Mars 2021

Tæknileg kröfulýsing vegna rafrænna þinglýsinga

Stjórnarráð Íslands
Fjármála- og efnahagsráðuneytið

Útgefandi:
Stafrænt Ísland, fjármála- og efnahagsráðuneytið

Mars 2021

Island@island.is

Island.is

Umbrot og textavinnsla:
Fjármála- og efnahagsráðuneytið / Stafrænt Ísland

Efnisyfirlit

1. Tæknileg kröfulýsing vegna rafrænna þinglýsinga

Rafrænar þinglýsingar er lykilþáttur í stafrænni stjórnsýslu. Grundvöllur fyrir framkvæmd rafrænna þinglýsinga er tækniuppbygging og hvernig gögn eigi að berast til sýslumanna með rafrænum hætti.

Til staðar er reglugerð Evrópuþingsins og Ráðsins (ESB) nr. 910/2014, gjarnan nefnd eIDAS, sem var innleidd í landsrétt með lögum nr. 55/2019 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti. Með lögunum var ákvæðum reglugerðarinnar veitt lagagildi hér á landi og er markmið laganna að tryggja að örugg rafræn auðkenning og sannvottun sé möguleg til aðgangs að nettengdri þjónustu yfir landamæri sem aðildarríki á EES-svæðinu bjóða einstaklingum og lögaðilum. Þá þjóna lögin jafnframt þeim tilgangi að auka traust í rafrænum viðskiptum með því að kveða á um réttaráhrif og kröfur til rafrænna auðkenningarleiða og traustþjónustu. eIDAS reglugerðina má finna hér: https://www.althingi.is/lagasafn/pdf/151a/i32014R0910.pdf

Við vinnslu á rafrænum þinglýsingum er búið að skilgreina tæknilega uppbyggingu sem uppfyllir kröfur fyrrgreindrar reglugerðar og þau viðmið að lausnum sem hún boðar fyrir rafræna auðkenningu og undirskriftir. Búið er að ákvarða hvernig undirritun, birting og varðveisla gagna eigi að fara fram, ásamt því að skilgreina framleiðsluferlið á skjölum hjá þeim sem nýta sér rafrænar þinglýsingar. Lausnin uppfyllir eins og fyrr greinir kröfur reglugerðarinnar og nýtir útgefna staðla sem virka fyrir PDF skjöl (PaDES) og XML (XaDES) skeyti.

Til hagsbóta fyrir hagsmunaaðila, hefur kröfulýsing verið samin/hönnuð með það að markmiði að útfæra gerð, undirritun og varðveislu skjala sem munu berast til þinglýsingar.

Tilgangur kröfulýsinga er tvíþættur:

- Að svara eftirspurn eftir leiðbeiningum um hvernig eigi að útbúa gögn til innsendingar í rafræna þinglýsingu, þ.e. hvaða staðla eigi að miða við í þeim efnum.
- Að útbúa staðla sem tryggja að gögn uppfylli kröfur til varðveislu og öryggis sem sett lög áskilja hverju sinni.

Lausnir og staðlar eru settir fram á ensku þar sem þeir byggja á regluverki ESB. Þá þykir enskan jafnframt líklegri til að tryggja að tæknileg kröfulýsing tapist ekki. Á síðari stigum má sjá fyrir sér að íslensk útgáfa verði útbúin ásamt því að leiðbeiningar og kynningarefni verði aðgengilegt á íslensku.

Kröfulýsing þessi var unnið í samstarfi og samráði við ráðgjafafyrirtækið Nowina sem er viðurkenndur ráðgjafi hjá ESB í rafrænum undirritunum.

1.2 Útdráttur úr kröfulýsingu

1.2.1 Ferli rafrænna þinglýsinga

Rafrænar þinglýsingar munu flæða í gegnum sama verkferli*, mikilvægt er að byggja upp tækniumhverfi fyrir ferlið og tryggja þannig öryggi og gæði.

