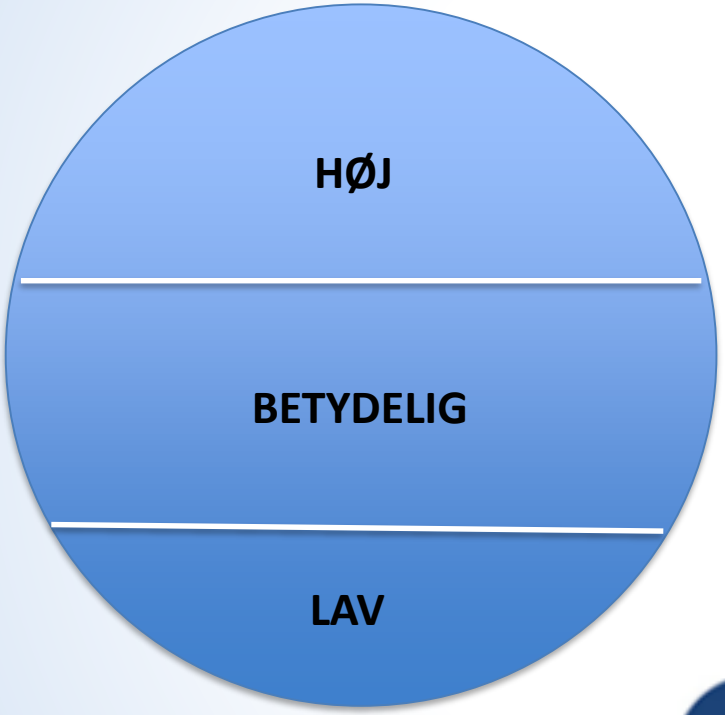
Verkstova um løgfrøði og standardir – 21. mars 2017

Talgildur samleiki

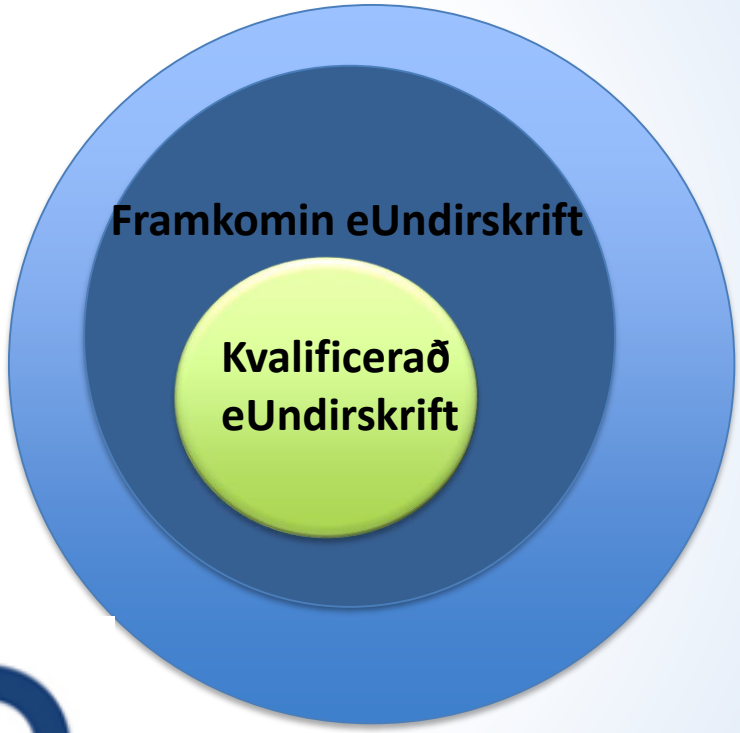
TALGILDU
FØROYAR
01100110 01101111

TALGILDU FØROYAR
01100110 01101111

Tænastur í Talgilda Samleikanum



eID
(authentication)



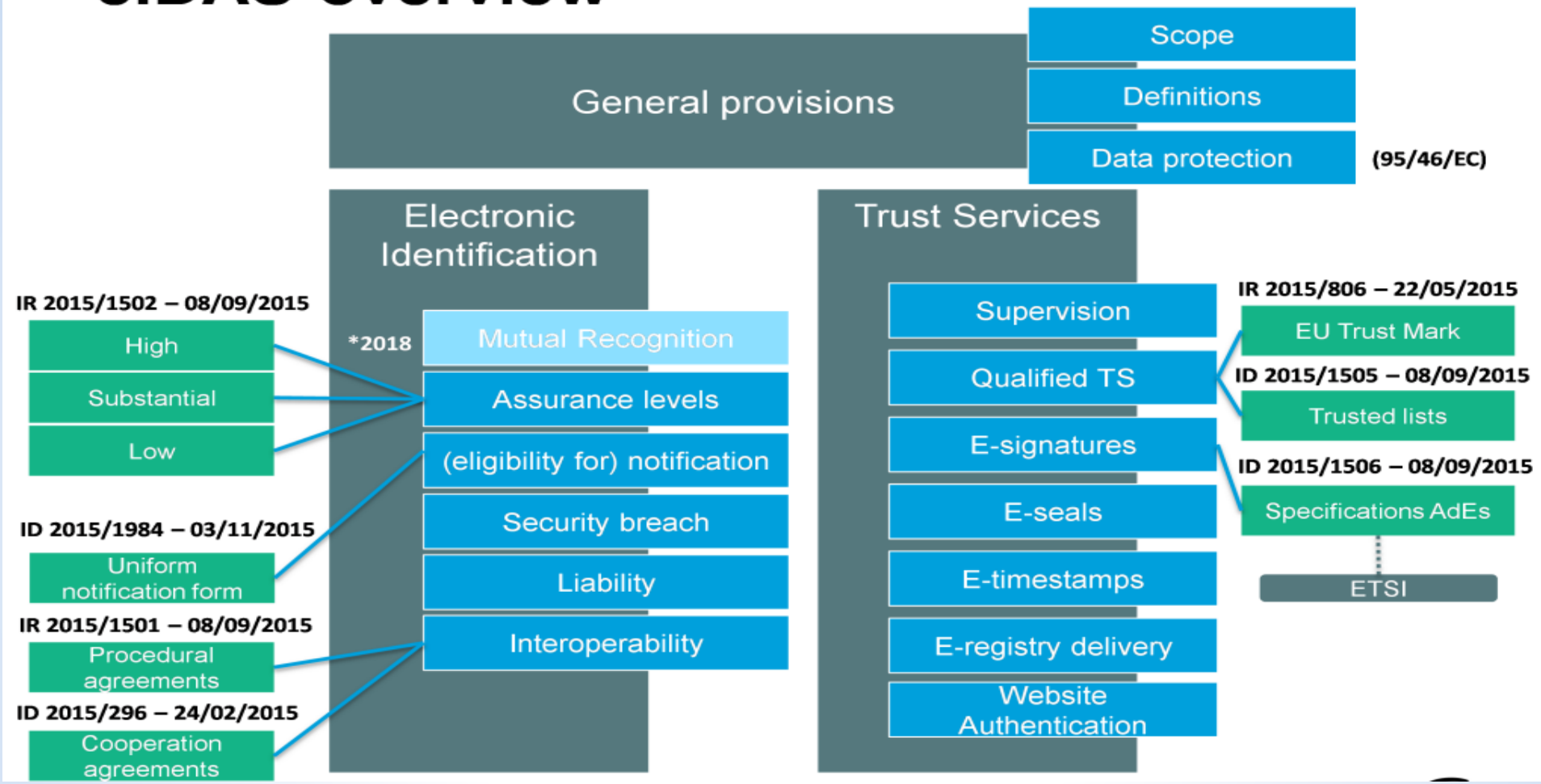
eUndirskrift

TALGILDU FØROYAR
01100110 01101111

eIDAS (EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) Nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF)

