

BS 8626:2020



BSI Standards Publication

**Design and operation of online
user identification systems —
Code of practice**

bsi.

AVA Documents
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2020

Published by BSI Standards Limited 2020

ISBN 978 0 539 01297 2

ICS 35.240.01; 35.030

The following BSI references relate to the work on this document:

Committee reference IST/33/5

Draft for comment 20/30379129 DC

Amendments/corrigenda issued since publication

Date	Text affected

Contents

	Page
Foreword	iii
Introduction	1
1 Scope	2
<i>Figure 1 — Generic model of user identification</i>	4
2 Normative references	5
3 Terms, definitions and abbreviations	5
4 Establishing or enhancing an OUIS	15
4.1 Strategic factors	15
<i>Figure 2 — Establishing an OUIS</i>	16
4.2 Requirements for an OUIS	21
4.3 Design and implementation of an OUIS	31
4.4 Operational management of an OUIS	32
5 Design for life cycle management of user digital identities	34
<i>Figure 3 — Digital identity life cycle</i>	35
5.1 Digital identity creation	35
5.2 Digital identity and credential usage	41
5.3 Digital identity and credential maintenance	41
5.4 Digital identity termination	42
5.5 Digital identity system management	42
6 Knowledge-based user authentication methods	43
6.1 Recovery from failure in knowledge-based user authentication	43
6.2 Creation, maintenance and recovery of authentication data	43
6.3 Personal identification number (PIN)	46
6.4 Passwords and passphrases	46
6.5 Partial PINs	48
6.6 Security questions	49
7 Possession-based user authentication methods	50
7.1 Recovery from failure in possession-based methods	50
7.2 General	51
7.3 One-time password (OTP)	52
7.4 Disconnected hardware security token (OTT) method	53
7.5 Software secret one-time token (OTT) method	53
7.6 Connected hardware security token (OTT) method	55
8 Inherence-based (biometric) user recognition methods	56
8.1 Recovery from failure in inherence-based recognition methods	56
8.2 Structured approach	56
8.3 Mitigation measures for biometric recognition systems	56
8.4 Using biometric recognition as a component of the identity proofing process	56
8.5 Biometric enrolment and registration	58
8.6 Biometric verification method	61
8.7 Privacy and data protection	64
8.8 Health and safety	64
8.9 Biometric information security	65
8.10 Biometric performance maintenance	67
9 Confirmatory evidence and contra-indicators	68
9.1 Confirmatory evidence	69
9.2 Contra-indicators	71
<i>Table 1 — Contra-indicators</i>	72

10	OUIS management	73
10.1	Establishing an service level agreement (SLA) between the IdP(s) and the RP(s)	73
10.2	Operational responsibilities and procedures	74
10.3	Life cycle management of the OUIS	74
10.4	Day-to-day system operation	79
Annex A	(informative) User identification assurance	85
	<i>Table A.1 — Levels of identity proofing assurance</i>	86
	<i>Table A.2 — Levels of user identification assurance</i>	87
	<i>Table A.3 — Selecting the appropriate level of user identification assurance</i>	88
Annex B	(informative) Supplementary information on biometrics	89
	<i>Figure B.1 — Components of a general biometric system [Source: PD ISO/IEC TR 24741:2018]</i>	89
	<i>Table B.1 — Decision error outcomes for biometric functions</i>	94
	<i>Table B.2 — Suggested FAR values for user identification assurance levels</i>	94
	<i>Figure B.2 — Examples of points of attack in a biometric system [Source: BS ISO/IEC 30107-1:2016]</i>	97
Annex C	(informative) Risks for biometric recognition methods	102
Annex D	(informative) Behavioural biometrics	103
	Bibliography	108

Summary of pages

This document comprises a front cover, and inside front cover, pages i to iv, pages 1 to 115, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 December 2020. It was prepared by Subcommittee IST/33/5, *Security techniques — Identity management and privacy technologies*, under the authority of Technical Committee IST/33, *Information security, cybersecurity and privacy protection*. A list of organizations represented on these committees can be obtained on request to the committee manager.

Relationship with other publications

[PAS 499:2019](#), *Code of practice for digital identification and strong customer authentication*, covers the management operations for identification and strong customer authentication, as required in the Second Payment Services Directive (PSD2) [1] and related regulations. BS 8626 provides recommendations to digital identity providers, including relying parties, covering the establishment of requirements for online user identification systems and their design and management operations.

The recommendations contained in [PAS 499:2019](#) will be reviewed and incorporated into the next edition of BS 8626.

While the ISO/IEC 24760 series specifies concepts and operational structures of identity management for entities in general, BS 8626 concentrates on the processes for managing digital identities for the sole purpose of online user identification. BS 8626 also provides recommendations on the use of knowledge-based and possession-based authentication methods and, additionally, biometric recognition methods for user identification, together with recommendations for managing the effectiveness and efficiency of deployments.

Information about this document

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at bsigroup.com/standards, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

The word “should” is used to express recommendations of this standard. The word “may” is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word “can” is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

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

Introduction

This British Standard uses the term “identification” in a general sense for the online recognition of individuals, as authorized users, by digital identity providers (IdPs) working with relying parties (RPs) that supply online services. In many cases the RP and the IdP are part of the same legal entity, although the operation of the online user identification system (OUIS) can be managed by a different department within that organization or by an entirely separate entity. This standard also uses and defines terms, such as identity proofing, authentication, verification, recognition and biometric identification, as specific types of identification processes.

Society and organizations are increasingly dependent on online information systems providing services which on access to restricted resources, such as sensitive data and controlled functions. These services, operating in diverse contexts, are provided by a range of entities, which include governmental, educational, commercial and charitable RPs. The services available today are pervasive, providing, for example, functionalities to users to manage personal tax information, accountants to send corporate tax communications, college administrators to distribute student course materials, consumers to purchase goods and services, customers to conduct online banking activities, customers to reserve hotel accommodation, and citizens to submit donations to charities.

Organizations providing user identification services need to ensure that access to these restricted resources is provided to the relevant authorized users, such as citizens, customers, consumers or employees, in an effective and efficient manner. Key to delivering this requirement is selecting the optimal access control systems so that the stakeholder benefits, including rewards to the intended user community, are realized and that the concomitant risks are managed by these parties in an informed, transparent and equitable manner. To meet these challenges, organizations need to balance complementary and conflicting stakeholder objectives; consider interrelated factors, such as cost containment, productivity impact, usability, accessibility, sustainability and performance; and evaluate user identification assurance.

To manage risks, RPs employ online user authentication methods and/or biometric recognition methods utilizing one or more types of user identification data and modes of operation to identify a user to a predetermined level of assurance. An RP can specify and manage the user identification processes for its own customers, e.g. banks, which utilize its services. RPs assess and manage risks directly. Alternatively, an RP may utilize a third-party digital identity provider (IdP) to manage its user identification processes. In this federated model, the IdP specifies the technical and process requirements and manages the user identification processes with any RPs, as part of its access control procedures for the RPs' online services. In these circumstances for the relevant application context, IdPs and possibly other organizations provide an input into an RP's assessment and management of risk. Multiple authentication methods and/or biometric recognition methods can be deployed for user identification, either to be used together to strengthen the assurance in determining the identity of the user to access the RP's service, or as user identification alternatives, if significant numbers of users are unable to use an authentication method and/or biometric recognition method in a reliable manner.

All user identification systems incur costs, both direct and indirect, possess technical and procedural vulnerabilities, and potentially attract deleterious intractable issues. Organizations face complex challenges in ascertaining their optimal user identification system and managing it for their applications in an online operating environment with ever-increasing threats, competition and regulation. This British Standard gives recommendations and guidance for resolving these challenges.

The recommendations in this standard are intended for organizations seeking to introduce an OUIS as part of the design for a new application service or a revision to an operational deployment.

The standard commences with recommendations for selecting or enhancing current user identification systems and then gives recommendations for the three main types of user identification system, knowledge-based authentication, possession-based authentication and biometric recognition methods. A clause on contra-indicators sets out the recommendations for using additional data to support the methods deployed in order to acquire confirmatory evidence or identify the possible compromise of user identification. The recommendations in [Clause 5](#) on digital identity life cycle management are then applicable based upon the types of methods deployed. The final clauses give general recommendations for managing user identification systems and supporting digital identity management systems (IdMS).

1 Scope

This British Standard gives recommendations and supporting guidance for the design and operation of an online user identification system (OUI) and the corresponding user digital identity management systems (IdMS). As authorized users, individuals can act in a personal capacity (e.g. consumer, customer or citizen) or on behalf of another individual (e.g. as a proxy) in a role in a digital identity provider (IdP) and/or relying party (RP), e.g. employee or authorized contractor. In particular, recommendations are given for:

- a) establishing or revising an OUI, including:
 - 1) business objectives and requirements for an OUI;
 - 2) requirements for protecting the life cycle management of digital identities associated with individuals;
 - 3) requirements for protecting data used specifically for identifying or authenticating individuals;
 - 4) requirements for protecting against attacks on specific types of user knowledge-based authentication methods, possession-based authentication methods and biometric recognition methods and modes of operation;
- b) the controls for managing the life cycle of users' digital identities for an OUI, including:
 - 1) creation, proofing and issuance of a digital identity and the formation of the digital identity's associated credential;
 - 2) identification together with credential usage (where applicable);
 - 3) activities to update credentials and associated data, and notification of these changes to the user;
 - 4) revocation, expiration, reinstatement, disqualification or user cancellation of a digital identity's credential and purging or archiving of digital identities; and
- c) evaluating the effectiveness of an OUI, including the management of user identification errors, such as false positives and false negatives, and efficiency, including the user identification transaction timings and demand on resources.

