

DIN CEN/TS 17631

ICS 35.240.15

**Persönliche Identifikation –
Biometrische Zugangskontrolle für Gruppen;
Englische Fassung CEN/TS 17631:2021**

Personal identification –
Biometric group access control;
English version CEN/TS 17631:2021

Gesamtumfang 20 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (CEN/TS 17631:2021) wurde vom Technischen Komitee CEN/TC 224 „Persönliche Identifikation und damit verbundene persönliche Geräte mit sicherem Element, Systeme, Verfahren und Privatsphäre in einem sektorübergreifenden Umfeld“ erarbeitet, dessen Sekretariat von AFNOR (Frankreich) gehalten wird.

Das zuständige nationale Normungsgremium ist der Arbeitsausschuss NA 043-01-37 AA „Biometrie“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Technische Spezifikationen sind nicht Bestandteil des Deutschen Normenwerks.

Eine Technische Spezifikation ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens von DIN noch nicht als Norm herausgegeben wird.

Zur vorliegenden Technischen Spezifikation wurde kein Entwurf veröffentlicht.

Dieses Dokument enthält unter Berücksichtigung des DIN-Präsidialbeschlusses 1/2004 nur die Englische Fassung von CEN/TS 17631:2021.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Begriffe und Abkürzungen

Reihenfolge und Inhalt der folgenden Begriffe sind identisch mit denen im Abschnitt Begriffe der Englischen Fassung.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach EN 17054:2019 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1 Kleingruppe
im Zusammenhang mit der Zugangskontrolle, Gruppe von bis zu 10 Personen mit gemeinsamem Ziel, die zusammen Zugang suchen

Anmerkung 1 zum Begriff: Beispiele für ein gemeinsames Ziel können gemeinsames Reisen oder ein gemeinsamer Besuch eines Gebäudes/Ortes sein.

Anmerkung 2 zum Begriff: Dieses Dokument ist fokussiert auf Familien oder begleitete Personen; die Maximalgröße hängt von der Anwendung ab.

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

Contents

Page

European foreword.....	3
Introduction	4
1 Scope	5
2 Normative references.....	5
3 Terms and definitions	6
4 Symbols and abbreviations	6
5 Group access control processes and technologies.....	6
5.1 Architecture	6
5.1.1 General.....	6
5.1.2 Biometric process and background integration	7
5.1.3 Segregated two steps access control.....	9
5.2 Integration of Access Control into other management systems	11
5.3 Applicable biometric technologies	11
5.3.1 General.....	11
5.3.2 Segregated two steps access control.....	12
5.4 Interoperability issues.....	12
5.5 Storage of reference data	12
5.5.1 General.....	12
5.5.2 Segregated two steps access control.....	13
5.6 Biometric performance and error rates.....	13
6 Accessibility, usability, and guidance	14
6.1 General.....	14
6.2 Accessibility	14
6.3 Usability.....	14
6.4 Guidance.....	14
6.5 Segregated two steps access control.....	15
7 Privacy and security considerations.....	15
7.1 Privacy.....	15
7.1.1 General.....	15
7.1.2 Segregated two steps access control.....	15
7.2 Presentation attack detection	16
7.3 Group internal linkage.....	16
Annex A (informative) Example for need of group internal linkage: Human being trafficking ...	17
A.1 Background	17
A.2 Detection of illegal activities in a two step travel application.....	17
Bibliography.....	18

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.