BS EN ISO/IEC 24760-3:2022
Incorporating corrigendum November 2022

BSI Standards Publication

Information technology — Security techniques — A framework for identity management

Part 3: Practice

bsi.

National foreword

This British Standard is the UK implementation of EN ISO/IEC 24760-3:2022. It is identical to ISO/IEC 24760-3:2016.

The UK participation in its preparation was entrusted to Technical Committee IST/33/5, Identity Management and Privacy Technologies.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2022

ISBN 978 0 539 24946 0

ICS 35.030; 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2022.

Amendments/corrigenda issued since publication

Date	Text affected
30 November 2022	Correction to national foreword. CEN/CENELEC pages added. Correction to ISO/IEC pages.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 24760-3

September 2022

ICS 35.030

English version

Information technology - Security techniques - A framework for identity management - Part 3: Practice (ISO/IEC 24760-3:2016)

Technologies de l'information - Techniques de sécurité - Cadre pour la gestion de l'identité - Partie 3: Mise en oeuvre (ISO/IEC 24760-3:2016)

Informationstechnik - Sicherheitsverfahren - Rahmenwerk für Identitätsmanagement - Teil 3: Umsetzung (ISO/IEC 24760-3:2016)

This European Standard was approved by CEN on 5 September 2022.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees 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, Türkiye and United Kingdom.

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

European foreword

The text of ISO/IEC 24760-3:2016 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 24760-3:2022 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2023, and conflicting national standards shall be withdrawn at the latest by March 2023.

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

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: 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, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 24760-3:2016 has been approved by CEN-CENELEC as EN ISO/IEC 24760-3:2022 without any modification.

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Symbols and abbreviated terms ... **2**

5 Mitigating identity related risk in managing identity information ... **2**
5.1 Overview ... 2
5.2 Risk assessment ... 2
5.3 Assurance in identity information ... 3
5.3.1 General ... 3
5.3.2 Identity proofing ... 3
5.3.3 Credentials ... 3
5.3.4 Identity profile ... 3

6 Identity information and identifiers ... **4**
6.1 Overview ... 4
6.2 Policy on accessing identity information ... 4
6.3 Identifiers ... 4
6.3.1 General ... 4
6.3.2 Categorization of identifier by the type of entity to which the identifier is linked 4
6.3.3 Categorization of identifier by the nature of linking ... 5
6.3.4 Categorization of identifier by the grouping of entities ... 6
6.3.5 Management of identifiers ... 6

7 Auditing identity information usage ... **6**

8 Control objectives and controls ... **6**
8.1 General ... 6
8.2 Contextual components for control ... 7
8.2.1 Establishing an identity management system ... 7
8.2.2 Establishing identity information ... 9
8.2.3 Managing identity information ... 10
8.3 Architectural components for control ... 11
8.3.1 Establishing an identity management system ... 11
8.3.2 Controlling an identity management system ... 13

Annex A (normative) **Practice of managing identity information in a federation of identity management systems** ... **15**

Annex B (normative) **Identity management practice using attribute-based credentials to enhance privacy protection** ... **24**

Bibliography ... **31**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

ISO/IEC 24760 consists of the following parts, under the general title *Information technology — Security techniques — A framework for identity management*

— *Part 1: Terminology and concepts*

— *Part 2: Reference architecture and requirements*

— *Part 3: Practice*

Introduction

Data processing systems commonly gather a range of information on their users, be it a person, piece of equipment, or piece of software connected to it and make decisions based on the gathered information. Such identity-based decisions may concern access to applications or other resources.

To address the need to efficiently and effectively implement systems that make identity-based decisions, ISO/IEC 24760 specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components, which operate on behalf of individuals or organizations.

For many organizations, the proper management of identity information is crucial to maintain security of the organizational processes. For individuals, correct identity management is important to protect privacy.

This part of ISO/IEC 24760 specifies fundamental concepts and operational structures of identity management with the purpose to realize information system management, so that information systems can meet business, contractual, regulatory and legal obligations.

This part of ISO/IEC 24760 presents practices for identity management. These practices cover assurance in controlling identity information use, controlling the access to identity information and other resources based on identity information, and controlling objectives that should be implemented when establishing and maintaining an identity management system.

This part of ISO/IEC 24760 consists of the following parts:

— ISO/IEC 24760-1: Terminology and concepts;

— ISO/IEC 24760-2: Reference architecture and requirements;

— ISO/IEC 24760-3: Practice.

ISO/IEC 24760 is intended to provide foundations for other identity management related International Standards including the following:

— ISO/IEC 29100, Privacy framework;

— ISO/IEC 29101, Privacy reference architecture;

— ISO/IEC 29115, Entity authentication assurance framework;

— ISO/IEC 29146, A framework for access management.

INTERNATIONAL STANDARD **ISO/IEC 24760-3:2016(E)**

Information technology — Security techniques — A framework for identity management —

Part 3: Practice

1 Scope

This part of ISO/IEC 24760 provides guidance for the management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1 and ISO/IEC 24760-2.

This part of ISO/IEC 24760 is applicable to an identity management system where identifiers or PII relating to entities are acquired, processed, stored, transferred or used for the purposes of identifying or authenticating entities and/or for the purpose of decision making using attributes of entities. Practices for identity management can also be addressed in other standards.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 24760-1, *Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 24760-1 and the following apply.

3.1
identity management system
system comprising of policies, procedures, technology and other resources for maintaining identity information including meta data

[SOURCE: ISO/IEC 24760-2:2015, 3.3]

3.2
identity profile
identity containing attributes specified by an identity template

3.3
identity template
definition of a specific set of attributes

Note 1 to entry: Typically, the attributes in a profile are to support a particular technical or business purpose as needed by relying parties.

3.4
identity theft
result of a successful false claim of identity

3.5
federation manager
actor in a federation responsible for managing the issues arising from the operation of the federation

Note 1 to entry: An existing federation member or an independent third party can carry out the role of federation manager.

3.6
principal
entity to which identity information in an identity management system pertains

[SOURCE: ISO/IEC 24760-2:2015, 3.4]

4 Symbols and abbreviated terms

For the purposes of this document, the following symbols and abbreviated terms apply.

ICT Information and Communication Technology

IIP Identity Information Provider

IIA Identity Information Authority

PII Personally Identifiable Information

RP Relying Party

5 Mitigating identity related risk in managing identity information

5.1 Overview

Clause 5 presents practices to address identity related risk when operating an identity management system conforming to ISO/IEC 24760-1, ISO/IEC 24760-2 and ISO/IEC 29115.

5.2 Risk assessment

One function of an identity management system is to manage the risk of identity errors, and the confidentiality, integrity and availability of identity information that it stores, processes and communicates. It is necessary to understand the level of risk, which will depend on the application. The owner of the application should conduct a risk assessment to determine the level of risk. The result will provide information, which can be used to determine the necessary risk management criteria and processes for the identity management system. The information an identity management system needs includes the level of assurance in identity information required and the requirements for confidentiality, integrity and availability of this information.

ISO/IEC 24760-2 specifies tools to manage risks as policies, regulation, design and architecture. In some contexts involving consumers, protecting personally identifiable information and giving principals control over the use of their personally identifiable information is paramount. ISO/IEC 29100, ISO/IEC 29101, ISO/IEC 29134 and ISO/IEC 29151 (to be published) specify requirements and provide guidance for the protection of privacy.

Identity information managed by an identity management system may also be managed by reference to identity information providers in another domain. For example, identity proofing may be undertaken by a service provider, which operates in a different domain to that of the identity management system.

When identity information is collected and stored, risk management measures shall be implemented by the identity management service to mitigate the risks identified by a risk assessment carried out in the

application domain by the relying party. Levels of assurance in regard to identity information and access services shall be determined and specified by the relying party according to assessed levels of risk.

5.3 Assurance in identity information

5.3.1 General

Confidence in identity information provided by an identity management system comes from processes that assure the validity of the information from its collection through its subsequent storage and maintenance by the system. Assurance is typically quantified in terms of assurance levels with higher levels corresponding to greater assurance. The level of assurance achieved depends on the quality of the identity information and the rigour of the identity validation processes. Levels of assurance are described in ISO/IEC 29115.

5.3.2 Identity proofing

Identity proofing, i.e. validating identity information for enrolment of an entity in a domain, shall meet a defined level of assurance. The level of assurance of identity proofing achievable depends on the type and characteristics of information and, in some case, the scope of this information, e.g. the number of independent identity information providers used as sources of the information.