- **eIDAS regulerar primært:**
    - Elektroniska eyðmerking (eID)
    - Álitistænastur (Trust Services)
        - eUndirskrift, eInnsigli, eTíðarsempul v.m.
- **Endamálið við eIDAS er, at:**
    - eID og álitistænastur (Trust Services) kunnu brúkast uppá tvørs í ES samstundis sum trygdin er nøktandi.
- **Hetta gerst við at stilla krøv um:**
    - Sínamillum góðkenning
    - Interoperabilitet (sikra at loysnirnar kunnu "tosa" saman reint tekniskt)

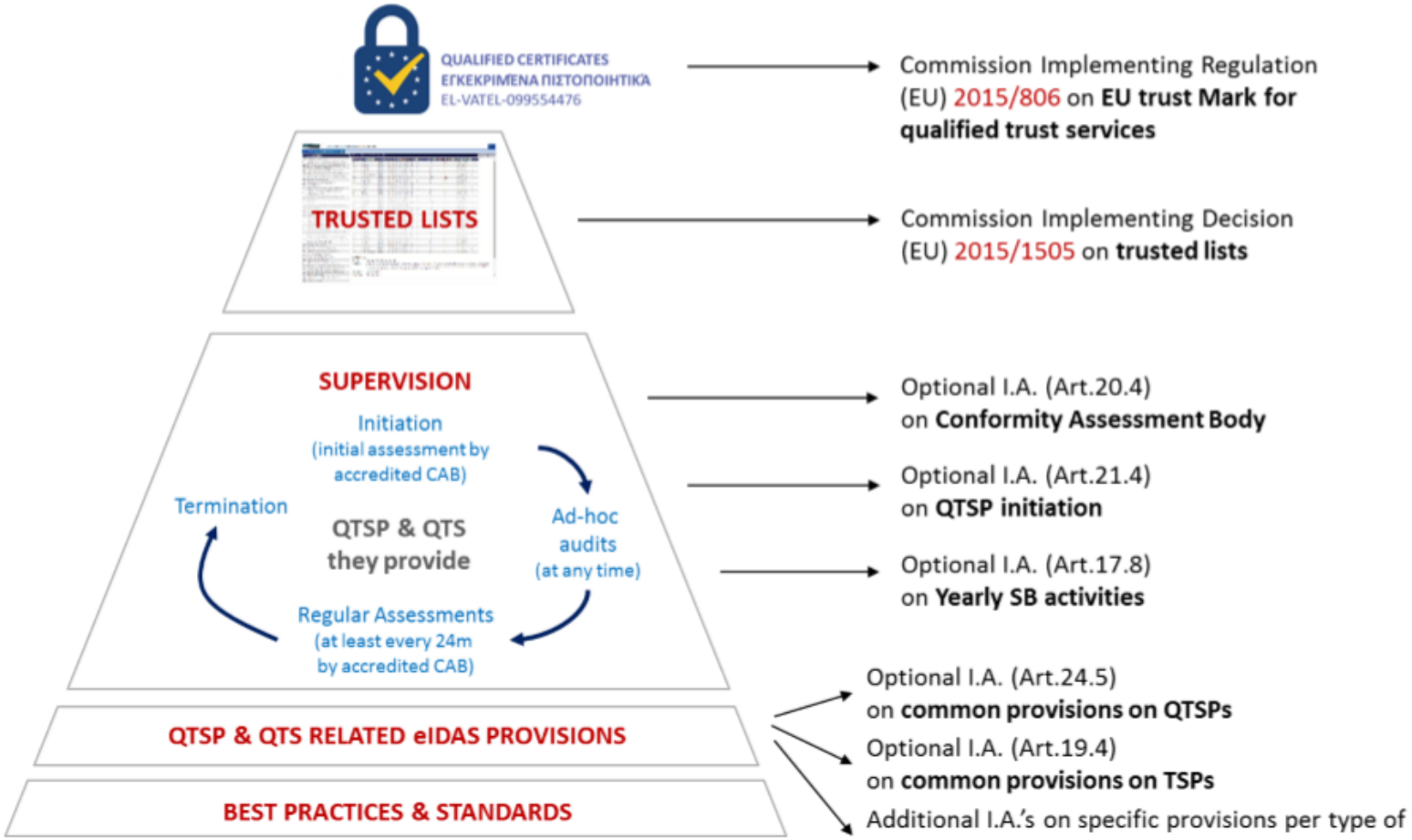
eIDAS overview



Um ein “gennemførelsesforodning” (grønu kassarnir) peikar á ein standard, skal hesin fylgjast. Um ikki, so stendur ein og hvørjum frítt.

Standardir, ið skulu fylgjast (krav í útboðstilfarinum):

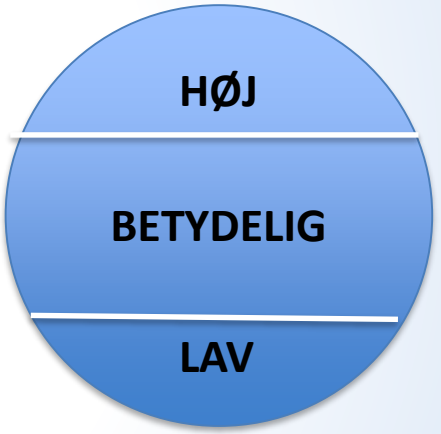
- ETSI EN 319 411-1 – krøv til Trust Service Provider
- ETSI EN 319 411-2 – krøv til kvalificeraðir Trust Service Provider
- ETSI EN 319 412-1 – Certificate Profiles Part 1 - General
- ETSI EN 319 412-2 - Certificate Profiles - Part 2 – Natural Persons
- ETSI EN 319 412-5 - Certificate Profiles - Part 5 - Statements
- adES standardir (sí EU Kommmissionens GENNEMFØRELSESAFGØRELSE (EU) 2015/1506 af 8. september 2015.)


QUALIFIED CERTIFICATES
ΕΓΚΕΚΡΙΜΈΝΑ ΠΙΣΤΟΠΟΙΗΤΙΚΆ
EL-VATEL-099554476
Commission Implementing Regulation (EU) 2015/806 on EU trust Mark for qualified trust services
TRUSTED LISTS
Commission Implementing Decision (EU) 2015/1505 on trusted lists
SUPERVISION
Initiation
(initial assessment by accredited CAB)
Ad-hoc audits
(at any time)
Regular Assessments
(at least every 24m by accredited CAB)
Termination
QTSP & QTS they provide
Optional I.A. (Art.20.4) on Conformity Assessment Body
Optional I.A. (Art.21.4) on QTSP initiation
Optional I.A. (Art.17.8) on Yearly SB activities
QTSP & QTS RELATED eIDAS PROVISIONS
BEST PRACTICES & STANDARDS
Optional I.A. (Art.24.5) on common provisions on QTSPs
Optional I.A. (Art.19.4) on common provisions on TSPs
Additional I.A.'s on specific provisions per type of (qualified) trust service & trust service provider

TALGILDU FØROYAR
01100110 01101111

ES lóggáva - eID (autentification)

- **eID deilt upp í trý trygdarstig: Lav, betydelig og høj**
- **ES lond skulu viðurkenna loysnir á sama stigi**
- **Krøv til elektroniska eyðmerking:**
  - Skráseting og kontrol av samleika
  - Útflýggjan av talgildum samleika
  - Login-faktorar
  - Sperring og endurnýggjan
  - Krøv til starvsfólk, bygnað og eftirlit



TALGILDU FØROYAR
01100110 01101111

ES lóggáva

- **Talgildi Samleikin skal sum minimum vera: betydelig**
- **Nøkur dømi um trygdarstig "betydelig" og "høj":**
  - Minimum tveir (av trimum) login faktorar skulu nýtast (felags fyri bæði "betydelig" og "høj")
    - Faktorarnir eru: nakað tú 1) hevur, 2) veit ella 3) ert
  - Høj: Skráseting krevur altíð at viðkomandi er tilstaðar (betydelig: opnar fyri fleiri møguleikum)
  - Høj: Krevur eksternt eftirlit við jøvnum millumbili (betydelig krevur internt eftirlit)
- **Hetta er nýtt umráði, ið manglar praksis, tí er ilt at siga, hvat munurin er á "betydelig" og "høj"**

  Sí eIDAS kapittul 2 (art. 6 til art. 12) og Kommissionens gennemførelsesforordning 2015/1502 og standard ISO/IEC 29115 fyri meira vitan. Eisini kann danski National Standard for Identiteters Sikringsniveauer lesast til íblástur.