This British Standard:

- i) describes various knowledge-based authentication methods, possession-based authentication methods and biometric recognition methods, together with their inherent vulnerabilities;
- ii) provides recommended measures to mitigate the potential exploitation of these identified vulnerabilities; and

- iii) assists in the development of a risk mitigation strategy, though it does not cover risk identification, protection, detection, response and recovery, as part of developing a supporting performance management strategy and plan.

The standard is applicable where the user initiates the process of user identification for an online service supplied by an RP and the processes of user identification to access an IdP's IdMS (if applicable).

This standard covers the management of digital identities by organizations, including IdPs, and individuals' management of the credentials allocated to them by an IdP and/or RP. It concentrates on the OUIS component of access control mechanisms. However, reference is made to the permission management associated with roles and authorization functions of associated policy decision points in decision authorization systems.

This standard is applicable to online authentication transactions that are associated with either online or offline identity proofing processes, but its recommendations might also be useful for the design of offline authentication transactions, though their applicability in these contexts requires careful consideration.

The scope of the transaction commences with the authentication/recognition request from an authorization system or access control mechanism through to the return response by the authentication/recognition subsystem, as illustrated in [Figure 1](#). The authentication/recognition subsystem includes capture of signals from an individual through an input device, e.g. keyboard or sensing apparatus (e.g. camera), through to a decision component, which determines whether the identification data presented are sufficient to authenticate or recognize an individual within predetermined user identification assurance parameters.

This standard covers the situations where the authentication and/or recognition decision engine resides either on the user's intelligent device or in a remote information system.

This standard covers "man-in-the-middle" (MITM) attacks on authentication methods and biometric recognition methods only. It does not cover MITM authentication attacks or similar substitution attacks on networks, computer operating systems, computer programs, applications, router and/or certificate repositories. The vulnerabilities and associated mitigation controls relating to these technologies are outside the scope of this standard.

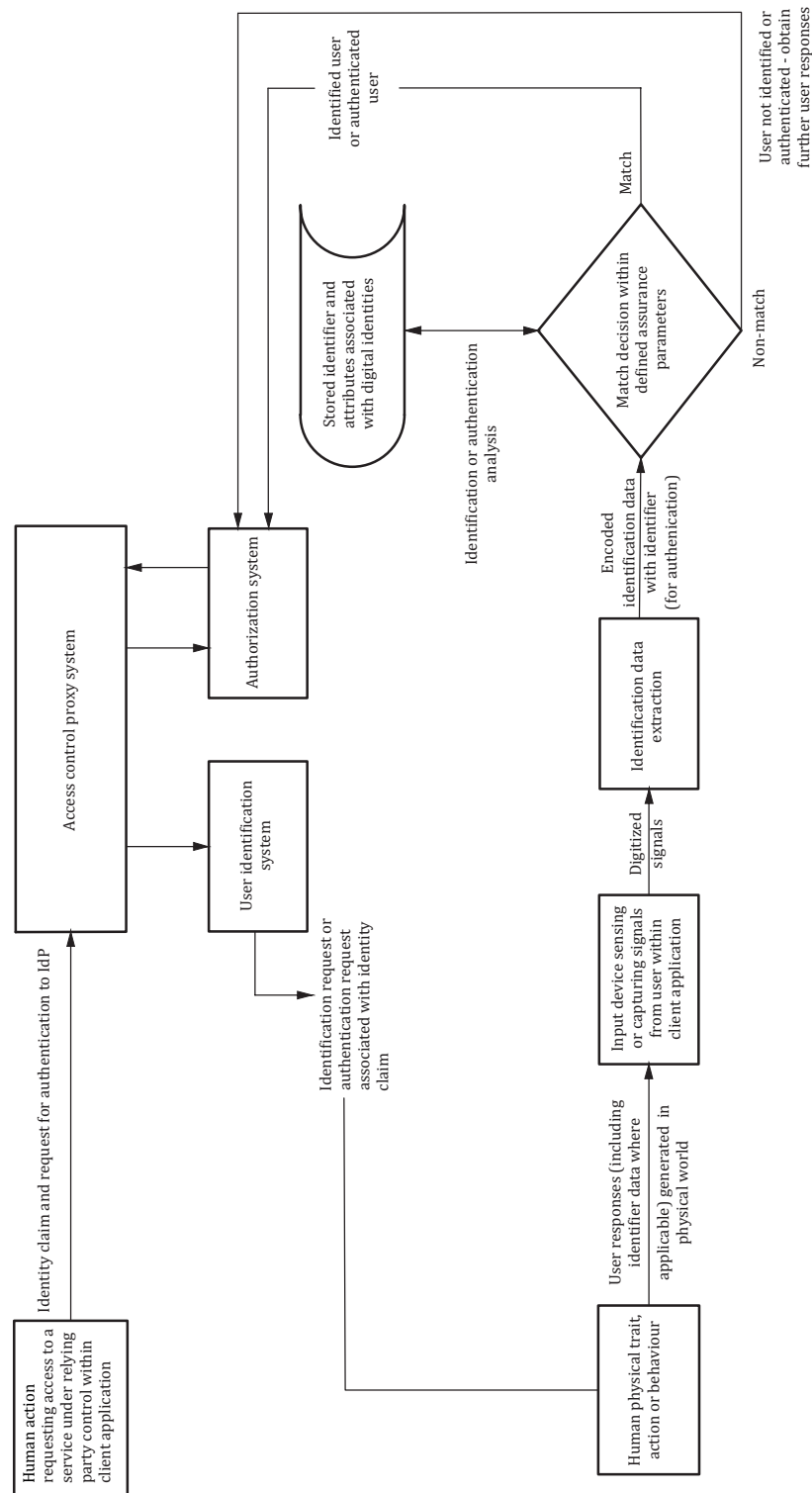
This standard does not cover security controls in networks, computers, operating systems, application software and supporting utilities or input devices.

This standard is not applicable to device identification, though, in most digital interactions, the user needs to bind their digital identity or their credential to the device, so that the device can be trusted by the network and/or IdP or RP. The exclusion of device identification applies equally to a user's device and the user's application authentication of a remote information system (e.g. web server gated cryptography hosting the RP's application or resource).

NOTE An example of the use of device identification is the binding of a user to their mobile phone's international mobile equipment identifier (IMEI) or to the subscriber identity module (SIM) or international mobile subscriber identity (IMSI), to prevent an attacker replacing the SIM in a stolen mobile phone and impersonating the genuine user.

This standard does not give specific recommendations for:

- single sign-on systems;
- digital identity federation schemes;
- password application managers and password generation software; and
- attributes sharing between organizations in a contractual relationship.

Figure 1 — Generic model of user identification

The de-identification of data relating to a digital identity is outside the scope of this standard, but guidance on this is given in [BS ISO/IEC 20889](#).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions of this document¹⁾. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[BS EN ISO/IEC 27001](#), *Information technology – Security techniques – Information security management systems – Requirements*

[BS EN ISO/IEC 27002](#), *Information technology – Security techniques – Code of practice for information security controls*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1.1 access control

granting or denying an operation to be performed on an information asset or online service

NOTE 1 A primary purpose of access control is to prevent unauthorized access to information or use of information communications technology (ICT) resources based on the business and security requirements; that is, the application of authorization policies to particular access requests.

NOTE 2 When an identified user makes a request, the resource owner will authorize (or not) access in accordance with access policy and user privileges.

[SOURCE: BS ISO/IEC 29146:2016, 3.1, modified]

3.1.2 applicant

individual undergoing the processes of registration, enrolment and identity proofing prior to becoming an authorized user

3.1.3 application (app)

computer program running on an individual's device

NOTE Examples of devices are a laptop and a mobile phone.

3.1.4 assertion

statement made by an entity without accompanying evidence of its validity

[SOURCE: BS ISO/IEC 29115:2013, 3.1]

3.1.5 assurance

degree of confidence that the user of a security credential is the same person to whom it was issued following the successful identity proofing and identity verification process

3.1.6 asymmetric keys

two related keys, consisting of a public key and a private key, that are used to perform complementary cryptographic operations, i.e. encryption and decryption

¹⁾ Documents that are referred to solely in an informative manner are listed in the Bibliography.

3.1.7 attack

attempt by an attacker to deceive an IdP or an RP into accepting that the attacker is the authorized user

3.1.8 attacker

unauthorized person or party who acts with malicious intent to infiltrate an information system through compromising the information system's access control mechanisms

3.1.9 attribute

characteristic or property used to describe and to control access to an information asset or online service

[SOURCE: BS ISO/IEC 29146:2016, 3.4, modified]

3.1.10 authentication assurance

degree of confidence reached in the authentication process that the person is who they claim to be

3.1.11 authentication data

data for the processes of authenticating a user

3.1.12 authentication method

process of determining the validity of one or more credentials used by a person to claim ownership of a specific digital identity, as identified by a unique system identifier

NOTE A user possesses knowledge and/or controls a device (for example, a password and/or a cryptographic module) which produces authentication data that are compared exactly by an IdP to validate that individual's claim to that specific digital identity.