An increased level of assurance in identity verification may be achieved

— with verification of additional credentials issued from multiple sources, and

— using a trusted external party that knows the entity to validate claimed identity information.

NOTE 1 ISO/IEC 29003 provides requirements for identity proofing.

NOTE 2 ISO/IEC 29115 specifies how to achieve different levels of assurance.

5.3.3 Credentials

An identity management system may issue multiple types of credential differing in the level of assurance of the identity information represented by the credential.

An identity management system issuing credentials with a high level of assurance supported by a cryptographic mechanism should provide a service for relying parties to actively support the cryptographic validation process.

5.3.4 Identity profile

An identity management system may use one or more identity profiles for gathering, structuring, or presenting identity information.

NOTE Although a profile can contain identity information, it is not intended for identification. Its purpose is to provide identity information about an entity to system processes that need the information for their processes.

An entity may have multiple identity profiles, each containing a different set of attributes for the entity. For instance, a language preference may be present in a profile for an access interface and not in a profile for book interests.

An identity template may be established as an international or industry standard. The use of a standardised identity template to record identity attributes would facilitate the usage of identity profiles across domains.

An identity profile may be used in access management to determine the required identity attributes for being authorized for a role or privilege in accessing information. An identity profile may be used as a pre-configured subset of identity information to be presented when interacting with a service.

An attribute in an identity profile may be associated with a level of assurance. Using an identity profile with associated levels of assurance to present identity information shall imply that each item of information has been validated at minimally its associated level of assurance. An identity profile specifying requirements for access to services or resources may be associated with a specific additional entity identifier that may indicate the activities linked to the specific privileges.

6 Identity information and identifiers

6.1 Overview

Organizations should understand the information security concerns for their business and for compliance with relevant legislation and should provide management support to meet the business needs. In regard to identity management, organizations should understand their liabilities and ensure that adequate controls are implemented to mitigate the risks and consequences of identity information leakage, corruption and loss of availability when collecting, storing, using, transmitting and disposing of identity information. Organizations should specify control objectives and controls to ensure that information security requirements are met.

6.2 Policy on accessing identity information

The identity information pertaining to an entity should be managed to ensure that the following:

— identity information remains accurate and up-to-date over time;

— only authorized entities have access to the identity information and are accountable for all uses and changes in identity information, guaranteeing traceability of any processing of identity information by any entity, whether a person, a process or a system;

— the organization fulfils its obligations with respect to regulations and contractual agreements;

— principals are protected against the risk of identity-related theft and other identity related crime.

NOTE Typically, an information security policy highlights the necessity to securely manage identity information. The preservation and protection of any entities identity information is also required when dealing with third parties as typically documented within the operational procedures.

6.3 Identifiers

6.3.1 General

An identifier allows distinguishing unambiguously one entity from another entity in a domain of applicability. An entity may have multiple, different identifiers in the same domain. This may facilitate the representation of the entity in some situations, e.g. hiding the entity's identity when providing the entity's identity information for use in some processes or within some systems. An identifier created in one domain may be reused intentionally in another domain provided the reused identifier continues to provide uniqueness of identity within the other domain.

6.3.2 Categorization of identifier by the type of entity to which the identifier is linked

6.3.2.1 Person identifiers

A person identifier may be, e.g. a full name, a date of birth, a place of birth, or various pseudonyms, such as a number assigned by an authority as a reference, e.g. a passport number, a national identity number or an identity-card number.

The use of pseudonyms as identifiers is frequent for person identifiers; see.6.3.3.2.

NOTE A pseudonym can enhance the privacy of persons in an identity-authentication exchange with a relying party as a pseudonym may reveal less personally identifiable information than if a real name is used as an identifier.

6.3.2.2 Identifier assigned to a non-person entity

Non-person entities, e.g. devices or other information objects, may have their activities identified and recorded as for persons.

Device identifiers allow distinction between devices in the domain in which they operate.

NOTE 1 Example: The International Mobile Equipment Identity (IMEI) is an identifier of the mobile telephone handset in the domain of GSM mobile telephone services.

NOTE 2 Example 2: The GSM SIM card number (ICCID) is a unique device identifier in the domain of a mobile telephone service. A SIM card also contains other identifiers including that of the user who registered the SIM card.

Information object identifiers may also need to be distinguished in their domains. One of their attributes of a combination of their attributes is usually used as identifier.

NOTE 3 Example: Process name, session name, path name, uniform resource names (URN), uniform resource identifier (URI) are examples of information-object identifiers.

NOTE 4 Example: URI is an example of identifier for a location, but the object at that location may change at any time.

6.3.3 Categorization of identifier by the nature of linking

6.3.3.1 Verinymous identifier

A verinymous identifier is an identifier, persistent in its domain of applicability that may be used within and across domains and allows a relying party to obtain further identity information for the entity associated with the identifier. Commonly observed verinimous identifiers includes email address, mobile phone number, passport number, driving license number, social security number and the name-date of birth pair.

A verynimous identifier may allow identity information for entities known in different domains to be correlated. While it is fine to correlate the identities if so desired by the person, unexpected correlation, e.g. profiling, has a negative privacy impact. By the nature of the veronymous identifier, if information leakage incident happens, it allows adversaries to perform such correlation and create threats, e.g. of generating any privacy-related information that the principal did not intend to disclose.

6.3.3.2 Pseudonymous identifier

A pseudonymous identifier is an identifier, persistent in its domain that does not disclose additional identity information. As long as no other identifying information is available in the domain, identities from different domain cannot be correlated using a pseudonymous identifier. A pseudonymous identifier may be used to prevent unwanted correlation of identity information for entities across domains.

NOTE The mere use of pseudonymous identifiers does not equate with identity data being pseudonymous. Other attributes combined at one point in time or across multiple points in time may be enough to derive verinymous identifiers.

6.3.3.3 Ephemeral identifier

An ephemeral identifier is an identifier that is used only for a short period of time and only within a single domain. It may change for multiple uses to the same service or resource.

NOTE 1 If used correctly, an ephemeral identifier will make it very difficult for two visits by an entity to be correlated.

NOTE 2 An ephemeral identifier is often used in the context of attribute based access control where access to a resource is granted if the entity has a particular attribute. For example, if the resource access is granted for a person because they are a member of a particular group, the identity would be composed of an ephemeral identifier and a group identifier. These would serve the access control purpose while minimizing the data disclosed or the possibility of linking multiple accesses, while still differentiating each entity.

6.3.4 Categorization of identifier by the grouping of entities

6.3.4.1 Individual identifier

An individual identifier is an identifier that is associated with only one entity within a domain of applicability.

6.3.4.2 Group identifiers

Entities are sometimes grouped in a group entity when the need exists to execute activities in a group. A distinct group identity will represent the group entity and group identifiers will help unambiguously identifying the group entity and recording activities of the group entity in their domains. Group identifiers serve the need for a person entity of performing activities in a group or on behalf of a group; they may hide the action originator of an activity in a group. Additional techniques may therefore be required to unambiguously identify a single entity as member of a group entity.

6.3.5 Management of identifiers

When updating identity information for a known entity an identity management system may assign a new identifier to the changed identity; it also may remove the association of the old identifier with the identity. Changed identity information may be proactively communicated to subsystems that rely on it.

7 Auditing identity information usage

Managing and processing identity information by authorized entities in a domain may be subject to various legal, regulatory and industry business requirements that necessitate some level of monitoring and traceability.

NOTE These requirements can be wide ranging, including everything from log-files and other measures for the protection of personally identifiable information, to maintaining required time-stamp accuracy and traceability; see ISO/IEC 18014.

An entity providing services associated with identity management should provide mechanisms assuring auditability.

8 Control objectives and controls

8.1 General

Clause 8 summarizes security objectives and associated controls to be verified when setting up or reviewing an identity management system.

The structure of the controls follows the structure presented in ISO/IEC 27002.

8.2 Contextual components for control

8.2.1 Establishing an identity management system

8.2.1.1 Objective

To establish a management system to initiate and control the implementation of managing identity information for entities.

8.2.1.2 Defining and documenting the domain of applicability

Control

The relying parties for which an entity, or a group of entities, is enabled to apply its identity and which may use the identity for identification and for other purposes shall be documented to be clearly understood both by the operators and the entities involved.