TALGILDU FØROYAR
01100110 01101111

Login faktorar

- **Betydelig:**
  1. Det elektroniske identifikationsmiddel gør brug af **mindst to autentifikationsfaktorer** fra forskellige kategorier.
  2. Det elektroniske identifikationsmiddel er udformet således, at det kan antages, at det kun kan bruges, når det er den person, som det tilhører, der har kontrol over og er i besiddelse af det.

- **Høj**
  Kravene til sikringsniveau "betydelig" samt:

1. Det elektroniske identifikationsmiddel er beskyttet mod kopiering og manipulation samt angribere med stor angrebskapacitet
2. Det elektroniske identifikationsmiddel er udformet således, at den person, som det tilhører, kan beskytte det sikkert mod, at andre bruger det.

Viðurkend (kvalificerað) eUndirskrift

TALGILDU FØROYAR
01100110 01101111

- **eIDAS artikel 3, nr. 12:**
- »kvalificeret elektronisk signatur«: en **avanceret elektronisk signatur**, der er genereret af et **kvalificeret elektronisk signaturgenereringssystem (QSCD)** og baseret på et **kvalificeret certifikat** for elektroniske signaturer
- Krøvini eru:
  - 1) Skal vera ein framkomin (avanceret) elektronisk undirskrift,
  - 2) ið er framleitt av einum viðurkendum (kvalificerað) elektroniskum signaturgeneringssystemi og
  - 3) grundað á viðurkent (kvalificerað) sertifikat til elektroniskar undirskrift

Ad.1 - framkomin (avanceret) elektronisk undirskrift – eIDAS art. 26

TALGILDU FØROYAR
01100110 01101111

- Ein framkomin elektronisk undirskrift er: Ein elektronisk undirskrift sum:
- a) er eintýðugt knýtt at tí, sum skrivar undir,
- b) ger tað møguligt at eyðmerkja tann, sum skrivar undir,
- c) den genereres ved hjælp af elektroniske signaturgenereringsdata, som underskriveren med en høj grad af tillid kan anvende og har fuld kontrol med, og
- d) er knýtt at teimum dátum, undirskriftin viðvíkur, á slíkan hátt, at ein og hvør seinni broyting av hesum dátum kann verða avdúkað.

Punkt a, b og d eru tey somu sum í føroysku lógini um elektroniska undirskrift, § 4, nr.2. Punkt c minnir nógv um, men er ikki heilt eins sum í eIDAS.

TALGILDU FØROYAR
01100110 01101111

Ad. 2 - Viðurkent (kvalificerað) elektroniskt signaturgenereringssystem (QSCD)

- Elektroniskt signaturgenereringssystem er: Konfigureret software eller hardware, der bruges til at generere en elektronisk signatur, art. 3, nr. 22 eIDAS.

- Fyri at vera viðurkent (kvalificerað) skal livast upp til krøv í eIDAS bilag 2

TALGILDU FØROYAR
01100110 01101111

Ad. 3 - viðurkent (kvalificerað) sertifikat

- **Certifikat for elektronisk signatur er:** en elektronisk attestering, som knytter elektroniske signaturvalideringsdata til en fysisk person og mindst bekræfter denne persons navn eller pseudonym, art. 3, nr. 14 i eIDAS.

- **Kvalificeret certifikat for elektronisk signatur er:** et certifikat for elektroniske signaturer, som er udstedt af en **kvalificeret tillidstjenesteudbyder** og opfylder kravene i bilag 1, art. 3, nr. 15 i eIDAS

- = Gjaldstovan má vera góðkend sum "kvalificeret tillidstjenesteudbyder" fyri at uppfylla krøvini.
  Hetta stillar ymisk krøv um t.d. eftirlit, endurgjaldsábyrgd, sí eIDAS art. 24

TALGILDU FØROYAR
01100110 01101111

Føroysk lóggáva

- **Løgtingslóg um elektroniska undirskrift**
  - Stillar krøv til framkomna undirskrift
  - Byggir á útgingið ES direktiv og skal tí endurnýggjast ella ógildast (eIDAS reglur innførast)
- **Persónsupplýsingarlógin**
  - Einans savna upplýsingar sum eru neyðugir og viðkomandi
  - Trygd í samband við viðgerð av persónsupplýsingum
  - Nýggj ES forordning kemur næsta ár – Dataforordningen 2016/679 af 27. april 2016
- **Breksáttmálin**
  - Loysnin skal taka hædd fyri teimum, ið bera brek ella á annan hátt hava serligar avbjóðingar

TALGILDU FØROYAR
01100110 01101111

Hvat er Etsi Esi?

The European Telecommunications Standards Institute (ETSI).

Electronic Signatures and Infrastructures (ESI)

ESI works, in collaboration will CEN TC 224, on the execution of EC Mandate M/460 to provide a rationalized framework for digital signatures standardization.

(CEN = European Committee for Standardization)

- **Kelda:**
  https://portal.etsi.org/TBSiteMap/esi/ESIActivities.aspx

The European Telecommunications Standards Institute (ETSI).

TALGILDU FØROYAR
01100110 01101111

ETSI TR 119 000 V1.2.1 (2016-04)

Electronic Signatures and Infrastructures (ESI);
The framework for standardization of signatures: overview

TALGILDU
FØROYAR
01100110 01101111

ETSI TR 119 000

- **This guidance focuses on the selection of standards relevant to particular trust services. Guidance is provided not only for trust service providers supporting digital signatures (e.g. trust service providers issuing qualified certificates) but also for those trust application providers offering value added services and applying digital signatures (e.g. registered electronic mail). The framework focuses on the simplification of the standards by reducing unnecessary options, avoiding diverging interpretations, by better mapping them to business driven practices and legal provisions and in particular to reaching cross-border interoperability.**

