International Telecommunication Union

ITU-T X.1254

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(09/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Entity authentication assurance framework

Recommendation ITU-T X.1254

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	**X.1250–X.1279**
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1254

Entity authentication assurance framework

Summary

Recommendation ITU-T X.1254 specifies three entity authentication assurance levels (AALs), and criteria for and threats to each of them.

Additionally, it:

- establishes a framework for managing AALs;
- provides guidance concerning control technologies that are to be used to mitigate authentication threats, based on a risk assessment;
- provides guidance for mapping the three AALs to other authentication assurance schemas; and
- provides guidance for exchanging the results of authentication that are based on the three AALs.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1254	2012-09-07	17	11.1002/1000/11608
2.0	ITU-T X.1254	2020-09-03	17	11.1002/1000/14260

Keywords

AAL, assurance, authentication, authentication assurance level, identity management, IdM, level of assurance, LoA.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Recommendation	2
4	Abbreviations and acronyms	3
5	Conventions	4
6	Digital authentication process flow	4
6.1	General	4
6.2	Digital identity assurance	5
6.3	Roles	6
6.4	Authentication processes components	7
7	Apply risk management to the authentication assurance framework	8
7.1	General	8
7.2	Authentication risk	8
8	Threat categories, risks and controls	9
8.1	Assurance levels	9
8.2	Authenticator compromise	11
8.3	Transaction compromise	13
8.4	Verifier impersonation	14
8.5	Subscriber impersonation	15
8.6	Authentication service compromise, risks and controls	20
8.7	Privacy, risks and controls	21
Appendix I – An example of strong authentication using [b-ITU-T X.1278]		23
I.1	Introduction	23
I.2	Threat categories	23
I.3	[b-ITU-T X.1278] enables "high-assurance strong authentication"	23
I.4	Old authentication with passwords	24
I.5	New authentication with [b-ITU-T X.1278]	25
I.1	Interoperability and certification	25
Bibliography		27

Introduction

A digital identity is the unique representation of an entity engaged in an online transaction. Assurance – or confidence – that the digital identity with which one is interacting is consistent with the claimed identity, lies at the heart of online trust, security and access control. Three types of assurance are identified to contribute to establishing trust in a digital identity: identity assurance; authentication assurance; and federation assurance.

This Recommendation provides a framework for authentication assurance. For the purposes of this Recommendation, authentication is the process by which a claimed identity is verified for the purpose of conducting an online transaction. For services in which return visits are applicable, a successful authentication provides reasonable risk-based assurances that the user accessing the service today is the same as that which accessed the service previously.

The framework established in this Recommendation provides online service providers – relying parties (RPs) and credential service providers (CSPs) – with a systematic approach to understanding their risks and identifying controls to help mitigate them. It is designed to facilitate the methodical selection of controls and risk mitigation strategies using a three-step process:

1. identification of roles and services to determine threat categories;
2. application of a targeted risk management process to determine the strength of controls required; and,
3. identification of which technologies – protocols, credential types, etc. – are employed to further refine controls.

A threat-based model

This Recommendation is designed to facilitate the methodical selection of controls and risk mitigation strategies. A preliminary step in being able to select appropriate controls and mitigation strategies is the identification of the types of risks and threats associated with the role(s) and services of an online service provider. See Figure 0-1.

Figure 0-1 – Services, risks, and controls

This framework is organized on the basis of risks and threat categories that provide online service providers with a functional link between risk assessment processes, and control and risk mitigation activities.

Identity service providers may provide all, some or only one of the functional components of these digital identity phases. As such, it is appropriate to assess risks and address controls and risk mitigation approaches on a similar componentized approach to the digital transaction lifecycle. This Recommendation addresses risks and controls to the credential management and authentication phases of this lifecycle. Other documents (e.g., [b-ISO/IEC TS 29003]) address the risks and controls for the enrolment and identity proofing activities, as well as organizational and management controls. It is anticipated that these documents, and others, will be aligned to represent a coordinated set of core identity management standards (as illustrated in Figure 0-2) that, when used in combination, provide the processes, risks, and controls for the digital identity transaction lifecycle.

This Recommendation also presents a catalogue of privacy threats, considerations and mitigating controls that are specific to its scope (authentication and credential management). This Recommendation does not include privacy considerations with respect to identity proofing or enrolment.

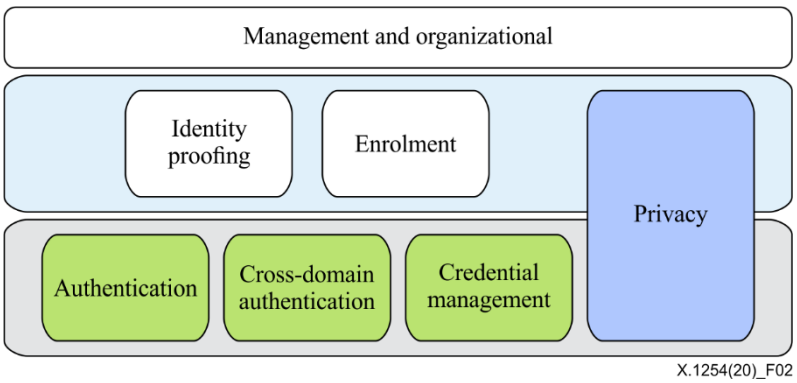

Figure 0-2 – Core aligned identity management standards

Relationship to the previous version of this Recommendation

The first edition of this Recommendation[b-ITU-T X.1254 (2012)] presented the lifecycle for digital identity transactions through three phases: enrolment and identity proofing; credential management; and entity authentication. The industry has evolved since 2012 and new concepts and approaches have emerged, such as password-free authentication and step-up authentication. As such, the industry has moved from the concept of a level of assurance (LoA) as a single ordinal that drives implementation-specific requirements. Instead, by combining appropriate business and privacy risk management side-by-side with mission need, implementers will select identity assurance levels (IALs), authentication assurance levels (AALs) and federation assurance levels (FALs) as distinct options. This Recommendation focuses on AALs. IALs and FALs lie outside the scope of this Recommendation.

Recommendation ITU-T X.1254

Entity authentication assurance framework

1 Scope

This Recommendation provides a framework for managing entity authentication assurance (EAA) in a given context. In particular, it:

– establishes three entity authentication assurance levels (AALs);

– gives guidelines for understanding these entity AALs;

– specifies criteria and guidelines for achieving identified levels of EAA;

– provides guidance for comparing and mapping across authentication assurance schemes;

– provides guidance for exchanging the results of authentication that are based on specific assurance levels; and

– provides guidance concerning controls that should be used to mitigate authentication threats, based on a risk assessment.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 assertion [b-ITU-T X.1252]: A statement made by an entity without accompanying evidence of its validity.

NOTE – The meaning of the terms 'claim' and 'assertion' are generally agreed to be somewhat similar, but with slightly different meanings. For the purposes of this Recommendation, an assertion is considered to be a stronger statement than a claim.

3.1.2 authentication [b-ISO/IEC 18014-2]: Provision of assurance of the claimed identity of an entity.

3.1.3 authentication factor [b-ISO/IEC 19790]: Piece of information and/or process used to authenticate or verify the identity of an entity.

NOTE – Authentication factors are divided into four categories:

– something an entity has (e.g., device signature, passport, hardware device containing a credential, private key);

– something an entity knows (e.g., password, PIN);

– something an entity is (e.g., biometric characteristic); or

– something an entity typically does (e.g., behaviour pattern).

3.1.4 authentication protocol [b-ISO/IEC 29115]: Defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

3.1.5 claim [b-ITU-T X.1252]: To state as being the case, without being able to give proof.

NOTE – The meaning of the terms 'claim' and 'assertion' are generally agreed to be somewhat similar, but with slightly different meanings. For the purposes of this Recommendation, an assertion is considered to be a stronger statement than a claim.