Implementation guidance

Documentation that describes the boundaries of the domain of a system for identity management should be made available to all interested parties. This documentation should specify the limits where the identity information can be verified. Any potential extensions to other domains or groups of entities should also be documented.

The documentation should clarify constraints, legally, or otherwise, and associated liabilities, on the control of identity information in a domain.

Other information

A domain of an identity is well defined in relation to a particular set of attributes defining groups of entities.

An IT system within an organization that allows a group of entities to login is a sub-domain in that organization.

8.2.1.3 Identifying identity information providers (IIP), identity information authorities (IIA), identity management authorities, and regulatory bodies

Control

Identity information authorities for identity information managed by an identity management system shall be specified for the domain of an identity management system.

Entities endorsing management and regulator responsibilities for the protection of identity information shall also be identified.

Implementation guidance

Entities associated with an identity management system as source of identity information (IIP), authoritative statement on available information (IIA), the identity management authority and any relevant regulatory bodies, government or otherwise, should be clearly identified.

The operations performed by an identity information provider are to create, maintain and make accessible identity information for entities known in a particular domain. The methods to access information or obtain services provided by these operational entities should also be provided.

Any changes in availability and methods for access and to obtain services should be actively communicated to interested parties.

Other information

An entity may combine the functions of identity information provider and identity information authority.

8.2.1.4 Identifying relying parties (RP)

Control

Relying parties shall be made known for the domain of the identity management system.

Implementation guidance

Relying parties have trust relationships with one or more identity information authorities. Relying parties related with an identity information authority may be known at the design stage. RPs may change over time, joining, or leaving a relationship with one or more identity information authorities in the domain.

Other information

A relying party is exposed to risk caused by incorrect or invalid identity information.

8.2.1.5 Maintaining an identity management system

Control

A process shall be described to ensure the maintenance of the important operational entities in an identity management system.

Implementation guidance

Over time, domains of an identity management system may use different identity information authorities, identity information providers and relying parties to support their interactions with entities. Domains may also be created and terminated or their conditions of applicability may change.

Important entities for use of an identity management system, e.g. IIA, IIP and RP, may also cease to exist after being replaced, being archived, or deleted. An identity management system should document policies and processes that ensure the control of these important entities and should ensure that valuable information of the identity management system is not lost.

8.2.1.6 Privacy assurance

Control

When human entities interact within an identity management system that manages identity information of them, it shall have documented policies and have established controls that assure the protection of their privacy.

Implementation guidance

A basic objective of establishing an identity management system is to ensure the privacy of entities is preserved at any time.

An identity management system shall document any sensitive information it processes about human entities to conform to ISO/IEC 24760-1.

Other information

Requirements for the handling of sensitive identity information are given in

— ISO/IEC 29100, and

— ISO/IEC 29101.

8.2.2 Establishing identity information

8.2.2.1 Objective

To define, document and communicate identity information.

8.2.2.2 Identity representation

Control

References of an entity in an identity management system, which remains the same for the duration the entity remains known in the domain(s) of the system, may be referred to as "reference identifier." The identity management system shall document controls for the identity management systems to guarantee the unique distinguishability of any entity in any domain of the identity management system.

Implementation guidance

A reference identifier should persist at least for the existence of the entity in an identity management system and may exist longer than the entity, e.g. for archiving purposes or authorities' needs.

Identity management system documentation should describe the use and reuse of identifiers. A reference identifier for an entity should not be reused while any identity information relating to that entity, including archived information, is recorded on the system.

A reference identifier generator is a tool that may help to provide unique values for reference identifiers.

Other information

To facilitate maintaining the recorded information for a specific identity, the identity management system may use a reference identifier generator to assign a unique record number to an identity being added.

8.2.2.3 Identity information

Control

The set of values of attributes required to compose identity information pertaining to an entity in domains of an identity management system shall be fixed, validated by the verifiers, and communicated, as requested, to relying parties.

Implementation guidance

Verification of the values of required attributes from an identity results in an authenticated identity for an entity.

The authentication process involves tests by a verifier of one or more identity attributes provided by an entity to determine, with the required level of assurance, their correctness.

8.2.2.4 Distinguishing different types of entity

Control

The number of distinct entity types in the domains of an identity management system shall be recognized and described with distinct attributes values composing their identity.

Implementation guidance

Items inside or outside an ICT system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence in domains of an identity management system, are distinct entity types that may be described with different attribute values.

Each entity type should be documented covering semantic and syntax with the list of required attribute values for their identity being validated.

8.2.2.5 Authenticating an identity

Control

A process shall be documented that verifies the identity information for an entity.

Implementation guidance

An authentication process involves operations by a verifier that should establish that identity information for an entity is correct to a level of assurance required by the service to be rendered to the entity.

Verifiers may be the same as, or act on behalf of, the identity information authority for a particular domain.

8.2.3 Managing identity information

8.2.3.1 Objective

To ensure that identity information is maintained and protected in all domains of an identity management system, from initial enrolment until archiving or deletion.

8.2.3.2 Assurance in collecting and managing identity information

Control

All information security responsibilities for the collection and the management of identity information shall be defined and allocated.

Implementation guidance

Allocation of information security responsibilities for collecting and managing identity information shall be established in accordance with the information security policies. Responsibilities for the protection of individual identity information and for carrying out specific information security processes on collecting and managing identity information should be identified.

Responsibilities for information security risk management activities and in particular for acceptance of residual risks when defining levels of assurance in collecting identity information should be defined.

Identity management activities should include the following:

— application(s) implementing an identity register;

— ensuring correctness of the identity information with a defined level of assurance;

— establishing the domain of origin of specific attribute values in identity information;

— maintaining the identity information over the lifecycle of the identity;

— authenticating the identity;

— mitigating the risk of identity information theft or misuse.

Other information

The information security manager of an organization, if identified, should take overall responsibility for the development and implementation of the levels of assurance to support the collection of identity information and for the management of identity information.

8.2.3.3 Defining and controlling identity lifecycle

Control

A formalized process that defines and maintains the lifecycle of identities in domains and controls the status of any identity in each domain shall be documented.

Implementation guidance

The lifecycle of identity information starts from enrolment and ends when all identity information for an entity is deleted from the system, including any archived information.

Other information

The following stages in the identity lifecycle are, according to ISO/IEC 24760-1, identified:

— unknown;

— established;

— active;

— suspended;

— archived;

— deleted.

8.3 Architectural components for control

8.3.1 Establishing an identity management system

8.3.1.1 Objective

To ensure a system is implemented and well documented for the management of identity information.

8.3.1.2 Documenting an identity management system

Control

An identity management system shall be documented prior to being implemented.

Implementation guidance

The documented design for the architecture of an identity management system should specify the system in its deployed context based on defined *stakeholders* and *actors* and established requirements.

The documented design should address requirements for both actor and non-actor stakeholders.

Other information

The documented design shall exhaustively describe

— actor requirements,

— stakeholder requirements,

— view points,

— models,

— components,

— maintenance processes, and

— information flows and actions.

The list of actor's types and their interactions with the systems should also be documented.

The documented design should specify the scenario used for the identity management system, e.g. enterprise, federated, service, or heterogeneous. The design should accordingly specify the components and flows of the selected scenario.

8.3.1.3 Identifying an identity registration authority

Control

An identity registration authority shall be identified for any identity management system.

Implementation guidance

An identity registration authority has the duty and capabilities to set and enforce operational policies for collecting, recording and updating identity information.

Responsibilities of an identity-registration authority include the following:

— to modify, create or revoke operational policies;

— to authorize modification of mechanisms to establish a required level of assurance in entity authentication for accessing identity information and system control functions;

— to authorize changes in the type of information recorded in the repository;

— to authorize modification of identity information recorded in the repository.

Other information

If not identified, the information security manager should play the role of the identity registration authority.

8.3.2 Controlling an identity management system

8.3.2.1 Objective

To ensure an identity management system is enclosing mechanisms for preserving and maintaining identity information.

8.3.2.2 Accessing an identity management system

Control

Access to an identity management system shall be limited to people dedicated to its maintenance, identity information providers and relying parties, and to individuals for the consultation of information collected on their person in the context of privacy protection.

Implementation guidance

An information management system should develop the required interfaces to provide access to the need-to-have entities, with appropriate rights authorized by the identity information authority or the identity registration authority.