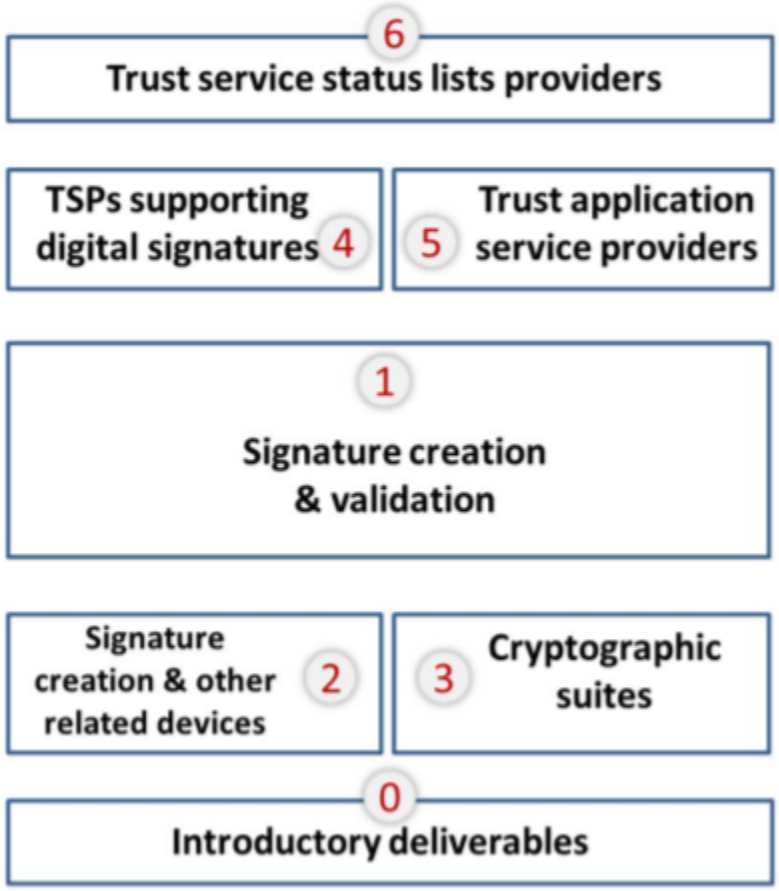


Figure 1: Overview of the structure of the framework for standardization of signatures

						Signature creation and validation	Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	1	0	0	Business driven guidance for implementing digital signature creation and validation	(new) TR 102 047	Feb. 2016
						Policy & Security Requirements		
TS	1	19	1	0	1	Security requirements for signature creation applications and signature validation applications	(new)	Nov. 2015
EN	4	19	1	1	1	Protection profiles for signature creation and validation application - Part 1: Introduction to the European Norm - Part 2: Signature creation application - Core PP - Part 3: Signature creation application - Possible Extensions - Part 4: Signature verification application - Core PP - Part 5: Signature verification application - Possible Extensions	CWA/prEN 14170	All parts published & to be updated: undefined Part 2 & 4 to be evaluated
						Technical Specifications		
EN	3	19	1	0	2	Procedures for creation and validation of AdES digital signatures - Part 1: Creation and validation - Part 2: Validation report	TS 102 853, CWA 14170, CWA 14171	Part 1: - TS: published - EN: Apr. 2016 Part 2: undefined
EN	3	19	1	2	2	CAdES digital signatures - Part 1: Building blocks and CAdES baseline signatures - Part 2: Extended CAdES signatures	TS 101 733, TS 103 173, TS 102 734	Parts 1 & 2: - TS: published - EN: Apr. 2016
EN	3	19	1	3	2	XAdES digital signatures - Part 1: Building blocks and XAdES baseline signatures - Part 2: Extended XAdES signatures	TS 101 903, TS 103 171, TS 102 904	Parts 1 & 2: - TS: published - EN: Apr. 2017
EN	3	19	1	4	2	PAdES digital signatures - Part 1: Building blocks and PAdES baseline signatures - Part 2: Additional PAdES signatures profiles - Part 3: Visual representations of digital signatures	- TS 102 778-1 - TS 103 172 - TS 102 778-2/5 - TS 102 778-6	Parts 1 & 2: - TS: published - EN: Apr. 2016 (Part 3: delayed)
TS	1	19	1	5	2	Architecture for AdES digital signatures in distributed environments	(new)	Undefined
EN	3	19	1	6	2	Associated Signature Containers (ASiC) - Part 1: Building blocks and ASiC baseline containers - Part 2: Additional ASiC containers	TS 102 918, TS 103 174	Parts 1 & 2: - TS: Sep. 2015 - EN: July 2016
TS	1	19	1	7	2	Signature policies - Part 1: Building blocks and table of contents for human readable signature policy documents - Part 2: XML format for signature policies - Part 3: ASN.1 format for signature policies - Part 4: Signature validation policy for European qualified electronic signatures/seals using trusted lists	- TR 102 041 / 045 - TR 102 038 - TR 102 272	- Part1: published - Other parts: undefined
						Conformity Assessment		
TS	4	19	1	0	3	Conformity assessment for signature creation & validation (applications & procedures)	(new) (CWA 14172-4 ?)	Feb. 2016 (hand over to CEN)
						Testing Conformance & Interoperability		
TS	1	19	1	2	4	CAdES Testing conformance & interoperability	(new)	April 2016
TS	1	19	1	3	4	XAdES Testing conformance & interoperability	(new)	April 2016
TS	1	19	1	4	4	PAdES Testing conformance & interoperability	(new)	April 2016
TS	1	19	1	5	4	Testing conformance & interoperability of AdES in mobile environments	(new)	April 2017
TS	1	19	1	6	4	ASiC Testing conformance & interoperability	(new)	April 2016

Table 2: Standards for signature creation and validation (source ETSI TR 119 000)

TALGILDU
FØROYAR
01100110 01101111

							Signature creation and other related devices	Replaces	Expected publication
							Sub-areas		
							Guidance		
TR	4	19	2	0	0	0	Business driven guidance for signature creation and other related devices	(new)	February 2016
							Policy & Security Requirements		
EN	4	19	2	1	1	1	Protection profiles for secure signature creation device - Part 1: Overview - Part 2: Device with key generation - Part 3: Device with key import - Part 4: Extension for device with key generation and trusted communication with certificate generation application - Part 5: Extension for device with key generation and trusted communication with signature creation application - Part 6: Extension for device with key import and trusted communication with signature creation application	 - (new part) - prTS 14169-2 - prTS 14169-3 - prTS 14169-4 - prEN 14169-5 - (new part)	published
EN	4	19	2	2	1	1	Protection Profiles for TSP cryptographic modules - Part 1: Overview - Part 2: Cryptographic Module for CSP signing operations with backup – Protection Profile (CMCSOB-PP) - Part 3: Cryptographic module for CSP key generation services – Protection Profile (CMCKG-PP) - Part 4: Cryptographic module for CSP signing operations without backup – Protection Profile (CMCSOPP) - Part 5: Cryptographic module for trust services	 - (new part) - prTS 14167-2 - prTS 14167-3 - prTS 14167-4 - (new part)	 By end 2015 By end 2015 By end 2015 By end 2015 In 2016
EN	4	19	2	3	1	1	Protection profile for trustworthy systems supporting time stamping	(new)	In 2016
EN	4	19	2	4	1	1	Security requirements for trustworthy systems supporting server signing - Part 1: Security requirements - Part 2: Protection profile for trustworthy signature creation module (PP-TSCM) - Part 3: Protection profile for signature activation data management and signature activation protocol (PPSAD+SAP)	CWA 14167-5	 - TS published (EN: 2015) - undefined - undefined
EN	4	19	2	5	1	1	Security requirements for device for authentication - Part 1: Protection profile for core functionality - Part 2: Protection profile for extension for trusted channel to certificate generation application - Part 3: Additional functionality for security targets	EN 16248 (PP-DAUTH)	published
EN	4	19	2	6	1	1	Security requirements for trustworthy systems managing certificates for electronic signatures	prTS 14167-1	published
							Technical Specifications		
EN	4	19	2	1	2	2	Application interfaces for secure elements used as qualified electronic signature (seal-) creation devices - Part 1: Introduction - Part 2: Basic services - Part 3: Device authentication - Part 4: Privacy specific protocols - Part 5: Trusted eServices	EN 14890	Parts 1 & 2: published Other parts: by end 2015
							Conformity Assessment		
							no requirement identified		
							Testing Conformance & Interoperability		
-		-	-	-	-	-	*no requirement identified*		

Table 3: Standards for signature creation and other related devices (source TR 119 000)

