SLOVENSKI STANDARD
SIST-TS CEN/TS 17631:2021

01-september-2021

Osebna identifikacija - Biometrični nadzor dostopa za skupine

Personal identification - Biometric group access control

Persönliche Identifikation - Biometrische Zugangskontrolle für Gruppen

Ta slovenski standard je istoveten z: **CEN/TS 17631:2021**

ICS:

35.240.15	Identifikacijske kartice. Čipne kartice. Biometrija	Identification cards. Chip cards. Biometrics

SIST-TS CEN/TS 17631:2021 **en,fr,de**

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 17631

June 2021

ICS 35.240.15

English Version

Personal identification - Biometric group access control

Persönliche Identifikation - Biometrische Zugangskontrolle für Gruppen

This Technical Specification (CEN/TS) was approved by CEN on 9 May 2021 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN/TS 17631:2021 E

Contents

Page

European foreword

This document (CEN/TS 17631:2021) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, the secretariat of which is held by AFNOR.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

Purpose and Justification:

— Non-discriminative applications: As many subjects as possible are expected to be able to access a biometric system. A large number of the overall public is smaller groups, such as families or accompanied persons, and they will not be discriminated against.

— High throughput: One main objective of the use of biometric access control systems for biometric subjects as well as for operators is the speed of the process and the prevention of queuing times. This would include the applicability of processes to as many persons as possible.

— Increasing automation: Automation can limit time spent on recurrent processes and can decrease the need for (e.g. human and financial) resources. As automation is increasing also in daily life applications, e.g. access to leisure facilities, applications in smart cities etc., the approach should be inclusive and cover most user groups. Such an inclusion of smaller groups into automated access control processes would be the expectation of the public, as such groups are a major fraction of all parties in real life.

— Focus sharpening: Human interaction and staff allocation could in such an automated system focus on more difficult and more complex cases. That way, as easier cases are processed automatically, the more complex cases themselves can be treated faster, and they do not slow down the overall process.

— Prevention of child trafficking: When designing biometric access systems for small groups, measures should be considered to prevent child trafficking e.g. by providing a group internal linkage. This could massively improve the security level as of today.

Benefit for Stakeholders include:

— usage harmonization,

— extension of the target user group compared to current biometric access control technology,

— interoperability in workflow and data formats,

— establishment of usable biometric group access in several application environments,

— facilitation of throughput of biometric processes used for access control, and

— integration of biometric technology into security technology.

1 Scope

This document provides guidance on providing access:

— to areas with physical access control, e.g. entertainment facilities, train stations, shops, libraries, banks, or border control,

— for small groups of persons, e.g. families with small children or seniors, or other accompanied persons in need of support,

— by means of biometric authentication technologies, e.g. facial, fingerprint, or vein recognition,

— in the European regulatory context.

The document addresses the following aspects, which are specific for biometric and group access:

— accessibility and usability,

— user guidance including group guidance and interaction control,

— privacy including data set content,

— presentation attack detection,

— applicable biometric technologies,

— storage of reference data,

— biometric process integration,

— specific needs considering biometrics for groups,

— biometric performance and error rates, and

— group internal linkage.

The following aspects which reflect on generic access control issues are out of scope:

— IT security,

— application specific physical security,

— policy definition,

— processes not related to biometric authentication, and

— specific performance requirements of identification (1:N) and verification (1:1) applications.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN 17054:2019, *Biometrics multilingual vocabulary based upon the English version of ISO/IEC 2382-37:2012*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 17054:2019 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
small group
in the context of access control, group of up to 10 persons with a common purpose that seek access together

Note 1 to entry: Examples for a common purpose can be a joint travel or a joint visit to a building / a site.

Note 2 to entry: This document is mainly focussing on families or accompanied persons; the maximum size depends on the application.

4 Symbols and abbreviations

FAR	false acceptance rate
FRR	false rejection rate
FTA	failure to acquire
MRZ	machine readable zone
PAD	presentation attack detection

5 Group access control processes and technologies

5.1 Architecture

5.1.1 General

The access point architecture shall support authentication of small groups of persons using biometric technology and additional token or documentation, e.g. mobile phone or tickets. Therefore, a system needs to have at least two elements: one for capturing biometric data and one for checking the authorization to access e.g. by an additional token or documentation.

EXAMPLE Family with a ticket for the zoo, or family going to a swimming pool with their credentials checked in a database.

NOTE 1 Whilst this document talks about access control applications, also exit control components are in scope. In some application contexts, especially where time and location of exit are relevant, e.g. in public transport or for a half-day spa ticket, the relevant biometric components and workflows to register an exit are analogous to the registration of an entry.

While 1:N-applications systems using only one element for capturing biometric data are possible, they would require high performance biometric comparison technology and high quality biometric data. These prerequisites might not be given in applications where the subjects are e.g. children or seniors. Also, such a system could be prone to privacy breach by e.g. profiling. Additionally, giving the users of the system physical proof of their subscription to a service is an advantage to users - they will know what they subscribed to and are given a means to get additional information such as a seat number.

Activating a system by presenting a token or documentation can prevent the acquisition of biometric data from persons not seeking access. For those reasons, this document only considers systems that use two-element architectures.

One-step applications will perform all steps of the authentication process at the same location. Then the users will not need to move from one location to the other while being authenticated.

Integrated two-step applications will perform the steps of the authentication process, i.e. the check of the token or documentation and biometric authentication process at two locations back to back in direct sequence.

Segregated two-step applications will perform the steps of the authentication process, i.e. the check of the token or documentation and biometric authentication process at two locations, which are separated from each other. In this case, the users will need to move from one location to the other to finish the authentication process.

