This document is a preview generated by EVS

INFOTEHNOLOOGIA
Turbemeetodid
Olemi autentimiskindluse karkass

Information technology
Security techniques
Entity authentication assurance framework
(ISO/IEC 29115:2013)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA	NATIONAL FOREWORD
See Eesti standard EVS-ISO/IEC 29115:2016 „Infotehnoloogia. Turbemeetodid. Olemi autentimiskindluse karkass“ sisaldab rahvusvahelise standardi ISO/IEC 29115:2013 „Information technology. Security techniques. Entity authentication assurance framework“ identset ingliskeelset teksti.	This Estonian Standard EVS-ISO/IEC 29115:2016 consists of the identical English text of the International Standard ISO/IEC 29115:2013 „Information technology. Security techniques. Entity authentication assurance framework“.
Ettepaneku rahvusvahelise standardi ümbertrüki meetodil ülevõtuks on esitanud EVS/TK 4, standardi avaldamist on korraldanud Eesti Standardikeskus.	Proposal to adopt the International Standard by reprint method has been presented by EVS/TK 4, the Estonian standard has been published by the Estonian Centre for Standardisation.
Standard EVS-ISO/IEC 29115:2016 on jõustunud sellekohase teate avaldamisega EVS Teataja 2016. aasta veebruarikuu numbris.	Standard EVS-ISO/IEC 29115:2016 has been endorsed with a notification published in the February 2016 issue of the official bulletin of the Estonian Centre for Standardisation.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Käsitlusala

See standard annab ühe karkassi, millega hallata olemi autentimiskindlust mingis konkreetses kontekstis. Sealhulgas ta

- spetsifitseerib olemi autentimiskindluse nelja taset;
- spetsifitseerib kriteeriumid ja juhised olemi autentimiskindluse iga taseme saavutamiseks nende nelja hulgast;
- annab juhiseid muude autentimiskindluse skeemide vastavusse seadmiseks nende nelja kindlustasemega;
- annab juhiseid nendel neljal kindlustasemel põhineva autentimise tulemite vahetuseks;
- annab juhiseid meetmete kohta, mis tuleks rakendada autentimise ohtude vähendamiseks.

This document is a preview generated by EVS

This document is a preview generated by EVS

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.040

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Aru 10, 10317 Tallinn, Eesti; koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:
Aru 10, 10317 Tallinn, Estonia; homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1
2.1 Identical Recommendations | International Standards 1
2.2 Paired Recommendations | International Standards 1
2.3 Additional references 1

3 Terms and definitions 1

4 Abbreviations 5

5 Conventions 6

6 Levels of assurance 6
6.1 Level of assurance 1 (LoA1) 7
6.2 Level of assurance 2 (LoA2) 7
6.3 Level of assurance 3 (LoA3) 7
6.4 Level of assurance 4 (LoA4) 8
6.5 Selecting the appropriate level of assurance 8
6.6 LoA mapping and interoperability 9
6.7 Exchanging authentication results based on the 4 LoAs 10

7 Actors 10
7.1 Entity 10
7.2 Credential service provider 10
7.3 Registration authority 11
7.4 Relying party 11
7.5 Verifier 11
7.6 Trusted third party 11

8 Entity authentication assurance framework phases 11
8.1 Enrolment phase 12
8.2 Credential management phase 14
8.3 Entity authentication phase 16

9 Management and organizational considerations 16
9.1 Service establishment 17
9.2 Legal and contractual compliance 17
9.3 Financial provisions 17
9.4 Information security management and audit 17
9.5 External service components 17
9.6 Operational infrastructure 18
9.7 Measuring operational capabilities 18

10 Threats and controls 18
10.1 Threats to, and controls for, the enrolment phase 18
10.2 Threats to, and controls for, the credential management phase 21
10.3 Threats to, and controls for, the authentication phase 26

11 Service assurance criteria 30

Annex A (informative) **Privacy and protection of PII** 31

Annex B (informative) **Characteristics of a credential** 33

Bibliography 35

This document is a preview generated by EVS

© ISO/IEC 2013 – All rights reserved

Foreword

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

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, *IT Security techniques*.

A similar text is published as ITU-T Recommendation X.1254. It differs from this text in three instances: 1) 3.8: the ISO/IEC definition includes asserted identities; 2) Table 10-1: ISO/IEC includes an example for impersonation that includes use of an identity for an entity that does not exist; 3) 10.2.2.1: ISO/IEC describes SSL as an example of a protected channel.

This document is a preview generated by EVS

© ISO/IEC 2013 – All rights reserved

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 International Standard provides a framework for entity authentication assurance. Assurance within this 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.

