FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
29115**

ISO/IEC JTC **1**

Secretariat: **ANSI**

Voting begins on:
2012-07-20

Voting terminates on:
2012-09-20

Information technology — Security techniques — Entity authentication assurance framework

Technologies de l'information — Techniques de sécurité — Cadre d'assurance de l'authentification d'entité

Reference number
ISO/IEC FDIS 29115:2012(E)

CONTENTS

Page

Foreword

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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 standardising telecommunications on a world-wide basis. The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups that, 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 that fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

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

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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

ISO/IEC 29115 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*. The identical text is published as ITU-T Recommendation X.1254.

Introduction

Many electronic transactions within or between ICT systems have security requirements which depend upon an understood or specified level of confidence in the identities of the entities involved. Such requirements may include the protection of assets and resources against unauthorized access, for which an access control mechanism might be used, and/or the enforcement of accountability by the maintenance of audit logs of relevant events, as well as for accounting and charging purposes.

This Recommendation | International Standard provides a framework for entity authentication assurance. Assurance within this Recommendation | International Standard refers to the confidence placed in all of the processes, management activities, and technologies used to establish and manage the identity of an entity for use in authentication transactions.

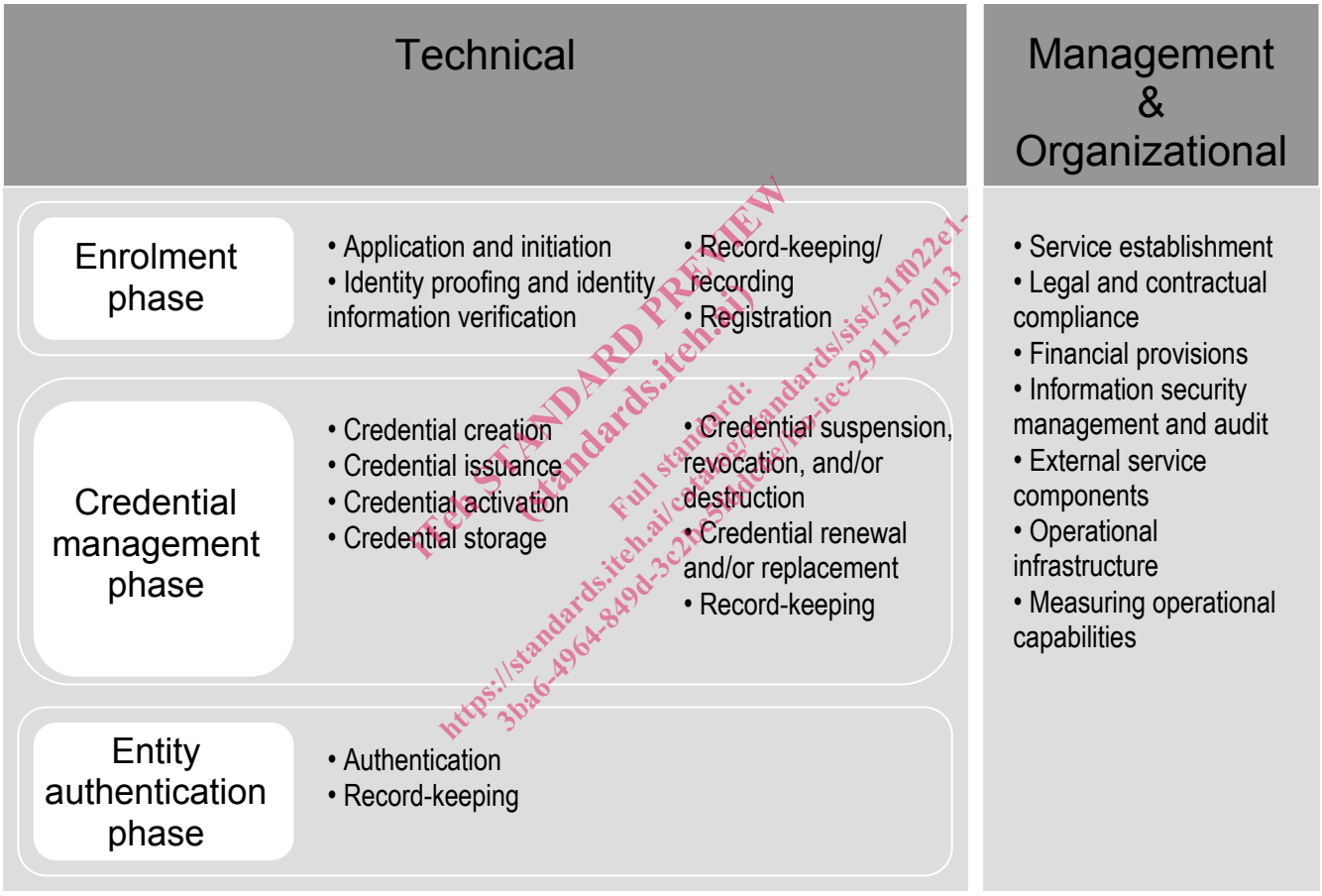

Figure 1 – Overview of the Entity Authentication Assurance Framework

Using four specified Levels of Assurance (LoAs), this Recommendation | International Standard provides guidance concerning control technologies, processes, and management activities, as well as assurance criteria, that should be used to mitigate authentication threats in order to implement the four LoAs. It also provides guidance for the mapping of other authentication assurance schemes to the specified four levels, as well as guidance for exchanging the results of an authentication transaction. Finally, this Recommendation | International Standard provides informative guidance concerning the protection of personally identifiable information (PII) associated with the authentication process.