3.1.6 context [b-ITU-T X.1252]: An environment with defined boundary conditions in which entities exist and interact.

3.1.7 credential [b-ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

NOTE – See Appendix I for additional characteristics of a credential.

3.1.8 entity [b-ITU-T X.1252]: Something that has separate and distinct existence and that can be identified in a context.

NOTE – For the purposes of this Recommendation, entity is also used in the specific case of something that is claiming an identity.

3.1.9 identity; partial identity [b-ISO/IEC 24760-1]: Set of attributes related to an entity.

NOTE – Within a particular context, an identity can have one or more identifiers to allow an entity to be uniquely recognized within that context.

3.1.10 identity information verification [b-ISO/IEC 29115]: Process of checking identity information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness and binding to the entity.

3.1.11 identity proofing [b-ISO/IEC 29115]: Process by which the registration authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance.

3.1.12 man-in-the-middle attack [b-ISO/IEC 29115]: Attack in which an attacker is able to read, insert and modify messages between two parties without their knowledge.

3.1.13 multifactor authentication [b-ISO/IEC 19790]: Authentication with at least two independent authentication factors.

3.1.14 mutual authentication [b-ISO/IEC 29115]: Authentication of identities of entities which provides both entities with assurance of each other's identity.

3.1.15 non-repudiation [b-ITU-T X.1252]: The ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action.

3.1.16 phishing [b-ISO/IEC 29115]: Scam by which an email user is duped into revealing personal or confidential information which the scammer can then use illicitly.

3.1.17 repudiation [b-ITU-T X.1252]: Denial in having participated in all or part of an action by one of the entities involved.

3.1.18 risk assessment [b-ISO/IEC 27000]: Overall process of risk identification, risk analysis and risk evaluation.

3.1.19 shared secret [b-ISO/IEC 29115]: Secret used in authentication that is known only to the entity and the verifier.

3.1.20 transaction [b-ISO/IEC 29115]: Discrete event between an entity and service provider that supports a business or programmatic purpose.

3.1.21 verification [b-ISO/IEC 29115]: Process of checking information by comparing the provided information with previously corroborated information.

3.1.22 verifier [b-ISO/IEC 29115]: Actor that corroborates identity information.

NOTE – The verifier can participate in multiple phases of the entity authentication assurance framework and can perform credential verification and/or identity information verification.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 credential service provider (CSP): A trusted actor that issues or manages credentials.

NOTE – This definition is based on that in [b-ISO/IEC 29115].

3.2.2 entity authentication assurance (EAA): A degree of confidence reached in the authentication process that the entity is what it is, or is expected to be.

NOTE 1 – The confidence is based on the degree of confidence in the binding between the entity and the identity that is presented.

NOTE 2 – This definition is based on that of authentication assurance given in [b-ITU-T X.1252].

3.2.3 identifier: One or more attributes that uniquely characterize an entity in a specific context.

NOTE – This definition is based on that in [b-ITU-T X.1252].

3.2.4 registration authority (RA): A trusted actor that establishes or vouches for the identity of an entity to a credential service provider (CSP).

NOTE – This definition is based on that in [b-ISO/IEC 29115].

3.2.5 relying party (RP): Actor that relies on an identity assertion or claim.

NOTE – This definition is based on that in [b-ISO/IEC 29115].

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAL Authentication Assurance Level

CSP Credential Service Provider

EAA Entity Authentication Assurance

FAL Federation Assurance Level

FIDO Fast Identity On-line

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol-Secure

IAL Identity Assurance Level

IdM Identity Management

IDP Identity Provider

LoA Level of Assurance

MAC Media Access Control

MITM Man-In-The-Middle

MITB Man-In-The-Browser

OAuth Open Authentication

OpenID Open Identity

OTP One-Time Password

PIA Privacy Impact Assessment

PII Personally Identifiable Information

PIN Personal Identification Number

RA Registration Authority

RP Relying Party

SAML Security Assertion Markup Language

TLS Transport Layer Security

URL Uniform Resource Locator

5 Conventions

This Recommendation applies the following verbal forms for the expression of provisions:

a) "shall" indicates a requirement;

b) "should" indicates a recommendation;

c) "may" indicates a permission;

d) "can" indicates a possibility or a capability.

6 Digital authentication process flow

6.1 General

Digital identity is the unique representation of an entity engaged in an online transaction. In its simplest form, digital authentication involves verification, to some degree of confidence, of an entity's claimed identity for the purpose of granting it access to an online service. A registered entity attempts to authenticate an online service by demonstrating possession of an authenticator, also known as a credential, with which they were issued at the time of registration. The online service – also known as a relying party (RP) in the transaction – then makes an attempt to verify the validity of the authenticator with the identity provider (IDP) or the credential service provider (CSP) or verifier. The entity is granted access to the online service after its credential has been verified by the CSP or verifier.

Figure 6-1 illustrates the following digital authentication process flow:

1. an entity accesses an online service of an RP;
2. the RP redirects the entity to the CSP for authentication;
3. the CSP verifies the entity's possession of the registered authenticator(s);
4. the CSP sends an authentication assertion to the RP to assert the entity's authentication status;
5. an authenticated session is established between the entity and the RP.

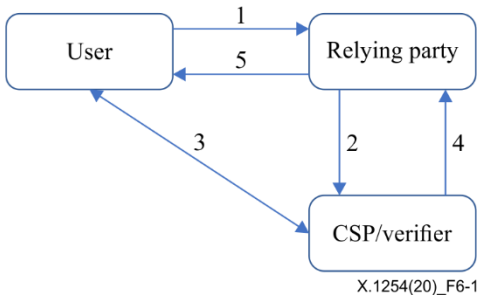

Figure 6-1 – Digital authentication process flow

Illustrating the digital authentication process flow in this manner provides a methodology for understanding the risks associated with the various roles and functions involved in digital authentication.

Although an RP may have its own identity management (IdM) solution and acts as its own CSP, this Recommendation presents the RP and the CSP as distinct roles. However, in either case, the functions of each role are the same.

In addition, Figure 6-1 combines the roles of the CSP and the verifier. Even though CSPs typically perform the verification function, in some cases, a CSP may use a separate verifier.

The digital authentication process flow described here assumes that entities have already enrolled with a CSP and have one or more registered authenticators. The processes for enrolment and registration lie outside the scope of this Recommendation.

6.2 Digital identity assurance

It is necessary to understand how the services that address the phases and functional components of the digital identity lifecycle interact to support trust and the overall confidence in an online transaction. Such trust is typically expressed as the level of confidence through degrees, or levels of assurance. This Recommendation provides requirements and guidance for the digital identity authentication assurance phase and component functions of an overall digital identity and authentication assurance framework. Figure 6-2 illustrates the components, assurance description and functional activities for a set of core, aligned IdM documents to address assurance and controls in such an overall digital identity framework.

Assurance component	Descriptions	Activities

IA *Identity assurance*	Robustness of the identity proofing process and the binding between the authenticator and the identity-proofed individual.	• Identity proofing
		  • Resolution
		  • Validation
		  • Verification
		• Enrollment
		• Binding

AA *Authentication assurance*	Confidence that a given claimant is the same as the previously authenticated subscriber.	• Authentication
		• Credential management
		  • Credential issuance
		  • Credential suspension, revocation, and/or destruction
		  • Credential renewal and/or replacement

FA *Federation Assurance*	Combines aspects of the federation model, assertion protection strength, and assertion presentation	• Key management • Runtime decisions • Attribute management

X.1254(20)_F6-2

Figure 6-2 – Digital identity assurance levels

Identity assurance: This assurance consists of the processes put in place to verify a subject's association with their real-world identity. Identity assurance is addressed in [b-ISO/IEC TS 29003].