TALGILDU
FØROYAR
01100110 01101111

Cryptographic suites							Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	3	0	0	Business guidance on cryptographic suites	(new)	published
						Technical Specifications		
TS	1	19	3	1	2	Cryptographic suites	TS 102 176-1	published
						Testing Conformance & Interoperability		
-		-	-	-	-	*no requirement identified*		

Table 4: Standards for cryptographic suites (source TR 119 000)

TALGILDU
FØROYAR
01100110 01101111

						TSPs supporting digital signatures and related services	Replaces	Expected publication
						Sub-areas		
						Guidance		
TR	1	19	4	0	0	Business driven guidance for TSPs supporting digital signatures	(new)	Published
						Policy & Security Requirements		
EN	3	19	4	0	1	General policy requirements for trust service providers	Replacing generic parts of TS 101 456, TS 102 042, (TR 102 040), TS	- TS: July 2015 - EN: March 2016
EN	3	19	4	1	1	Policy and security requirements for trust service providers issuing certificates - Part 1: General requirements - Part 2: Requirements for TSP issuing EU qualified certificates - Part 3: *To be made historical* - Part 4: Requirements for TSP issuing code signing certificates	- TS 102 042 (EV & BR), EN 319 411-3 - TS 101 456 (& TR 102 458), EN 319 411-3 - historical - (new)	- TS: July 2015 - EN: March 2016 - historical - undefined
EN	3	19	4	2	1	Policy & security requirements for trust service providers issuing time-stamps	TS 102 023	- TS: July 2015 - EN: March 2016
EN	3	19	4	3	1	Policy and security requirements for trust service providers providing AdES digital signature generation services	(new)	Undefined
EN	3	19	4	4	1	Policy and security requirements for trust service providers providing AdES digital signature validation services	(new)	Undefined
						Technical Specifications		
EN	3	19	4	1	2	Certificate profiles - Part 1: Overview and common data structures - Part 2: Certificate profile for certificates issued to natural persons - Part 3: Certificate profile for certificates issued to legal persons - Part 4: Certifcate profile for web site certificates issued to organisations - Part 5: QCStatements	- (new part) - TS 102 280 & TS 101 862 - (new part) - (new part)	All parts: - TS: July 2015 - EN: March 2016
EN	3	19	4	2	2	Time-stamping protocol and time-stamp profiles	TS 101 861	- TS: July 2015 - EN: March 2016
EN	3	19	4	3	2	Protocol profiles for trust service providers providing AdES digital signature generation services	(new)	Undefined
EN	3	19	4	4	2	Protocol profiles for trust service providers providing AdES digital signature validation services	(new)	Undefined
						Conformity Assessment		
EN	3	19	4	0	3	Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers	CWA 14172 (2&8), TS 119 403	- TS: Nov. 2014 - EN: end 2015
						Testing Conformance & Interoperability		
-	-	-	-	-	-	*no requirement identified for such a document*		

Table 5: Standards for TSPs supporting digital signatures and related services (source TR 119 000)

Trust application service providers								Replaces	Expected publication
				Sub-areas					
				Guidance					
TR	1	19	5	0	0		Business driven guidance for trust application service providers	(new)	Undefined
SR	0	19	5	1	0		Scoping study and framework for standardization of long term data preservation services, including preservation of/with digital signatures	(new)	Undefined
				Policy & Security Requirements					
EN	3	19	5	1	1		Policy & security requirements for trust service providers providing long term data preservation services, including preservation of/with digital signatures	TS 102 573, TR 102 572	Undefined
EN	3	19	5	2	1		Policy & security requirements for electronic registered delivery service providers	(new)	Undefined
EN	3	19	5	3	1		Policy & security requirements for registered electronic mail (REM) service providers	TS 102 640	Undefined
				Technical Specifications					
EN	3	19	5	1	2		Long term data preservation services, including preservation of/with digital signatures		Undefined
EN	3	19	5	2	2		Electronic registered delivery services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Bindings	(new)	Undefined
EN	3	19	5	3	2		Registered electronic mail (REM) services: - Part 1: Framework and architecture - Part 2: Semantic contents - Part 3: Formats - Part 4: Interoperability profiles	TS 102 640	Undefined
				Conformity Assessment					
-	-	-	-	-			*no requirement identified for such a document - relying on TS 119 403 / EN 319 403*		
				Testing Conformance & Interoperability					
TS	1	19	5	0	4		General requirements for technical conformance and interoperability testing for trust application service providers and the services they provide		Undefined
TS	1	19	5	2	4		Testing conformance and interoperability of electronic registered delivery services: - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of electronic registered delivery service providers	TR 103 071	Undefined
TS	1	19	5	3	4		Testing conformance & interoperability of registered electronic mail services. - Part 1: Testing conformance - Part 2: Test suites for interoperability testing of providers using same format and transport protocols - Part 3: Test suites for interoperability testing of providers using different format and transport protocols		Undefined

Table 6: Standards for trust application service providers

TALGILDU
FØROYAR
01100110 01101111

Trust service status lists providers						Replaces	Expected publication
					Sub-areas		
					Guidance		
TR	1	19	6	0	0 Business guidance for trust service status lists providers	new	published
					Policy & Security Requirements		
TS	1	19	6	1	1 Policy & security requirements for trusted lists providers		Undefined
					Technical Specifications		
TS	1	19	6	1	2 Trusted lists	TS 102 231	published
					Conformity Assessment		
-	-	-	-	-	*no requirement identified for such a document - relying on TS 119 403 / EN 319 403*		
					Testing Conformance & Interoperability		
TS	1	19	6	1	4 Testing conformance & interoperability of trusted lists: - Part 1: Test suites for testing interoperability of XML representation of trusted lists. - Part 2: Specifications for testing conformance of XML representation of trusted lists	(new)	Undefined