Aðilar sem koma að þinglýsingu eru:

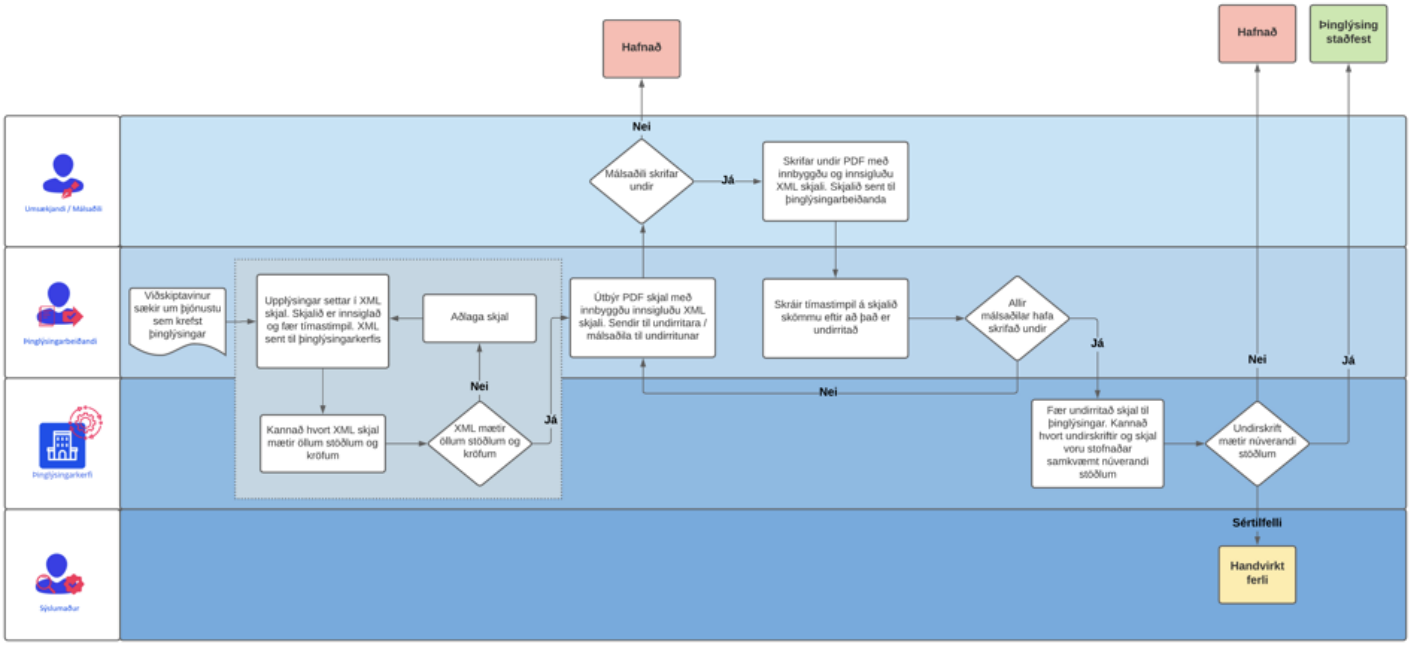
- Undirritari/málsaðili (e. signer)
  Skráður í viðkomandi skjali sem þinglýsingarbeiðandi mun leggja fram til skráningar

- Þinglýsingarbeiðandi (e. Registration applicant)
  Aðilar sem hafa heimild samkvæmt þinglýsingalögum nr. 39/1978, til að leggja fram þinglýsa með rafrænni færslu. Útbýr skjal til undirritunar málsaðila. Sendir undirritað skjal til sýslumanns til skráningar

- Sýslumaður (e. District commissioner)
  Þinglýsir og/eða framkvæmir viðbótar eftirlit á undirrituðu skjali eftir að það hefur verið samþykkt af þinglýsingarkerfinu

Hér má sjá flæðirit rafrænna þinglýsinga:

Þinglýsingabeiðandi útbýr XML og PDF og sendir til þinglýsingar, XML þarf að vera innsiglað af þinglýsingarbeiðanda og PDF undirritað af málsaðila. Í boði verður þjónusta til að prófa inntak XML fyrir hverja tegund færslu. Þinglýsingabeiðandi sendir inn undirritað PDF til rafrænna þinglýsinga, kerfið metur hvort beiðnin fari í sjálfvirka þinglýsingu, handvirka meðferð eða er frávísað.



*aflýsingar og skilmálabreytingar vegna Covid-19 eru undantekningar á verkferli

1.2.2 Útfærsla á XML og PDF

Þinglýsingarbeiðandi þarf að útbúa skjöl til rafrænnar þinglýsingar. Hægt er að skrá tvenns konar skjöl, annars vegar XML skjöl og hins vegar PDF/A-3 sköl.