Authentication assurance: Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. This assurance consists of the processes used to verify that a claimed identity is the same as the one that participated in the registration process and has previously been authenticated by the system.

Federation assurance: This assurance consists of the process(es) used to communicate, protect and validate identity assertions being provided across different security domains. Identity federation is the sharing of online identity and authentication information between two or more parties.

Identity assurance components and activities that support federation assurance lie outside the scope of this edition of this Recommendation.

6.3 Roles

6.3.1 General

As a risk-centred model, the digital authentication process flow helps identify the threat categories associated with three primary roles: CSPs, RPs and entities.

6.3.2 Online service providers

Online service providers are organizations that offer online services, applications and information that require restricted access, such as banking services, healthcare provider services and retailers. Depending on how the service is implemented, online service providers can play one or more of the following roles:

- CSP;
- identity service provider;
- verifier;
- RP.

6.3.3 Credential service provider

CSPs are responsible for verifying a credential (i.e., an authenticator) as presented by the entity. The process, and degree of rigour, by which they do this is determined by the level of risk associated with the online transaction and the environment in which the identity will be used. The CSP function can either be performed by an online service provider's in-house IdM system, or by a third-party identity service. Additionally, the CSP role is often responsible for credential management activities.

6.3.4 Identity service provider

Identity service providers are responsible for identity proofing an entity's claimed identity and ensuring that this claimed identity is associated with the credential used by the entity. The process and degree of rigour by which they do this is determined by the level of risk associated with the online transaction and the environment in which the identity will be used. The IDP may also be responsible for registering and enrolling entities in specific programs and services. The risks and controls that address these IDP component functions lie outside the scope of this Recommendation.

Additionally, the IDP may play the role of the CSP. Since this Recommendation focuses on authentication and credential management, where the term CSP is used, it is intended also to represent an IDP playing that role in a transaction.

6.3.5 Verifier

Verifiers are responsible for confirming the entity's identity by verifying the entity's possession and control of an authenticator(s), using an authentication protocol. To do this, the verifier may also need to validate credentials that link the authenticator(s) to the entity's identifier and check their status. The role of verifier is often played by the CSP or IDP providing credential services.

6.3.6 Relying party

RPs accept (rely upon) and utilize entity authentication status assertions from their own IdM services or from external CSPs. RPs must be able to trust the identity information they receive from these services in order to make risk-based decisions about whether to allow specific entities access to their online services and products.

6.3.7 Entities

For the purposes of this Recommendation, entities are the users of the services offered by online service providers.

Entities are responsible for protecting their identities and digital credentials from fraud and misuse, and for using their credentials in the manner for which they are intended.

6.4 Authentication processes components

This Recommendation provides a methodology for service providers to identify the threats and risks associated with their service, based on their role(s) – as described in clause 6.3 – and enabling technologies.

To facilitate the assessment of the specific risks and threats associated with an online service, it is important to identify which functions and supporting technologies are involved in the authentication process.

Process components include:

- authenticators, e.g., memorized secrets (such as passwords), one-time password (OTP) devices, smart cards, digital certificates and biometrics (such as fingerprints);
- client and server software;
- communication and authentication protocols, e.g., hypertext markup language (HTML), security assertion markup language (SAML), transport layer security (TLS), open authentication (OAuth) and open identity (OpenID).

Authentication transactions are subject to transaction compromise attacks, which target vulnerabilities associated with one or more of the components listed in the previous paragraph. Most authentication technologies, including hardware, software and communication protocols, have specific, associated threats and vulnerabilities. As part of their risk assessment activities, online service providers shall consider the vulnerabilities associated with each component. Clause 8 describes specific threat categories, risks and controls.

6.4.1 Authenticators

An authenticator is something an entity possesses and controls that is used to authenticate the entity's identity. An entity may have more than one associated authenticator. Authentication factors include something you know, like a password; something you have, like a smartcard; and something you are, like a biometric. The strength of an authentication transaction is increased by the use of one or more different factors.

An online service provider shall consider their service's risk profile when selecting which authenticators are acceptable for authentication of that service. Additionally, an RP shall consider their service's assurance requirements before accepting services from a CSP.

Types of authenticators include:

- memorized secrets;
- look-up secrets;
- out-of-band devices;
- single factor OTP devices;
- multi-factor OTP devices;
- single factor cryptographic software;
- single factor cryptographic devices;
- multi-factor cryptographic software;

- multi-factor cryptographic devices.

6.4.2 Authenticator

An object or data structure that authoritatively binds an identity – via an identifier or identifiers – and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber. While common usage often assumes that the entity maintains the authenticator, this Recommendation also uses the term to refer to electronic records maintained by the CSP that establish a binding between the subscriber's authenticator(s) and identity. The most common form of authenticator is a username and associated user record that is bound to a password or other authenticator.

7 Apply risk management to the authentication assurance framework

7.1 General

An effective IdM system depends on understanding the levels of risk associated with the types of online services offered by the organization. To understand these risks, online service providers shall consider their specific role(s) within the framework; the nature of their users; and, the types of data and transactions processed by their applications.

Application of structured risk management methodology will result in the following: the identification of risks and threats; decisions as to how they should be treated; as well as the inputs needed to select and implement controls. In the area of IdM, specific guidelines exist to help organizations understand how those levels of risk equate to levels of assurance; i.e., to the relative degrees of confidence in the integrity of online identities.

Online service providers shall employ a risk management methodology and develop a plan to manage their digital authentication-related risks.

The scope of the digital identity-associated risk assessment shall consider, at a minimum, the type and level of impact associated with each identified risk. The likelihood of each risk occurring may also be considered.

7.2 Authentication risk

When considering authentication risk, the fundamental question is what is at stake if authentication fails, i.e., what the impact is if access is granted to an entity that is not the rightful owner of the credential and associated account.

Online service providers shall consider the following when assessing their risks associated with authentication failure.

- Data – Identification o the types of data that is processed and protected within the system boundaries is a key element in determining what is at stake. Types of data include personally identifiable information (PII), financial, proprietary, publicly available and highly sensitive.
- Users – Identification and understanding of the users of a system or an enterprise is fundamental to be able to identify and classify specific risks. Categories of users include internal, external and privileged. Organizations should also consider whether their users are bound by any contractual, legal or other types of agreements.
- Attack motivations – By first defining its users and data types, an organization will be in a better position to understand attack motivations, e.g., if the system processes and protects bank account information, an attacker may be motivated to fraudulently access the system for financial gain.

Online service providers shall choose controls and other threat mitigation options based on assessed risks.

8 Threat categories, risks and controls

This clause provides a threat and control catalogue organized around threat categories. Identity service providers should identify the specific threat categories they are subject to, based on their authentication-related role(s) and service(s). The controls are grouped by the following threat categories:

- authenticator compromise;
- transaction compromise;
- CSP impersonation;
- entity impersonation;
- authentication service compromise.

RPs and CSPs share responsibility for protection against all authentication threats. The roles and responsibilities within an authentication transaction shall be clearly established and agreed upon by all parties.

Table 8-1 presents authentication threat categories and the roles typically assigned responsibility for mitigating those threats.

Table 8-1 – Roles and thread categories

Role	Threat categories
RPs	• Verifier impersonation • Transaction compromise • Privacy • Federation
CSPs	• Verifier impersonation • Transaction compromise • Subscriber impersonation • Authenticator compromise • Authentication service compromise • Privacy • Federation

8.1 Assurance levels

In this Recommendation, authentication is the process by which a claimed identity is verified for the purpose of conducting an online transaction. Increased rigour in the processes used to verify claimed identities results in increased confidence that the authenticated identity represents the intended subject of that identity. Authentication assurance is a measure of that confidence, and systems – or schemas – exist that establish a series of relative levels of confidence, known as AALs.