Some access control applications will not use doors. It can be sufficient to have capturing areas in which biometric data of the users are captured. Situations are possible where a guard is alerted if access is denied or problems with access arise.

Depending on the application, the token or documentation is checked at a dedicated fixed location.

NOTE 2 For a description of the architecture of biometric systems in general, see ISO/IEC TR 24741.

For small group, it is recommended to either use a segregated two-step application or to design a one-step application so that the use is intuitive and waiting times are short e.g. by capturing of biometric data when approaching the access point. In the latter case, privacy aspects shall be considered, as no data shall be taken of persons that are not involved, e.g. by location of the access point and organization of queuing. Integrated two-step applications can generate an impression of an isolating device and should therefore only be used where this impression is intended. For applications with high security requirements such a design might be appropriate, for applications where comfort has a high relevance this design cannot be recommended.

5.1.2 Biometric process and background integration

The biometric process can be distinguished in three major use cases, which are described in Table 1.

Table 1 — Use cases of biometric processes

Use Case 1		
Token	One or several copies of the same	Description: Every member or some members have a token. If the group arrives together, only one token is needed to start the process. When there are subgroups, at least one member of each subgroup needs to be authenticated. Benefit: Fast process. Every member can hold a token. The group could be split in subgroups. Disadvantage: In case of several copies the cost factor has to be considered. It is unclear which members of the group already entered; only the authenticated member and possibly the number of nonauthenticated members is known. Example: one singular family ticket, where all adults are enrolled, at least one of them is authenticated and the children are counted if necessary, hotel room, meeting room etc.
Enrolees	One or more	
Authenticated subjects	One or more (subset of enrolees)	
Counted only subjects	All nonauthenticated, if necessary	

Use Case 2		
Token	One	Description: Several variants are possible: to capture the biometric data of all group members and to use the best or to capture the biometric data of one group member after the other and to use the first match, or to fuse results in a chosen combination. If all subjects are authenticated this will potentially provide high security, but the process will be slowed down. Also, the whole group is denied access if one false non match occurs. Benefits: All group members can be the holder of the token. Depending on the sytem design, one or few false non matches might not influence the overall acceptance decision. Situation-based scaling of the security level is possible, e.g. more group members can be authenticated in a critical situation. Disadvantages: If there is only one token, the group has to seek access together and it is not possible that some members arrive later. All group members need to be enroled. Example: train ticket for groups.
Enrolees	All	
Authenticated subjects	One or more (subset of enrolees) up to all	
Counted only subjects	All nonauthenticated	
Use Case 3		
Token	every member of the group has a personal token	Description: By pre-processing, i.e. by using a physical or virtual meta-token ("family" passport) the individuals can be linked together to one group. Benefits: Very high security. The group can be processed together or individually or in subgroups as they choose. Disadvantage: The whole group is denied access if one false non-match occurs. Example: ABC gates. Note: According to pre-defined criteria there can be exceptions to the number of enrolled and authenticated members, e.g. children under 5 years old holding a passport, who are not enrolled, not authenticated, but counted.
Enrolees	preferably all with exceptions	
Authenticated subjects	preferably all with exceptions	
Counted only subjects	preferably none with exceptions	

The process (see use cases above) shall be chosen according to security, usability and business requirements, taking into account the benefits and disadvantages mentioned.

Use cases 1 or 2 show usability and speed advantages for biometric group access control. Use case 2 can be recommended if the group usually seeks access together. As use case 1 involves several copies of a token, it can be recommended if the group usually splits in subgroups, e.g. if a meeting room is shared but meeting participants do not necessarily arrive at the same time.

Use case 3 provides the highest security and is therefore recommended for applications with high security requirements, e.g. governmental applications. As any failure can cause the whole group to be denied access, special care should be taken to error management, as for example described in the two step process in 5.1.3

Especially in the cases where only parts of the group seek access at the same time, it shall be defined when the process is completed and access is given. It is assumed that the access process is completed if:

a) there is a notification by the group about the total number of persons seeking access,

b) the last entering group member notifies on the completion,

c) all group members have gained access,

d) an individual not belonging to the group is detected, e.g. by presenting a token of another group, or

e) a time-out applies.

NOTE Waiting for the next group or for a time-out might reduce the application throughput and increase the waiting time for the group.

If not all group members seek access at the same time, it is recommended to complete the access process using one of the steps described in a) or b), as this prevents unauthorized access by individuals not belonging to the group, e.g. by following a sub-group.

Processes need to be in place to address system failures such as low data quality, failure to acquire, wrong presentation, usability problems, poor environmental conditions. Such system failures shall be detected by the system and potential deadlocks shall be resolved by the system. Adequate feedback shall be given to the users in all situations.

Feedback processes, user guidance and usability of the system (see Clause 6) are essential to ensure reliable biometric processes. The main facilitator for high throughput is a good process design taking into account the needs of the users (see Clause 6).

5.1.3 Segregated two steps access control

In some contexts, such as airport border control, managing groups faces the challenges of applying consistent and measurable checkpoint identity screening with the same level of efficiency as for single travellers without discrimination.

While fully automated biometric access control solves these challenges for single users, managing groups has the following technological issues:

— Reliably counting the number of people in the closed environment of the access point. It needs to be considered that babies or young children may be asleep in their parents' arms or in a body-worn sling.

— Offering a convenient way to acquire biometric data and process tokens of all members of the group in said closed environment.

— Acquiring biometric data of young if the group is a family with children.

For the example of eGates, the end-result of the fully automated eGate environment is that the eGate needs to precisely determine the number of people inside, obtain both biometric reference data (for instance from a passport) and live biometric data for comparison. It is impractical and prone to errors to perform these actions in sequence.