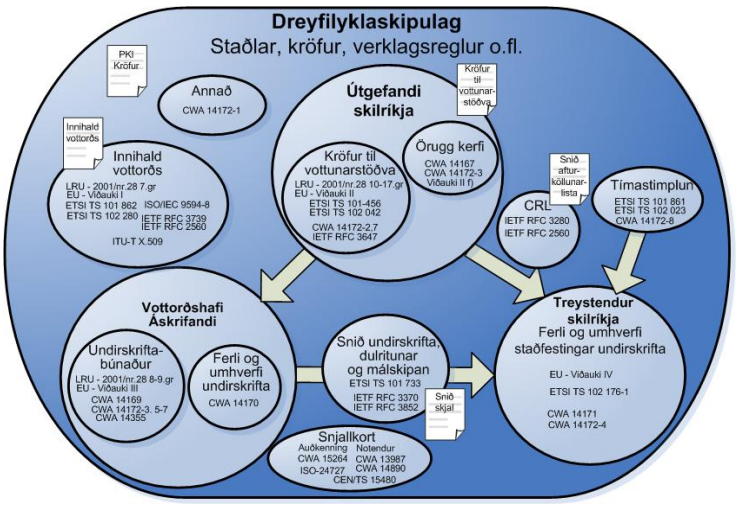
TÆKNINEFND UM DREIFILYKLASKIPULAG Á ÍSLANDI
(RAFRÆN SKILRÍKI)

VERKEFNI NEFNDARINNAR

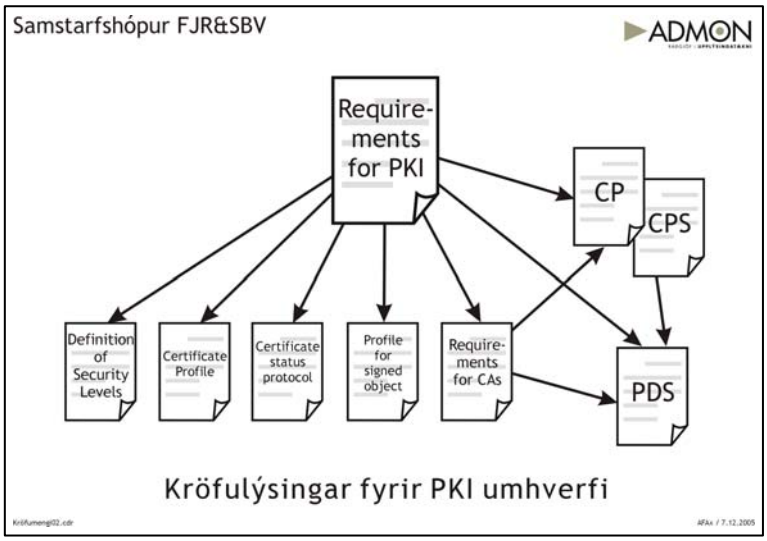
Til að dreifilyklaumhverfi sé opið og skilvirkt þarf að skilgreina ýmsa þætti þess. Myndin hér til hliðar sýnir helstu kröfumengi í PKI umhverfi og helstu skjöl sem skilgreina umhverfið.



Á myndinni Kröfulýsingar fyrir PKI umhverfi er sett fram ein möguleg ásýnd á þessi skjöl og gefið til kynna hvernig þau tengjast. Nokkur skjöl eru ekki á vettvangi Tækninefndar FUT um dreifilyklaskipulag, en það eru CP (vottunarstefna), CPS (yfirlýsing um vottunarframkvæmd) og PDS (birtingarskýrsla dreifilyklaumhverfis).

Einnig þarf að skilgreina almennar tæknilegar kröfur í PKI umhverfi, sem varða stafasett, samskiptahætti og annað það sem þarf til að kerfi og búnaður vinni saman.

Þessar kröfur varða vottunarþjónustu, innihald skilríkja, tæknilega samþættingu í PKI umhverfi, öryggisstig, dreifilyklaskipulag, samskiptahætti, form og málreglur.



