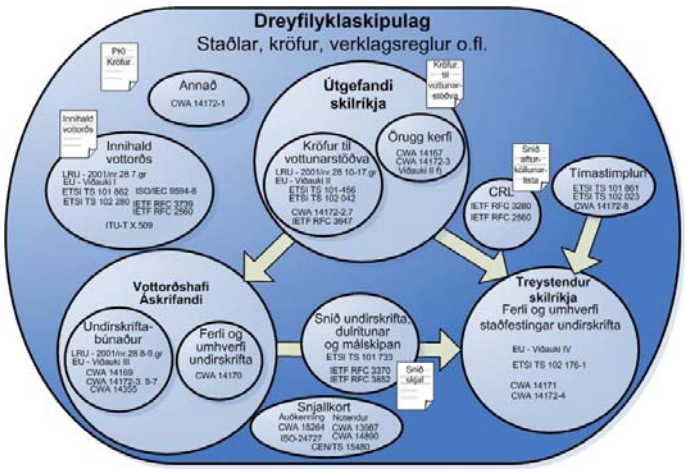
TÆKNINEFND UM DREIFILYKLASKIPULAG Á ÍSLANDI
(RAFRÆN SKILRÍKI)

STAÐLAR OG VIÐMIÐ

Myndin hér til hliðar sýnir helstu kröfumengi í PKI umhverfi. Þar eru sett fram helstu viðmið sem varða sérhvert kröfumengi; staðlar, lög, samþykktir, tilskipanir, tæknilegar tillögur og tæknilýsingar. Þetta eru helstu skjöl sem varða þessa ásýnd, en listinn er ekki tæmandi.

Eftirfarandi er umfjöllun um helstu staðla og viðmið sem eiga við um dreifilyklaskipulag í heild, um innihald skilríkja, samskiptahætti um stöðu þeirra og um dulritaða og undirritaða hluti.



DREIFILYKLASKIPULAG

Tilskipun Evrópuþingsins og ráðsins um rafrænar undirskriftir:

Tilskipun Evrópuþingsins og ráðsins 1999/93/EB frá 13. desember 1999 um ramma bandalagsins varðandi rafrænar undirskriftir

Tilgangurinn með þessari tilskipun er að greiða fyrir notkun rafrænna undirskrifta og stuðla að lagalegri viðurkenningu þeirra. Með tilskipuninni er settur lagarammi um rafrænar undirskriftir og tiltekna vottunarþjónustu í því skyni að tryggja eðlilega starfsemi innri markaðarins.

Tilskipunin fjallar hvorki um þætti sem varða gerð og gildi samninga eða aðrar lagaskyldur, þar sem fram koma kröfur með tilliti til forms sem mælt er fyrir um í landslögum eða lögum bandalagsins, né heldur hefur hún áhrif á reglur og skorður sem eru settar í landslögum eða lögum bandalagsins og stýra notkun skjala.

Íslensk lög:

Lög um rafrænar undirskriftir, nr. 28/2001, með síðari breytingum.
Sjá www.althingi.is – leitarorð „rafrænar undirskriftir".

Lög um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000, með síðari breytingum.
Sjá www.althingi.is – leitarorð „persónuvernd".

Grunnstaðall fyrir dreifilyklaskipulag:

ISO/IEC 9594-8/ITU-T Recommendation X.509: *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

ISO/IEC 9594-8:2005 provides specifications for how information about objects, e.g. persons, is organized, created, maintained and retrieved. Multiple entities are likely deployed to provide the directory service. Communication amongst these entities is authenticated and/or encrypted.

ISO/IEC 9594-8:2005 specifies three frameworks and a number of data objects that can be used to authenticate and secure the communication between two entities, e.g. between two directory service entities or between a web browser and web server. The data objects can also be used to prove the source and integrity of data structures such as digitally signed documents.

Athugið að útgáfa 2005 af ISO/IEC staðlinum er nokkuð nýleg, en ég hef ekki staðfest að hann samsvari nýjasta ITU staðlinum sem er frá 2005. ISO útgáfur eru oft nokkrum árum á eftir ITU-T.

Sjá http://www.iso.org/iso/en/CatalogueListPage.CatalogueList.

Staðlar fyrir fjármálaþjónustu:

ISO 15782-1:2003: *Certificate management for financial services -- Part 1: Public key certificates.*

ISO 15782-1:2003 defines a certificate management system for financial industry use for legal and natural persons that includes credentials and certificate contents, certification authority systems (including certificates for digital signatures and encryption key management), certificate generation, distribution, validation and renewal,

authentication structure and certification paths, revocation and recovery procedures, and extensions to the definitions of public-key certificates and certificate revocation lists. It also recommends some useful operational procedures (e.g. distribution mechanisms, acceptance criteria for submitted credentials). While providing for the generation of certificates that could include a public key used for encryption key management, it does not address the generation or transport of keys used for encryption.