Eftirfarandi skilyrði gilda um skjöl sem send eru til þinglýsingar:

- Innihald XML þarf að uppfylla kröfur hverrar vefþjónustu fyrir rafrænar þinglýsingar (skilgreint í swagger)
- Þinglýsingarbeiðandi innsiglar XML með .cer skilríki (t.d. útgefið af Auðkenni)
- Umfang hvers XML innsiglis skal vera XML skjalið í heild sinni

- Þegar XML-eyðublaðið er innsiglað, skuldbindur þinglýsingarbeiðandi sig til að hafa safnað og staðfest gögnin sem notuð eru til að fylla út þinglýsingarbeiðnina í samræmi við reglugerð nr. 360/2019, um rafrænar þinglýsingu, með áorðnum breytingum
- PDF er útbúið samkvæmt PDF/A-3 og nýtir eigindi úr XML og staðlað sniðmát frá þinglýsingarbeiðanda
- XML skal vera viðhengt í PDF skjalið (embedded)
- Innihald PDF skjals má ekki stangast á við innihald XML
- PDF skal vera undirritað í heild sinni með fullgildri rafrænni undirritun
- Þegar fleiri en ein undirritun eru á sama skjali, skal ekki bæta við gögnum í skjal milli hverrar undirritunar
- XML innsigli og PDF undirskriftir skulu aðeins tengjast einu skjali sem berst til þinglýsingar með rafrænni færslu

1.2.3 Kröfur til rafrænna undirritana

Þinglýsingarbeiðandi sér um að fá undirritanir frá öllum málsaðilum áður en skjöl eru send til þinglýsingar. Þinglýsingarbeiðandi getur nýtt sér undirritunar þjónustu við framkvæmd undirritana, en þinglýsingarbeiðandi ber ábyrgð á að undirritanir uppfylli skilyrði rafrænna undirritana.

Skilyrði á undirskriftir má skipta í fimm hluta:

- Lögleg sniðmát
- Formsatriði
- Skilyrði tímastimpla
- Auðkenni undirritara/málsaðila
- Varðveisla og langlífi

XAdES og PAdES undirritanir skulu uppfylla kröfur um háþróuð rafræn innsigli eins og skilgreint er í lögum um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti, nr. 55/2019

Formsatriði undirritunar:

Lagt er til að þinglýsingarbeiðandi útbúi PDF þannig að “það sem þú sérð er það sem þú skrifar undir” (e. What you see is what you sign). Sýna skal skýrt og sjónrænt hvaða upplýsingar verða skráðar, þetta felur í sér að birta þær upplýsingar sem eru til staðar í innfellda innbyggða XML forminu, sýna skal með skýrum hætti hvaða skuldbindingu, framsal eða afsal réttinda eða eigna undirritun felur í sér.

1.2.4 Staðfesting og varðveisla

Þinglýsingarbeiðandi skal ekki staðfesta undirritun áður en skjal er sent til þinglýsingar með rafrænni færslu (aðeins nota PAdES-B-T). Þinglýsingarbeiðandi skal ekki búa til PAdES-B-LT eða PAdES-B-LTA undirskriftir eða styrkja undirskrift að því marki áður en skjöl eru send til þinglýsingar með rafrænni færslu. Þetta er til að koma í veg fyrir að afturköllunarefni sem gefið er út fyrir stofnun undirskriftar verði bætt við undirskrift.

Þinglýsingarbeiðandi ber ábyrgð á varðveita undirskriftir til lengri tíma. Varðveisla undirskrifta skal fara fram á viðeigandi formi til að tryggja áreiðanleika undirskriftar yfir langan tíma. Þinglýsingarbeiðendur skulu ekki reiða sig á vettvang sýslumanns til að varðveita undirskriftir.

2. Introduction

2.1 Business or Application Domain

2.1.1 Scope and boundaries of signature policy

The present document describes the technical specifications that electronic signatures in electronic registrations submitted to the National Registry of Iceland shall meet in order to be accepted as technically valid by the national electronic registration signature validation process.

Other requirements bearing on electronic registration not specific to the signature itself are out of scope of the present document.

