8.6 Support for human-initiation and human-review
- 8.7 Support for oversight
- 8.8 Support for testing during operation

9 Operational practice
- 9.1 Resources
- 9.2 Competence
- 9.3 Operational planning and control
- 9.4 Transparency
  - 9.4.1 Public awareness
  - 9.4.2 Provision Documented information
  - 9.4.3 Communication
- 9.5 Performance evaluation
  - 9.5.1 Monitoring, measurement, analysis and evaluation
  - 9.5.2 Management review
  - 9.5.3 Internal audit
  - 9.5.4 External audit
  - 9.5.5 Nonconformity and corrective action
- 9.6 Improvement
  - 9.6.1 Threshold management
  - 9.6.2 Continual improvement
  - 9.6.3 Upgrades

Annex A: Use Case Profiles
Annex B: Sample Audit Report

Scenarios and use cases considered

Description of use cases :

- search for missing persons
- law enforcement by public authorities
  - Watchlist
  - Investigation after a criminal event
- security of public and private locations

Discussion on characteristics and entailments of passive biometric capture:

- Acquisition frequently in publicly accessible space
- Lower quality than active capture
  - Possible discrepancy between quality of probe and enrolment
  - Need of human assessment to confirm a candidate

Table of content

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviated terms
5 Scenarios and use of biometric systems involving passive capture subjects
6 Consideration of risk arising from passive biometric identification systems
7 Design and development practice
- 7.1 Algorithms
- 7.2 Sensors
- 7.3 Integration of System Components and User Processes

8 Technical capabilities of the system
- 8.1 Performance
- 8.2 Adaptation
- 8.3 Security and integrity
- 8.4 Privacy measures
- 8.5 Biometric data management
- 8.6 Support for human-initiation and human-review
- 8.7 Support for oversight
- 8.8 Support for testing during operation

9 Operational practice
- 9.1 Resources
- 9.2 Competence
- 9.3 Operational planning and control
- 9.4 Transparency
  - 9.4.1 Public awareness
  - 9.4.2 Provision Documented information
  - 9.4.3 Communication
- 9.5 Performance evaluation
  - 9.5.1 Monitoring, measurement, analysis and evaluation
  - 9.5.2 Management review
  - 9.5.3 Internal audit
  - 9.5.4 External audit
  - 9.5.5 Nonconformity and corrective action
- 9.6 Improvement
  - 9.6.1 Threshold management
  - 9.6.2 Continual improvement
  - 9.6.3 Upgrades

Annex A: Use Case Profiles
Annex B: Sample Audit Report

Risk-based framework and high risk system

High level requirements related to risk for systems described in the document :

- Risk assessment
- Testing of systems to ensure fair, safe, and reliable performance
- Operational oversight
- Keeping data private and secure

Table of content

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviated terms
5 Scenarios and use of biometric systems involving passive capture subjects
6 Consideration of risk arising from passive biometric identification systems
7 Design and development practice
- 7.1 Algorithms
- 7.2 Sensors
- 7.3 Integration of System Components and User Processes

8 Technical capabilities of the system
- 8.1 Performance
- 8.2 Adaptation
- 8.3 Security and integrity
- 8.4 Privacy measures
- 8.5 Biometric data management
- 8.6 Support for human-initiation and human-review
- 8.7 Support for oversight
- 8.8 Support for testing during operation

9 Operational practice
- 9.1 Resources
- 9.2 Competence
- 9.3 Operational planning and control
- 9.4 Transparency
  - 9.4.1 Public awareness
  - 9.4.2 Provision Documented information
  - 9.4.3 Communication
- 9.5 Performance evaluation
  - 9.5.1 Monitoring, measurement, analysis and evaluation
  - 9.5.2 Management review
  - 9.5.3 Internal audit
  - 9.5.4 External audit
  - 9.5.5 Nonconformity and corrective action
- 9.6 Improvement
  - 9.6.1 Threshold management
  - 9.6.2 Continual improvement
  - 9.6.3 Upgrades

Annex A: Use Case Profiles
Annex B: Sample Audit Report

Design and development process

7.1 Algorithm :

Recommendations on :

- Development practices
- Internal reporting on accuracy evaluation, including effort to reach sufficient accuracy for the use case and to reduce demographic differentials
- Need to have representative testing dataset

7.2 Sensors

Recommendations on :

- Quality control of captured data
- Management of variety of sensors at training

7.3 Integration of System Components and User Processes

Description of process for human review of candidates proposed by the system, including implementation of double blind review.