ISO 15782-2:2001: *Banking -- Certificate management -- Part 2: Certificate extensions.*
No abstract available

ISO 21188:2006: *Public key infrastructure for financial services -- Practices and policy framework.*
Sjá http://www.iso.org/iso/en/CatalogueListPage.CatalogueList.

ISO 21188:2006 sets out a framework of requirements to manage a PKI through certificate policies and certification practice statements and to enable the use of public key certificates in the financial services industry. It also defines control objectives and supporting procedures to manage risks.

ISO 21188:2006 draws a distinction between PKI systems used in open, closed and contractual environments. It further defines the operational practices relative to financial services industry accepted information systems control objectives. ISO 21188:2006 is intended to help implementers to define PKI practices that can support multiple certificate policies that include the use of digital signature, remote authentication and data encryption.

ISO 21188:2006 facilitates the implementation of operational, baseline PKI control practices that satisfy the requirements for the financial services industry in a contractual environment. While the focus of ISO 21188:2006 is on the contractual environment, application of this document to other environments is not specifically precluded. For the purposes of this document, the term "certificate" refers to public key certificates. Attribute certificates are outside the scope of ISO 21188:2006.

Samþykktir frá CEN um rafræna undirskriftir:

CEN Workshop Agreement 14365-1:2004: *Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects*.
The purpose of this CWA is to give guidance on the use of electronic signatures. Whilst the focus often has been on "qualified electronic signatures" as specified in Article 5.1 of the Directive, a side effect was that the requirements of employing general electronic signatures (referred to as "5.2 signatures") in e-commerce were not sufficiently addressed.

The purpose of this part of the CWA is therefore to describe the general legal and technical aspects of electronic signatures, and thus extend the work to e-commerce scenarios, paying special attention to technologies with a high deployment capacity, to enable trust, without the need to meet all the strict requirements for "Article 5.1 Signatures".

This part of the CWA is intended for use by both legal and technical experts in the area of electronic signatures, as well as designers of systems and products in this area.

Sjá http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/cwa/electronic+signatures.asp.

CEN Workshop Agreement 14365-2:2004: *Guide on the Use of Electronic Signatures - Part 1: Protection Profile for Software Signature Creation Devices*.
The purpose of this CWA is to give guidance on the use of electronic signatures. Whilst the focus often has been on "qualified electronic signatures" as specified in Article 5.1 of the Directive, a side effect was that the requirements of employing general electronic signatures (referred to as "5.2 signatures") in e-commerce were not sufficiently addressed.

The purpose of this part of the CWA is to specify the security requirements for a signature-creation device that can be implemented in software, and thus fulfil a wider market need than the "Secure Signature-Creation Device" required for qualified electronic signatures.

The part of the CWA is intended for use technical experts and designers of systems and products in the area of electronic signatures.

Sjá http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/cwa/electronic+signatures.asp.

Aðrar vísanir:

SEID verkefnið í Noregi, sem reyndar lauk í júní 2005:
SEID-prosjektet har vært et samarbeidsprosjekt om elektronisk ID (eID) og elektronisk signatur (eSignatur) med deltakelse fra 15 forskjellige aktører fra offentlig og privat sektor.

Prosjektet har blant annet vært forankret i Regjeringens IT politikk stadfestet i "eNorge 2005", og hadde som mål å bidra til og legge til rette for

- størst mulig grad av samtrafikk mellom aktuelle PKI-leverandører,
- en forenkling av dagens infrastruktur for brukersteder, samt
- fjerning av tekniske og praktiske hindere for å ta i bruk infrastrukturen,

og gjennom dette legge til rette for allmenn bruk av eID og eSignatur på tvers av aktørene i det norske markedet.

Prosjektet hadde hovedsakelig teknisk fokus, og har primært utarbeidet omforente tekniske spesifikasjoner på områder hvor disse enten manglet eller var sprikende, og på den måten utgjorde en barriere for å oppnå samtrafikk og enkel bruk av eID og eSignatur.

SEID-prosjektet ble avsluttet i juni 2005.

Sjá http://odin.dep.no/fad/norsk/tema/ITpolitikk/pkiorgan/seid.