Table 7: Standards for trust service status lists providers

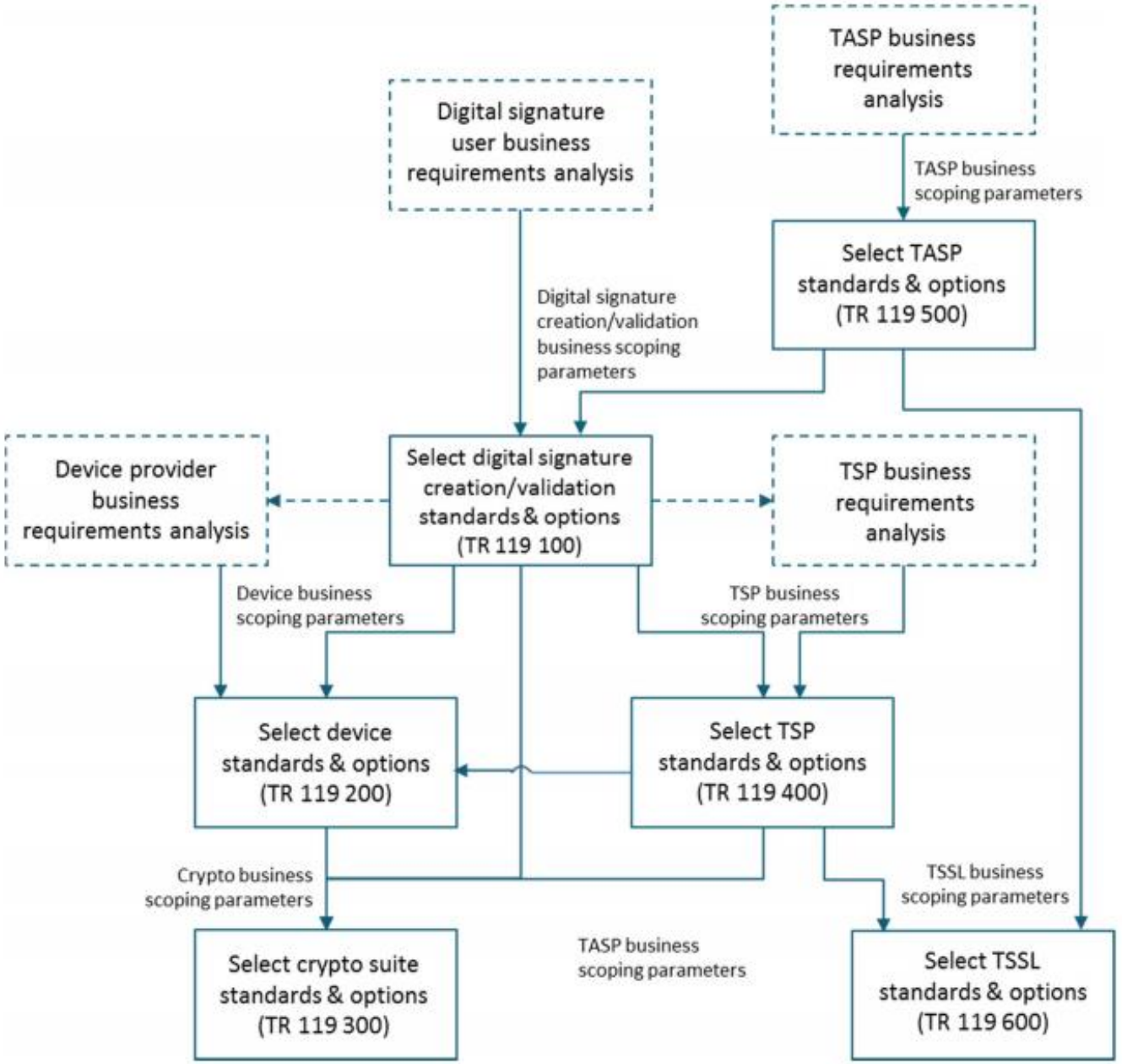


Figure 3: Dependencies of the business scoping parameters among the functional areas

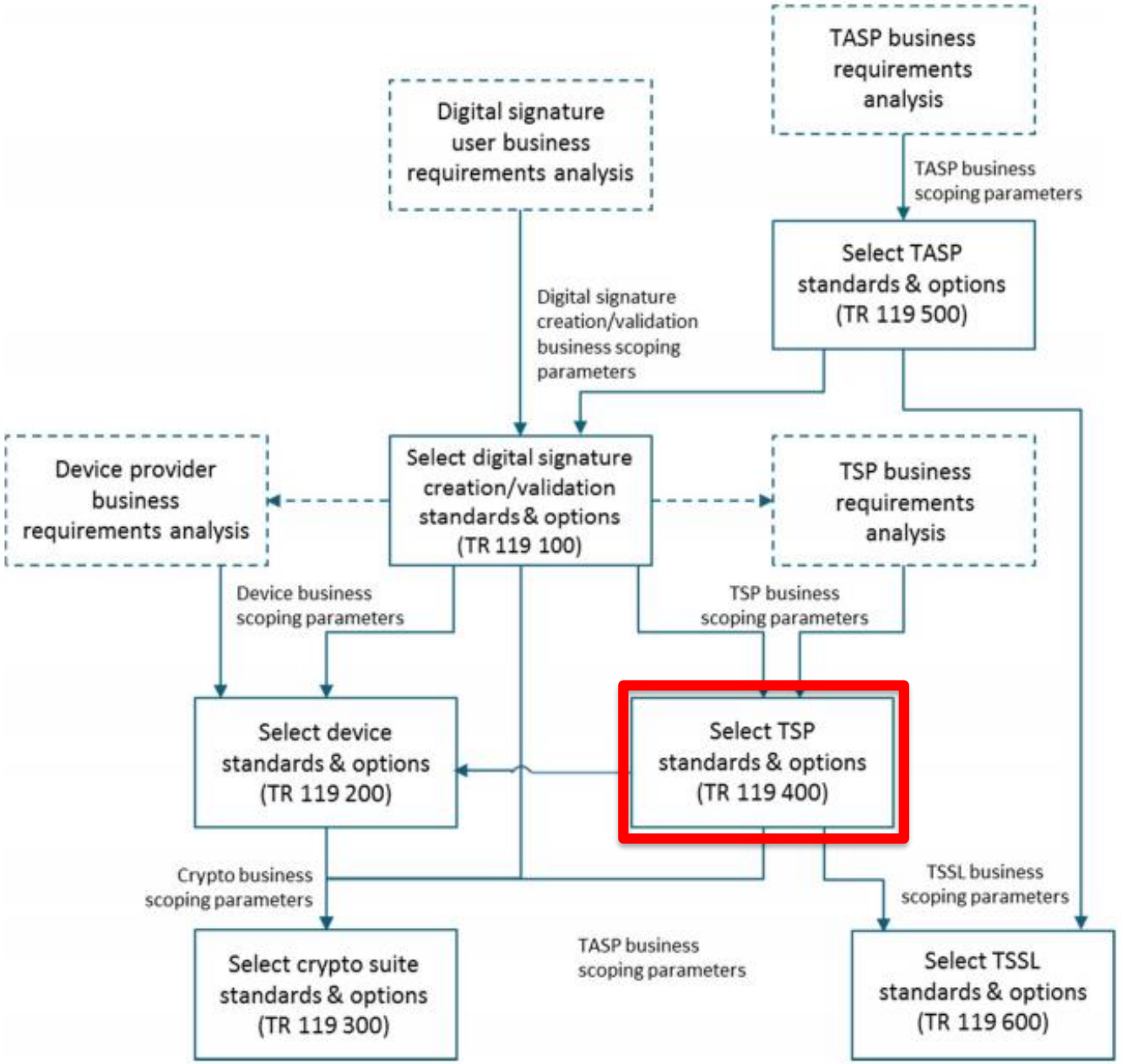


Figure 3: Dependencies of the business scoping parameters among the functional areas