This Recommendation describes an authentication assurance model that is based on the concept of identifying and mitigating threats and risks to authentication transactions. In many instances, organizations, national bodies and communities of interest may choose to establish an AAL schema that groups risks, threats and controls relevant to the environments in which they operate. Doing so provides many tangible benefits, including establishment of requirements for participation in transactions at commonly defined levels, and the ability to create standard product packages to address community needs.

This Recommendation withdraws the concept of a level of assurance (LoA) as a single ordinal that drives implementation-specific requirements. Rather, by combining appropriate business and privacy risk management side-by-side with mission need, implementers will select IAL, AAL and federation

assurance level (FAL) as distinct options. While many systems will have the same numerical level for each of IAL, AAL and FAL, this is not a requirement and implementers should not assume they will be the same in any given system.

The components of identity assurance detailed in these guidelines are as follows:

- IAL is the identity proofing process;
- AAL is the authentication process;
- FAL is the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to an RP.

The separation of these categories provides implementers flexibility in choosing identity solutions and increases the ability to include privacy-enhancing techniques as fundamental elements of identity systems at any assurance level. For example, this model supports scenarios that will allow pseudonymous interactions even when strong, multi-factor authenticators are used.

In today's environment, an organization's identity solution need not be a monolith, where one system or vendor provides all functionality. An identity services can be comprised of multiple components, allowing organizations and agencies to employ standards-based, pluggable identity solutions based on mission needs.

The three AALs define the subsets of options implementers can select based on their risk profile and the potential harm caused by an attacker taking control of an authenticator and accessing agencies' systems. The AALs are as follows.

AAL1: AAL1 provides some assurance that the entity controls an authenticator bound to the entity's account. AAL1 requires either single factor or multi-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant proves possession and control of the authenticator through a secure authentication protocol.

AAL2: AAL2 provides high confidence that the entity controls authenticator(s) bound to the entity's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Globally accepted cryptographic techniques are required at AAL2 and above.

AAL3: AAL3 provides very high confidence that the entity controls authenticator(s) bound to the entity's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication shall use a hardware-based cryptographic authenticator and an authenticator that provides verifier impersonation resistance; the same device may fulfil both these requirements. To authenticate at AAL3, claimants shall prove possession and control of two distinct authentication factors through secure authentication protocol(s). Globally accepted cryptographic techniques are required.

This edition of this Recommendation does not propose a single set of standardized, normative assurance levels. Attempting to create a single, standardized assurance structure for all communities undercuts the ability of specific communities to manage risk as appropriate to their environment. It does, however, acknowledge that these different assurance schemas exist and that identity service providers must often be able to demonstrate adherence to one or more sets of AALs.

Because AAL schemas represent increasing levels of confidence in the verification of a claimed identity, with correspondingly increasing levels of rigour in the authentication process, the control descriptions in this Recommendation use relative terms instead of discreet AALs. For those controls that can be modified to provide increased confidence, the conditions that provide the least amount of confidence are indicated by "lowest AAL(s)"; subsequently, more confidence is indicated by "higher AAL(s)"; and, the conditions that result in the most confidence are indicated by "highest AAL(s)". Table 8-2 provides a notional idea of how this convention might equate to some of the more common authentication assurance schemas. (Please note that the alignment in Table 8-2 is in no way intended to establish direct equivalency between the various schemas.)

Table 8-2 – Authentication assurance levels

AAL	Four AAL schema	Three AAL schema	Three level schema
Highest	AAL 4	AAL 3	High
Higher	AAL 3	AAL 2	Substantial
	AAL 2		
Lowest	AAL 1	AAL 1	Low

The remainder of this clause provides a superset of normative controls, grouped according to the threats they mitigate. Identity service providers shall identify the specific threats to which they are subject based on their roles and services, as described in this Recommendation. Once this is determined, and in order to be able to assess conformance to this Recommendation, identity service providers shall document the threats, and corresponding control descriptions and desired outcomes, as provided in the remainder of this clause.

8.2 Authenticator compromise

8.2.1 Authenticator compromise risks

Authenticator compromise is any attack that duplicates, tampers with, or results in the unauthorized disclosure of credential information that may be used to successfully authenticate and gain unauthorized access to an information system. Authenticator compromise can occur at any point in the IdM lifecycle. However, threats and controls that lie within the scope of this Recommendation are only intended to address authentication.

Credentials can be compromised by a number of attack vectors, including phishing, theft, credential duplication, replay attack and online or offline brute force attacks. Protecting against the risk of credential compromise is not exclusive to the controls in this threat category. It should be noted that a consequence of control failures in any of the threat categories may result in credential compromise. For example, if an authentication service provider suffers a data breach, the information obtained may be used to gain unauthorized access to the information system.

8.2.2 Authenticator compromise controls

Table 8-3 lists authenticator compromise controls.

Table 8-3 – Authenticator compromise controls

CTRL #	Control description	Desired outcome
AC-1	For the highest AAL, authentication should use a hardware-based cryptographic authenticator and an authenticator that provides verifier-impersonation resistance – the same device may fulfil both these requirements.	The appropriate authenticators are used to achieve the desired AAL.
AC-2	For the highest AAL, claimants should prove possession and control of two distinct authentication factors through secure authentication protocol(s).	The appropriate authentication protocols are followed to achieve the desired AAL.
AC-3	Multifactor authenticators used at the highest AAL should be validated to extent required by an approved cryptographic module verification program.	Authenticator cryptography is validated to the extent necessary to achieve the desired AAL.

Table 8-3 – Authenticator compromise controls

CTRL #	Control description	Desired outcome
AC-4	Authenticators procured by IDPs should be validated to meet the requirements of approved cryptographic module verification program.	Approved cryptography is used.
AC-5	The verifier should implement controls to protect against online guessing attacks if applicable to the authenticator type.	The verifier implements controls to protect authenticators against online guessing attacks.
AC-6	Unless otherwise specified in the description of a given authenticator, the verifier should limit consecutive failed authentication attempts on a single account to no more than 100.	The verifier implements controls to protect authenticators against online guessing attacks.
AC-7	Cryptographic authenticators should use approved cryptography.	Approved cryptography is used.
AC-8	If more than one authenticator is being used to authenticate, at least one should be replay resistant.	Authenticators are protected against replay attack.
AC-9	All cryptographic device authenticators should be replay resistant.	Controls are employed to protect authenticators from replay attack.
AC-10	Relevant side-channel attacks should be determined by a risk assessment performed by the CSP.	The appropriate risk assessments are performed by the CSP.
AC-11	Communication between the claimant and verifier (using the primary channel in the case of an out-of-band authenticator) should be via an authenticated protected channel.	Communication between the claimant and verifier is protected.
AC-12	Single factor cryptographic devices used at the highest AAL should be validated to the extent required by an approved cryptographic module verification program.	Authenticator cryptography is validated to the extent necessary to achieve the desired AAL.
AC-13	When a device such as a smartphone is used in the authentication process, the unlocking of that device (typically done using a personal identification number (PIN) or biometric) should not be considered one of the authentication factors.	The appropriate authenticators are used to achieve the desired AAL.
AC-14	The biometric system should allow no more than 10 consecutive failed authentication attempts. Once that limit has been reached, the biometric authenticator should either: • impose a delay of at least 30 s before the next attempt, increasing exponentially with each successive attempt (e.g., 1 min before the following failed attempt, 2 min before the second following attempt), or • disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/password if it is not already a required factor) if such an alternative method is already available.	The biometric system implements controls to protect authenticators against guessing attacks.

8.3 Transaction compromise

8.3.1 Transaction compromise risks

Transaction compromise is an attack that disrupts the confidentiality or availability of data in transit as it is being exchanged between two parties. Common attacks that can result in transaction compromise are man-in-the-middle (MITM), man-in-the-browser (MITB), eavesdropping and session hijacking.