INNIHALD SKILRÍKJA

Fjöldi staðla og almennra viðmiða skilgreina innihald skilríkja. Alþjóðastaðallinn ISO/IEC 9594-8/ITU-T Recommendation X.509 er grunnstaðallinn en staðlar frá ETSI og skilgreiningar frá IETF (RFC skjöl) tilgreina nánar hvernig tryggja skal samræmi í útfærslu í dreifilyklaskipulagi í þeim tilgangi að notkun verði sem víðtækust.

Tilskipun Evrópuþingsins og ráðsins 1999/93/EB setti fram kröfur til lagasetningar um rafrænar undirskriftir, vottun og rafræn skilríki í aðildarríkjum Evrópusambandsins. Lög um rafrænar undirskriftir, nr. 28/2001, staðfesta þessar kröfur hér á landi.

ETSI TS 101 862 v1.3.1 (2004-03): *Qualified Certificate Profile.*

The purpose of this standard is to specify format and contents of Qualified Certificates. The standard is based on the IETF draft "X.509 Public Key Infrastructure Qualified Certificates Profile", specifying amendments to meet the requirements as laid down in the European Directive on electronic signatures (1999/93/EC), in Annex 1.

ETSI TS 102 280 v1.1.1 (2004-03): *X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.*

This document defines a common profile for ITU-T Recommendation X.509 based certificates issued to natural persons. The scope of the document is to provide a certificate profile, which will allow actual interoperability of certificates issued for the purposes of qualified electronic signatures, peer entity authentication and data authentication.

Sjá http://pda.etsi.org/pda/queryform.asp.

IETF RFC 3280, apríl 2002: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

This memo profiles the X.509 v3 certificate and X.509 v2 Certificate Revocation List (CRL) for use in the Internet. An overview of this approach and model are provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described and two Internet-specific extensions are defined. A set of required certificate extensions is specified. The X.509 v2 CRL format is described in detail, and required extensions are defined. An algorithm for X.509 certification path validation is described. An ASN.1 module and examples are provided in the appendices.

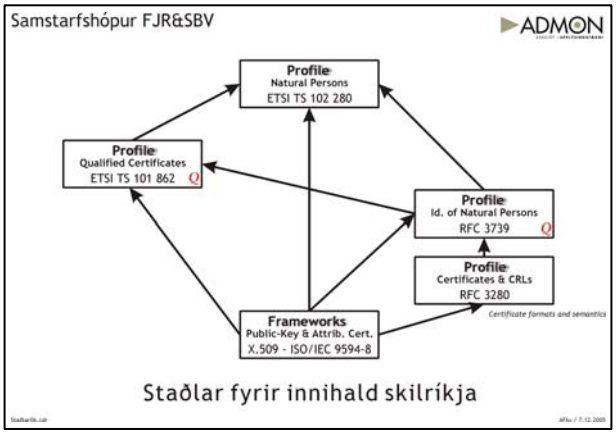
Þessi staðall er með áherslu á notkun X.509 v3 skilríkja í tölvupóstsamskiptum, Ipsec og www viðföngum yfir Internetið.

Sjá http://www.ietf.org/rfc/rfc3280.txt?number=3280.

IETF RFC 3739, mars 2004: *Internet X.509 Public Key Infrastructure Qualified Certificates Profile.*

This document forms a certificate profile, based on RFC 3280, for identity certificates issued to natural persons. The profile defines specific conventions for certificates that are qualified within a defined legal framework, named Qualified Certificates. However, the profile does not define any legal requirements for such Qualified Certificates. The goal of this document is to define a certificate profile that supports the issuance of Qualified Certificates independent of local legal requirements. The profile is however not limited to Qualified Certificates and further profiling may facilitate specific local needs.

Sjá http://www.ietf.org/rfc/rfc3739.txt?number=3739.



Myndin hér til hægri sýnir samhengi þessara staðla. ***Q*** stendur fyrir *Qualified* og vísar til krafna til fullgildra skilríkja.

Sjá sem dæmi SEID skjal Norðmanna um innihald skilríkja:
http://odin.dep.no/filarkiv/265358/SEID_Leveranse_1_-_v1.02.pdf.

SAMSKIPTAHÆTTIR FYRIR STÖÐU SKILRÍKJA

Stöðu skilríkja má miðla með afturköllunarlistum (CRL) sem dreift er reglulega til hagsmunaaðila eða með beinum tengingum hagsmunaaðila við þjónustukerfi, með OCSP samskiptahætti.

Auk IETF RFC 3280 skilgreinir eftirfarandi viðmið OCSP samskiptaháttinn.