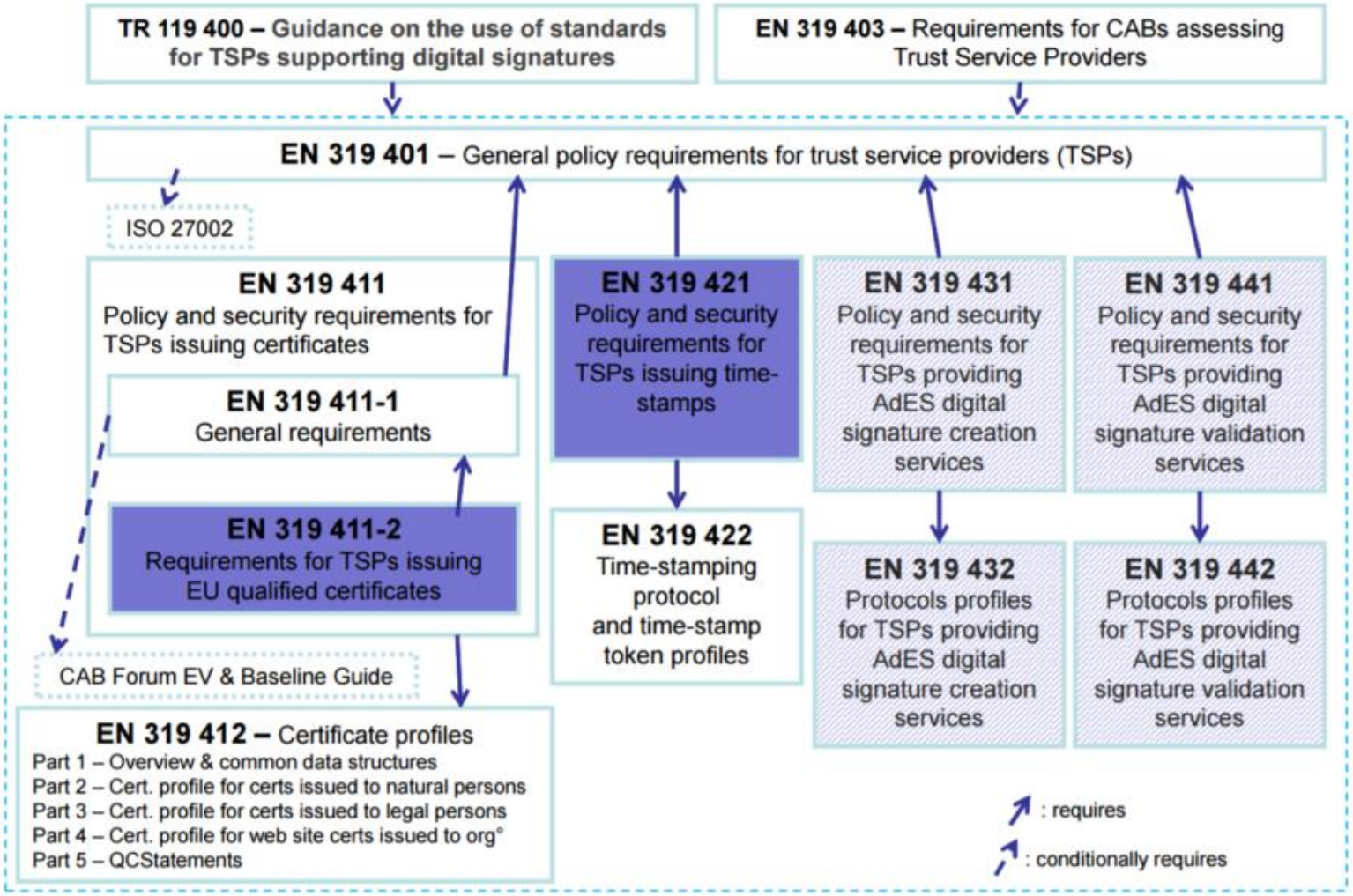
ETSI TR 119 400

TALGILDU FØROYAR
01100110 01101111

Standard	Topic	Business scoping parameters									
		Issuing certificate								Issuing time-stamp	
		General				EU Qualified				General	EU Qualified
		Natural		Legal		Natural		Legal			
		Dig Sig	Web Site	Dig Sig	Web Site	Dig Sig	Web Site	Dig Sig	Web Site		
ETSI EN 319 401 [i.4] (see note 1)	General policy requirements for TSPs	X	X	X	X	X	X	X	X	X	X
ETSI EN 319 411-1 [i.5]	General policy and security requirements for TSP issuing certificates	X	X	X	X	X	X	X	X		
ETSI EN 319 411-2 [i.6]	Policy and security requirements for TSP issuing EU qualified certificates					X	X	X	X		
ETSI EN 319 421 [i.7]	Policy and security requirements for TSPs issuing time-stamps									X	X

eIDAS Regulation & standards – Candidate standards

SEALED



ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

Information technology -- Security techniques -- Entity authentication assurance framework

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

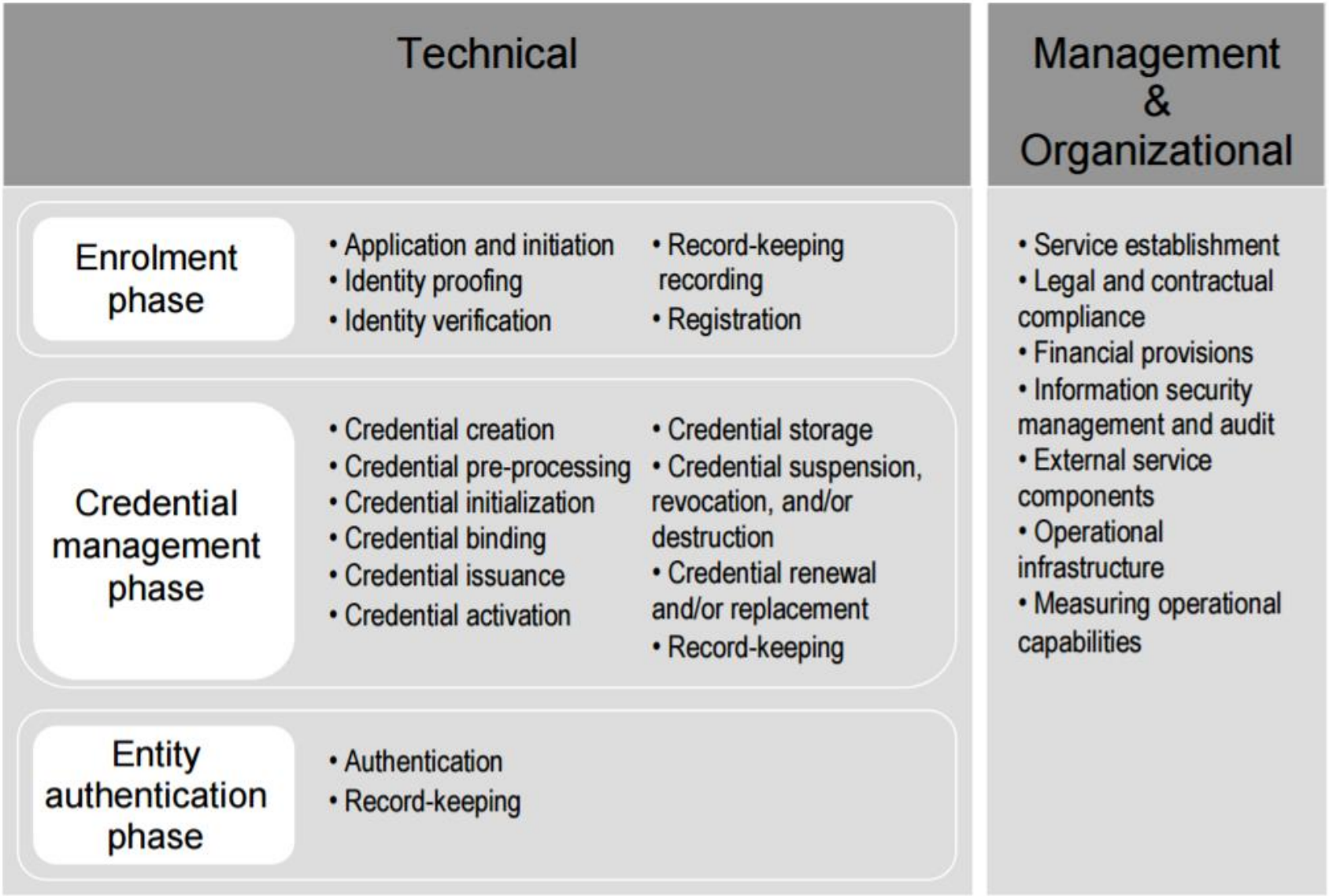


Figure 1 – Overview of the Entity Authentication Assurance Framework

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

Table 6-1 – Levels of assurance[2]

Level	Description
1 – Low	Little or no confidence in the claimed or asserted identity
2 – Medium	Some confidence in the claimed or asserted identity
3 – High	High confidence in the claimed or asserted identity
4 – Very high	Very high confidence in the claimed or asserted identity

2 LoA is a function of the processes, management activities, and technical controls that have been implemented by a CSP for each of the EAAF phases based on the criteria set forth in clause 10.