3.1.13 authentication protocol

defined sequence of messages between a user and an IdP and/or RP which enables the IdP to perform authentication of an authorized user

[SOURCE: BS ISO/IEC 29115:2013, 3.4, modified]

3.1.14 biometric data

extracted information taken from a biometric sample and used to generate either a reference template or a match template

[SOURCE: ISO 19092:2008, 4.6, modified]

3.1.15 biometric enrolment

act of creating and storing a biometric data enrolment record in accordance with an enrolment policy

NOTE 1 The enrolment data record is attributed to a data subject, contains non-biometric data and is bound to a biometric reference identifier (a pointer to a biometric reference in a database of biometric references).

NOTE 2 A biometric reference is one or more stored samples, templates or models attributed to the user and is used as the object of biometric comparison. Examples of references are a face image stored digitally on a passport, fingerprint minutiae template on a national ID card or a Gaussian mixture model for speaker recognition in a database.

[SOURCE: [BS ISO/IEC 2382-37:2017](#), 3.5.3, 3.3.10, 3.3.19 and 3.3.16]

3.1.16 biometric identification method

process of searching (one-to-many) against a biometric enrolment database to find and return the biometric reference identifier attributable to a single user

NOTE 1 The biometric reference identifier is a pointer to a biometric reference in a database of biometric references.

NOTE 2 A biometric reference is one or more stored samples, templates or models attributed to the user and is used as the object of biometric similarity comparison.

NOTE 3 Use of the term “authentication” as a substitute for biometric identification is deprecated.

[SOURCE: [BS ISO/IEC 2382-37:2017](#), 3.8.2, 3.3.10, 3.3.19 and 3.3.16]

3.1.17 biometric recognition method

automated recognition of users based on their biological and behavioural characteristics

NOTE 1 The general meaning of biometrics encompasses counting, measuring and statistical analysis of any kind of data in the biological sciences, including the relevant medical sciences.

NOTE 2 Biometric recognition encompasses biometric verification and biometric identification.

NOTE 3 Automated recognition implies that a machine-based system is used for user identification.

NOTE 4 Behavioural and biological characteristics cannot be completely separated, which is why the definition uses “and” instead of “and/or”. For example, a fingerprint image results from the biological characteristics of the finger ridge patterns and the behavioural act of presenting the finger.

NOTE 5 Use of “authentication” as a synonym for “biometric verification” or “biometric identification” is deprecated; the term biometric recognition is preferred.

[SOURCE: [BS ISO/IEC 2382-37:2017](#), 3.1.3, modified]

3.1.18 biometric verification method

process of confirming a biometric claim through biometric similarity comparison (one-to-one)

NOTE 1 The biometric claim is that a user whose biometric sample is captured is or is not the bodily source of a specified or unspecified biometric reference.

NOTE 2 Biometric comparison is the estimation, calculation or measurement of similarity or dissimilarity between a biometric probe(s) and biometric references.

NOTE 3 Use of the term “authentication” as a substitute for biometric verification is deprecated.

[SOURCE: [BS ISO/IEC 2382-37:2017](#), 3.8.2, 3.6.4 and 3.5.7]

3.1.19 certificate

data comprising the public key and identity of the entity controlling the corresponding private key (together with other relevant cryptographic information), secured by the digital signing of these data by a certification authority

NOTE In this British Standard, “public key certificates” are referred to as “certificates”.

3.1.20 certification authority (CA)

entity trusted by one or more entities to create, assign and revoke public key certificates operating within a public key infrastructure (PKI)

[SOURCE: [BS ISO 21188:2018](#), 3.2, modified]

3.1.21 claim

statement that something is the case, without being able to give proof

[SOURCE: BS ISO/IEC 29115:2013, 3.6, modified]

3.1.22 claimed identity

declaration of unvalidated and unverified personal attributes by the applicant

3.1.23 contra-indicator

pieces of information that either contradict statements from a user or raise some doubt over whether the user is legitimate or genuine

NOTE 1 Contra-indicators are also known as indicators of compromise (IOCs).

NOTE 2 Contra-indicators are discovered either during identity proofing, authentication, or during the lifetime of a user's account. The discovery of a contra-indicator does not necessarily mean that a user is not legitimate, but rather that more stringent checks on the user are necessary to mitigate potential risks. Most contra-indicators require further investigation.

3.1.24 credential

set of data presented as evidence of a claimed or asserted digital identity and/or entitlements

[SOURCE: BS ISO/IEC 29115:2013, 3.8, modified]

NOTE While common usage often assumes that the credential is maintained by the user, this document also uses the term to refer to electronic records maintained by the IdP that establish a binding between the user's identification data and their identity. A credential has the following characteristics:

- a) comprises data that are evidence of an identity and/or entitlements;
- b) can be accompanied by other data useful to the authentication and identification process, but which do not form part of the credential;
- c) can be a derived credential;
- d) can be used for authentication, identification or authorization of the entity, or a combination of all three;
- e) is verified before it can be accepted as authentic and trustworthy for the intended purpose [see d)]; and
- f) can be authentic but not valid in all contexts, e.g. a credential held on a prepaid telephone chip card can be authentic but might only be valid for calls made using the facilities of the issuer.

3.1.25 cryptographic key

data value used to control cryptographic operations, such as decryption, encryption, signature generation or signature verification

3.1.26 de-identification

process of removing the association between a set of identifying attributes and the data principal or, in this instance, a user

[SOURCE: [BS ISO/IEC 20889:2018](#), 3.6, modified]

3.1.27 digital identity

data used by computer systems to represent a user

[SOURCE: *Digital identity: Call for evidence* [2]]

3.1.28 digital identity provider (IdP)

party that manages the user's primary digital identity data, including the digital identity identifier, together with authentication credentials and/or biometric data which can issue assertions derived from those credentials and data

3.1.29 digital signature

asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature

NOTE Digital signatures provide authenticity protection, integrity protection and non-repudiation, but not confidentiality protection.

3.1.30 enrollee

user who has a biometric reference template for use by the OUIS

[SOURCE: BS ISO/IEC 24713-2:2008, 4.17, modified]

3.1.31 identification

process of proving an individual's identity

3.1.32 identification data

information used in processes to prove the individual's claimed identity

3.1.33 identifier

label used to identify a user

NOTE Labels used by OUIS are typically context dependent.

3.1.34 identity

characteristics determining who an individual is

NOTE The characteristics used by the OUIS to denote identity are typically context dependent.

3.1.35 identity data

attributes relating to an individual

3.1.36 identity proofing

process to verify identifying attribute(s) to be entered into an identity management system (IdMs) and to establish that the identifying attributes pertain to the subject to be enrolled

[SOURCE: PD ISO/IEC TS 29003:2018, 4.1]

3.1.37 level of assurance (LoA)

degree of confidence in the processes leading up to and including the user identification method(s) itself, thus providing assurance that the entity that uses a specific digital identity is in fact the entity to which that digital identity was assigned

[SOURCE: BS ISO/IEC 29115:2013, Clause 6]

3.1.38 level of identity proofing (LoIP)

confidence achieved in the identity proofing process

[SOURCE: PD ISO/IEC TS 29003:2018, 3.11]

3.1.39 modes of operation

varying methods of functioning to achieve specified outcomes

3.1.40 multi-factor authentication (MFA)

user identification based on more than one user authentication method and/or biometric recognition method

NOTE 1 In the context of this standard, the multiple user authentication factors encompass biometric + password, password + token, biometric + token, and password + biometric + token. Combinations of biometrics, such as iris + fingerprint, are not included.

NOTE 2 The word factor is used colloquially; however, this standard distinguishes between the various user authentication and biometric recognition methods together with data associated with each method and mode of operation.

[SOURCE: PD ISO/IEC TR 29156:2015, 3.8, modified]

3.1.41 network

open communications medium, typically the internet, that is used to transport messages between the user, the RP and IdP and other intermediary parties

NOTE Unless otherwise stated, no assumptions are made about the security of the network; it is assumed to be open and subject to active (e.g. impersonation, man-in-the-middle, session hijacking) and passive (e.g. eavesdropping) attack at any point between the parties.

3.1.42 nonce

number that is unique per instantiation of a cryptography protocol as part of a measure to thwart cryptanalytic and other cryptographic attacks

[SOURCE: BS ISO/IEC/IEEE 8802-15-6:2017, 3.1]

3.1.43 one-time password (OTP)

token, generated by the IdP, consisting of an alpha/numeric string demonstrating possession of the user's device registered with the IdP

NOTE An OTP is generated by the IdP and delivered to the user through a separate channel, e.g. a short message service (SMS) to the user's mobile phone. An OTP has a limited time validity, e.g. one minute from generation.