Recommendations on data access authorization based on roles and responsibilities.

Table of content

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviated terms
5 Scenarios and use of biometric systems involving passive capture subjects
6 Consideration of risk arising from passive biometric identification systems
7 Design and development practice
- 7.1 Algorithms
- 7.2 Sensors
- 7.3 Integration of System Components and User Processes

8 Technical capabilities of the system
- 8.1 Performance
- 8.2 Adaptation
- 8.3 Security and integrity
- 8.4 Privacy measures
- 8.5 Biometric data management
- 8.6 Support for human-initiation and human-review
- 8.7 Support for oversight
- 8.8 Support for testing during operation

9 Operational practice
- 9.1 Resources
- 9.2 Competence
- 9.3 Operational planning and control
- 9.4 Transparency
  - 9.4.1 Public awareness
  - 9.4.2 Provision Documented information
  - 9.4.3 Communication
- 9.5 Performance evaluation
  - 9.5.1 Monitoring, measurement, analysis and evaluation
  - 9.5.2 Management review
  - 9.5.3 Internal audit
  - 9.5.4 External audit
  - 9.5.5 Nonconformity and corrective action
- 9.6 Improvement
  - 9.6.1 Threshold management
  - 9.6.2 Continual improvement
  - 9.6.3 Upgrades

Annex A: Use Case Profiles
Annex B: Sample Audit Report

Technical capabilities of the system

8.1 Performance :

- Reference to ISO/IEC standards on how to evaluate system performance
  - → 19795-1 for recognition metrics
  - → 30107-3 for concealer attacks
  - → 19795-10 for demographics factors evaluation

8.2 Adaptation

Recommendation to only authorize retraining on production data under control by the system developer. Continuous training is forbidden.

8.3 Security and integrity

High level recommendations and references to relevant security standards.

Call for contribution on more detailed cybersecurity requirements (against several attack scenarios, covering data poisoning, security of logs and access)

Technical capabilities of the system

8.4 Privacy measures

High level recommendations and references to relevant standards.

Call for contribution to provide details on technical means for implementation.

8.5 Biometric data management

Recommendation for :

- Mechanisms to enrol and remove identifiers, possibly with automatic deletion or notification
- Quality feedback for new samples
- Deduplication checks

8.6 Support for human-initiation and human-review

Recommendations for mechanisms to:

- Help operators performing human review
- Allow several reviews and log all decisions

Technical capabilities of the system

8.7 Support for oversight

Recommendations on :

- Logging transactions and integrity protection for audit trails
- Providing training to operators

8.8 Support for testing during operation

Recommendation for checking accuracy remains constant after algorithm update or biometric sensor update.

Reference to ISO/IEC 19795-6 for how to manage testing of a system in production, and impact of passive capture on the test plan,

Table of content

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviated terms
5 Scenarios and use of biometric systems involving passive capture subjects
6 Consideration of risk arising from passive biometric identification systems
7 Design and development practice
- 7.1 Algorithms
- 7.2 Sensors
- 7.3 Integration of System Components and User Processes

8 Technical capabilities of the system
- 8.1 Performance
- 8.2 Adaptation
- 8.3 Security and integrity
- 8.4 Privacy measures
- 8.5 Biometric data management
- 8.6 Support for human-initiation and human-review
- 8.7 Support for oversight
- 8.8 Support for testing during operation