The document currently addresses only signatures created in the context of electronic registrations made to the District Commissioners of Iceland and in the specific use case of web services used by automatic processes by domestic creditors and real estate brokers who submit registrations to the District Commissioners of Iceland. Documents issued by citizens, public and private organizations (e.g. banks or the government), or other parties in possession of an Icelandic National registry ID. Any signature created outside of this context are out of scope of the present document. In this context, signers are expected to be in possession of signing means provided by the Icelandic qualified trust service provider “Auðkenni”. More use cases are expected to be added in the future.

Finally, the present document also describes technical specifications for electronic seals created on XML forms that are submitted to the Registration System for verification of business content, however no validation of such seals is currently foreseen, and those specifications are provided as guidelines.

2.1.2 Domain of applications

Not applicable.

2.1.3 Transaction context

Not applicable.

2.2 Document and policy names, identification and conformance rules

2.2.1 Signature policy document and signature policy name

The name of the present signature policy is: “District Commissioner registration platform (DCRP) technical signature policy”.

2.2.2 Signature policy document and signature policy identifier

The reference for this signature policy is “DCRP_TECH_SIG_POL_v1.0”.

2.2.3 Conformance rules

Not applicable: this document is structured as per ETSI TS 119 172-1 (https://www.etsi.org/standards) , the reader is advised to refer to that document for more information about the content of each section.

2.2.4 Distribution points

The latest version of the present signature policy will be available at the URL: https://island.is/rafraenar-thinglysingar

2.3 Signature policy document administration

2.3.1 Signature policy authority

Digital Iceland is the authority responsible for the present technical signature policy:

Digital Iceland, Ministry of finance and economic affairs

Arnarhvoli við Lindargötu, 101 Reykjavík, Iceland

Phone: (+354) 545 9200

2.3.2 Contact person

Questions pertaining to the present signature policy can be addressed to Digital Iceland via:

- The email address island@island.is; or
- The contact form available at the URL: https://island.is/stafraent-island/hafa-samband

2.3.3 Approval procedures

Any modification made to this document is formally approved by the Steering committee for DCRP during a meeting or through email exchanges. Approved updates to the signature policy currently in force are communicated and published prior to this new policy becoming applicable. An amended signature policy shall not take effect earlier than 30 days after publication

2.4 Definitions and Acronyms

2.4.1 Definitions

- Electronic signature: data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.
- Advanced electronic signature: electronic signature which is
    - uniquely linked to the signatory;
    - capable of identifying the signatory;
    - is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
    - linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

- **Qualified electronic signature:** advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.
- **Electronic seal:** data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;
- **Advanced electronic seal:** electronic seal which is
    - uniquely linked to the creator of the seal;
    - capable of identifying the creator of the seal;
    - is created using electronic seal creation data that the signatory can, with a high level of confidence, use under his sole control; and
    - linked to the data sealed therewith in such a way that any subsequent change in the data is detectable.
- **Qualified electronic seal:** advanced electronic seal that is created by a qualified electronic seal creation device, and which is based on a qualified certificate for electronic seal.
- **Signatory:** natural person who creates an electronic signature.
- **Creator of seal:** legal person who creates an electronic seal.
- **Signer:** Signatory or creator of seal.
- **Electronic signature creation device:** configured software or hardware used to create an electronic signature.
- **Qualified electronic signature creation device:** electronic signature creation device that has been certified as meeting the appropriates requirements laid down in the eIDAS Regulation by a certification body notified to the European Commission, and that has been published by the European Commission in the list of certified qualified electronic signature creation devices.
- **Electronic signature creation data:** unique data which is used by the signatory to create an electronic signature.
- **Electronic seal creation device:** configured software or hardware used to create an electronic seal.
- **Qualified electronic seal creation device:** electronic seal creation device that has been certified as meeting the appropriates requirements laid down in the eIDAS Regulation by a certification body notified to the European Commission, and that has been published by the European Commission in the list of certified qualified electronic seal creation devices.
- **Electronic seal creation data:** unique data which is used by the creator of seal to create an electronic seal.
- **Signature augmentation:** process of incorporating to a digital signature information aiming to maintain the validity of that signature over the long term.
- **Signature validation:** process of verifying and confirming that a digital signature is technically valid.
- **Conformity assessment body:** a body defined in eIDAS Art. 3(18).
- **District commissioner**: as defined in Act no. 50/2014 about power of execution and administration for the government in Icelandic´s districts (i. Lög nr. 50/2014 um framkvæmdarvald og stjórnsýslu ríkisins í héraði). The law describes the nine Commissioner's offices around Iceland and their legal power within each district.
- **Registers Iceland**: as defined in Act no. 70/2018 about registers Iceland (i. Lög nr. 70/2018 um Þjóðskrá Íslands).
- **National electronic registration signature validation service**: the validation service provided by the DCR platform as part of its Registration System.
- **Validation service**: a signature and/or seal validation service as described in act no. 55/2019, on electronic identification and trusted service for electronic transactions (i. Lög um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti, nr. 55/2019).
- **DCR platform**: as defined in Registration act, no. 39/1978, with later amendments (i. Þinglýsingalög nr. 39/1978) and regulation no. 360/2019 on electronic registration (i. Reglugerð nr. 360/2019 um rafrænar þinglýsingar).
- **Registration System**: The technical IT system that provides assertions on the technical and/or business validity of the electronic registration submitted on the DCR platform.