3.1.44 one-time token (OTT)

token, generated by the user, consisting of an alpha/numeric string demonstrating user possession of a specific device, a specific registered application or possession or direct sole control of a private key element of an asymmetric key pair

3.1.45 online

assured connectivity to services on a network

3.1.46 online user identification system (OUIS)

user identification functionalities delivered by an IdP to RPs to an agreed level of assurance

NOTE An IdP delivers a user identification function to RPs, to an agreed level of assurance, either acting as an intermediary between a user and an RP or within an RP itself.

3.1.47 password

user authentication data, used as part of a user authentication process, consisting of a secret character string, known only to the user, intended to be memorized, recalled and reproduced in a secure manner by the user

3.1.48 personally identifiable information (PII)

information:

- a) that identifies or can be used to identify, contact or locate the individual to whom such information pertains;
- b) from which identification or contact information of an individual can be derived; or
- c) that is or might be directly or indirectly linked to an individual

3.1.49 personal identification number (PIN)

secret number sequence used for user identification, which is a memorized weak secret

[SOURCE: BS ISO/IEC 11770-1:2010, 2.34, modified]

3.1.50 presentation attack

presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

NOTE 1 Presentation attack can be implemented through a number of methods, e.g. artefact, mutilations, replay.

NOTE 2 Presentation attacks can have a number of goals, e.g. impersonation or not being recognized.

NOTE 3 Biometric systems might not be able to differentiate between biometric presentation attacks with the goal of interfering with the systems operation and non-conformant presentations.

[SOURCE: BS ISO/IEC 30107-1:2016, 3.5, modified]

3.1.51 privacy impact assessment (PIA)

overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of PII, framed within an organization's broader risk management framework

NOTE This process is also known as a privacy risk assessment.

[SOURCE: BS EN ISO/IEC 29134:2020, 3.7, modified]

3.1.52 private key

key of a user's asymmetric key pair that is kept secret and which is intended for use only by that user

[SOURCE: BS ISO/IEC 9798-1:2010, 3.22, modified]

3.1.53 privilege

authorization to a user to access an information asset or online service

NOTE 1 Privilege is a necessary but not sufficient condition for access. Access occurs when the access request is granted according to the access control policy. The access control policy is based on privileges and can include other environmental factors (e.g. time-of-day, location).

NOTE 2 Privileges take the form of data presented by a subject or obtained for a subject that are used by a policy decision point in order to grant or deny an operation that a subject is willing to perform on a resource.

NOTE 3 A resource can have multiple distinct privileges associated with it which correspond to various defined levels of access. For example, a data resource could have read, write, execute and delete privileges available for assignment to subjects. A request by a subject for access to the resource might be allowed for some levels of access

request but disallowed for other levels depending on the level of access requested and the resource privileges that have been assigned to the subject.

[SOURCE: BS ISO/IEC 29146:2016, 3.8, modified]

3.1.54 public key

key of an entity's asymmetric key pair which can be made public

[SOURCE: BS ISO/IEC 11770-1:2010, 2.36, modified]

3.1.55 public key infrastructure (PKI)

structure of hardware, software, people, processes and policies that employs digital signature technology to facilitate a verifiable association between the public component of an asymmetric public key pair with a specific subscriber that possesses the corresponding private key

NOTE The public key may be provided for digital signature verification, authentication of the subject in communication dialogues, and/or for message encryption key exchange or negotiation.

[SOURCE: [BS ISO 21188:2018](#), 3.48]

3.1.56 registration

process through which an individual, as an applicant, applies to an IdP to become an authorized user of an OUIS, which involves the IdP conducting identity proofing and identity verification tasks and then assigning a unique identifier to the authorized user

NOTE Biometric enrolment of the user and/or the provision of credentials, and possibly the provision of token devices, normally follows successful identity validation.

3.1.57 relying party (RP)

entity that relies on the verification of the user by the OUIS

NOTE 1 An RP is exposed to risk caused by incorrect identity information. Typically, it has a trust relationship with one or more identity information authorities.

NOTE 2 An RP can also act as an IdP.

[SOURCE: ISO/IEC 24760-1:2019, 3.3.7, modified]

3.1.58 remote

exchange of information between network-connected devices where the information cannot be reliably protected end-to-end by a single IdP and/or RP's security controls

NOTE Any data exchanged across the internet are considered remote.

3.1.59 risk

likelihood of a security threat materializing and the consequences

[SOURCE: BS ISO 28004-1:2007, 3.1]

3.1.60 risk assessment

process of identifying, quantifying and prioritizing risks to IdP and/or RP operations (including objectives, functions, image or reputation), IdP and/or RP assets, users, and other organizations

3.1.61 risk management

programme and supporting processes to manage information risk to IdP and/or RP operations by:

- a) establishing the context for risk-related activities;
- b) assessing risk;

- c) risk treatment (avoidance, reduction, sharing and retention); and
- d) monitoring risk over time

3.1.62 service

online information resources, products or utilities supplied by an RP

3.1.63 stakeholder

user or IdP and/or RP that can affect, be affected by, or perceive itself to be affected by a decision or activity

3.1.64 symmetric key

cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code

3.1.65 Termination**3.1.65.1 cancellation**

annulment of the user's digital identity

3.1.65.2 disqualification

removal of a user's eligibility to use an allocated digital identity for an activity because of an offence or infringement of the rules governing use of that allocated digital identity

3.1.65.3 expiration

cessation of the validity of the digital identity at a specified time

3.1.65.4 revocation

process of withdrawing an entitlement to access resources

NOTE An entitlement may sometimes be withdrawn by the organization which originally issued it and the entitlement schema enables the recording of entitlement revocations. Specific transactions may also be withdrawn, to correct errors or record the rescinding of entitlement allocations. It is also possible to disable the use of a credential, e.g. by revoking a user's digital certificate relating to their private key.

[SOURCE: BS ISO/IEC 19770-3:2016, **3.1.21**, modified]

3.1.66 threat

potential cause of an unwanted incident, which can result in harm to a system or IdP and/or RP

[SOURCE: BS EN ISO/IEC 27000:2020, **3.74**, modified]

3.1.67 user

individual who has obtained authorization to consume an online service supplied by an RP and has completed the registration, enrolment and identity proofing processes with an IdP

3.1.68 user enrolment

process of capturing, processing and storing data to allow an applicant to be registered with an IdP as a user of online services

3.1.69 user identification

online identification of a user by an IdP employing a user authentication method and/or biometric recognition method

NOTE Terms such as "identity proofing", "authentication", "verification", "recognition" and "biometric identification" are specific types of identification processes. Similarly, terms such as "user authentication mechanisms" or "identification mechanisms" refer to specific types of devices.

3.1.70 user identification assurance

degree of confidence, reached by the IdP, in the user identification method(s) that the claim to a specific digital identity is genuine

3.1.71 verifier

entity that verifies the claimant's identity using a user authentication protocol

NOTE To do this, the verifier might also need to validate credentials that link them to the user's identifier and check their status.

3.1.72 vulnerability

weakness in the security of an IT-system that can be exploited or triggered by a threat

[SOURCE: PD CEN ISO/TR 22100-4:2020, 3.19]

3.2 Abbreviations

For the purposes of this British Standard, the following abbreviations apply.

FAR	False accept rate
FMR	False match rate
FNMR	False non-match rate
FOG	Fraudulently obtained genuine
FRR	False reject rate
FTAR	Failure-to-acquire rate
FTER	Failure-to-enrol rate
HTTP	Hypertext transfer protocol
ICO	Information Commissioner's Office (UK)
IdAMS	Identity and access management system
IdP	Identity provider
IMEI	International mobile equipment identifier
IOC	Indicator of compromise
IOTP	Internet open trading protocol
LoA	Level of user identification assurance
LoIP	Level of identity proofing
MFA	Multi-factor authentication
MRZ	Machine-readable zone
NFC	Near-field communication
OTP	One-time password

OTT	One-time token
OUIS	Online user identification system
PIA	Privacy impact assessment
PII	Personally identifiable information
PIN	Personal identification number
PKI	Public key infrastructure
RFID	Radio-frequency identification
RP	Relying party
SIM	Subscriber identity module
SMS	Short message service
TLS	Transport Layer Security
USB	Universal serial bus
VPN	Virtual private network

4 Establishing or enhancing an OUIS

COMMENTARY ON CLAUSE 4

This clause gives recommendations for introducing or enhancing an OUIS for an application context. It recommends a multi-disciplinary approach for the selection of the most effective and efficient OUIS for the intended application context. The four phases of this approach are shown in [Figure 2](#).

A description of the stakeholders (including users), strategic goals, motivations and objectives assists in the understanding of the strategic factors for introducing or enhancing an OUIS. These documented factors form the basis of the requirement specifications for an OUIS. Candidate OUIS designs can then be evaluated against these specified requirements in order to assess fulfilment capabilities and to identify potential design vulnerabilities and issues and also investment projections. The operational management requirements related to the selected OUIS design are stated at the outset before the deployment becomes operational. All OUIS deployments possess vulnerabilities, incur costs and attract issues; therefore, an OUIS requires to be assessed for its effectiveness and efficiency regularly.