9 Operational practice
- 9.1 Resources
- 9.2 Competence
- 9.3 Operational planning and control
- 9.4 Transparency
  - 9.4.1 Public awareness
  - 9.4.2 Provision Documented information
  - 9.4.3 Communication
- 9.5 Performance evaluation
  - 9.5.1 Monitoring, measurement, analysis and evaluation
  - 9.5.2 Management review
  - 9.5.3 Internal audit
  - 9.5.4 External audit
  - 9.5.5 Nonconformity and corrective action
- 9.6 Improvement
  - 9.6.1 Threshold management
  - 9.6.2 Continual improvement
  - 9.6.3 Upgrades

Annex A: Use Case Profiles
Annex B: Sample Audit Report

Operational practice

9.1 Resources

⇒ Empty section

9.2 Competence

Recommendations on :

- Providing training to operators
- Certification and validation of competence

9.3 Operational planning and control

⇒ Empty section

Operational practice - Transparency

9.4.1 Public awareness

Recommendations about public information and signage around the system to inform the public.

9.4.2 Provision Documented information

Description of documentation provided by system developer to system owner describing functionalities and limitations of the system. It covers the various required functionalities,

9.4.3 Communication

⇒ Empty section

Operational practice – Performance evaluation

9.5.1 Monitoring, measurement, analysis and evaluation

General recommendations about system validation and monitoring.

More details needed.

9.5.2 Management review

⇒ Empty section

9.5.3 Internal audit

Recommendations about continuous evaluation and internal report on accuracy and quality.

Operational practice – Performance evaluation

9.5.4 External audit

Recommendations on mechanisms to support third party evaluation.

Call for contribution for improved guidance to external certifiers for testing/verification procedures

9.5.5 Nonconformity and corrective action

Recommendations on how public and end-users can provide feedback to the developer.

Operational practice – Improvement

9.6.1 Threshold management

Text about score interpretation to manage threshold.

9.6.2 Continual improvement

⇒ Empty section

9.6.3 Upgrades

⇒ Empty section

Table of content

1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviated terms
5 Scenarios and use of biometric systems involving passive capture subjects
6 Consideration of risk arising from passive biometric identification systems
7 Design and development practice
- 7.1 Algorithms
- 7.2 Sensors
- 7.3 Integration of System Components and User Processes

8 Technical capabilities of the system
- 8.1 Performance
- 8.2 Adaptation
- 8.3 Security and integrity
- 8.4 Privacy measures
- 8.5 Biometric data management
- 8.6 Support for human-initiation and human-review
- 8.7 Support for oversight
- 8.8 Support for testing during operation

9 Operational practice
- 9.1 Resources
- 9.2 Competence
- 9.3 Operational planning and control
- 9.4 Transparency
  - 9.4.1 Public awareness
  - 9.4.2 Provision Documented information
  - 9.4.3 Communication
- 9.5 Performance evaluation
  - 9.5.1 Monitoring, measurement, analysis and evaluation
  - 9.5.2 Management review
  - 9.5.3 Internal audit
  - 9.5.4 External audit
  - 9.5.5 Nonconformity and corrective action
- 9.6 Improvement
  - 9.6.1 Threshold management
  - 9.6.2 Continual improvement
  - 9.6.3 Upgrades

Annex A: Use Case Profiles
Annex B: Sample Audit Report

Use Case Profiles

Annex A describes some scenario of applications for usage of face recognition for law enforcement

Annex B is an informative sample audit report

How to contribute ?

How to help

Several empty sections and open calls for contributions

Most needed

- Need more specific technical content for security and privacy sections
- Need contributions for all aspects of operational practice sections

  ⇒ Contributions of end-users would be particularly welcome

How to contribute

- Experts from ISO/IEC SC37, SC27 and SC42 can comment and contribute

  → Only SC37 experts take part in the meeting to dispose of comments and accept contributions

⇒Contact your national bodies (AFNOR, AENOR, BSI, etc) to be registered as an expert in one of these committees and participate