2.4.2 Acronyms

RI	Registers Iceland
NERSVS	National electronic registration signature validation service
SCSP	Signature Creation Service Provider
DCR	District Commissioner Registration

3. Signature application practices statements

3.1 Requirements for the Signature Creation Application

The recommended set of policy and security requirements that the SCSP should meet is specified in the standard [ETSI TS 119 431-2].

3.2 Requirements for the Driving Application

The recommended set of policy and security requirements that the Driving Application (e.g. the web banking application contacting the SCSP) should meet is specified in the standard [ETSI TS 119 101].

4. Business Scoping Parameters

4.1 BSPs mainly related to the concerned application/business process

4.1.1 BSP (a): Workflow (sequencing and timing) of signatures

This signature policy takes place in a workflow where 3 actors are concerned:

- The signer(s), who issues an “
- which will be submitted for registration by the registration applicant;

  NOTE 1: Signers are expected to be in possession of signing means provided by the Icelandic qualified trust service provider “Audkenni”.
- The registration applicant, who submits the agreement signed by the signer to the Registration System;
- The district commissioners, who register and/or perform additional checks on the submitted signed agreement when it has been accepted by the Registration System of the DCR platform.

In this workflow, two types of signed/sealed documents are addressed by this signature policy:

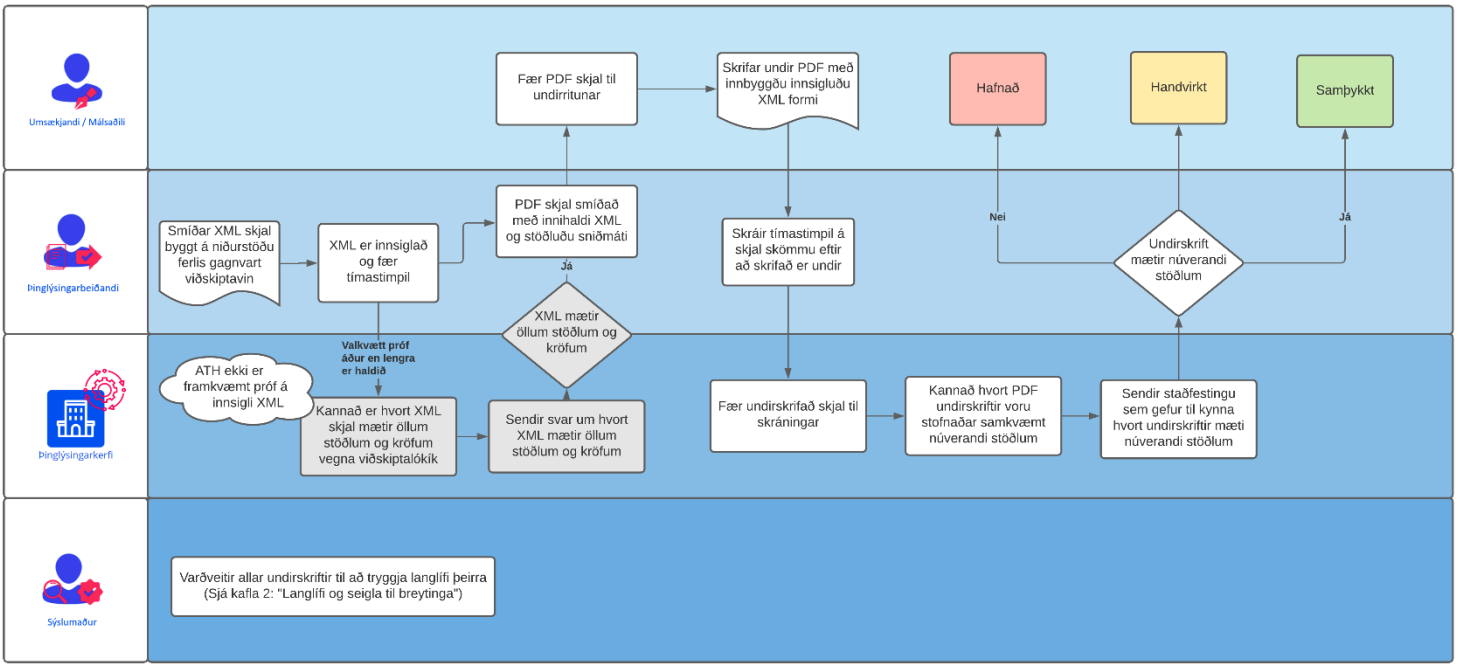
- A sealed XML form; and
- A signed PDF.