4.1 Strategic factors

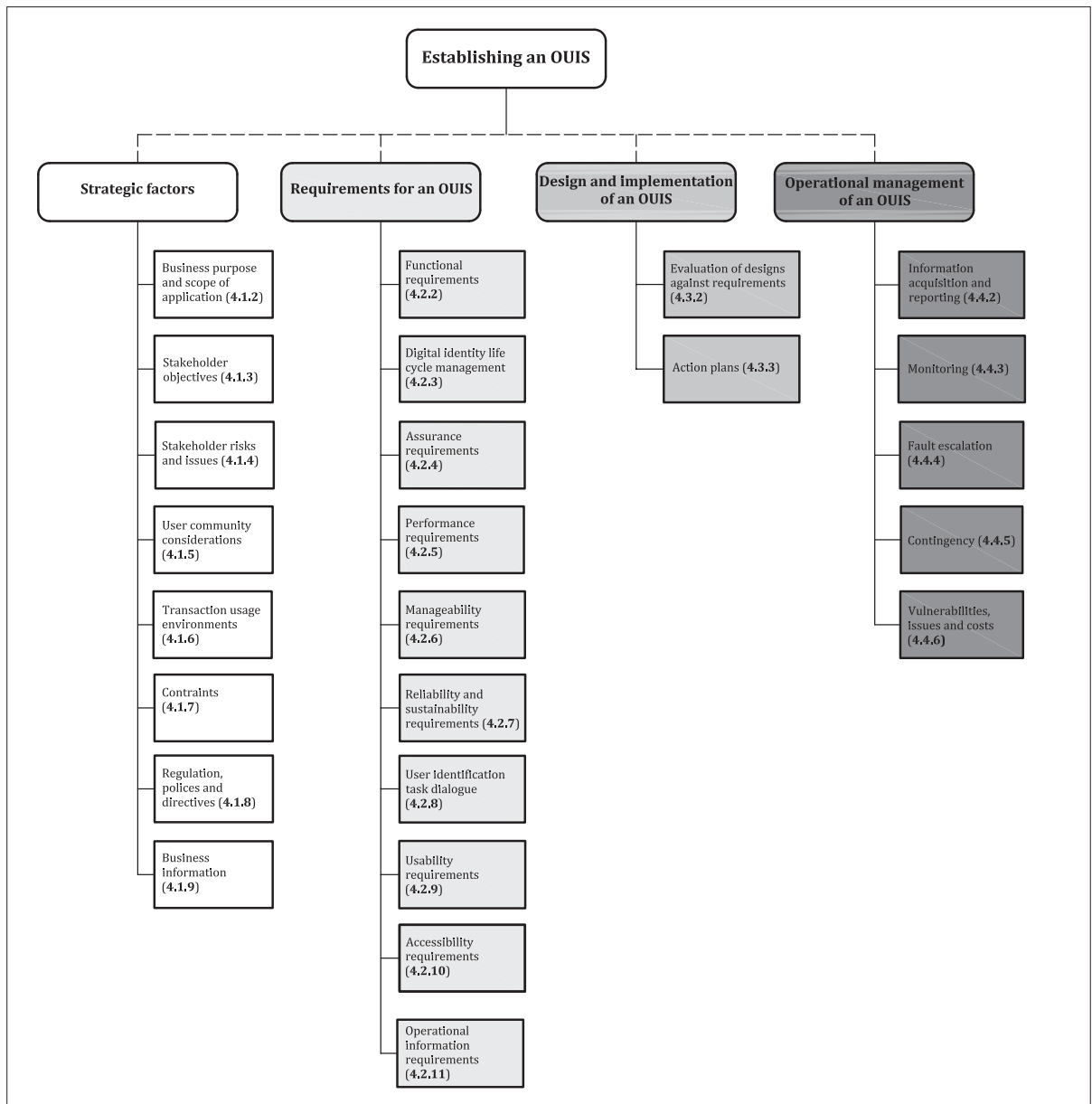
4.1.1 General

The following interrelated strategic factors should be determined for an OUIS in the intended application context, before the requirements themselves are specified:

- a) business purpose and scope of application;
- b) stakeholder objectives;
- c) stakeholder risks and issues;
- d) user community considerations;
- e) transaction usage environments;
- f) constraints;
- g) regulation, policies and directives; and

h) business information.

Figure 2 — *Establishing an OUIS*



4.1.2 Business purpose and scope of application

COMMENTARY ON 4.1.2

RPs introduce access control incorporating OUIs to minimize risks to information assets. A description of the business problem and the scope of issues, together with an explanation of the rationale for stakeholder investment, aid the introduction or revision of an OUIS. For example, the business problem could be individuals establishing multiple accounts or digital identities with the dishonest aim of receiving recurring entitlements or repeated financial rewards.

The relationships between the stakeholders in the application context might also need to be outlined, particularly when formal rules, i.e. contractual arrangements, exist.

The business problem and its scope in the application context should be expressed in the form of problem statements, rather than attributes of a potential design.

The benefits to stakeholders and other motivations should be documented, to aid understanding of stakeholder objectives.

4.1.3 Stakeholder objectives

COMMENTARY ON 4.1.3

Stakeholder objectives are often complementary, though there can be situations where they appear contradictory. Stakeholder business rationales for introducing or revising an OUIS are normally supported by arguments to protect their business interests. It is also important to understand a user's perspective as to why they might accept an OUIS and the intended impact on their daily tasks.

A stakeholder's rationale for an OUIS should be documented, expressing the desired business outcomes, covering as a minimum the following aspects:

- a) risk control;
- b) productivity impact;
- c) regulatory compliance;
- d) utilization impact (increasing or decreasing usage);
- e) investment levels; and
- f) reduction of business-related issues.

NOTE The objectives of users of an OUIS, as stakeholders, are mainly concerned with issues around privacy, usability, accessibility and personal risk.

4.1.4 Stakeholder risks and issues

COMMENTARY ON 4.1.4

All OUISS contain vulnerabilities, incur costs and attract issues and it is essential to gain a comprehensive understanding of stakeholder risks and issues at the outset before instigating plans to allocate resources to the deployment or enhancement of an OUIS. Stakeholders can possess different perceptions of risk, alternative understandings of issues and knowledge of costs; therefore, it is important to articulate these diverse understandings in order to avoid any misunderstandings and impacts upon stakeholder strategies.

The risks to stakeholder assets and the risks to the users in providing restricted online services should be identified and articulated at the outset. While stakeholders might have different risks to manage, different risk appetites and, possibly, varying risk management strategies (i.e. mitigation, transference, avoidance and acceptance), each risk should be identified to formulate an understanding of the likely impact upon each stakeholder.

Equally, there might be outstanding issues on existing deployments, such as adverse impacts on employee productivity, and these too should be understood.

NOTE Similarly, the failure of an OUIS can prevent partial or total customer access to services.

To formulate the requirements for an OUIS, risk assessments should be conducted to:

- a) identify the risks to all stakeholders, including those risks for the intended user community;
- b) provide a description of the likely impact on all stakeholders (including data privacy compliance) and, where possible, quantitative estimations on expected costs, or an impact rating value, whether the consequences of failures are likely to be borne directly or indirectly by each stakeholder;
- c) describe the envisaged compromise scenarios, e.g. based upon social engineering attacks or technologically mediated or insider attacks;

- d) determine the probability of a deliberate attack on an OUIS, taking account of the value of the assets, the known vulnerabilities, if already deployed, and the threat motivation of attackers;
- e) describe the underlying stimuli or goals of potential attackers which might lead them to attempt to exploit the apparent weaknesses of a deployed OUIS;
- f) indicate the required level of assurance in user identification (expressed conventionally in terms of 3 or 4 levels or quantitatively as a percentage), to permit access to a resource or a specific function; this assessment should be stated at the outset, independently of a specific solution employing a user authentication method and/or biometric recognition method; and
- g) explain why users experience difficulties in using a deployed OUIS or particular user authentication method and/or biometric recognition method.

To formulate the requirements for introducing or revising a deployed OUIS, all the outstanding stakeholder issues, whether user usability, excessive stakeholder costs, deficient performance or inadequate user identification assurance, should be articulated at the outset.

There should be a resolution process to verify that the resulting documentation establishes a consistent and coherent stakeholder perspective on all significant risks and issues, using a common vocabulary and defined terms.

A privacy impact assessment (PIA) should be conducted prior to introducing an OUIS and undertaken periodically for a deployed OUIS, to assist in formulating the requirements for the OUIS.

Where a new information system for an application is to be introduced, reference should be made to similar types of application so that the issues likely to be encountered are identified.

4.1.5 User community considerations

COMMENTARY ON 4.1.5

An understanding of the user community assists in creating the requirements for an OUIS. The business application may be targeted at specific individuals carrying out a single rarely used task, e.g. IdP and/or RP employee registration/enrolment processes, or it may be made widely available to the general public.

The design and operation of the OUIS should take account of the expected population characteristics of the user community and other relevant factors, such as the following, that could affect users' legitimate usage of the system, as designed for the application context:

- a) the intended user community, including whether there are any restrictions on membership;
- b) the characteristics of the intended user community, if any, in terms of demographics, physiology, behaviours, appearance, etc.;
- c) the proposition or the benefits of using the application to the intended user community;
- d) the social attitudes towards the use of the type of application to be deployed;
- e) the relationship, if trust is already in existence, between the stakeholders providing the application and the intended user community;
- f) whether the intended user community is likely to use an OUIS, as designed, willingly or voluntarily;
- g) whether the intended user community is capable and motivated sufficiently to absorb the requisite new technical or operational skills;
- h) the user identification assurance which is likely to be sought to demonstrate anonymity, unlinkability, unobservability and de-identification; and

- i) the users' obligations in terms of responsibilities or liabilities for accessing the resource and whether the consent to these conditions is likely to influence acceptance or consent to using an OUIS properly, as designed.