Undirritaðir telja að Tækninefnd FUT um dreifilyklaskipulag þurfi að meta hvað af eftirfarandi skilgreiningum nefndin vinni að. Mikilvægt er að byggja upp samstöðu allra hagsmunaaðila og tryggja að almennt samkomulag sé um þær skilgreiningar sem gerðar verða.

LÝSING VERKEFNA

Kröfur til dreifilyklaskipulags

Requirements for PKI

Heildarskjal sem tilgreinir kröfur sem eiga við um dreifilyklaskipulag. Myndar heildarásýnd á kröfur í dreifilyklaskipulagi og vísar í aðrar kröfulýsingar.

Skilgreining á öryggisstigum

Definition of Security Levels

Skilgreining og lýsing á öryggisstigum skilríkja, til dæmis í samræmi við skilgreiningar ETSI; LCP, NCP, NCP+, QCP public og QCP public + SSCD. Skilgreining á notkunarsviði mismunandi öryggisstiga, t.d. fyrir undirskriftir, auðkenningu, sannvottun, heimildir og dulritun.

Samstarfshópur FJR og SBV hefur unnið í slíku skjali en ekki tekið saman formleg drög.

Innihald skilríkja

Certificate Profile

Skilgreining á samræmdum kröfum til innihalds skilríkja byggt á alþjóðlegum stöðlum og viðmiðunum en tilgreinir sértækar staðbundnar kröfur fyrir Ísland. Lagt er til að miðað sé við skilríki sem byggja á X.509 v3 og allar gerðir skilríkja eins og skilgreint er í ETSI TS 102 042 og ETSI TS 101 456 (einka-, starf-, búnaðar- og skipulagsheildarskilríki). Einnig er lagt til að tekið sé byggt á IETF RFC 3280. Mikilvægt er að áhersla sé á einfaldleika og lágmarkskröfur um innihald skilríkjanna þar sem byggt er sem mest á alþjóðlegum og almennt viðurkenndum stöðlum og tæknilýsingum.

Sérfræðingar ríkis og banka hafa tekið saman og gefið út skjalið Innihald rafrænna skilríkja: Samræmt innihald rafrænna skilríkja sem gefin eru út á Íslandi (útgáfa 1.4 frá 30. nóvember 2006). Það skjal er opið öllum sem vilja miða við þær skilgreiningar sem þar eru.

Samskiptahættir fyrir stöðu skilríkja

Certificate Status Protocol

Skilgreining á samræmdum kröfum til samskipta vegna upplýsinga um stöðu skilríkja og sannvottunar á þeim. Varðar bæði afturköllunarlista (CRL) og samskiptahætti fyrir beintengda miðlun (OCSP). Lagt er til að miða m.a. við IETF RFC 3280 (fyrir CRL) og RFC 2560 (fyrir OCSP).

Form og málreglur fyrir dulritaða og undirritaða hluti

Profile for Signed Objects

Skilgreining á samræmdu sniði og málreglum fyrir þá hluti sem miðlað er milli vottorðshafa og hagsmunaaðila, eftir undirritun og/eða dulritun á rafrænum gögnum. Tekur m.a. mið af ETSI TS 101 733, IETF RFC 3370 og RFC 3852.

Kröfur til vottunarstöðva

Requirements for CAs

Skilgreining á stefnumarkandi kröfum til vottunarstöðva fyrir útgáfu skilríkja í rafrænni þjónustu byggt á alþjóðlegum stöðlum og viðmiðunum en tilgreinir sértækar staðbundnar kröfur fyrir Ísland. Lagt er til að miðað sé við skilríki sem byggja á X.509 v3. Í tækniviðmiðum ETSI TS 102 042 og ETSI TS 101 456 eru skilgreind mismunandi skilgríki; einka-, starf-, búnaðar- og skipulagsheildarskilríki og mismunandi öryggisstig (LCP, NCP, NCP+, QCP public og QCP public + SSCD). Kröfur til vottunarstöðva tilgreinir þær kröfur sem vottunarstefna (CP) og yfirlýsing um vottunarframkvæmd (CPS) vottunarstöðva verða að uppfylla.

Í samstarfsverkefni FJR og SBV hafa verið unnin drög að kröfulýsingu fyrir vottunarstöðvar. Þau drög eru byggð á ETSI TS 102 042 og ETSI TS 101 456.

Tæknileg samþætting

Technical Integration

Samþykkt yfirlýsing á tæknilegum og framkvæmdalegum lágmarks kröfum til vottunarstöðva, skilríkja, upplýsingatæknikerfa og annarra þátta dreifilyklaumhverfis. Skjalið inniheldur þær kröfur sem

eru háðar tæknilegri þróun og taka breytingum oftar en stefnumarkandi kröfur, sem eru megin áhersla í öðrum kröfulýsingum.

Lögð er áhersla á að tilgreina megin þætti tæknilegrar samþættingar en ekki tæknileg smáatriði í útfærslu. Meðal þess sem skilgreina þarf er notkun stafasetta og samskiptahættir milli aðila.

Samstarfshópur FJR og SBV hefur unnið í slíku skjali en ekki tekið saman formleg drög.

Tímastimplun

Time Stamping

Ákveðið var á fundi Tækninefndarinnar 8. janúar 2007 að bæta við verkefni um tímastimplun.

Tímastimplun (*time stamping*) staðfestir að tiltekið stafrænt efni, t.d. innihald rafrænna gagna, hafi verið til fyrir tiltekinn tíma (*crypto time stamping*). Hér er ekki átt við stimplun á tímasetningu atburðar (*timestamp*), sem stundum er kallað tímasamstilling (*time synchronisation*).

GILDI SAMÞYKKTA

Fagstaðlaráð í upplýsingatækni hefur stofnað Tækninefnd um dreifilyklaskipulag á Íslandi í samræmi við starfsreglur Staðlaráðs Íslands. Tækninefndin er opinn vettvangur hagsmunaaðila á Íslandi. Samþykkt tækninefndarinnar á skölum hefur því að mati nefndarinnar stöðu tæknilýsingar.

Erlendis er algengt að tækninefndir gefi út svokallaðar samþykktir vinnuhópa (*workshop agreements*) og tæknilegar tillögur (*technical recommendations*), sem hafa ekki stöðu samþykktra tæknilýsinga eða staðla. Þar sem Tækninefnd um dreifilyklaskipulag á Íslandi er opin og formleg tækninefnd á vegum fagstaðlaráðs í upplýsingatækni (FUT) hjá Staðlaráði Íslands er talið að skjöl sem nefndin samþykkir hafi meira gildi en samþykktir vinnuhópa eða tæknilegar tillögur.

Tækninefndin getur farið fram á að samþykkt skjöl verði lögð fram sem frumvarp að ÍST stöðlum.

FORGANGSRÖÐUN

Í eftirfarandi töflu er listi yfir verkefni Tækninefndar um dreifilyklaskipulag á Íslandi eins og hann var samþykktur á fundi nefndarinnar 8. janúar 2007.

Forg.	Verkefni eða afurð	Enskt heiti verkefnis	Tæknilýsing [*Technical Specification*]	ÍST staðall	Áb.
1	Innihald skilríkja	*Certificate Profile*	Samþykkt 8.1.2007		-
2	Samskiptahættir fyrir stöðu skilríkja	*Certificate Status Protocol*			RTJ
3	Form og málreglur fyrir dulritaða og undirritaða hluti	*Profile for Signed Object*			ÓTÞ
4	Skilgreining á öryggisstigum	*Definition of Security Levels*			AFAx /HAB
5	Kröfur til vottunarstöðva	*Requirements for CAs*			
6	Tæknileg samþætting	*Technical Integration*			
-	Kröfur til dreifilyklaskipulags	*Requirements for PKI*			
13	Tímastimplun	*Time stamping*			

Skammstafanir:

AFAx:	Arnaldur F. Axfjörð
HAB:	Haraldur A. Bjarnason
ÓTÞ:	Ólafur Tr. Þorsteinsson
RTJ:	Ragnar T. Jónasson

21. janúar 2007

Haraldur A. Bjarnason
Arnaldur F. Axfjörð