The workflow is the following:

a) The registration applicant receives an XML form completed by its client.
b) The registration applicant seals and then timestamps the XML form.
c) The registration applicant submits the sealed XML to the Registration System for validation of the business payload.

   NOTE 2: The Registration System does not perform seal validation.
d) The Registration System provides to the registration applicant an indication of whether XML form complies with the appropriate business requirements.
e) If the Registration System provided an indication that the XML form does indeed comply with those requirements, the registration applicant requests to its client to sign a PDF with the sealed XML form embedded in that PDF.
f) The client signs the PDF. Multiple signers can be concerned.
g) The registration applicant timestamps the signed PDF each time a signature is created, shortly after the signature creation.
h) The registration applicant submits to the Registration System the signed document for registration.
i)
j) The Registration System provides to the registration applicant an indication of whether the PDF signature(s) was/were created according to the present policy, in the form of a validation report.
k) If the DCR platform concludes that the signature(s) does/do not comply with the present policy, the registration is rejected.
l) The signature is later augmented by the district commissioner to ensure long term preservation. Multiple augmentations can occur.

NOTE 3: As stated in “BSP (j): Longevity and resilience to change”, registration applicants are also expected to preserve the signatures of the signed documents.



When CRLs are used for retrieving revocation data, signature augmentation shall not occur before 24h have passed since signature creation.

Signature augmentation shall be made in compliance with section “BSP (j): Longevity and resilience to change”.

4.1.2 BSP (b): Data to be signed

As described in the workflow, only two types of data can be signed/sealed:

- XML documents; and
- PDF/A-3 documents.

PDF documents shall include embedded sealed XML but shall not include any dynamic content.

The scope of each PDF signatures shall be the full document, including the embedded sealed XML.

The scope of the XML seals shall be the full XML document.

When multiple signatures are created on a PDF document, there shall not be any additional data added between each signature creation.

NOTE 1: This mitigates the risk of PDF shadow attacks.

NOTE 2: This means, in particular, that if a PDF document contains N signatures and M revisions with the earliest signatures appearing in revision number K < M, then each PDF revision starting from revision K up until revision K+N contains a signature with scope the full document.

4.1.3 BSP (c): The relationship between signed data and signatures

XML seals and PDF signatures shall only bear on one data object.

XML seals shall be created in one of the XAdES baseline formats, complying with [ETSI EN 319 132-1].

XAdES signature shall be enveloped, using the void string ("") to reference the root element of the signed data object. This mitigates the risk of wrapping attacks.

The PDF signatures shall be created in one of the PAdES baseline formats, complying with [ETSI TS 319 142-1]

NOTE: PAdES signatures cannot be detached nor enveloping.

4.1.4 BSP (d): Targeted community

The targeted community are the entities allowed by national law to submit electronic registration according to Registration act, no. 39/1978, with later amendments (i. Þinglýsingalög nr. 39/1978) as well as the district commissioners.

4.1.5 BSP (e): Allocation of responsibility for signature validation and augmentation

Not applicable.

