ISO/IEC 29115:2013-04 (E)

Information technology - Security techniques - Entity authentication assurance framework

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