8.3.2 Transaction compromise controls

Table 8-4 lists transaction compromise controls.

Table 8-4 – Transaction compromise controls

CTRL #	Control description	Desired outcome
TC-1	In situations where the verifier and CSP are separate entities, communications between the verifier and CSP should occur through a mutually authenticated secure channel (such as a client-authenticated TLS connection) using approved cryptography.	Communications between the verifier and CSP are protected.
TC-2	A session secret should be shared between the subscriber's software and the service being accessed.	Session secrets are implemented and protected.
TC-3	Uniform resource locators (URLs) or HTTP POST [b-IETF RFC 7231] content should contain a session identifier that should be verified by the RP to ensure that actions taken outside the session do not affect the protected session.	Session identifiers are verified by the RP.
TC-4	The secret should be presented directly by the subscriber's software or possession of the secret should be proven using a cryptographic mechanism.	Session secrets are generated randomly, implemented appropriately and properly disposed of after use.
TC-5	Secrets used for session binding should not be available to insecure communications between the host and subscriber's endpoint. Authenticated sessions should not fall back to an insecure transport, such as from hypertext transfer protocol-secure (HTTPS) to hypertext transfer protocol (HTTP), following authentication.	The transmission of session secrets is protected.
TC-6	Secrets for session bindings should be generated by the session host during an interaction, typically immediately following user authentication.	Session secrets are generated randomly, implemented appropriately and properly disposed of after use.
TC-7	Secrets used for session bindings should be generated by an approved random bit generator and contain at least 64 bits of entropy.	Session secrets are generated randomly, implemented appropriately and properly disposed of after use.
TC-8	Secrets used for session bindings should be erased or invalidated by the session subject when the user logs out.	Session secrets are generated randomly, implemented appropriately and properly disposed of after use.
TC-9	Secrets used for session bindings should be sent to and received from the device using an authenticated protected channel.	The transmission of session secrets is protected.

Table 8-4 – Transaction compromise controls

CTRL #	Control description	Desired outcome
TC-10	Secrets used for session bindings should time out and not be accepted after CSP defined times.	The transmission of session secrets is protected.
TC-11	The secret used for session binding should be generated by the session host in direct response to an authentication event.	Session secrets are generated randomly, implemented appropriately and properly disposed of after use.
TC-12	Browser cookies should be tagged to be accessible only in HTTPS sessions.	The transmission of session secrets is protected.
TC-13	Browser cookies should be accessible to the minimum practical set of hostnames and paths.	The transmission of session secrets is protected.
TC-14	Continuity of authenticated sessions should be based upon the possession of a session secret issued by the verifier at the time of authentication and optionally refreshed during the session.	Session secrets are generated randomly, implemented appropriately and properly disposed of after use.
TC-15	If comparison is performed centrally, all transmission of biometrics should be over the authenticated protected channel.	The transmission of biometric information is protected.
TC-16	An authenticated protected channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and verifier should be established.	Communications between the verifier and endpoints are protected.

8.4 Verifier impersonation

8.4.1 Verifier impersonation risks

Verifier impersonation is an attack where an entity interacts with a counterfeit verifier and is tricked into revealing credential information. The information obtained by an attacker would pose a significant risk to either the subscriber impersonation or credential compromise threat categories. One of the most common attacks associated with verifier impersonation is phishing. An attacker is able to lure the entity into transmitting subscriber credential information to an untrusted client, server or service and use the credential information obtained to gain unauthorized access to the information system.

8.4.2 Verifier impersonations controls

Table 8-5 lists verifier impersonation controls.

Table 8-5 – Verifier impersonation controls

CTRL #	Control description	Desired outcome
VI-1	Verifiers should be validated to meet the requirements of an approved cryptographic module verification program.	Approved cryptography is used.
VI-2	A verifier impersonation-resistant authentication protocol should establish an authenticated protected channel with the verifier.	Authenticator output is protected.

Table 8-5 – Verifier impersonation controls

CTRL #	Control description	Desired outcome
VI-3	An authenticated protected channel should strongly and irreversibly bind a channel identifier that was negotiated in establishing the authenticated protected channel to the authenticator output.	Authenticator output is protected.
VI-4	The verifier should validate the signature or other information used to prove verifier impersonation resistance.	Verifiers perform validation effectively.
VI-5	Approved cryptographic algorithms should be used to establish verifier impersonation resistance where it is required.	Approved cryptography is used.
VI-6	Keys used establish verifier impersonation resistance should provide at least the minimum security strength specified in an applicable cryptographic standard.	Verifiers are not impersonated.
VI-7	To be considered verifier compromise resistant, public keys stored by the verifier should be associated with the use of approved cryptographic algorithms and should provide at least the minimum security strength specified in an applicable cryptographic standard.	Verifiers are not compromised.
VI-8	Verifier compromise resistant secrets should use approved hash algorithms and the underlying secrets should have at least the minimum security strength specified in an applicable cryptographic standard.	Verifiers are not compromised.
VI-9	Authenticators that involve the manual entry of an authenticator output, such as out-of-band and OTP authenticators, should not be considered verifier impersonation-resistant because the manual entry does not bind the authenticator output to the specific session being authenticated.	Authenticators that require manual entry are not used to protect against verifier impersonation.

8.5 Subscriber impersonation

8.5.1 Subscriber impersonation risks

Subscriber Impersonation is an attack that involves the falsification of a legitimate identity to subvert the authentication process and gain unauthorized access to a network or information system. Common subscriber impersonation attacks include spoofing and session hijacking. An example of a spoofing attack would be when an attacker impersonating the RP spoofs a media access control (MAC) address that belongs to an authenticated device that gains unauthorized access to the network. Another example, masquerading, is an attacker who impersonates a legitimate user by providing falsified or stolen evidence and is able to successfully follow a credential reset protocol.

8.5.2 Subscriber impersonation controls

Table 8-6 lists of subscriber impersonation controls.

Table 8-6 – Subscriber impersonation controls

CTRL #	Control description	Desired outcome
SI-1	The result of an authentication process is an identifier that should be used each time that a subscriber authenticates to that RP.	Authenticator(s) are bound to the appropriate subscriber.
SI-2	To satisfy the requirements of a given AAL, a claimant should be authenticated with at least a given level of strength to be recognized as a subscriber.	The subscriber is authenticated using the appropriate authenticator(s) at the proper level of strength to achieve a desired AAL.
SI-3	All authentication and reauthentication processes should demonstrate authentication intent from at least one authenticator.	Authenticator intent is demonstrated.
SI-4	CSPs should provide subscriber instructions on how to appropriately protect the authenticator against theft or loss.	The subscriber is able to recover authenticator(s) without circumventing the desired AAL.
SI-5	Authentication at the lowest AAL should occur by the use of any of the following authenticator types: • memorized secret; • look-up secret; • out-of-band devices; • single factor OTP device; • multi-factor OTP device; • single factor cryptographic software; • single factor cryptographic device; • multi-factor cryptographic software; • multi-factor cryptographic device	The subscriber is authenticated using the appropriate authenticator(s) at the proper level of strength to achieve a desired AAL.
SI-6	Authentication at higher AAL should occur by the use of either a multi-factor authenticator or a combination of two single factor authenticators. When a multi-factor authenticator is used, any of the following may be used: • multi-factor OTP device; • multi-factor cryptographic software; • multi-factor cryptographic device	The subscriber is authenticated using the appropriate authenticator(s) at the proper level of strength to achieve a desired AAL.
SI-7	When a combination of two single factor authenticators is used, it should include a memorized secret authenticator and one possession-based (i.e., "something you have") authenticator from the following list: • look-up secret; • out-of-band device; • single factor OTP device; • single factor cryptographic software; • single factor cryptographic device	The subscriber is authenticated using the appropriate authenticator(s) at the proper level of strength to achieve a desired AAL.