In particular, the IdP should:

- 1) take into account that there are some users in the community who might struggle with their selected user authentication method and/or biometric recognition methods; and
- 2) provide alternative methods of user identification without sacrificing access or user identification assurance.

4.1.6 Transaction usage environments

COMMENTARY ON 4.1.6

An understanding of the environments in which the intended users are likely to conduct their transactions assists in creating the requirements for an OUIS.

The characteristics of the physical environments in which the users conduct their online interaction with the target resources impacts the requirements for the OUIS. For example, the completion of a lengthy interaction dialogue to complete an application form or gathering information from several documents in an office is different from quickly purchasing train tickets while travelling or while sitting in a cafe. Similarly, the envisaged physical usage environments, e.g. hotel, home, train, cafe, street or car, can present variable or even unknown characteristics relevant to the optimal operation of one or more of the user authentication methods and/or biometric recognition methods on certain types of user device.

A description of the characteristics of the envisaged environments in which users are to use the RP's services and the OUIS should be articulated, including details, where possible, focusing on the following factors:

- a) the ergonomic characteristics of the envisaged usage environments;
- b) the degree of physical and logical control that the user has in those usage environments;
- c) the types of special devices required for the application or whether users are allowed to use permitted ubiquitous devices, unrestricted networks and readily available software applications, e.g. browser; and
- d) the physical environments or geographic locations in which access to the application is prohibited or functionality reduced.

Where appropriate, use cases for the application should be developed to enhance the ability to identify the characteristics of the environments in which the user interacts with their allowed devices and the remote resource (and the respective OUIS).

4.1.7 Constraints

COMMENTARY ON 4.1.7

A documented understanding of the various types of constraints of the application context, whether regulatory, economic, social acceptability and technological, assists in understanding and formulating the requirements for an OUIS. The business application has a defined purpose as stated in the business case for investment in an information system and its associated control mechanisms. The constraints on costs might be to protect an IdP and/or RP's investment in conducting its business online.

The constraints that might influence the requirements for an OUIS should be identified, taking account of the following aspects:

- a) the political issues between stakeholders that relate to the application context;
- b) the economic rationale of stakeholder participation in the application context;

- c) the commercial or contractual relationship between the stakeholders;
- d) the legal and regulatory imperatives imposed upon the stakeholders and the application context;
- e) the contextual legacies of the application context, which might relate to technological restrictions, respecting social norms or the proposition to user acceptability;
- f) the restrictions imposed by logistical or procedural activities that dictate how data for user identification are to be acquired;
- g) the specifications of a scheme in which the application context is to operate;
- h) the performance benchmarks of similar applications, which might impact stakeholder expectations;
- i) the responsibilities, costs and liabilities to the users, which might relate to purchase of special devices or applications for ubiquitous devices;
- j) the interoperability requirements of standards relating to the application context; and
- k) the circumstances of the application context, which might inhibit the recovery of an OUIS in the event of partial or total failure.

4.1.8 Regulation, policies and directives

COMMENTARY ON 4.1.8

An understanding of the external rules, e.g. law and industry standards or operating specifications, and internal stakeholder IdP and/or RP policies applicable for the intended application context assists in the formulation of the requirements for an OUIS.

At the outset, the IdP and/or RP should establish for the OUIS:

- a) which regulations, industry conventions and directives apply in the relevant jurisdictions in the intended application context;
- b) the specific user identification assurance requirements following a risk assessment; and
- c) their obligations in support of fraud detection and investigation, and the efforts of law enforcement agencies.

The following internal IdP and/or RP policies should be reviewed periodically to identify those rules which could impact the requirements for an OUIS:

- 1) the retention of the data used to identify an individual;
- 2) the stakeholder procedures for archiving data as stated in data retention policies;
- 3) the policies relating to privacy protection of users' personal data;
- 4) the stakeholder authorized identity evidence (i.e. evidence deemed acceptable or authorized for the identity proofing process, the entities that are acceptable sources and the acceptable format of the evidence data or information);
- 5) the processes relating to the resolution of issues between stakeholders; and
- 6) the management of sanctions that might be imposed upon stakeholders or users in the event of misdemeanours or substandard performance.

4.1.9 Business information

COMMENTARY ON 4.1.9

IdP and/or RPs require information from their operational systems to demonstrate compliance with regulations, manage risks and determine the effectiveness and efficiency of OUIs as an integral element of their access control systems.

The following should be ascertained and documented at the outset:

- a) information required for demonstrating compliance with regulations, e.g. the General Data Protection Regulation (GDPR) [3], and laws in the relevant jurisdictions;
- b) information required for stakeholders to manage their risks and issues;
- c) criteria for acquiring the data necessary to evaluate the effectiveness and efficiency of a deployed OUI; and

NOTE Establishing criteria at the outset facilitates the acquisition of relevant data to enable an objective assessment of an OUI against the effectiveness of the statement of requirements for the OUI to fulfil stakeholder objectives, e.g. identification accuracy, regulatory compliance, reliability, risk reduction and other measurable parameters. The efficiency of the candidate OUI or deployed OUI can be measured in terms of the effort, e.g. resources, to satisfy those stipulated requirements, e.g. identification task time, utilization of resources and stakeholder costs and other measurable parameters.

- d) acquisition of information, including the legal and regulatory requirements, as part of evidence gathering.

From items a) to c), the type of data and the frequency of capture should be expressed in the form of requirements for an OUI.

4.2 Requirements for an OUI

COMMENTARY ON 4.2

This subclause gives recommendations for producing requirement statements to establish or enhance an OUI. The articulation of these user identification requirements enables the quantitative and qualitative assessment of different knowledge-based and/or possession-based user authentication methods and/or biometric recognition methods and to evaluate the effectiveness and efficiency of candidate solutions.

4.2.1 General

From the factors determined in accordance with 4.1, the type of data and the frequency of capture should be expressed in the form of requirements for an OUI.

The requirements for an OUI should be expressed in accordance with 4.2.2 to 4.2.11 to establish the integrity, completeness and appropriateness of the OUI. Clearly articulated statements should be used to facilitate the objective evaluation of candidate systems' capabilities to meet a set of requirements.

4.2.2 Functional requirements

The following characteristics should be used to assist with the formulation of the description of functional requirements for the OUI:

- a) positive identification of an enrolled user or negative identification that the user is not enrolled;
- b) overt or covert identification of the user, or both;
- c) structured identifier or random identifiers associated with the user, or none;
- d) the need to link the unique assigned identifier with other identifiers;

- e) the ability for users to enter, update and delete their personal data, e.g. autobiographical information, associated with their digital identity profile;
- f) the degree of supervision (if any) received by the applicant during enrolment and during an identification session;
- g) the type and capability of the devices permitted to be used by the users;
- h) the type and capability of the applications permitted to be used by the users;
- i) the preferred means by which data for user identification are acquired from the users;
- j) the expected type and number of identification data elements to be used to identify an individual to meet the stated level of identification assurance for user identification;
- k) the rules for which access to the resource is not permitted using a single sign-on mechanism;
- l) the user's device attributes to be collected during the user identification process and whether the attributes are to be shared with other resources to aid the identification decision;
- m) the stage(s) during the application usage (beginning, critical task or data submission) when the user is required to be identified;
- n) the location(s) where user identification data are to be stored;
- o) the physical or logical location where the user identification decision process is to take place;
- p) the means by which the user is notified of the success or failure of an identification attempt;
- q) the number of user identification attempts allowed before the user is refused access to the resource or completion of a task;
- r) the recovery of the user's ability to access a resource in the event of a partial failure specific to that user and/or total system failure affecting all users; and
- s) the systems and processes to be used by the operators/administrators of the OUIS to enable them to perform their duties to support the life cycle management of digital identities and the user identification processes and protect the user data upon which user identification is based.

Once these initial descriptions have been written, they should be reviewed to identify further specific functional requirements or further refinement of these requirements.

4.2.3 Digital identity life cycle management

COMMENTARY ON 4.2.3

The integrity of the OUIS is underpinned by digital identity life cycle management comprising governance practices and support functions consisting of five main phases:

- a) *creation of a digital identity;*
- b) *usage of a digital identity using issued credentials with the selected user authentication method and/or biometric recognition method;*
- c) *maintenance of digital identities and credentials;*
- d) *termination of a digital Identity; and*
- e) *governance and operation of the IdMS.*

This subclause gives recommendations for describing the digital identity assurance governance requirements by outlining the main processes in each of the life cycle phases.

4.2.3.1 Creation

4.2.3.1.1 General

The characteristics set out in [4.2.3.1.2](#) to [4.2.3.1.4](#) should be used to describe digital identity life cycle management requirements for the creation of digital identities for the OUIS.