8.3.2.3 Required components of an identity management system

Control

An identity management system shall include, at a minimum

— repository of identity information related to the entities recognized in its domains, possibly organised using identity templates,

— management system operating under a unified policy, capable of collecting identity information from various validated sources (attributes domains of origins), and deleting the information when the conditions for storing identity information cease to exist,

— management interfaces for providing access to identity information, and

— storage component archiving the information on entities that ceased to exist.

Implementation guidance

Identity management systems may vary in components depending on the model developed for its implementation. It is also very common to see an identity management function on a system dedicated of running organizational functions, such as the Human Resource management or the procurement management as these systems represent main authoritative sources for an IMS. However, an identity management system should remain independent from any other IT system in a domain as it responds to functional requirements largely different from these other management functions.

8.3.2.4 Auditing an identity management system

Control

An identity management system shall be assessed or audited on a regular basis (annually per default).

Implementation guidance

The audit or assessment should validate that the identity management system is operating in accordance with its documented policies and procedures and is compliant with legal and other externally imposed requirements, e.g. privacy requirements.

Assessments or audits should

— include statements describing the operations performed by the identity management system, in particular in respect to meeting operational policies, and

— validate that the identity management system reports on specific operations, e.g. vulnerabilities, assess if the operations meet applicable policies, e.g. privacy control, and alert on any discrepancies.

Annex A
(normative)

Practice of managing identity information in a federation of identity management systems

A.1 General

Identity federation represents an agreement between two or more domains specifying how identity information will be exchanged and managed. Federation agreements include common protocols, formats and procedures to be used across the federation covering security, privacy, governance and auditing.

Identity federations are typically established with the objective to broaden the interoperable exchange of identity information and leverage the benefits derived from it, such as expanded consumer e-Commerce and enterprise productivity and efficiency that in turn enable a growing and prosperous digital economy.

In an identity federation, other domains in the federation formally recognize an identity management system for a particular domain so that entities known in that latter domain are recognizable in the other domain and are able to access authorized resources and services there. A federation could be internal to a larger organization, e.g. a multi-division corporation, informal (for example, among friendly groups), or created as a distinct entity depending on the threat and risk vectors and the extent of controls required for managing risks. If a federation does assert trust, it should be able to accept risk, which points to the establishment of some form of legal entity.

The information asymmetry inherent in the federation structure is source of risks. How the parties trust and rely on each other's depends then on policies and other management processes that establish a trust framework, also known as a circle of trust, or chain of trust.

An identity federation establishes rules for the format and the encoding for the exchanges of identity information. An identity federation shall specify security and operational requirements, rules and mechanisms:

— to request, deliver, store, use and dispose of identity information;

— to recognize the identity information providers of participating domains;

— to assert identity information requested by a relying party in one of the federated domains;

— to protect the privacy of human entities;

— for identity proofing for enrolment in any of the federated domains;

— for the security and privacy of operating the identity management system;

— to join the federation;

— to establish levels of assurance, according to ISO/IEC 29115

  — for identity proofing for credential issuance;

  — for entity authentication within the federation.

NOTE 1 The specified requirements provide the basis for trust in the identity information exchanges.

NOTE 2 The specification may refer to a recognition process, e.g. the provision of agreed evidences, a certification process, the provision of evidences of being accredited by independent third party, bilateral or centrally organized.

NOTE 3 A federation may be formed with a commonly established requirement or by mutual recognition of these requirements as independently established by each domain or chain of trust.

A.2 Models of trusted identity federations

Identity federations come in a range of structures and sizes. A simple identity federation may have a mix of actors performing different roles, such as

— trust framework operator (in some contexts known as federation operator, FO),

— identity information authority (IIA),

— identity information provider (IIP),

— associated brokers, delivering identity attribute or credential,

— relying party (in some contexts known as a service provider, RP), and

— subject (in some contexts known as principal, subscriber or requester).

At a minimum, a federation involves two types of actor (Figure 1), the identity information provider (IIP) and the relying party (RP). An IIP manages entity identity-relevant information, and the RP offers services to entities that satisfy the policy requirements associated with these services.

Three party federation models that include a subject are the typical baseline in user-centric consumer contexts, but may be expanded to four and five party models. Many identity federations are more complex and involve more actors to reflect their objectives, such as those models described as hub-and-spoke, and federation of federations (in some contexts known as inter-federations).

A pair-wise federation is most basic federation as depicted in Figure 1.

Figure A.1 — Pair-wise federation model

A more typical federation may comprise four, five, or more parties as depicted in Figure 2.

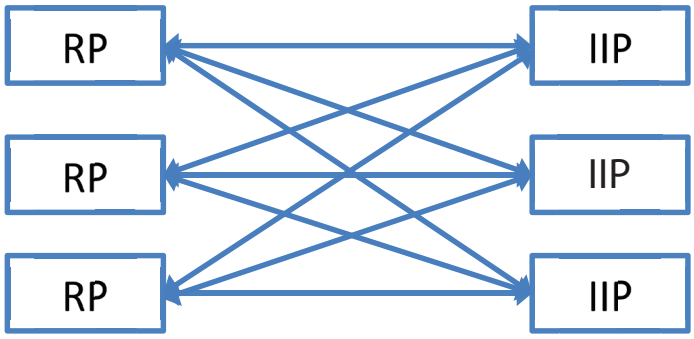

Figure A.2 — Complex federation model

Federations at this complexity and beyond begin to exhibit additional features to assist their ease of operation (such as an Identity Information Authority—IIA).

The role of federation operator is to manage the issues arising from the operation of the federation. The role may be carried out by an existing federation member or an independent third party.

In Figure 2, the user (requester) is not involved in the communication between the relying party (RP) and identity information provider (IIP). A practice more suitable for user-centric and privacy-friendly discovery processes is for the user to intermediate in the message exchange between the RP and IIP in order to be able to explicitly give consent to the release of identity information by the IIP.

The federations themselves may take on different structural forms to manage their complexity. Hub and spoke structures as depicted Figure 3 offer the benefits of a central gateway with concentrated technical expertise. The gateway is tasked to manage anonymity, un-linkability and un-observability.

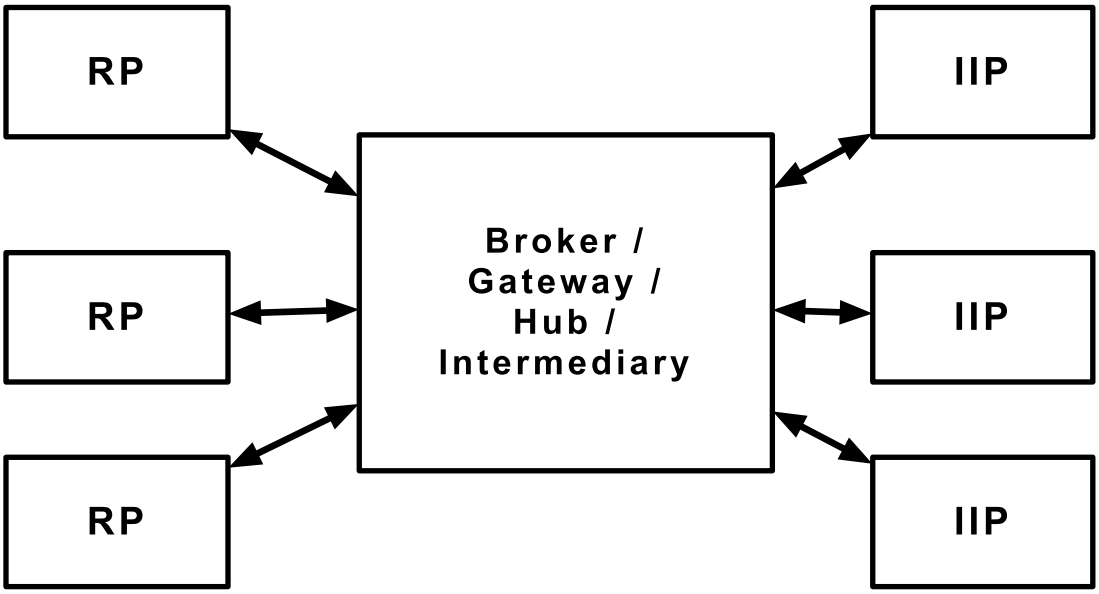

Figure A.3 — Gateway federation model

An identity federation uses a communication network. This network may be open with peer-to-peer communication between all participating identity information providers or it may use hierarchical relations where identity information is provided via one or more intermediate identity information providers.