Table 8-6 – Subscriber impersonation controls

CTRL #	Control description	Desired outcome
SI-8	Authentication at the highest AAL should occur by the use of one of a combination of authenticators. Possible combinations are drawn from: • multi-factor cryptographic device; • single factor cryptographic device used in conjunction with memorized secret; • multi-factor OTP device (software or hardware) used in conjunction with a single factor cryptographic device; • multi-factor OTP device (hardware only) used in conjunction with a single factor cryptographic software; • single factor OTP device (hardware only) used in conjunction with a multi-factor cryptographic software authenticator; • single factor OTP device (hardware only) used in conjunction with a single factor cryptographic software authenticator and a memorized secret	The subscriber is authenticated using the appropriate authenticator(s) at the proper level of strength to achieve a desired AAL.
SI-9	The CSP should provide a mechanism to revoke or suspend the authenticator immediately upon notification from subscriber that loss or theft of the authenticator is suspected.	Invalid authenticators cannot be used to successfully authenticate an individual.
SI-10	To facilitate secure reporting of the loss, theft, or damage to an authenticator, the CSP should provide the subscriber with a method of authenticating to the CSP using a backup or alternate authenticator. This backup authenticator should be either a memorized secret or a physical authenticator.	The subscriber is able to recover authenticator(s) without circumventing the desired AAL.
SI-11	The suspension should be reversible if the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of an authenticator suspended in this manner.	The subscriber is able to recover authenticator(s) without circumventing the desired AAL.
SI-12	If and when an authenticator expires, it should not be usable for authentication.	Invalid authenticators cannot be used to successfully authenticate an individual.
SI-13	The CSP should require subscribers to surrender or destroy any physical authenticator containing attribute certificates signed by the CSP as soon as practical after an authenticator becomes invalid either by expiration, revocation, termination, renewal or other means as defined by the CSP.	Invalid authenticators cannot be used to successfully authenticate an individual.

Table 8-6 – Subscriber impersonation controls

CTRL #	Control description	Desired outcome
SI-14	CSPs should revoke the binding of authenticators promptly when an online identity ceases to exist, when requested by the subscriber, or when the CSP determines that the subscriber no longer meets its eligibility requirements.	Invalid authenticators cannot be used to successfully authenticate an individual.
SI-15	Biometrics should be used only as part of multi-factor authentication with a physical authenticator (something you have).	Biometrics are used appropriately as authenticators.
SI-16	At higher AAL, the CSP should bind at least one, and should bind at least two, physical (something you have) authenticators to a subscriber's online identity, in addition to a memorized secret or one or more biometrics.	Authenticator(s) are bound to the appropriate subscriber.
SI-17	For higher AAL, if enrolment and binding cannot be completed in a single physical encounter or electronic transaction, the following methods should be used to ensure that the same party acts as the applicant throughout the processes: For remote transactions: 1. applicants should identify themselves in each new transaction by presenting a temporary secret that was either established during a prior transaction or sent to the applicant's phone number, email address or postal address of record; 2. long-term authenticator secrets should only be issued to the applicant within a protected session. For in-person transactions: 1. applicants should identify themselves in person by either using a secret as described under remote transaction entry 1 in the previous paragraph or through use of a biometric that was recorded during a prior encounter. 2. Temporary secrets should not be reused. 3. If the CSP issues long-term authenticator secrets during a physical transaction, then they should be loaded locally on to a physical device that is issued in person to the applicant or delivered in a manner that confirms the address of record.	Authenticator(s) are bound to the appropriate subscriber.
SI-18	When binding an additional authenticator to a subscriber's account, the CSP should first require the subscriber to authenticate to at least the AAL at which the new authenticator will be used.	Authenticator(s) are bound to the appropriate subscriber.

Table 8-6 – Subscriber impersonation controls

CTRL #	Control description	Desired outcome
SI-19	For higher AAL, if a subscriber loses all authenticators of a factor necessary to complete multifactor authentication, that subscriber should repeat the identity proofing process.	The subscriber is able to recover authenticator(s) without circumventing the desired AAL.
SI-20	When replacing a lost authentication factor for higher AAL, the CSP should require the claimant to authenticate using an authenticator of any remaining factor to confirm binding to the existing identity.	The subscriber is able to recover authenticator(s) without circumventing the desired AAL.
SI-21	Periodic reauthentication of sessions should be performed to confirm the continued presence of the subscriber at an authenticated session.	The subscriber is required to reauthenticate periodically with the proper authenticator(s) at strength necessary to achieve a desired AAL.
SI-22	Periodic reauthentication of subscriber sessions should be performed. (a) At the lowest AAL, reauthentication of the subscriber should be repeated at least once every 30 days during an extended usage session, regardless of user activity. (b) At the lowest AAL, the session should be terminated (i.e., logged out) when this time limit is reached. (c) At higher AAL, reauthentication of the subscriber should be repeated at least once every 12 h during an extended usage session, regardless of user activity. (d) At higher AAL, reauthentication of the subscriber should be repeated following any period of inactivity lasting 30 min or more. (e) At higher AAL, the session should be terminated (i.e., logged out) when either of these time limits is reached. (f) At the highest AAL, authentication of the subscriber should be repeated at least once every 12 h during an extended usage session, regardless of user activity. (g) At the highest AAL, reauthentication of the subscriber should be repeated following any period of inactivity lasting 15 min or more. (h) At the highest AAL, the session should be terminated (i.e., logged out) when either of time limits (f) or (g) is reached. (i) At the highest AAL, periodic reauthentication of subscriber sessions should be performed using all original authentication factors.	The subscriber is required to reauthenticate periodically with the proper authenticator(s) at strength necessary to achieve a desired AAL.

Table 8-6 – Subscriber impersonation controls

CTRL #	Control description	Desired outcome
SI-23	A session should not be extended based on presentation of the session secret alone.	The subscriber is required to reauthenticate periodically with the proper authenticator(s) at strength necessary to achieve a desired AAL.
SI-24	When a session has been terminated, due to a time-out or other action, the user should be required to establish a new session by authenticating again.	The subscriber is required to reauthenticate periodically with the proper authenticator(s) at strength necessary to achieve a desired AAL.
SI-25	Session secrets should be non-persistent. That is, they should not be retained across a restart of the associated application or a reboot of the host device.	The subscriber is required to reauthenticate periodically with the proper authenticator(s) at strength necessary to achieve a desired AAL.

8.6 Authentication service compromise, risks and controls

8.6.1 Authentication service compromise risks

Authentication service compromise is an attack on the entity providing the identity service that renders it invalid, inaccurate, unavailable or unable to function as intended. Any exploited weakness in the entity's information system control environment has the potential to compromise the authentication service. An example is when an attacker is able to exploit a software vulnerability that was not patched and is able to gain unauthorized privileged access to the authentication service's information system.

8.6.2 Authentication service compromise controls

Table 8-7 lists of authentication service compromise controls.

Table 8-7 – Authentication service compromise controls

CTRL #	Control description	Desired outcome
ASC-1	The CSP should employ appropriately tailored security controls for a given level of security as specified in [b-ISO/IEC 27002] or equivalent standard.	The integrity of the authentication service is protected from compromise.
ASC-2	The CSP should ensure that the minimum assurance-related controls are satisfied given the context of overall system risk.	The integrity of the authentication service is protected from compromise.
ASC-3	If comparison is performed centrally, biometric revocation, referred to as biometric template protection in [b-ISO/IEC 24745], should be implemented.	The authentication service protects biometric information.
ASC-4	Authentication intent should be established by the authenticator itself, although multi-factor cryptographic devices may establish intent by re-entry of the other authentication factor on the endpoint with which the authenticator is used.	Authentication intent is only established by the authenticator.