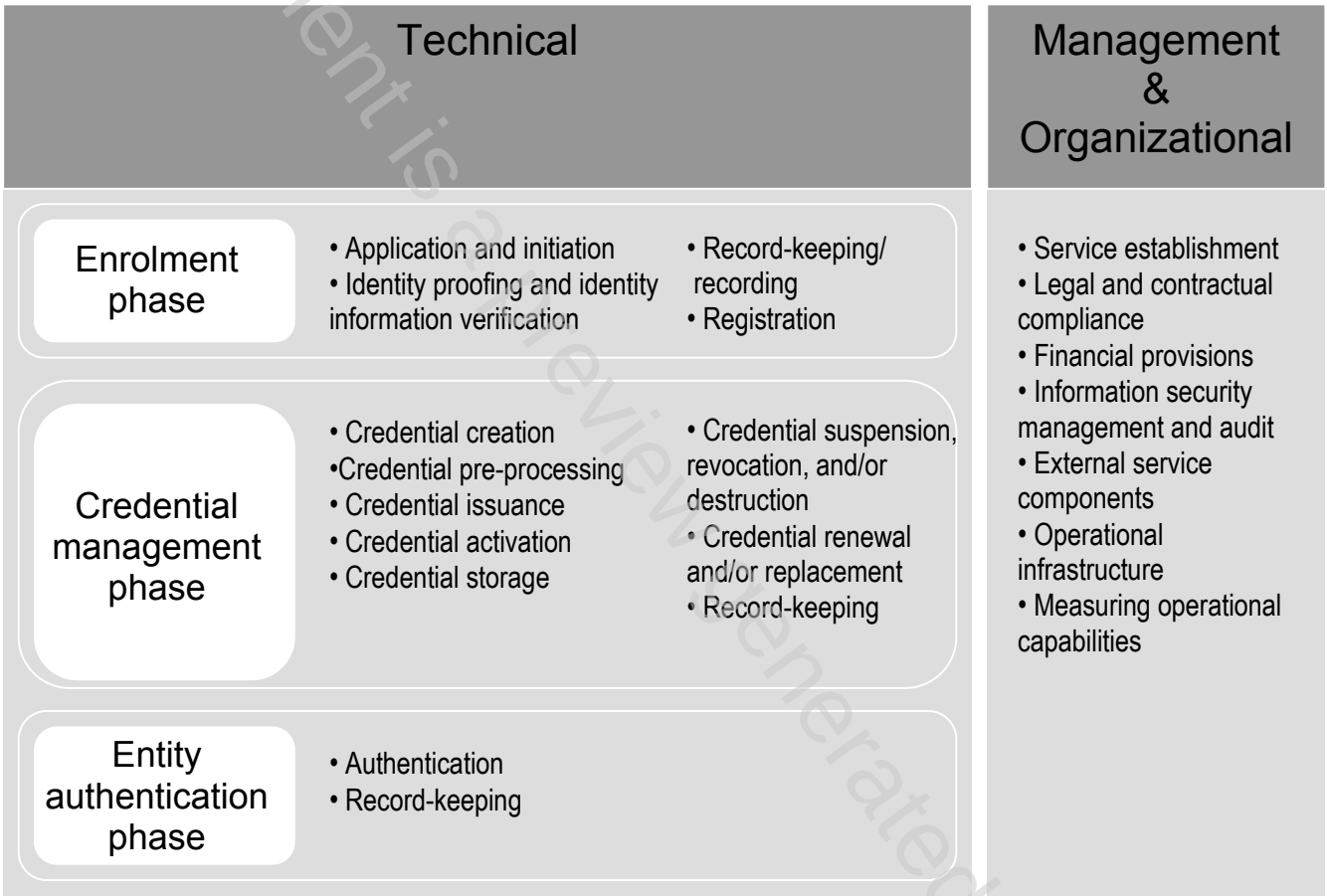

Figure 1 — Overview of the Entity Authentication Assurance Framework

Using four specified Levels of Assurance (LoAs), this 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 International Standard provides informative guidance concerning the protection of personally identifiable information (PII) associated with the authentication process.

This document is a preview generated by EVS

© ISO/IEC 2013 – All rights reserved

This International Standard is intended to be used principally by credential service providers (CSPs) and by others having an interest in their services (e.g., relying 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 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.

This document is a preview generated by EVS

 © ISO/IEC 2013 – All rights reserved

Information technology — Security techniques — Entity authentication assurance framework

This document is a preview generated by EVS

1 Scope

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

2.1 Identical Recommendations | International Standards

None.

2.2 Paired Recommendations | International Standards

None.

2.3 Additional references

None.

3 Terms and definitions

For the purposes of this document, the following terms and 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 International Standard, an assertion is considered to be a stronger statement than a claim.

© ISO/IEC 2013 – All rights reserved