NOTE: Validation of electronic signatures are expected to be performed by the DCR during preservation processes. No responsibility is allocated to other parties.

4.2 BSPs mainly influenced by the legal/regulatory provisions associated to the concerned application/business process

4.2.1 BSP (f): Legal type of the signatures

The XAdES signatures shall meet the requirements for advanced electronic seals as defined in the [eIDAS Regulation] and implemented in Act no. 55/2019 about electronic identification and trusted service for electronic transactions (i. Lög um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti, nr. 55/2019).

The PAdES signatures shall meet the requirements for qualified electronic signatures as defined in the [eIDAS Regulation] and implemented in Act no. 55/2019 about electronic identification and trusted service for electronic transactions (i. Lög um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti, nr. 55/2019).

NOTE: The requirements laid down by the present signature policy aim, among other, to ensure that upon creation signatures that comply to the present signature policy can be determined as technically suitable for meeting those eIDAS requirements under the applicability rules specified in [ETSI TS 119 172-4].

4.2.2 BSP (g): Commitment assumed by the signer

The XML form contains data that has been gathered and verified by the registration application. Due diligence is expected from the registration application, and consequently: When sealing the XML form, registration applicants commit to having gathered and verified the data used to fill the XML form in compliance with Regulation no. 360/2019, on electronic registration, with later amendments (i. Reglugerð nr. 360/2019 um rafrænar þinglýsingar, með áorðnum breytingum).

When signing the PDF document, signers acknowledge having duly read and approved its content, subsequently being bound by it. The commitment-type-indication attribute defined in ETSI EN 319 122-1 clause 5.2.3 (whose presence is conditioned according to ETSI EN 319 142-1 clause 6.3) shall be present, and

shall indicate the commitment type “Proof of approval” identified by the OID 1.2.840.113549.1.9.16.6.5 as defined in ETSI TS 119 172-1 Annex B.

4.2.3 BSP (h): Level of assurance on timing evidences

All signed/sealed documents shall be timestamped by the registration applicant each time a signature/seal is created, no longer than 30 seconds after the creation of that signature/seal.

NOTE 1: This means that PDF documents submitted for electronic registration must be submitted in PAdES-B-T format.

NOTE 2: On currently existing compatible signing platforms, signatures created by signing means provided by the Icelandic qualified trust service provider “Audkenni” are always created with a signature timestamp.

All timestamps used shall meet the requirements of qualified electronic timestamps, as defined in the eIDAS Regulation and implemented in Act no. 55/2019 about electronic identification and trusted service for electronic transactions (i. Lög um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti, nr. 55/2019).

4.2.4 BSP (i): Formalities of signing

For PDF signatures, prior to signing, signers shall be presented with:

- A What You See Is What You Sign environment that, in particular:
    - Clearly and visually displays what information will be registered;
      NOTE: This implies displaying the information present in the embedded XML form, as this XML form is the machine-processable information that will be registered by the District Commissioners.
    - Allows the signer to clearly and visually identify which information he has provided, and which information has been added by the registration applicant;
- A clear indication of which content they are committing to;
- Which kind of commitment they are assuming when signing;

Signers shall only be able to sign when there is a high degree of assurance they have read the entire content they are committing to upon signing.

For XML seals, the registration applicant shall:

- Verify using appropriate means that the XML form submitted for sealing reflects the information submitted by the client, soon to be signer of the PDF.

4.2.5 BSP (j): Longevity and resilience to change

No validation material issued prior to signature/seal creation time shall be added to a signature/seal or be kept/used in a preservation/augmentation process.

Registration applicants should preserve the signatures of the signed documents they submitted for registration. Registration applicants shall not rely on the DCR platform for the preservation of signatures.

Preservation of signatures shall be done in a suitable form, appropriate to ensure trustworthiness of the signature over long period of times.

NOTE 1: Examples of appropriate forms are, among others, recurrent signature augmentations to -LTA level locally, or submission to a QTSP offering a qualified preservation service for qualified electronic signatures.

Registration applicants shall not create PAdES-B-LT or PAdES-B-LTA signatures, or augment a signature to that level prior to submitting a document for electronic registration.

NOTE 2: This is to ensure that no revocation material issued prior to signature creation time will be added to a signature. In most cases documents are submitted for electronic registration shortly after signature creation.