4.2.3.1.2 Application and enrolment processes

The requirements descriptions should be established for:

- the entity or applications authorized to capture an applicant's personal data to be used to register an application and to create a digital identity profile;
- how the acceptable applicants are to be distinguished in a policy statement, e.g. "Users must be over 18 years old"; and
- any need for the identifier assigned to the applicant to be structured, unstructured and linked to other identifiers for that user.

4.2.3.1.3 Identity proofing processes

The requirements descriptions should be established for:

- the entities authorized or registered to undertake applicant identity proofing processes;
- the acceptable forms of identity evidence and how the data are verified;
- the rules for administrators and/or processes to follow to evaluate evidence submitted by an applicant;
- the rules for administrators and/or processes to follow where evidence submitted by an applicant is deficient; and
- the processes for advising applicants that evidence they submitted as proof of identity is insufficient.

4.2.3.1.4 Credential issuance processes

The requirements descriptions should be established for:

- the entities authorized or registered to acquire credentials; and
- the processes for acquiring or manufacturing credentials that are contingent upon the choice of methods for user identification.

4.2.3.2 Usage

The requirements descriptions should be established for:

- a) the level of identification assurance for user identification;
- b) trusted communication protocols; and
- c) the conditions, the procedures and the protocols to support digital identity attribute sharing between IdPs and RPs.

4.2.3.3 Digital identity and credential maintenance

The requirements descriptions for updating data and user notification should be established for:

- a) the processes needed to respond to users or applicants who are denied access to the target information system or to their digital identity profile;
- b) processes for updating digital identity profile data by the user;

- c) processes for revising the credential data and other metadata upon which identification decisions are based;
- d) processes for users to notify IdPs or other authorized IdPs and/or RPs that their credentials are being rejected by RPs; and
- e) processes for notifying users in a secure manner of how to re-establish credentials and other user identification data to re-enable them to access resources.

4.2.3.4 Digital identity and credential termination

COMMENTARY ON 4.2.3.4

Termination of the user access and the possible removal of the digital identity from the identity management system might be required where the IdP or the user, or another authorized entity, wishes to prevent the user from utilizing their credential to access the services offered by RPs.

The requirement statements for the termination of access to the OUIS should be established for one or more of the following processes.

- a) Revocation – processes to:
 - verify that the reason for revocation is valid;
 - revoke the user's access to the target information system (which may be operated by a separate RP) and to their digital identity profile;
 - inform the user that this access has been revoked if operationally appropriate; and
 - remove the user's personally identifiable information (PII) from the IdMS and other related systems and, if applicable, inform the user when this process has been completed.
- b) Disqualification – processes to:
 - verify that the reason for disqualification is valid;
 - revoke the user's access to the target information system (which may be operated by a separate RP) and to their digital identity profile;
 - if appropriate, inform the user that this access has been revoked and inform them of the reason for disqualification; and
 - remove the user's PII from the IdMS and/or other related systems and, if applicable, inform the user when this process has been completed;
- c) Cancellation – processes to:
 - verify that the request for cancellation of the digital identity is valid and does not infringe the rules governing the IdMS and/or other related systems;
 - revoke the user's access to the target information system (which may be operated by a separate RP) and to their digital identity profile, and inform the user that this access has been revoked; and
 - remove the user's PII from the IdMS and/or other related systems and inform the user when this process has been completed.
- d) Expiration – processes to:
 - verify that the reason for expiration conforms to the rules governing the system;
 - determine whether a user's access is to be reinstated and, if so, initiate processes to reinstate it, or, if not, revoke the user's access to the target information system (which may be operated by a separate RP) and to their digital identity profile;

- inform the user that this access has expired or that processes to reinstate it have been initiated (or completed); and
- if access has expired, remove the user's PII from the system and inform the user when this has been completed.

If required, the PII should be archived in accordance with the IdP's personal data protection policy.

NOTE The operator of the OUIS may exercise the option of temporary suspension of the user's access to the OUIS, for example at the user's request.

4.2.3.5 Governance and IdMS operations

The requirements descriptions should be established for:

- a) the roles, responsibilities and processes for decision-making on managing digital identities, particularly in the event of compromise and the requirement to inform the Information Commissioner's Office and/or other regulatory authority; and
- b) the roles, responsibilities and processes for managing the IdMS which need to align with the selected user authentication method and/or biometric recognition method prior to deployment, and the documentation for which should be completed prior to deployment.

4.2.4 Assurance requirements

4.2.4.1 Investigation policies

Investigation policies should be established for:

- a) the procedures for carrying out investigations into violations of any of the digital identity management processes;
- b) the mechanism for enforcing these policies to provide investigative access to identity data and services; and
- c) specifying which entities are empowered to undertake authorized investigations.

4.2.4.2 Privacy protection policies

Privacy protection policies should be established for:

- a) the entities authorized or registered to acquire, store, maintain and use users' personal data;
- b) allowing users to establish all operations for which their PII is used and requiring users to give their consent to these uses;
- c) the processes necessary to enable only authorized administrators to have access to users' personal data represented in their digital identity profile;
- d) the processes necessary to enable only authorized administrators to have access to users' identification data;
- e) the processes necessary to protect the confidentiality of users' identification data while stored and during the identification process;
- f) the processes necessary to coordinate responses to notification of suspected privacy violations;
- g) the processes necessary to allow authorized inspection of the privacy asset register;
- h) the processes necessary to verify that the controls on users' and administrators' access to users' autobiographical data and user identification data are not eroded;
- i) the processes needed by data controllers and/or data processors to respond to requests for access, correction and deletion of data by users and other locally required rights of users; and

- j) the processes for subject access requests.

4.2.4.3 Identification policies

Identification policies (relating to identify proofing and user verification) should be established for:

- a) the procedures for exchanging and negotiating identification policies amongst users, IdPs and RPs;
- b) the mechanism for enforcing these policies to control access to identity data and services; and
- c) policies on user roles or attributes to align a user group with a set of system privileges.

4.2.4.4 Audit trails

Audit trail policies should be established for:

- a) the procedures and mechanisms for protecting audit logs and audit trails in a secured and privacy-aware manner;
- b) attribute sharing comprising the user identity of the requestor of the transaction and details of when the transaction happened, whose digital identity was accessed and for what purposes; and
- c) the alignment of the audit trail of identity data with IdP and/or RP-wide internal control frameworks.

4.2.4.5 Description of assurance requirements

The following characteristics should be used to describe assurance requirements for the OUIS:

- a) the assurance assessment methodology for evaluating the assurance capabilities of a candidate OUIS;
- b) a testing plan to verify that a candidate OUIS is able to fulfil the stated level of assurance sought;
- c) the resources and skills to successfully compromise the OUIS for a user and in totality;
- d) the tools, facilities and skills of the assessors needed to perform functional and assurance tests as described in the test plan;
- e) the documentation and test data to be made available to the assessors to test the assurance of the candidate OUIS;
- f) the description of the expected behaviours, to verify that the OUIS behaves in a reliable and predictable manner;
- g) the audit data required to demonstrate the veracity of the processes and data used to successfully identify a user or deny access to a resource;
- h) the impact of employing two or more methods of user identification or using biometrics to reach the desired level of assurance;
- i) the accreditation conditions prevailing before a user identification system can be deployed or partially migrated;
- j) the scope of the usage conditions in which the assurance tests are to be undertaken; and
- k) the specification on the level of assurance required, expressed in quantitative terms, e.g. 1 failure in 100 000 user identification attempts, so that actual performance can be measured quantitatively from acquired data to determine effectiveness and, where appropriate, efficiency.

4.2.4.6 User identification assurance requirements

COMMENTARY ON 4.2.4.6

User identification assurance is the confidence that can be placed in the user identification decision using a user authentication method and/or a biometric recognition method. For person identification systems this translates to the confidence that a person possessing a claimed identity is the true owner of that digital identity. User identification assurance is typically expressed in terms of level of assurance (LoA).

Levels of user identification assurance are usually represented in terms of a small number of levels, e.g. LoA 1 to LoA 4 in ascending order of confidence. These levels are often described using corresponding names, e.g. Low, Medium, High, Very High. Further details of user identification assurance levels and how they relate to the requirements for entity authentication assurance are given in BS ISO/IEC 29115. User identification assurance may also be expressed quantitatively, e.g. as a percentage.

The determination of user identification assurance requirements and the associated level of assurance for an application should be based on the result of a methodical risk assessment process.

Risk assessment should be an ongoing activity which identifies all risks, including risks that might be caused by countermeasures introduced to address other risks, e.g. strong passwords mandated to counter guessing or technical attacks on passwords might lead to human weaknesses whereby passwords are written down and left in conspicuous places.

NOTE 1 For requirements and guidance on risk management, see the following:

- [BS EN ISO/IEC 27001](#);
- [ISO/IEC 27005](#);
- *BS ISO 31000*; and
- [BS EN IEC 31010](#).

Selection and implementation of user identification mechanisms for a given LoA should take account of the technical strength of the user identification method (e.g. password entropy, biometric recognition performance and error rates), susceptibility to human and procedural weaknesses and resistance to technical attacks.

Where risk assessment indicates a very high LoA, multi-factor user identification should be employed. For a high LoA, multi-factor user identification should be taken into account.

NOTE 2 Multi-factor user identification can also be used to provide other benefits, such as improvements in usability and accessibility independent of the LoA. For further information, see [Annex A](#).