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

Table 6-2 – Potential impact at each level of assurance

Potential impact of authentication errors	Level of assurance*			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Min	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to the entity, its programs, or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Mod	Sub	High
Personal safety	N/A	N/A	Min Mod	Sub High
Civil or criminal violations	N/A	Min	Sub	High
* Min=Minimum; Mod=Moderate; Sub=Substantial; High=High				

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

Table 8-1 – Applying identity proofing objectives to the LoAs

LoA	Description	Objective	Controls	Method of processing[4]
LoA1 – low	Little or no confidence in the claimed or asserted identity	Identity is unique within a context	Self-claimed or self-asserted	Local or remote
LoA2 – medium	Some confidence in the claimed or asserted identity	Identity is unique within context and the entity to which the identity pertains exists objectively	Proof of identity through use of identity information from an authoritative source	Local or remote
LoA3 – high	High confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from an authoritative source + identity information verification	Local or remote
LoA4 – very high	Very high confidence in the claimed or asserted identity	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from multiple authoritative sources + identity information verification + entity witnessed in person[5]	Local only

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

Table 10-1 – Threats to the enrolment phase

Threat	Examples
Impersonation	Some examples of impersonation are when an entity illegitimately uses another entity's identity information, and when a device registers with a network using a spoofed media access control (MAC) address.

Table 10-2 – Enrolment phase controls for each LoA

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
Impersonation	IdentityProofing: PolicyAdherence	#1	#1	#1	#1
	IdentityProofing: In Person				#2
	IdentityProofing: AuthoritativeInformation	#3	#4	#5	#6

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

#6. The following controls apply:

- all controls from #5.

  In addition:

  a) For humans
     - The entity shall provide identity information from at least one additional policy-compliant authoritative source.

  b) For NPEs:
     - Additional devices connected to a computer, smartphone or similar processor shall be recorded at issuance and cryptographically bound to the anchor device (e.g., trusted hardware enabled device, biometric reader, smart cards, GPS geo-authenticator).
     - Any changes in the binding arrangements between devices shall be managed through the RA. Where possible, the network management capability should alert the RA or network management of any changes in device relationships and any corrective action taken.
     - Capability shall be in place to prevent any altered device relationships from working; and
     - a LoA4 software code shall be digitally signed with an LoA4, human-issued credential and shall be counter-signed by the RA as proof of acceptance before being taken into use.

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

Table 10-4 – Credential management controls for each LoA

Threats	Controls	Required controls			
		LoA1	LoA2	LoA3	LoA4
CredentialCreation: Tampering	AppropriateCredentialCreation	#1	#1	#2	#2
	HardwareOnly				#3
	StateLocked				#4
CredentialCreation: UnauthorizedCreation	TrackedInventory	#5	#5	#5	#5
CredentialIssuance: Disclosure	AppropriateCredentialIssuance	#6	#7	#7	#8
CredentialActivation: UnauthorizedPossession CredentialActivation: Unavailability	ActivatedByEntity	#9	#9	#10	#11
CredentialStorage: Disclosure CredentialStorage: Tampering CredentialStorage: Duplication CredentialStorage: DisclosureByEntity	CredentialSecureStorage	#12	#13	#14	#15
CredentialRevocation: DelayedRevocation CredentialRevocation: UseAfterDecommissioning	CredentialSecureRevocation &Destruction	#16	#16	#16	#16
CredentialRenewal: Disclosure CredentialRenewal: Tampering CredentialRenewal: UnauthorizedRenewal	CredentialSecureRenewal	#17	#17	#18	#19
CredentialRecordkeeping: Repudiation	RecordRetention	#20	#20	#21	#21

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

Table 10-5 – Summary of threats to the use of credentials in the authentication phase

Threat	Examples
General threats	General threats to authentication include many categories of threat common to any type of ICT. Some examples include keystroke loggers, social engineering, and user errors. Except for the use of multifactor authentication, controls against these threats are beyond the scope of this Recommendation. Note that multifactor authentication does not protect against all possible general threats.
OnlineGuessing	An attacker performs repeated logon attempts by guessing possible values of the credential.
OfflineGuessing	Secrets associated with credential generation are exposed using analytical methods outside the authentication transaction. Password cracking often relies upon brute force methods, such as the use of dictionary attacks. With dictionary attacks, an attacker uses a program to iterate through all of the words in a dictionary (or multiple dictionaries in different languages), computes the hash value for each word, and checks the resultant hash value against the database. The use of rainbow tables is another password cracking method. Rainbow tables are pre-computed tables of clear text/hash value pairs. Rainbow tables are quicker than brute-force attacks because they use reduction functions to decrease the search space. Once generated or obtained, rainbow tables can be used repeatedly by an attacker.
CredentialDuplication	The entity's credential, or the means to generate credentials, has been illegitimately copied. An example would be the unauthorized copying of a private key.
Phishing	An entity is lured to interact with a counterfeit verifier, and tricked into revealing his or her password or sensitive personal data that can be used to masquerade as the entity. An example is when an entity is sent an email that redirects him or her to a fraudulent website and asks the user to log in using his or her username and password.

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

Table 10-6 – Summary of controls for threats to the use of credentials according to LoA

Threats	Controls	Required controls				
		LoA*	LoA1	LoA2	LoA3	LoA4
General**	MultiFactorAuthentication				#1	#1
OnlineGuessing	StrongPassword CredentialLockOut DefaultAccountUse AuditAndAnalyze	#2 #3 #4 #5				
OfflineGuessing	HashedPasswordWithSalt	#6				
CredentialDuplication	AntiCounterfeiting	#7				
Phishing	DetectPhishingFromMessages AdoptAntiPhishingPractice MutualAuthentication	#8 #9 #10				
Eavesdropping	NoTransmitPassword EncryptedAuthentication DifferentAuthenticationParameter	#11 #12 #13				
ReplayAttack	DifferentAuthenticationParameter Timestamp PhysicalSecurity	#13 #14 #15				
SessionHijacking	EncryptedSession FixProtocolVulnerabilities CryptographicMutualHandshake	#16 #17 #18				
ManInTheMiddle	MutualAuthentication EncryptedSession	#10 #16				

ISO/IEC 29115

TALGILDU FØROYAR
01100110 01101111

EncryptedSession

#16. Encrypted sessions shall be used.

FixProtocolVulnerabilities

#17. Platform patches to fix protocol vulnerabilities (e.g., TCP/IP) shall be used.

CryptographicMutualHandshake

#18. A mutual handshake exchange based on cryptography (e.g., TLS) shall be used.

CredentialActivation

#19. An activation feature shall be required to use the credential (e.g., entering a PIN or biometric information into the hardware device containing the credential).

CodeDigitalSignature

#20. Digital signatures shall be verified against a trusted source to counter the downloading of software that has been modified by unauthorized parties.

LivenessDetection

#21. Liveness detection techniques shall be used to identify the use of artificial biometric characteristics (e.g., forged fingerprints).

TALGILDU
FØROYAR
01100110 01101111

National Standard for Identiteters Sikringsniveauer (NSIS)

Standarden indeholder en række krav til ID-tjenester på fire forskellige sikringsniveau'er (Niveau 1 – 4). Det laveste niveau (1) har relativt lave krav, mens de høje niveau'er (3 og 4) har relativt høje krav. Tilgangen med fire niveau'er er valgt med udgangspunkt i gængs praksis for rammeværk som ISO 29115, STORK QAA, NIST SP 800-63 og Kantara Initiative's IAF. eIDAS-forordningen opererer med tre niveau'er ("low", "substantial" og "high") der svarer til niveau hhv. 2, 3 og 4 i denne standard.

TALGILDU
FØROYAR
01100110 01101111

Takk fyri!