Table 8-7 – Authentication service compromise controls

CTRL #	Control description	Desired outcome
ASC-5	Throughout the digital identity lifecycle, CSPs should maintain a record of all authenticators that are or have been associated with each identity.	Authenticator information is recorded and maintained.
ASC-6	The CSP or verifier should also maintain the information required for throttling authentication attempts when required.	Authenticator information is recorded and maintained.
ASC-7	The record created by the CSP should contain the date and time the authenticator was bound to the account.	Authenticator information is recorded and maintained.
ASC-8	Authenticators should be bound to subscriber accounts by either: • issuance by the CSP as part of enrolment; or • associating a subscriber-provided authenticator that is acceptable to the CSP.	Authenticators are bound appropriately to subscriber accounts.
ASC-9	When any new authenticator is bound to a subscriber account, the CSP should ensure that the binding protocol and the protocol for provisioning the associated key(s) are done at a level of security commensurate with the AAL at which the authenticator will be used.	Authenticators are bound appropriately to subscriber accounts.
ASC-10	Binding of multifactor authenticators should require multifactor authentication or association with the session in which identity proofing has just been completed in order to bind the authenticator.	Authenticators are bound appropriately to subscriber accounts.

8.7 Privacy, risks and controls

8.7.1 Privacy risks

Digital authentication supports privacy protection by mitigating risks of unauthorized access to individuals' information. At the same time, because identity proofing, authentication, authorization and federation involve the processing of individuals' information, these functions can also create privacy risks. These guidelines therefore include privacy requirements and considerations to help mitigate potential associated privacy risks.

The CSP shall conduct a privacy risk assessment for records retention. The contents of a privacy risk assessment may include the following:

1. the likelihood that record retention could create a problem for the subscriber, such as invasiveness or unauthorized access to the information;
2. the impact if such a problem did occur.

CSPs should be able to reasonably justify any response they take to identified privacy risks, including accepting the risk, mitigating the risk and sharing the risk. The use of subscriber consent is a form of sharing the risk, and therefore appropriate for use only when a subscriber could reasonably be expected to have the capacity to assess and accept the shared risk.

8.7.2 Privacy controls

Table 8-8 lists privacy controls.

Table 8-8 – Privacy controls

CTRL #	Control description	Desired outcome
P-1	An IDP should select at minimum an appropriate AAL when self-asserted PII or other personal information is made available online.	The CSP enforces privacy policies and privacy controls with respect to authentication.
P-2	The CSP should comply with its respective records retention policies in accordance with applicable laws, regulations and policies that may apply. If the CSP opts to retain records in the absence of any mandatory requirements, the CSP should conduct a risk management process, including assessments of privacy and security risks, to determine how long records should be retained and should inform the subscriber of that retention policy.	The CSP authenticates subscribers in accordance with applicable laws, regulations and policies.
P-3	Care should be taken to ensure that use of PII is limited to its original purpose for collection.	The CSP collects the minimum amount of PII to achieve the desired AAL.
P-4	If the use of PII does not fall within uses related to authentication or to comply with law or legal process, the CSP should provide notice and obtain consent from the subscriber.	The CSP authenticates subscribers in accordance with applicable laws, regulations and policies.
P-5	The IDP should conduct or publish a privacy impact assessment (PIA) to cover collection of PII and other personal information in accordance with applicable laws and regulations.	The CSP conducts PIAs.
P-6	CSPs should not use or disclose information about subscribers for any purpose other than conducting authentication, related fraud mitigation or to comply with the law or legal process, unless the CSP provides clear notice and obtains consent from the subscriber for additional uses.	The CSP authenticates subscribers in accordance with applicable laws, regulations and policies.
P-7	The CSP should employ appropriately tailored privacy controls specified in [ISO/IEC 27002] or equivalent standard.	The CSP enforces privacy policies and privacy controls with respect to authentication.
P-8	CSPs should not make consent a condition of the service.	The CSP authenticates subscribers in accordance with applicable laws, regulations and policies.
P-9	While a CSP may bind a lower AAL authenticator to a higher AAL identity, if the subscriber is authenticated at the lower AAL the CSP should not expose personal information, even if self-asserted, to the subscriber.	The CSP collects the minimum amount of PII or personal information to achieve the desired AAL.
P-10	Acceptance by the subscriber of additional uses should not be a condition of providing authentication services.	The CSP authenticates subscribers in accordance with applicable laws, regulations and policies.

Appendix I

An example of strong authentication using [b-ITU-T X.1278]

(This appendix does not form an integral part of this Recommendation.)

I.1 Introduction

The universal authentication framework [b-ITU-T X.1277] and client to authenticator protocol/universal 2-factor framework [b-ITU-T X.1278] present approaches to authentication and authentication assurance that provide strong authentication based on open, interoperable Recommendations. This appendix presents an example of strong authentication using [b-ITUT X.1278].

I.2 Threat categories

Figure I.1 highlights threats grouped into two categories:

1. Scalable attacks – whether 1 000 or 1 000 000 targets are attacked does not have an impact on the attack costs.
    a. Remote attacks on servers and password theft. This attack is very serious because users cannot protect against it – the RPs have to do it. However, users can make it worse: if they share passwords across multiple RPs, the least secure RP could be hacked affecting all others.
    b. Remote attacks on lots of user devices. For example, trying to steal data from the device to impersonate the user.
    c. Remote attacks can also lead to misuse of data on user devices for user impersonation.
    d. Remote attacks on lots of user devices to misuse a strongly authenticated session. This is known as a MITB attack.

It is interesting to note that smartcards alone do not protect against the misuse of credentials, as the smartcard cannot know whether a PIN was entered by the user or injected by some malware that had previously phished the PIN from the user.

2. Physical attacks – where physical access to the device is required. Physical attacks are not scalable as stealing (active) smartphones has significant costs per target.
    a. Physical attacks on user devices to steal data for impersonation.
    b. Physical attacks on user devices to misuse them for impersonation.

I.3 [b-ITU-T X.1278] enables "high-assurance strong authentication"

High-assurance strong authentication means:

1. use of two or more factors;
2. at least one factor leverages public key cryptography;
3. not susceptible to phishing, MITM or other attacks targeting credentials.

Key differentiators of the fast identity on-line (FIDO) approach include:

- no shared secrets – uses what you have (e.g., hardware devices) and what you are (e.g., fingerprints);
- uses public key cryptography instead of symmetric shared secrets;
- a user is verified by an authenticator, and then the authenticator authenticates with the RP; and
- phishing resistant multi-factor authentication.

These approaches support the following security and privacy principles:

- no linkability between services or accounts;
- no third party in the protocol;
- biometrics, if used, never leave the device;
- crypto keys stay on the device;
- no server-side shared secrets; and,
- basis of public key cryptography.