The main actors of a federation, identity information providers (IIP) and the relying parties (RP), may establish formal trust relationships, e.g. a circle of trust. Formal trust relationships may facilitate arrangements between federation members, allowing identity information exchanges and cross-domain business transactions by entities registered in the various domains forming the federation.

A.3 Management and organizational considerations

An identity federation shall establish rules governing the establishment of policies and subsequent operational mechanisms of the trust framework to delineate the responsibilities of the parties. Management responsibilities include the following:

— maintaining and/or adjudicating the semantics and/or syntax of identity information;

— discovering and recognizing the identity information providers and other actors of participating domains;

— authenticating and asserting identity information claims by a relying party in one of the federated domains;

— protecting the security and privacy of entities, and the confidentiality, integrity and availability of the operation;

— defining and agreeing what inter-federation records may be maintained for auditing purposes, for how long, and under what circumstances they may be accessed;

— defining and agreeing standards, mechanisms, processes, technologies to transfer the identity information between federation participants;

— participating in funding and/or cost recovery models;

— joining and leaving the federation.

NOTE 1 The specified rules provide the basis for trust in the identity information.

NOTE 2 The specified rules may serve to membership compliance and accreditation, e.g. providing evidences of being audited by an independent third party, bilateral or centrally organized entity such as the federation operator.

NOTE 3 Federations may be formed when establishing specified rules or by mutual recognition of these rules as independently established by each domain, or by a combination.

Federations are structured to recognize for each subject an IIP of reference that verifies the subject's authoritative identity information in a federation for the purposes of recognition, authentication and subsequent confirmation. The IIP of reference will guarantee identity proof, register, enrol, request, deliver, store, use and dispose of identity information within an agreed identity lifecycle and scope, noting that, in the human context, identity information may exist before birth and remain after death, with similar concepts of creation and destruction applying to non-human entities.

A typical process flow may then see the subject attempt to access a resource at an RP, and the RP assembles the information at applicable assurance levels it requires, and re-directs the subject to an IIP to authenticate using a credential. Subsequent message exchange may involve the RP seeking additional attributes from the subject's attribute provider/associated broker of reference, which may be released to the RP subject to (in the case of humans) the subject's consent, after which the subject is given access to the requested resource.

The merge of identity information from different authorities in two distinct domains is a typical requirement when two organizations are merging in a federation. In these use cases, procedures shall be specified to resolve collisions and inconsistencies such that within the resulting domain,

— reference identifiers are unique,

— where applicable pseudonyms are used, and

— it is not possible to associate an identity with the wrong entity.

Means should exist for arbitration between authorities of identity providers that contain conflicting identity information.

A.4 Discovery

A.4.1 IIP General

The technique of discovery may be used to exchange required identity information within a federation; it enables locating parties in the federation quickly and dynamically. This is particularly useful in large federations where there is membership churn. Federations and the trust frameworks that underpin them may operate listing services to further enhance discovery and interoperability.

Guidance on Discovery organization is required. Depending on contextual and cross-contextual rules the mechanisms for discovery are enforced in different ways. This feature is an intrinsic part of trusted

identity federation and its development has been motivated by the increasingly complex requirements of trust frameworks.

The most common targets for discovery are typically identity information providers. The discovery process is the capability provided by the IIPs and IIA in a federation, with the user/subject/requester's consent or by a legislative/regulatory requirement, to dynamically locate an identity information authority for a particular entity to provide a particular required attribute where

— identity information does not exist,

— the RP lacks the level of confidence in the information sufficient to mitigate the subject's identity related risk for the service being accessed, or

— the RP does not indicate which IIP to use.

Discovery throughout the federation may be achieved using static methods, such as white lists, or reference to listing services. Listing services expose the existence of a range of identity services, typically Trust Frameworks, the Federation Operators involved in managing them, participating entities in the federation, and their certification status. The listing service function may be augmented by the use of dynamic methods of discovery, such as the publication and consumption of metadata of the services. Dynamic discovery helps the efficient operation of modern federations which typically see an ebb and flow of parties joining and leaving the federation.

Benefits of discovery include relying parties being relieved of the burden to cache or retain identity information, as long as the requirements or obligations of the relying party do not necessitate data retention, thereby substantially reducing the liability of handling PII, and the freshness and accuracy of the data. Discovery mechanisms also facilitate dynamic registration and de-registration of federation relationships. Dynamic discovery may support "bring your own identity" and personal (device or cloud) data store use cases depending on the particular approach taken to enable it.

As for any other element of an identity management system, applicable requirements, e.g. law, regulation, or policy, may limit the discovery activities. Identity providers and relying parties should be able to support mechanisms for discovering other identity providers in a federation.

A.4.2 IIP Discovery

IIP Discovery is the process of finding in the federation an IIP to provide identity information for an entity. This process may be

— a user providing a reference to the IIP, e.g. by selecting from a presented list of options,

— a user providing a hint, e.g. an email address that contains a reference to the IIP, and

— a user providing an identifier that is broadcasted to all IIPs, with the one knowing the identifier responding.

It could be the process in which the user selects the IIP from the list of providers or the automatic discovery of the IIP from the user agreeing to provide information such as username or email address.

A.4.3 IIA Discovery

IIA Discovery is the process of finding in the federation an IIA that is suitable for authenticating information for a particular IIP. The discovery process may use a capability provided by an IIP in the federation to dynamically locate an identity information authority for a particular entity to provide a particular required attribute where available identity information does not indicate which IIA to use.

As for any other element of an identity management system, applicable requirements, e.g. law, regulation or policy, may limit the discovery activities. Identity information providers and relying parties should be able to support mechanisms for discovering other identity information providers in a federation.

NOTE 1 A benefit of discovery capabilities in an identity management system is that relying parties are not required to cache or retain identity information, as long as the requirements or obligations of the relying party do not necessitate data retention. The resultant benefits to a relying party include the substantial reduction in the liability of handling PII and the freshness and accuracy of the data.

NOTE 2 A discovery mechanism facilitates dynamic registration and de-registration of federation relationships.

Figure 4 is an example of a basic discovery dialogue in an enterprise context. Precise protocol flows may vary to some extent depending on the federation's objectives and context and should include additional user directed information release consent steps to satisfy privacy requirements and support trust. It also demonstrates the fulfilment of the need to support multiple sources of identity information.