IETF RFC 2560, júní 1999: *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*.

This document specifies a protocol useful in determining the current status of a digital certificate without requiring CRLs. Additional mechanisms addressing PKIX operational requirements are specified in separate documents.

Þessi staðall fjallar um OCSP, sem er samskiptaháttur til að miðla stöðu skilríkja.

Sjá http://www.ietf.org/rfc/rfc2560.txt?number=2560.

Sjá sem dæmi SEID skjal Norðmanna um miðlun á stöðu skilríkja:
http://odin.dep.no/filarkiv/265359/SEID_Leveranse_2_-_v1.02.pdf.

FORM OG MÁLREGLUR FYRIR DULRITAÐA OG UNDIRRITAÐA HLUTI

Til að dulritun eða undirskrift sé túlkanleg og hafi gildi þarf að skilgreina ýmsa þætti, eins og staðfestingu þeirra og sannvottun, tímastimplun, safnvistun, gagnvottun og afturköllun. Mikilvægt er að samræmi sé í stefnukröfum um undirritun og tæknilegt samræmi við sannprófun.

Þar sem miðlun dulritaðra og undirritaðra hluta felst í mjög mörgum þáttum þarf að taka tillit til mjög margra viðmiða í mörgum skjölum. Hér fyrir neðan er vísun í eina tækniforskrift frá ETSI sem byggir á X.509 og IETF RFC 3280, 3852 og 3161. ETSI tækniforskriftin og IETF RFC skjölin vísa síðan á fjölda annarra skjala sem varða ýmsa þætti.

ETSI TS 101 733 v1.6.3 (2005-09-26): *Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*.

The document defines a number of Electronic Signature Formats, including electronic signature that can remain valid over long periods. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the electronic signature. The document specifies use of trusted service providers (e.g. Time-Stamping Authorities), and the data that needs to be archived (e.g. cross certificates and revocation lists) to meet the requirements of long term electronic signatures. An electronic signature defined by the document can be used for arbitration in case of a dispute between the signer and verifier, which may occur at some later time, even years later. The present document includes the concept of signature policies that can be used to establish technical consistency when validating electronic signatures but does not mandate their use.

The document also specifies the use of time-stamping and time-marking services to prove the validity of a signature long after the normal lifetime of critical elements of an electronic signature. It also, as an option, defines ways to provide very long-term protection against key compromise or weakened algorithms.

Sjá http://pda.etsi.org/pda/queryform.asp.

IETF RFC 3370, ágúst 2002: *Cryptographic Message Syntax (CMS) Algorithms*.

The Cryptographic Message Syntax (CMS) [CMS] is used to digitally sign, digest, authenticate, or encrypt arbitrary message contents. This companion specification describes the use of common cryptographic algorithms with the CMS. Implementations of the CMS may support these algorithms; implementations of the CMS may also support other algorithms as well. However, if an implementation chooses to support one of the algorithms discussed in this document, then the implementation MUST do so as described in this document.

Sjá http://www.ietf.org/rfc/rfc3370.txt?number=3370.

IETF RFC 3852, júlí 2004: *Cryptographic Message Syntax (CMS)*.

This document describes the Cryptographic Message Syntax (CMS). This syntax is used to digitally sign, digest, authenticate, or encrypt arbitrary message content.

The CMS describes an encapsulation syntax for data protection. It supports digital signatures and encryption. The syntax allows multiple encapsulations; one encapsulation envelope can be nested inside another. Likewise, one party can digitally sign some previously encapsulated data. It also allows arbitrary attributes, such as signing time, to be signed along with the message content, and provides for other attributes such as countersignatures to be associated with a signature.

Sjá http://www.ietf.org/rfc/rfc3852.txt?number=3852.

IETF RFC 3161, ágúst 2001: *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).*

A time-stamping service supports assertions of proof that a datum existed before a particular time. A TSA may be operated as a Trusted Third Party (TTP) service, though other operational models may be appropriate, e.g., an organization might require a TSA for internal time-stamping purposes.

Non-repudiation services [ISONR] require the ability to establish the existence of data before specified times. This protocol may be used as a building block to support such services. An example of how to prove that a digital signature was generated during the validity period of a public key certificate is given in an annex.

Sjá http://www.ietf.org/rfc/rfc3161.txt?number=3161.

Sjá sem dæmi SEID skjal Norðmanna um form og málreglur fyrir undirritaða hluti: http://odin.dep.no/filarkiv/265357/SEID_Leveranse_3_-_v1.0.pdf.

22. janúar 2007

Arnaldur F. Axfjörð