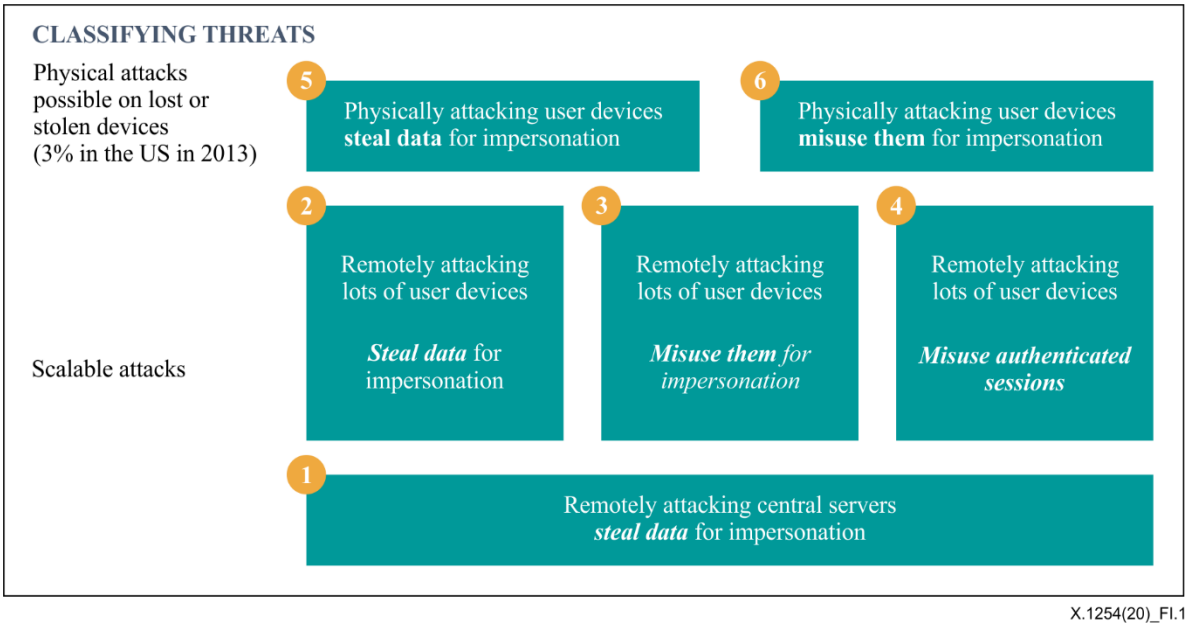

Figure I.1 – Classifying threats

I.4 Old authentication with passwords

Typical password-based authentication processes have several inherent risks as shown in Figure I.2:

1. passwords can be stolen from the server (data breaches);
2. passwords might be entered in untrusted apps or websites (phishing);
3. too many passwords to remember leads to greater reuse (easier to guess passwords across sites);
4. inconvenient to type passwords on phones (users select passwords that are easier to guess).

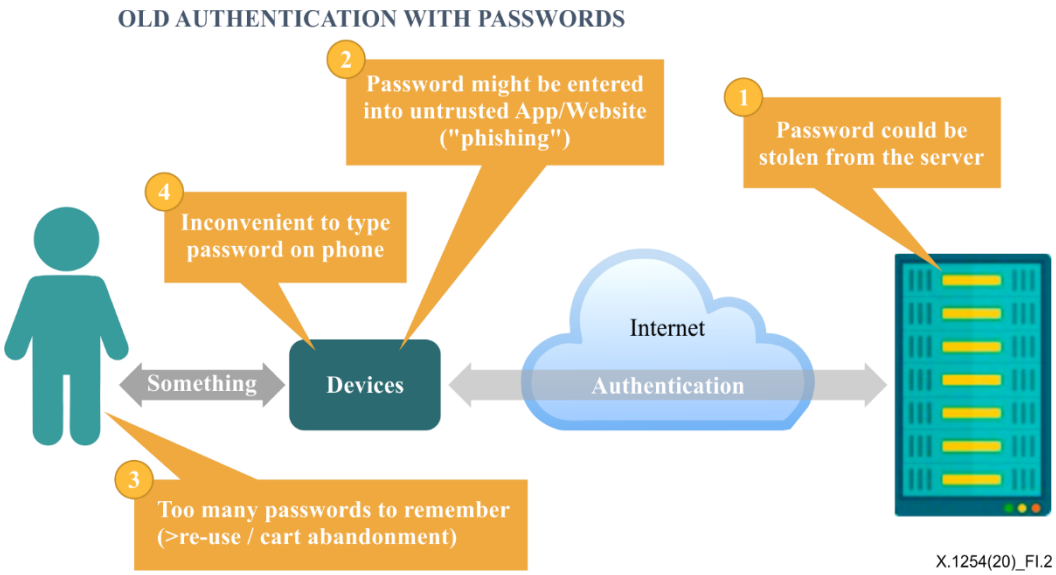

Figure I.2 – Old authentication with passwords

I.5 New authentication with [b-ITU-T X.1278]

FIDO separates the authentication aspect from the identity aspect. Figure I.3 shows the benefits of this approach:

1. no secrets are stored on the server (protects against data breaches);
2. authenticators cannot be tricked by phishing;
3. no passwords to remember and no friction added to the authentication process;
4. single gesture convenience for the user.

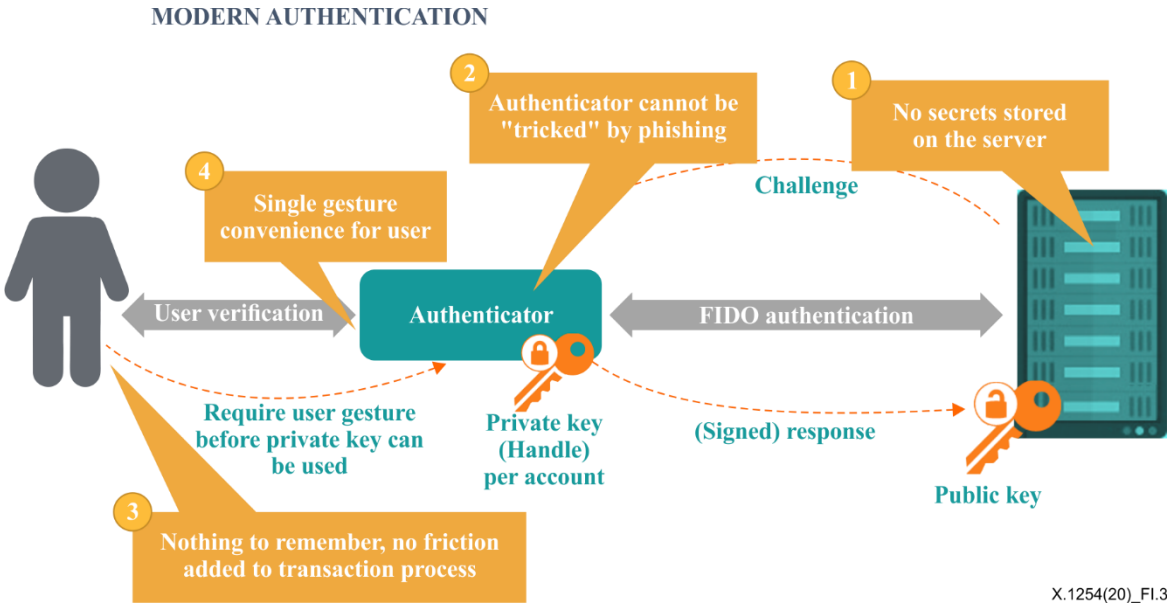

Figure I.3 – New authentication with [b-ITU-T X.1278]

I.6 Interoperability and certification

In addition to creating new methods of authentication, the strength of authentication solutions are increased via interoperability and certification testing.

- Increased user or consumer acceptability of strong authentication.

- Reduced risk and impact of identity theft through more widespread deployment of strong authentication.
- Convenience and improved user experience through a broad range of authentication devices and services.
- Cost reduction increases adoption of strong authentication.

Bibliography

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1254 (2012)] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

[b-ITU-T X.1277] Recommendation ITU-T X.1277 (2018), *Universal authentication framework.*

[b-ITU-T X.1278] Recommendation ITU-T X.1278 (2018), *Client to authenticator protocol/Universal 2-factor framework.*

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-ISO/IEC 24745] ISO/IEC 24745:2011, *Information technology — Security techniques — Biometric information protection*.

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2019, *IT security and privacy – A framework for identity management – Part 1: Terminology and concepts*.

[b-ISO/IEC 27000] ISO/IEC 27000 (2018), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.*

[b-ISO/IEC TS 29003] Technical Specification ISO/IEC TS 29003:2018, *Information technology – Security techniques – Identity proofing*.

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Information technology – Security techniques – Entity authentication assurance framework*.

[b-IETF RFC 7231] IETF RFC 7231 (2014), *Hypertext transfer protocol (HTTP/1.1): Semantics and content*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2021