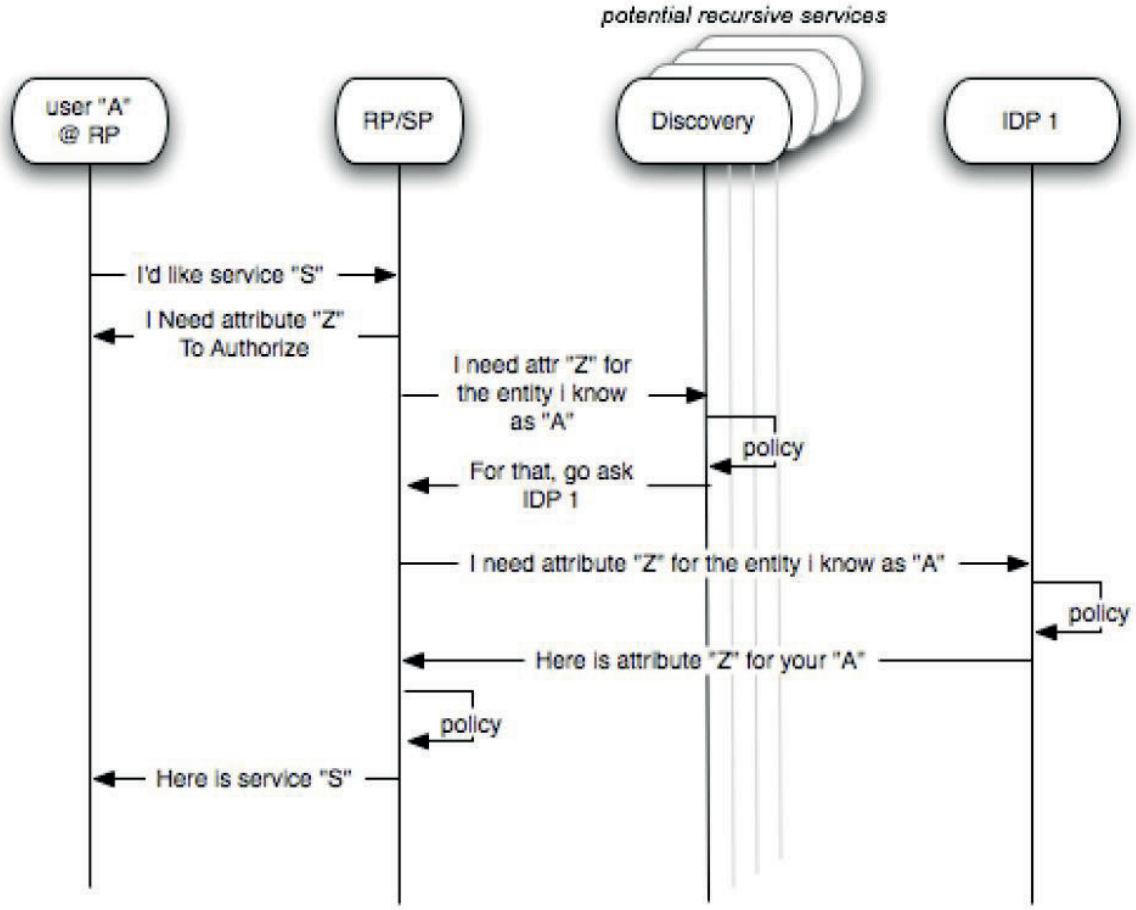

Figure A.4 — Federation basic discovery dialogue example

NOTE Identity discovery process (IDP), for example, is an IIP.

A.5 Considerations in inter-federation scenarios

A.2 specifies inter-federations. In addition to considerations applicable to a federation, further considerations for inter-federation fall into two categories: *trust* and *interoperability*. Where an entity with an identity in one federation may need, or want, to access services provided by another federation, an inter-federation agreement should be reached, such that at least one IIP in the first

federation has a trust relationship with the appropriate IIP in the other federation. Interoperability between heterogeneous federations (each may use different federation software, different platforms, or different deployment profiles) requires strong adherence to agreed fixed policies and procedures to avoid identity and identifier duplication and ultimate collision.

When developing agreed procedures for inter-federation, the following requirements should be considered:

— compare policies and procedures of the participating federations to ensure they are consistent and there is no gap;

— compare terms of service and license agreements to ensure they are consistent and there is no issue;

— mechanisms for access control to information for individuals, based on their identity in one federation or another, shall be explicitly defined, and should be exposed and reside in the home federation;

— defined controls to prevent identity theft while roaming between federations;

— defined rules on the use of privacy enhancing techniques, such as anonymity or pseudonymity and consent when identity information is exchanged in the federation;

— defined controls to meet applicable requirements expectations, e.g. law, regulation, policy, from the various federations, particularly in pan jurisdiction contexts;

— compare law, regulation, and policy, from the various federations (particularly in pan jurisdiction contexts) of the participating federations to ensure they are consistent.

A.6 Threats and controls

A.6.1 General

An identity federation faces a range of threats and risks that arise from the information asymmetry amongst the different parties with regard to the considerations, characteristics and requirements above. The range of threats applies, to a great or lesser extent, depending on the context (for example, enterprise or user-centric consumer). Phases in the identity lifecycle applying to users of the federation, such as identity proofing, enrolment, provisioning, authentication and authorization, along with processes involved with the operation of the federation itself, such as on-boarding the participants in the federation, all carry inherent threats that require controls to mitigate and manage those risks. Identity related threats and controls are described in ISO 24760-1 and ISO 24760-2, along with ISO/IEC 29115, and for privacy threats and controls in ISO/IEC 29100, ISO/IEC 29101 and ISO/IEC 27018. This part of ISO 24760 does not repeat those but describes the most common threats and controls as they relate to identity federation.

Typical identity authentication and authorization threats and their respective controls should be considered as shown below.

A.6.2 Requesting authenticated identity

A.6.2.1 General

When a user requests access to a resource provided by the ICT application system, the ICT application system requests authenticated identity that holds the attributes it requires making decisions as to the access authorization is concerned. It may also request the additional attributes that are needed for the business process in addition.

The following threats and controls should be considered.

A.6.2.2 Unauthorized request

It is also known as request forgery. An attacker masquerading as an authorised user of the ICT application fabricates a request for identity information.

The following controls apply:

— the request should be signed by the requester;

— request disclosure.

Request may contain sensitive information, thereby disclosing it making a security and privacy risk. In particular, the disclosure of the credential would cause a grave security risk to the entire system.

The following controls apply:

— audience of the request should be restricted through the authentication of the destination;

— the request should be encrypted or transmitted through a protected channel.

A.6.2.3 Request tampering

In this threat, the attacker modifies a request for identity information.

Following control applies, the request should be integrity protected either by having the request signed or message authenticated or by transmitting it through a protected channel.

A.6.2.4 Request substitution

In this attack, the request is substituted with other request. Cross-site request forgery (CSRF) is a typical example of such threat.

Following control applies, the request should be cryptographically bound to the session between the user agent and the requester, user agent and IIP.

A.6.3 Authorizing the release of attributes

A.6.3.1 General

Authorization of the release of attribute may be decided by the subject or by the policy set by the administrator of the domain. The following threats and controls apply.

A.6.3.2 Policy injection

The attacker may inject the policy to the policy engine through policy administration point.

The following controls apply:

— if an entity is pushing a policy, the entity should be authenticated and policy should be cryptographically bound to the entity;

— the policy being pushed into should be authenticated (tamper proofed/signed);

— SQL injection and other application vulnerability should be closed.

A.6.3.3 Access interface hijacking

The attacker hijacks the access interface of a system and manages to release attributes. Typical example of such attack is click jacking.

A.6.3.4 Term obfuscation

The attacker hides the attributes that is being requested, their purpose, and their distribution range by including them in a long agreement.

Following control applies, the federation operator or other entity should certify that the request conforms to the requirements set by the federation.

A.6.4 Obtaining auxiliary attributes

For the purpose of the authorization decision and other business processing, the ICT resource may require additional attributes. They may be obtained from IIP or IIA.

All the threats and controls previously mentioned apply. In addition, the following controls apply

A.6.4.1 IIA location control

An attribute may be available from multiple IIA. Attribute value may be different among them, and what is correct may be determined by context.

Following control applies, the location of the IIA for the context should be obtained through the IIP in the context of the original request of source of attributes for a control.

A.6.4.2 Resource registration

Required attributes may contain confidential information. The resource requesting the identity information may compromise this confidentiality. The resource may be required to fulfil conditions for obtaining the required information.

Following control applies, registration of the resource requesting additional attributes should be obtained before the source of attributes for a control may be obtained.

A.7 Merging identity information authorities

The merge of identity information of different authorities is sometimes required. This typically happens when two organizations are merging in a federated organization. But before merging identity management systems of two distinct domains, procedures shall be specified to resolve inconsistencies and, in particular, ensure that within the resulting domain,

— reference identifiers are unique, and

— it is not possible to associate an identity with the wrong entity.

Means should exist for arbitration between authorities of identity information providers that contain conflicting identity information.

Annex B
(normative)

Identity management practice using attribute-based credentials to enhance privacy protection

B.1 General

An identity management system may be built using attribute-based credentials.

Attribute-based credentials are a user-centric approach for an identity management system to enhance privacy protection of the user, while also respecting the multilateral interests of all the entities.[11]

B.2 Actors

B.2.1 Overview

An attribute based identity management system recognizes the following main actors:

— principal, which carries one or more credentials that may be used to claim that certain attributes are applicable when presented to a relying party;

— relying party, which accepts proofs from the credentials of the principal, and trusts the authority that has issued the credential (the identity information provider);

— identity information provider, which issues attribute-based credential(s) to the Principal, vouching for the correctness of the information contained;

— identity information authority, which is responsible for maintaining the level of assurance in identity information made available to a relying party.

Figure B.1 shows an overview of actors in this architecture of an identity management system.