Registration applicants shall not create XAdES-B-LT or XAdES-B-LTA signatures, or augment a signature to that level, prior to submitting an XML document for validation.

4.2.6 BSP (k): Archival

Registration applicants shall not rely on the DCR platform for archiving the submitted documents and shall perform their own archiving process.

When archiving submitted documents, registration applicants should also archive the validation report issued by the NERSVS.

4.3 BSPs mainly related to the actors involved in creating/augmenting/validating signatures

4.3.1 BSP (l): Identity (and roles/attributes) of the signers

No requirements on the identity of the signers are specified in the present document. Such identity attributes are nevertheless present in the business payload of the XML form. Future version of the present document may add identity requirements.

Registration applicant may add identity attributes in the PDF signatures provided it reflects exactly the identity attributes present in the business payload of the embedded XML form.

4.3.2 BSP (m): Level of assurance required for the authentication of the signer

The identity of the signers of PDF signatures shall be ensured by means of a qualified certificate for electronic signature.

The identity of the legal entity creating the XML seal should be ensured by means of a qualified certificate for electronic seal. If compliance to the present policy is claimed by the XML seal, the identity of the legal entity creating the XML seal shall be ensured by means of a qualified certificate for electronic seal.

4.3.3 BSP (n): Signature creation devices

PDF signatures created on files that are to be submitted for registration shall be created by means of a qualified signature creation device.

NOTE: Seals are not accepted for electronic registrations.

XML seals should be created by means of a qualified seal creation device. If compliance to the present policy is claimed by the XML seal, this seal shall be created by means of a qualified seal creation device.

4.4 Other BSPs

4.4.1 BSP (o): Other information to be associated with the signature

Signatures and seals created under the present policy shall reference the present policy using the OID defined in clause " Signature policy document and signature policy identifier" in:

- For XAdES seals, the `SignaturePolicyIdentifier` element described in [ETSI EN 319 132-1] clause 5.2.9 of the `SignedSignatureProperties` container described in clause 4.3.4 of the same document.
- For PAdES signatures, the CAdES `signature-policy-identifier` attribute described in clause 5.2 of [ETSI EN 319 142-1].

For the ease of validation, XAdES and PAdES signatures/seals shall be created with the full chain of certificates from the signing certificate up to the applicable trust anchor included within.

4.4.2 BSP (p): Cryptographic suites

Any signature/seal created under this policy shall use cryptographic algorithms and parameters compliant with the latest version of [ETSI TS 119 312] at the time of creation of the signature/seal with the following amendments:

- For legacy purpose, signatures/seals may be created with a signing certificate whose certificate chain contains certificates that have been created with a signature value computed using a signature algorithm relying on SHA-1.
- The SHA-1 algorithm is only accepted when it has been used to create the signature of X.509 certificates. It is not accepted when it has been used to create the signature of the signed PDF/XML document.

NOTE: Most QTSPs do not create certificates with the SHA-1 algorithm anymore. Still, there may exist already-issued certificates with SHA-1.

The time stated by the timestamps required as timing evidence in clause "BSP (h): Level of assurance on timing evidences" will be the time of reference used for the determination of the suitability of the cryptographic algorithms and parameters used for creating and, when applicable, augmenting the signatures/seals.

4.4.3 BSP (q): Technological environment

Generation of signatures using remote signing technologies may be supported by implementers of the present signature policy.

5. Requirements / statements on technical mechanisms and standards implementation

5.1 Technical counterparts of BSPs – Statement summary

Not applicable.

5.2 Input and output constraints for signature creation, augmentation and validation procedures

5.2.1 Input constraints to be used when generating, augmenting and/or validating signatures in the context of the identified signature policy

Signature generation and augmentation shall comply with the procedures described in [ETSI EN 319 102-1].

When validating PDF signatures, the rules described in [ETSI TS 119 172-4] shall be followed.

NOTE: When multiple signatures are created on a PDF document, validation of each previous PDF signature might be used prior to the creation of any additional signature as a control for ensuring compliance with the requirements described in clause “BSP (b): Data to be signed”.

5.2.2 Output constraints to be used when validating signatures in the context of the identified signature policy

6. Other business and legal matters

See Annex A.5 of [ETSI TS 119 172-1]

7. Compliance audit and other assessments

See Annex A.6 of [ETSI TS 119 172-1]. Whether should perform an audit, etc.