4.2.5 Performance requirements

Performance requirements should be expressed in numerical terms so that the accuracy of the OUIS's decision on user identification can be tested objectively. Equally, the required timings for the user identification process should be expressed in seconds, and words such as "prompt" or "as quickly as possible" should not be used as they do not enable objective assessment. The following characteristics should be used to describe performance requirements for the OUIS:

- a) the rate at which there is a failure to identify authorized users, expressed as a decimal value;
- b) the rate at which there is a failure to detect unauthorized users, expressed as a decimal value;
- c) the throughput rates for identifying users in terms of minimum numbers in a specific periodicity;

- d) the maximum number of user identification attempts in a user's session with the application and the number of unsuccessful attempts before the user's access to a resource is denied and the user's access to all resources potentially suspended;
- e) the maximum user identification time, in seconds, from a user's perspective;
- f) the maximum user identification time limit permitted before another identification attempt is allowed;
- g) the impact of different types of operational environments on the user identification processes and what allowances to accuracy and timings are needed when specific conditions are detected;
- h) the processes necessary when data acquired from the user are of insufficient quality for the user identification process; whether a toleration rate needs to be reached before further data are acquired under the same method or sought under an alternative method of user identification;
- i) the maximum number of attempts allowed for a user to enrol their identification data;
- j) the minimum time permitted for a user to enrol their identification data;
- k) the controls necessary to protect users' identification (individually and collectively) data during storage; and
- l) the controls necessary to protect users' identification data during the identification matching processes to give assurance that these data are reliable for the identification of users.

4.2.6 Manageability requirements

COMMENTARY ON 4.2.6

The introduction of an OUIS can occur in scenarios where there are no existing infrastructures, resources or capabilities. This subclause assumes, though, that there are existing networks, devices, systems and infrastructures that are supported by administrative personnel.

The following characteristics should be used to describe manageability requirements for the OUIS:

- a) the technological impact on the infrastructures and systems available to ensure business-as-usual operating;
- b) the impact on current resources available, including skills and capabilities of administrative staff;
- c) the impact on processing capacity and scalability of current infrastructures;
- d) the impact upon the ability support contingency plans;
- e) the impact upon system backup strategies and methods;
- f) the impact upon administrative support roles;
- g) the limitation of resources, including costs, on supporting current capabilities and deliverables and the introduction or revision of an OUIS;
- h) the need for specially trained individuals and/or expertise with unique skills;
- i) the need to calibrate signal capture devices or update software on users' devices;
- j) the need for an alternative means of user identification in the event of user lockout or total or partial failure which would adversely impact the stated performance requirements; and
- k) the need to integrate with existing legacy systems and/or OUIs.

4.2.7 Reliability and sustainability requirements

The following characteristics should be used to describe reliability and sustainability requirements for a candidate OUIS:

- a) the minimum availability of the candidate OUIS in terms of full outage or partial failure and the degradation of response times or accuracy;
- b) assurance evidence required to demonstrate that the candidate OUIS is capable of meeting assurance requirements;
- c) performance evidence required to demonstrate that the candidate OUIS is capable of meeting performance requirements;
- d) evidence that the candidate OUIS has the capability to meet data privacy requirements and generate relevant data to support claims of compliance;
- e) evidence that users accept the candidate OUIS and are able to use it confidently;
- f) evidence of impact upon users' costs and usage of devices;
- g) evidence of actual repair response times from other deployments;
- h) the extent to which the candidate OUIS can be integrated with existing operation infrastructures;
- i) the anticipated processes for updating internal systems and for ensuring compatibility with operating systems that a user might have, as they are updated, and supporting operating systems (e.g. which versions of operating systems are going to be supported and to how many previous versions is that support going to apply);
- j) the extent to which users' devices can interface with the candidate OUIS;
- k) the known exploitable vulnerabilities of the candidate OUIS;
- l) the costs limitation of the candidate OUIS in terms of:
 - 1) artefact device or software distribution costs;
 - 2) implementation costs;
 - 3) infrastructure costs;
 - 4) additional resource costs;
 - 5) maintenance costs; and
 - 6) OUIS's life expectancy; and
- m) evidence of practical experience of the candidate OUIS to meet similar requirements and the issues, costs and vulnerabilities encountered.

4.2.8 User identification task dialogue

The following characteristics should be used to describe user identification task dialogue requirements for the OUIS:

- a) the interaction points where user identification routines are invoked during use of the application or access to the resource, i.e. at the beginning or prompted by a critical function or event;
- b) the logical alignment of the user identification routine with the user's task to achieve a desired goal;
- c) how the security status of the interaction is conveyed to the user;
- d) the conveyance of security features to the user, including the means of recovery;

- e) the reporting of input errors and user identification to the user in a logical and clear manner; and
- f) the intuitiveness of the task dialogue for the application and the user identification routine, and the necessity for training or educational aids.

NOTE It might be more convenient to use process flow diagramming or similar utility to represent the required interactions between the user, input devices, intermediary system processes and host system processes during the use of the application and invoking the user identification routine.

4.2.9 Usability requirements

The IdP and/or RP should promote ease of use of the OUIS, which may involve, for example:

- a) making the OUIS available across as wide a range of fixed and mobile technologies and devices as is practicable;
- b) minimizing the number and complexity of operations to be performed by the user at each stage of operation;
- c) enabling users to access the system from the permitted geographic locations, as defined in the application/business context;
- d) avoiding the requirement for the user necessarily to possess a particular item of hardware to use the system; and
- e) avoiding the need for a fast data connection for effective access.

The IdP and/or RP should anticipate the need to provide easily understandable information about how best to use the system and how to deal with potential problems with access.

NOTE This information may include, for example, how to restore access when the user forgets a password.

4.2.10 Accessibility requirements

The IdP and/or RP should take into account the characteristics and abilities of the whole range of individuals who could potentially use the OUIS.

NOTE These requirements might include, for example, individuals with physical limitations, such as sensory or motor impairments, individuals with reduced mental capacity, and individuals who have a responsible third party as a carer. An individual who is normally able to use a system without a problem might nevertheless be vulnerable because of circumstances that render them temporarily less able to interact effectively with the system, e.g. bereavement.

The IdP and/or RP should determine how best to accommodate individuals who are incapable of using the OUIS, providing them with alternative means of access to the application.

The IdP should offer a process to an individual with the required authority, e.g. lasting power of attorney, to access specific OUIS resources on behalf of the user. Access to the OUIS resources should not necessarily grant this person authority to use the OUIS to access RP services.

4.2.11 Operational information requirements

COMMENTARY ON 4.2.11

The minimum requirements are derived from an understanding of the type of business information needs and the granularity of reporting, and the frequency of reporting provides input into determining the data acquisition requirements.

The IdP and/or RP should determine their business operational information requirements so that the relevant data can be acquired, collated, synthesized and presented for management information reporting.

The following characteristics should be used, as a minimum, to describe the data collection requirements for the OUIS:

- a) log records to be collected during the user's interaction with the application [additional data required during the user identification transaction could be used as confirmatory or contradictory evidence to the user authentication and/or biometric recognition method deployed (see [Clause 9](#))];
- b) logs records to be collated from the OUIS;
- c) errors to be reported to the help desk;
- d) resetting suspended digital identity accounts;
- e) numbers and type of new users added to the community, the number and type of suspended accounts and the number of deleted user accounts;
- f) the costs incurred on infrastructure and resources to support the OUIS;
- g) the recording of data or importation of audit records from an external or supplemental process which enables the collation of data from analysis and reporting;
- h) a methodology to collate the acquired data so that analysis and reporting can be consistent, accurate and complete for business decision-makers; and
- i) data to enable the evaluation of the effectiveness of the OUIS and the assessment of its efficiency.

NOTE OUISs attract issues, incur costs and possess vulnerabilities that require organizations to invest in ongoing operational management of the OUISs to ensure that these systems continue to be effective and efficient to fulfil documented requirements.

4.3 Design and implementation of an OUIS

COMMENTARY ON 4.3

This subclause gives recommendations for evaluating OUIS designs, together with various configurations and the subsequent deployment of the selected OUIS into the environments relating to the business context. The selected design needs to align with stakeholder objectives and fulfil the corresponding requirements. The deployment of the OUIS depends upon the context; however, testing the OUIS provides evidence to support claims of conformity to stipulated requirements.

4.3.1 General

The IdP and/or RP should evaluate a candidate OUIS design's effectiveness and efficiency to fulfil the stipulated requirements for an OUIS prior to implementation.

The requirements for an OUIS should be documented and be expressed using the themes in accordance with [4.2.2](#) to [4.2.11](#) to ensure the integrity, completeness and appropriateness of the OUIS. These clearly articulated statements should then be used to facilitate the objective evaluation of candidate design capabilities to meet a set of stipulated requirements. This evaluation should also include the evaluation of different configurations for a design in order to identify optimal effectiveness and efficiency.

4.3.2 Evaluation of designs against requirements

The IdP and/or RP should evaluate candidate OUIS designs and configurations, particularly the proposed user authentication methods and/or biometric recognition methods, against stipulated and agreed:

- a) stakeholder objectives for an OUIS;
- b) identity management requirements for an OUIS;