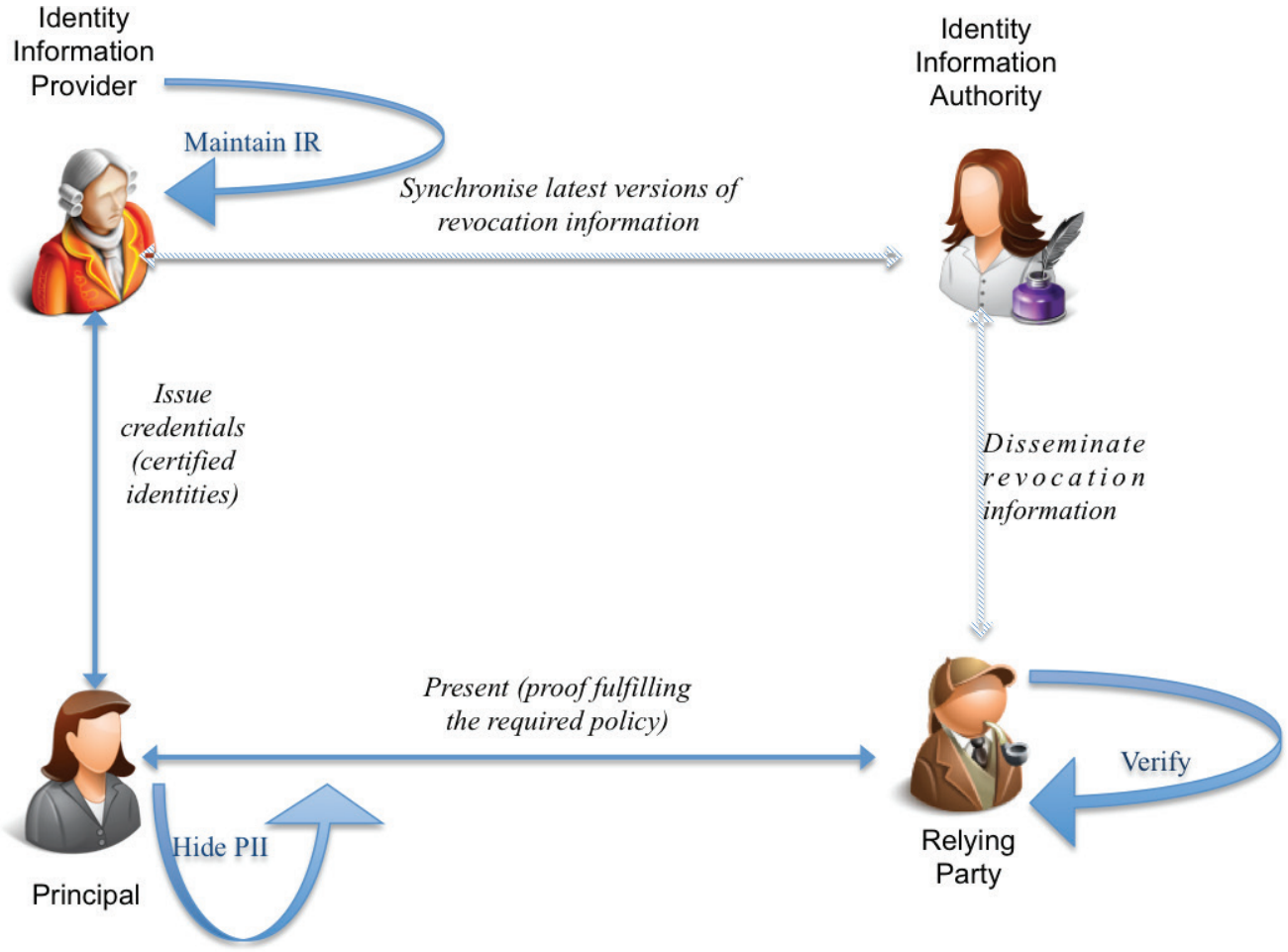

Figure B.1 — Actors of an attribute-based credential architecture and their interactions

B.2.2 Principal

A principal is the central actor in the architecture, whose interests are

— using services offered by the relying party,

— to remain anonymous when using services of a relying party,

— to have the possibility to remain un-linkable for different communications with the relying party (avoid profiling),

— to avoid linkage of the use of his or her identity information with a relying party with the issuance of the attributes from the identity information authority, and

— to be able to create pseudonyms, whenever he or she likes to create a profile with a certain relying party.

The principal operates an IT device, referred to in this annex as "principal's token," that contains the credentials and is able to communicate with equipment operated by a relying party.[11]

B.2.3 Relying party

A relying party is a service provider, which provides services to principals. In doing so, the interest of the relying party is to be able to provide the services to authenticated principals only. The relying party publishes a presentation policy, which specifies the conditions the principals are required to fulfil for authentication in order to use its services.

The relying party has an established relation with the identity information authority, whose certification it accepts.

The interests of the relying party are

— the accepted identity information should be verifiably correct,

— that only the identity information authority is able to issue/manipulate certified identity information about principals,

— it needs to be assured that the principal cannot manipulate the certified attribute values of the principal, and

— be synchronized with the identity information authority about the latest version of the identity register in order to check credentials received and to prohibit any invalidated (revoked) credentials from being accepted as valid.

B.2.4 Identity information provider

An identity information provider is a system component to provide principals with certified identity information to be presented as needed by the principal.

The identity information provider vouches for the correctness and validity of provided information.

This actor is the one who is able to

— issue credentials for one or more attributes to the principal, and

— determine that previously provided identity information of an identity is no longer valid.

A credential of which the contained identity information is no longer valid is revoked.

B.2.5 Identity information authority

The task of the identity information authority is to

— pro-actively provide relying parties information on credentials that have been revoked consisting of

  — synchronizing the latest revocation (invalidation) information with the identity information provider,

  — synchronizing the versions of the identity register,

  — disseminating the latest Identity Register version to the relying parties,

— upon request of a relying party assist in validation of a credential, and

— provide information to be included in a credential to enable its validation.

B.3 Control steps

B.3.1 General

An attribute based identity management system recognizes the following main control steps:

— the credential issuance, pertaining of providing the principal with the adequate attributes;

— the presentation, when the principal requires interaction with the system;

— the invalidation, when the principal has attributes being revoked.

B.3.2 Credential issuance

Credential issuance is an interactive protocol between the principal's token and an identity information provider. As result of credential issuance, a principal is in possession of one or more attribute credentials, each representing identity information pertaining to the principal.

An attribute credential consists of the following information:

— a description of the attribute type;

— an encoded representation of the attribute value;

— parameters for the cryptographic process of validating the identity information;

— a specification of the identity information authority that asserts the validity of the credential.

B.3.3 Presentation

Figure B.2 shows the system components and their interaction involved in "*presentation*." Presentation is a process of communication between a principal's token and relying party equipment performed when the principal requires access to a service offered by the relying party.

Presentation starts when the principal's token receives from the relying party the information describing its presentation policy. A presentation policy defines the following:

— information to be provided to the relying party including

  — the type of attribute,

  — the level of disclosure of the attribute value;

— authentication mechanisms to be used to validate the attribute value;

— identity information authorities, that are accepted by the relying party as providing security in validation.

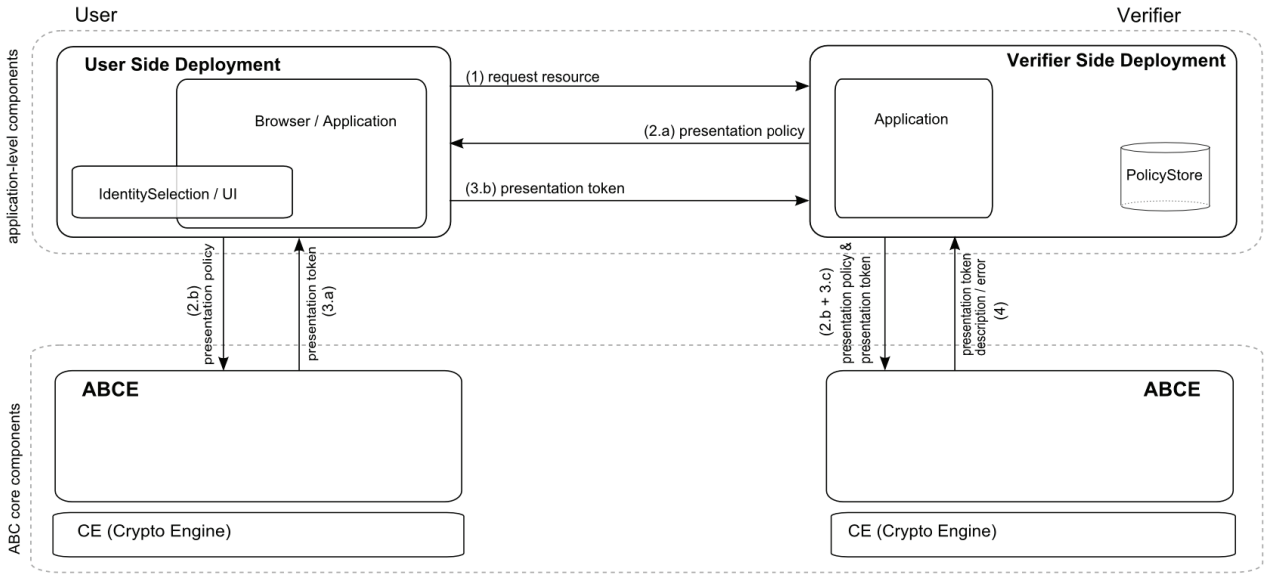

Figure B.2 — Main components of a principal's token and relying party equipment

On the principal's token, a process determines which combinations of the credentials in its memory will meet the policy of the relying party, in which the interaction of the principal may be required (in case different combinations are possible, e.g. if the principal uses different credentials from different identity information providers). The principal then sends the completed claim to the relying party.

Upon receiving the presentation token, the relying party verifies the claims in it as valid (authentic from one of the trusted identity information providers it trusts), but also whether they are still valid. The final outcome of the verification is an "accept" or "reject", depending on the validity of the presentation token.

B.3.4 Invalidation

It is the responsibility of the system using the identity management system to define the cases when certain credentials need to be invalidated (revoked). This is typically when certain relations of the principal with the issued credentials (certified identity information) do not hold, such as cases of violation of terms of use by the Principal, termination of the legal contract between the principal and the identity information provider, etc.

In any case, invalidation is an important process in the lifecycle of the identity management using privacy-enhancing attribute based credentials. When an attribute is invalidated, the credential containing that attribute is also invalid. In the architecture process above, this would be an update of the Identity Register by the identity information provider, thereby ending the validity of the previously issued credential. This update then will be synchronized with the Identity Information Authority.

B.4 Architecture layers and components

B.4.1 General

Entities in an identity management system based on attribute-based credentials may have distinct functional components required for their interaction with the system. The architecture for an identity management system based on attribute-based credentials specifies for each entity the functional components required to operate with attribute-based credentials. Figure B.2 shows an overview of the functional components for the principal's and relying party's side, whereas a more detailed presentation of the components on the principal's side is shown in Figure B.3. The functional components of each party may be presented in two main layers:

— application deployment layer;

— core components—proof generation/verification layer.

B.4.2 Application deployment layer

The application layer is not part of the Privacy-ABC architecture, but will operate on top of that. Roughly, this layer comprises all application-level components, which in the case of the User-side (Principal) deployment includes the main application and the Identity Selection (see description below). The application layer of Verifiers and Issuers will also contain the policy store and access control engine.

The Identity Selection component provides methods, possibly presented by a graphical user interface, to support a User in choosing a preferred combination of credential and/or pseudonyms, if there are different possibilities to satisfy a given presentation policy. A user interface is also used to obtain User consent, whenever personal data is revealed.

B.4.3 Core components — proof generation/verification layer

B.4.3.1 General

The proof layer contains the attribute-based credential engine (ABCE) and the underlying technology specific components, as depicted in Figure B.3.

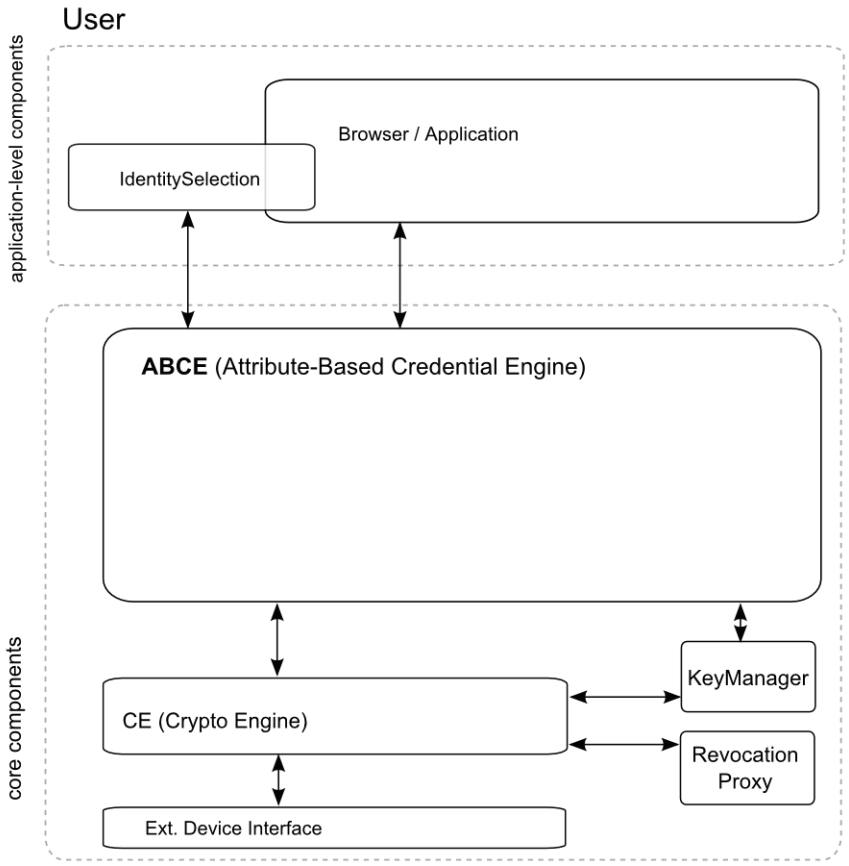

Figure B.3 — Architecture of principal's token

The ABCE contains all technology-agnostic methods and functional components for an identity management system based on attribute-based credentials. It contains functions to parse an obtained presentation policy, perform the selection of applicable credentials for a given policy or to trigger the mechanism-specific generation or verification of the cryptographic evidence. The upper (deployment) layer then communicates with the same layer on the other entity (relying party or identity information provider) side.

The ABCE is invoked by the application-layer and calls out the other components, as shown in Figure B.3:

— Crypto Engine;

— Key Manager;

— Revocation Proxy;

— Policy Store;

— External Device Interface.

B.4.3.2 Crypto Engine

Crypto Engine is the first component to be called by the ABCE the mechanism-specific cryptographic data. It provides common interfaces to generate the cryptographic information required, e.g. to create, present, verify, or inspect a presentation/issuance token. It internally orchestrates and performs the mechanism-specific cryptographic methods, such as the computation of signatures, e.g. U-Prove signature, commitments, zero-knowledge proofs, etc.

B.4.3.3 Key Manager

The Key Manager deals with the (cryptographic) keys of all parties and keeps them up to date (key life cycle management). On input of an identifier (URI) for a key, it returns a (list of) cryptographic key(s) that are currently valid for that URI. This component also takes care of fetching the current (public) revocation information that will be needed to keep the credentials up to date or to verify whether a received presentation token is still valid.

B.4.3.4 Revocation Proxy

The Revocation Proxy handles the communication between the Crypto Engine and the Revocation Authority for the generation or presentation of tokens/credentials that are subject to revocation (invalidation). The concrete communication pattern strongly depends on the specific revocation mechanisms, which may be chosen.

B.4.3.5 Device Interface

The Device Interface components provide optional generic interfaces to ease the integration of external devices, such as smart cards, for both the “outsourcing” of computation and also to obtain data stored externally on the device. The integration of an external device might for instance be necessary, if key binding to a smart card is required.

B.4.3.6 Policy Store

On the side of the relying party, the Policy Store stores the presentation policies accepted by the entity and may also save the received presentation tokens for archiving or other security-related purposes (see Figure B.3).

Bibliography

[1] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[2] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[3] ISO/IEC 29003, *Information technology — Security techniques — Identity proofing*

[4] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[5] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[6] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*

[7] ISO/IEC 29134, *Information technology — Security techniques — Privacy impact assessment – Guidelines*

[8] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*

[9] ISO/IEC 29151, *Information technology — Security techniques — Code of practice for personally identifiable information protection*

[11] Jan Camenisch, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin, and Harald Zwingelberg. "*D2.1 Architecture for Attribute-based Credential Technologies*," 2011 https://abc4trust.eu/index.php/pub/107-d21architecturev1 (accessed 2014-01-02)

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than one device provided that it is accessible by the sole named user only and that only one copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than one copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright and Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member.**

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email cservices@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email: cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK