

DIN EN 419241-1:2018-09 (E)

Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements

Contents		Page
European foreword		4
Introduction		6
1	Scope	7
1.1	General	7
1.2	Outside of the scope	7
1.3	Audience	7
2	Normative references	8
3	Terms and definitions	8
4	Symbols and abbreviations	10
5	Description of trustworthy systems supporting server signing	11
5.1	General	11
5.2	Signature creation and server signing objectives	11
5.3	Signature bound to a natural person or seal bound to a legal person	11
5.4	Sole control assurance levels	11
5.5	Batch server signing	12
5.6	Signing key and cryptographic module	12
5.7	Signer's authentication	12
5.7.1	Electronic identification means	12
5.7.2	Authentication Mechanism	12
5.7.3	Authentication target	13
5.7.4	Delegation of authentication to an external party	13
5.8	Signature activation data	14
5.9	Signature activation protocol	14
5.10	Signer's interaction component	14
5.11	Signature activation module	15
5.12	Environments	15
5.12.1	Tamper protected environment	15
5.12.2	TSP protected environment	15
5.12.3	Signer's environment	16
5.13	Functional model	16
5.13.1	General	16
5.13.2	Scope of requirements	16
5.13.3	Signature activation mechanisms	17
5.13.4	TW4S components	19
6	Security requirements	20
6.1	General	20
6.2	General security requirements (SRG)	20
6.2.1	Management (SRG_M)	20
6.2.2	Systems and operations (SRG_SO)	22
6.2.3	Identification and authentication (SRG_IA)	22
6.2.4	System access control (SRG_SA)	23
6.2.5	Key management (SRG_KM)	23
6.2.6	Auditing (SRG_AA)	26
6.2.7	Archiving (SRG_AR)	28

6.2.8	Backup and recovery (SRG_BK)	28
6.3	Core components security requirements (SRC)	29
6.3.1	Signing key setup (SRC_SKS) - Cryptographic key (SRC_SKS.1)	29
6.3.2	Signer authentication (SRC_SA)	29
6.3.3	Digital signature creation (SRC_DSC) - Cryptographic operation (SRC_DSC.1)	30
6.4	Additional security requirements for SCAL2 (SRA)	30
6.4.1	General	30
6.4.2	Signature activation protocol and signature activation data (SRA_SAP)	30
6.4.3	Signing key management (SRA_SKM)	32
Annex A (normative) Requirements for electronic identification means, characteristics and design		34
A.1	Enrolment	34
A.1.1	Application and registration	34
A.1.2	Identity proofing and verification (natural person)	34
A.1.3	Identity proofing and verification (legal person)	37
A.1.4	Binding between the electronic identification means of natural and legal persons	39
A.2	Electronic identification means and authentication	40
A.2.1	Electronic identification means characteristics and design	40
A.2.2	Authentication mechanism	41
Bibliography		42