This Recommendation | International Standard is intended to be used principally by credential service providers (CSPs) and by others having an interest in their services (e.g., replying parties, assessors and auditors of those services). This Entity Authentication Assurance Framework (EAAF) specifies the minimum technical, management, and process requirements for four LoAs to ensure equivalence among credentials issued by various CSPs. It also provides some additional management

and organizational considerations that affect entity authentication assurance, but it does not set forth specific criteria for those considerations. Relying Parties (RPs) and others may find this Recommendation | International Standard helpful to gain an understanding of what each LoA provides. Additionally, it may be adopted for use within a trust framework to define technical requirements for LoAs. The EAAF is intended for, but not limited to, session-based and document-centric use cases using various authentication technologies. Both direct and brokered trust scenarios are possible, within either bilateral or federated legal constellations.

INTERNATIONAL STANDARD <29115>
ITU-T RECOMMENDATION <X.eaa>

Information technology — Security techniques — Entity authentication assurance framework

1 Scope

This Recommendation | International Standard provides a framework for managing entity authentication assurance in a given context. In particular, it:

- specifies four levels of entity authentication assurance;
- specifies criteria and guidelines for achieving each of the four levels of entity authentication assurance;
- provides guidance for mapping other authentication assurance schemes to the four LoAs;
- provides guidance for exchanging the results of authentication that are based on the four LoAs; and
- provides guidance concerning controls that should be used to mitigate authentication threats.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards

None.

2.3 Additional references

None.

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.1 **Assertion:** Statement made by an entity without accompanying evidence of its validity [ITU-T X.1252].

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 | International Standard, an assertion is considered to be a stronger statement than a claim.

3.2 **Authentication:** Provision of assurance in the identity of an entity [ISO/IEC 18014-2].

3.3 **Authentication Factor:** Piece of information and/or process used to authenticate or verify the identity of an entity [ISO/IEC 19790].

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).

3.4 Authentication Protocol: Defined sequence of messages between an entity and a verifier that enables the verifier to perform authentication of an entity.

3.5 Authoritative Source: Repository which is recognized as being an accurate and up-to-date source of information.

3.6 Claim: Statement that something is the case, without being able to give proof [ITU-T X.1252].

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 | International Standard, an assertion is considered to be a stronger statement than a claim.

3.7 Context: Environment with defined boundary conditions in which entities exist and interact [ITU-T X.1252].

3.8 Credential: Set of data presented as evidence of a claimed or asserted identity and/or entitlements.

NOTE – See Annex B for additional characteristics of a credential.

3.9 Credential Service Provider: Trusted actor that issues and/or manages credentials.

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

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

3.11 Entity Authentication Assurance: Degree of confidence reached in the authentication process that the entity is what it is, or is expected to be [X.1252].

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

3.12 Identifier: One or more attributes that uniquely characterize an entity in a specific context.

3.13 Identity: Set of attributes related to an entity [ISO/IEC 24760].

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

3.14 Identity Information Verification: 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.

3.15 Identity Proofing: Process by which the Registration Authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance.

3.16 Man-in-the-middle Attack: Attack in which an attacker is able to read, insert, and modify messages between two parties without their knowledge.

3.17 Multifactor Authentication: Authentication with at least two independent authentication factors [ISO/IEC 19790].

3.18 Mutual Authentication: Authentication of identities of entities which provides both entities with assurance of each other's identity.

3.19 Non-repudiation: Ability to protect against denial by one of the entities involved in an action of having participated in all or part of the action [X.1252].

3.20 Phishing: Scam by which an email user is duped into revealing personal or confidential information which the scammer can then use illicitly.

3.21 Registration Authority: Trusted actor that establishes and/or vouches for the identity of an entity to a CSP.

3.22 Relying Party: Actor that relies on an identity assertion or claim.

3.23 Repudiation: Denial in having participated in all or part of an action by one of the entities involved [X.1252].

3.24 Salt: Non-secret, often random, value that is used in a hashing process.

NOTE - It is also referred to as sand.

3.25 Shared Secret: Secret used in authentication that is known only to the entity and the verifier.

3.26 Time Stamp: Reliable time variant parameter which denotes a point in time with respect to a common reference.

3.27 Transaction: Discrete event between an entity and service provider that supports a business or programmatic purpose.

3.28 Trust Framework: Set of requirements and enforcement mechanisms for parties exchanging identity information.

3.29 Trusted Third Party: Authority or its agent, trusted by other actors with respect to specified activities (e.g., security-related activities).

NOTE - A trusted third party is trusted by an entity and/or a verifier for the purposes of authentication.

3.30 Validity Period: Time period during which an identity or credential may be used in one or more transactions.

3.31 Verification: Process of checking information by comparing the provided information with previously corroborated information.

3.32 Verifier: Actor that corroborates identity information.

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

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

CSP	Credential Service Provider
EAA	Entity Authentication Assurance
EAAF	Entity Authentication Assurance Framework
IdM	Identity Management
ICT	Information and Communications Technology
IP	Internet Protocol
LoA	Level of Assurance
LoAs	Levels of Assurance
MAC	Media Access Control
NPE	Non-Person Entity
PII	Personally Identifiable Information
PIN	Personal Identification Number
RA	Registration Authority
RP	Relying Party
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol