Skilgreiningar á hugtökum

Eftirfarandi orðskýringar eru notaðar í samstarfi ríkis, banka og sparisjóða um uppbyggingu á dreifilyklaskipulagi á Íslandi. Samsvarandi orð á ensku eru skáletruð í sviga.

Afturköllun skilríkja (*certificate revocation*): Óafturkræf aðgerð er felur í sér að skilríki eru gerð ógild áður en gildstími þeirra rennur út. Ekki er hægt að gera afturkölluð skilríki gild aftur.

Afturköllunaraðgangsorð (*revocation password*): Afturköllunaraðgangsorð er viðhaldsaðgangsorð sem þarf ef vottorðshafi eða áskrifandi skilríkja vill afturkalla skilríkin en hefur ekki aðgang að einkalyklinum til að undirrita beiðni um afturköllun.

Afturköllunarlisti skilríkja (*certificate revocation list*): Skrá yfir skilríki sem eru ekki lengur í gildi vegna þess að þau hafa verið afturkölluð (gerð ógild) áður en gildistími þeirra rennur út.

Áskrifandi skilríkja (*certificate subscriber*): Einstaklingur eða lögaðili sem er áskrifandi hjá vottunarstöð fyrir einn eða fleiri vottorðshafa. Áskrifandi getur jafnframt verið vottorðshafi í skilríkjum.

Auðkenningar-PIN (*identification PIN*): PIN-númer sem vottorðshafi notar sem notkunaraðgangsorð fyrir beitingu rafrænna skilríkja til auðkenningar, þegar treystandi vill bera kennsl á vottorðshafann.

Búnaðarskilríki (*device certificate* eða *system certificate*): Skilríki búnaðar sem veitir sjálfvirka þjónustu. Búnaðarskilríki staðfesta að búnaður sem veitir þjónustu sé sá sem skilríkin tilgreina og að skilríkin séu tengd þeim ábyrgðaraðila sem kemur fram í skilríkjunum. Í búnaðarskilríkjum er eigandi búnaðarins áskrifandi skilríkjanna og búnaðurinn vottorðshafi.

Búnaður (*device* eða *system*): Tæki eða kerfi. Búnaður getur verið hvort sem er vélbúnaður eða hugbúnaður.

Dreifilykill (*public key*): Dulmálslykill sem er ætlaður hvaða einindi (e. entity) sem er, til nota fyrir dulritunarsamskipti við eiganda samsvarandi einkalykils. Við tvílykla dulritun er dreifilykill bæði notaður til dulritunar og til að sannprófa rafræna undirskrift.

Dreifilyklaskilríki (*public key certificate*): Rafrænt vottorð sem tilgreinir dreifilykil vottorðshafa og sem tengir dreifilykilinn við vottorðshafann á ótvíræðan hátt. Sjá einnig „vottorð” og „skilríki”.

Dreifilyklaskipulag (*public key infrastructure*): Það skipulag sem þarf til að framleiða og afhenda lykla og skilríki, viðhalda stöðuupplýsingum um skilríkin, gera afturköllunarlista aðgengilega og safnvista viðeigandi upplýsingar. Dreifilyklaskipulag gerir notendum meðal annars kleift að hafa samskipti yfir almenn netkerfi eins og Internetið á öruggan hátt með því að nota par af dulmálslyklum, einkalykil og dreifilykil. Framleiðsla lyklanna ásamt tengingu þeirra við vottorðshafa er staðfest af aðila sem nýtur trausts.

Dreifilyklaveldi (*PKI domain*): Safn óháðra þátta (þar með talið vottunarstöðvar, skráningarstöðvar, virkir notendur í dreifilyklaskipulagi o.fl.) sem starfa í samræmi við stefnumarkandi kröfur fyrir rafræn skilríki sem tilgreindar eru af þeirri reglustjórn sem tengist dreifilyklaskipulaginu.

Dulmálseining (*cryptographic module*): Vélbúnaðareining sem meðal annars framleiðir og varðveitir lykla og notar rafræna undirskrift. Dulmálseining er sérstakt tilvik af varbúnaði sem ætlaður er fyrir framleiðslu, varðveislu og notkun einkalykla í dreifilyklaskipulagi.

Eigind (*attribute*): Gögn sem tengjast einindi (e. entity) sem tilgreina eiginleika sem tengist einindinu.

Eigindaskilríki (*attribute certificate*): Gagnaskipan sem inniheldur safn af eigindum fyrir endanotanda og aðrar upplýsingar, dulritað með einkalykli vottunarstöðvarinnar sem gaf skilríkin út.

Einkalykill (*private key*): Leynilykill (dulmálslykill) sem er ætlaður einum notanda, eiganda lykilsins. Í tvílykla dulritun, eins og í dreifilyklaumhverfi, er einkalykill bæði notaður til dulráðningar og til að búa til rafræna undirskrift.

Einkalykill vottunarstöðvar (*certification authority key*): Einkalykill sem tilheyrir vottunarstöð og er notaður til að undirrita skilríkin sem vottunarstöðin gefur út.

Einkaskilríki: (*private certificate*) Persónuleg rafræn skilríki einstaklinga. Einkaskilríki staðfesta að áskrifandi skilríkja sé sá sem skilríkin tilgreina. Í einkaskilríkjum er áskrifandi skilríkja og vottorðshafi sami aðilinn.

Endanotandi (*end user*): Áskrifendur og vottorðshafar kallast endanotendur þar sem skilríki þeirra eru á enda vottunarslóðar og verða því ekki notuð til að sannvotta önnur skilríki.

Endaskilríki (*end-entity certificate*): Skilríki endaaðila eða endaeinindar. Einindið getur verið persónutengt sem einka- eða starfsmannaskilríki. Endaskilríki geta einnig verið skilríki sem eru ekki tengd persónum s.s.. búnaði, tölvukerfi eða skipulagseiningu eins og félagi, sviði eða deild í fyrirtæki.

Fullgild rafræn undirskrift (*qualified electronic signature*): Útfærð (e. advanced) rafræn undirskrift sem er studd fullgildu skilríki og gerð með öruggum undirskriftarbúnaði (e. secure signature-creation device).

Fullgild skilríki (*qualified certificate*): Skilríki sem hafa að geyma upplýsingar sem kveðið er á um í 7. gr. laga um rafrænar undirskriftir, nr. 28/2001 og er gefið út af vottunarstöð (vottunaraðila) sem fullnægir skilyrðum V. kafla laganna.

Hagsmunaaðili (*relying party* eða *verifier*): Notað um þá sem sannprófa skilríki eða treysta á þau. Sjá einnig hugtökin „treystandi“ og „sannprófandi“.

Íslandsrót: Rót sem er efst í stigveldi trausts í dreifilyklaskipulagi á Íslandi. Einkalykill Íslandsrótar er notaður til að undirrita önnur skilríki sem byggja á því trausti.

Kennimark viðfangs (*object identifier - OID*): Auðkenni í svæðinu „certificate policy” í skilríkjum sem tilgreinir tegund skilríkja og vísar til þeirrar vottunarstefnu sem gildir um útgáfu þeirra og notkun.

Lykill (*key*): Í umfjöllun um þætti dreifilyklaskipulags er oftast átt við dulmálslykil (e. cryptographic key). Bitastrengur af breytilegri lengd sem aðgerðir við dulritun eða dulráðningu ráðast af.

Lyklahafi (*key holder*): Samheiti fyrir „vottorðshafa” í dreifilyklaskipulagi.

Lögaðili (*legal entity*): Stofnun eða félag sem viðurkennt er að geti átt réttindi og borið skyldur. Ríki, sveitarfélög, stofnanir og félög eru lögaðilar og hafa öll sínar kennitölur.

Lögbær fulltrúi (*agent*): Einstaklingur sem valinn er og samþykktur af yfirstjórn fyrirtækis sem tengiliður og sem hefur umboð til að koma fram fyrir hönd fyrirtækisins til að samþykkja og sækja um skilríki, og/eða hafa umsjón með skilríkjum fyrirtækisins.

Milliskilríki (*intermediate certificate*): Milliskilríki eru undirskilríki sem gefin eru út af tryggilegri rót eða af öðru milliskilríki í þeim tilgangi að gefa út önnur milliskilríki eða

endaskilríki. Milliskilríki liggja á milli endaskilríkja og rótarskilríkja í traustaslóð skilríkja. Endaskilríki, milliskilríki og rótarskilríki mynda þannig skilríkjakeðju sem treystandi kannar þegar hann staðfestir það traust sem hann getur borið til endaskilríkja.

Móttakandi skilríkja (*certificate recipient*): Sá sem tekur á móti skilríkjum í rafrænum samskiptum og getur þurft að staðfesta það traust sem hann ber til dreifilykils vottorðshafa.

Notkunaraðgangsorð (*enabling password*): Aðgangsorð sem verndar einkalykil vottorðshafa. Þegar notkunaraðgangsorð er notað þarf vottorðshafinn að slá það inn þegar einkalykillinn er notaður. Þegar skilríki eru varðveitt í örgjörva snjallkorta er algengt að persónulegt kenninúmer (PIN) sé notað sem notkunaraðgangsorð.

OCSP samskiptaháttur (*Online Certificate Status Protocol*): Samskiptaháttur til að kalla eftir upplýsingum um stöðu skilríkja yfir nettengingar.

Persónulegt kenninúmer (*personal identification number*): Stutt númer sem einstaklingur notar sem aðgangsorð að virkum búnaði, til dæmis símakorti, greiðslukorti eða rafrænum skilríkjum á snjallkorti. Persónulegt kenninúmer fyrir rafræn skilríki virkar sem notkunaraðgangsorð sem vottorðshafinn slær inn þegar einkalykillinn er notaður. Stundum kallað „PIN-númer“, „kenninúmer einstaklings“ eða „persónulegt innsláttarnúmer“.

PIN-lausnarlykill (*PIN unblocking key*): Lykill, oftast númer eða textastrengur, sem veitir aðgang að öruggum búnaði, til dæmis símakorti, greiðslukorti eða snjallkorti, þrátt fyrir að aðgangi með PIN-númeri hafi verið lokað. Stundum kallað „PUK-númer“.

Rafræn skilríki (*electronic certificate*): Vottorð á rafrænu formi sem tengir sannprófunargögn við vottorðshafa og staðfestir hver hann er. Í umfjöllun um þætti dreifilyklaskipulags er oftast átt við dreifilyklaskilríki. Í skilríkjum er dreifilykill vottorðshafa ásamt öðrum gögnum, dulritað með einkalykli vottunarstöðvar.

Rafræn undirskrift (*electronic signature*): Gögn í rafrænu formi sem fylgja eða tengjast rökrænt öðrum rafrænum gögnum og eru notuð til að sannprófa frá hverjum hin síðarnefndu gögn stafa.

Reglustjórn (*policy authority*): Stofnun eða nefnd sem velur eða þróar vottunarstefnu og heldur henni við.

Rót (*root*): Upphaf trausts í tilteknu léni dreifilyklaskipulags. Rót er útfærð með skilríki sem kallast rótarskilríki.

Rótarlykill (*root key*): Einkalykill vottunarstöðvar sem er efst í tilteknu stigveldi trausts. Rótarlykillinn er notaður til að undirrita önnur skilríki sem byggja á því trausti.

Rótarskilríki (*root certificate*): Dreifilyklaskilríki sem eru efst í stigveldi trausts og gefin út af vottunarstöð til að undirrita önnur skilríki. Rótarskilríki eru undirrituð með einkalykli þess lyklapars sem tilheyrir sjálfu skilríkinu. Rótarskilríki eru því sjálfundirrituð.

Sjálfundirrituð skilríki (*self-signed certificate*): Skilríki (dreifilykill) sem eru undirrituð með eigin einkalykli og þar sem útgefandinn og vottorðshafinn er sami aðilinn. Í sjálfundirrituðum skilríkjum er einkalykillinn sem vottunarstöðin notar til að undirrita skilríkin samsvarandi þeim dreifilykli sem vottaður er í skilríkjunum. Sjá einnig skilgreiningu á „rótarskilríki“.

Sannprófandi (*verifier*): Viðtakandi skilríkja sem sannprófar þau og/eða rafræna undirskrift sem er staðfest með þeim. Stundum kallaður „hagsmunaaðili“.

Sannprófunargögn (*signature verification data*): Gögn, svo sem kótar eða dreifilykill dulritunar, sem notuð eru til að sannreyna rafræna undirskrift.

Skilríki (*certificate*): Í umfjöllun um þætti dreifilyklaskipulags er átt við rafræn skilríki nema annað sé skýrt af samhengi í texta. Stundum er orðið „vottorð" samheiti fyrir „skilríki".

Skilríki vottunarstöðvar (*CA certificate*): Skilríki fyrir vottunarstöð gefin út af annarri vottunarstöð.

Skipulagsskilríki (*organizational certificate*): Skilríki skipulagsheildar. Skipulagsheild getur verið félag, fyrirtæki, deild í fyrirtæki eða önnur afmörkuð og formleg skipulagseining. Skipulagsskilríki staðfesta að skipulagsheildin sé afmörkuð og skráð eins og skilríkin tilgreina og að skilríkin séu tengd þeim ábyrgðaraðila sem kemur fram í skilríkjunum. Í skipulagsskilríkjum er sá ábyrgðaraðili sem skipulagsheildin tilheyrir áskrifandi skilríkjanna og skipulagsheildin er vottorðshafi.

Skráningarstöð (*registration authority*): Aðili sem er ábyrgur fyrir auðkenningu og sannvottun á vottorðshafa en undirritar ekki skilríki né heldur gefur þau út. Skráningarstöð getur tekið að sér þannig verkefni fyrir hönd vottunarstöðvar.

Starfsskilríki: Skilríki starfsmanna fyrirtækja og stofnana. Starfsskilríki staðfesta að vottorðshafi sé sá sem skilríkin tilgreina og að skilríkin séu tengd þeim lögaðila sem kemur fram í skilríkjunum. Í starfsskilríkjum er lögaðilinn, t.d. fyrirtæki eða stofnun, áskrifandi skilríkjanna og starfsmaðurinn vottorðshafi.

Stigveldi trausts (*trust hierarchy*): Skipulag rótar og milliskilríkja þar sem traust á tilteknum skilríkjum byggir á trausti til þeirra skilríkja sem notuð voru til að undirrita þau og sem eru ofar í skipaninni (nær rótinni).

Stofnaðgangsorð (*activation code*): Aðgangsorð sem vottunarstöð úthlutar vottorðshafa til að búa til, eða stofna, skilríkin og mynda lyklapar. Vottorðshafinn þarf ekki að nota stofnaðgangsorðið aftur.

Tímabundin ógilding (*suspension*): Aðgerð sem felur í sér að vottunarstöð skráir skilríki sem ógild í afmarkaðan tíma. Vottunarstöð getur gert skilríkin virk að nýju með því að breyta stöðu þeirra þannig að þau séu ekki lengur ógild.

Treystandi (*relying party*): Viðtakandi skilríkja sem treystir á þau og/eða rafræna undirskrift sem er staðfest með þeim. Stundum kallaður „treystir", „hagsmunaaðili", „notandi vottorðs" eða „notandi skilríkja".

Tvískipt stjórnun (*dual control*): Öryggisverklag sem krefst samvinnu tveggja einstaklinga til að fá aðgang að vernduðum gögnum, skrám, búnaði eða kerfum.

Undirskriftar-PIN (*non-repudiation PIN*): PIN-númer sem vottorðshafi notar sem notkunaraðgangsorð fyrir beitingu rafrænna skilríkja til undirritunar.

Undirskriftarbúnaður (*signature-creation device*): Hugbúnaður eða vélbúnaður sem notaður er til að mynda rafræna undirskrift með hjálp undirskriftargagna.

Undirskriftargögn (*signature-creation data*): Einstök gögn, svo sem kótar eða einkalykill dulritunar, sem undirritandi notar til að mynda rafræna undirskrift.

Varbúnaður (*hardware security module*): Vélbúnaður sem notaður er til að framleiða og vista leynilykla sem notaðir eru í dulritun og til að vernda aðgang og notkun á leynilyklunum. Stundum kallað „öruggur lyklamiðlari" eða „öruggur vélbúnaður" Varbúnaður sem ætlaður er sérstaklega fyrir dulritun í dreifilyklaskipulagi er stundum kallaður „dulmálseining".

Viðhaldsaðgangsorð (*maintenance password*): Aðgangsorð sem notað er gagnvart vottunarstöð til að viðhalda og breyta skilríkjum. Neyðaraðgangsorð (e. emergency

password), afturköllunaraðgangsorð (e. revocation password) og ógildingaraðgangsorð (e. suspension password) eru allt viðhaldsaðgangsorð.

Virkjunargögn (*activation data*): Gagnagildi, önnur en lyklar, sem þarf til að nota dulmálsbúnað. Virkjunargögn þarf að vernda. Virkjunargögn eru t.d. lykilorð (notkunarlykilorð), PIN, lyklahluti eða lífkenni.

Vottorð (*certificate*): Í umfjöllun um þætti dreifilyklaskipulags er orðið „vottorð" oft samheiti fyrir „skilríki".

Vottorðshafi (*subject*): Einstaklingur, lögaðili, skipulagseining eða búnaður sem auðkenndur er í skilríkjum sem handhafi þess lyklapars, einkalykils og dreifilykils, sem tilgreint er í skilríkjunum. Vottorðshafi getur verið áskrifandi sem fær lyklapar í eigin nafni.

Vottunarstefna (*certificate policy*): Safn af reglum sem skilgreina nothæfni skilríkja á tilteknu notkunarsviði þar sem öryggiskröfur eru samskonar. Í vottunarstefnu kemur fram hvernig stefnt er að því að standa að útgáfu og meðferð rafrænna skilríkja. Í vottunarstefnu eru líka settar reglur um þær kröfur sem gerðar eru í þjónustunni til öryggis og eftirlits.

Vottunarstöð (*certification authority*): Aðili sem nýtur trausts hagsmunaaðila til að framleiða, undirrita og gefa út skilríki. Stundum kallað „vottunaraðili".

Vottunarþjónusta (*certification service provider*): Aðili sem veitir öllum hagsmunaaðilum alhliða þjónustu varðandi þætti dreifilyklaskipulags.

Yfirlýsing um framkvæmd vottunar (*certification practice statement*): Formleg yfirlýsing vottunarstöðvar um starfsvenjur og framkvæmd við útgáfu og viðhald skilríkja. Yfirlýsing um vottunarframkvæmd lýsir ferlum og reglum skilríkjaútgefanda sem uppfylla kröfur í tiltekinni vottunarstefnu.

Öruggur notendabúnaður (*secure user device*): Búnaður sem geymir einkalykil vottorðshafa, verndar hann gegn ógnum og framkvæmir undirritun eða dulritun fyrir vottorðshafann. Öruggur notendabúnaður sem ætlaður er fyrir rafræna undirritun og sem uppfyllir kröfur sem kveðið er á um í 8. gr. laga um rafrænar undirskriftir, nr. 28/2001 kallast „öruggur undirskriftarbúnaður".

Öruggur undirskriftarbúnaður (*secure signature-creation device*): Búnaður fyrir rafræna undirritun sem uppfyllir kröfur sem kveðið er á um í 8. gr. laga um rafrænar undirskriftir, nr. 28/2001. Öruggur undirskriftarbúnaður er sérstakt tilvik af öruggum notendabúnaði sem ætlaður er fyrir rafrænar undirskriftir.

Skammstafanir

Eftirfarandi eru algengar skammstafanir í enskum texta um dreifilyklaskipulag. Skýringar á ensku eru skáletraðar í sviga.

CA	Vottunarstöð (***C**ertification **A**uthority*).
CP	Vottunarstefna (***C**ertificate **P**olicy*).
CPS	Yfirlýsing um framkvæmd vottunar (***C**ertification **P**ractice **S**tatement*).
CSP	Vottunarþjónusta (***C**ertification **S**ervice **P**rovider*).
CRL	Afturköllunarlisti (***C**ertificate **R**evocation **L**ist*).
HSM	Varbúnaður (***H**ardware **S**ecurity **M**odule*).

ISRS	**Ís**lensk **r**afræn **s**kilríki - skilríki í rafrænni þjónustu á Íslandi sem uppfylla samræmdar kröfur í samstarfsverkefni ríkis, banka og sparisjóða.
LCP	Léttvægar vottunarkröfur (***L**ightweight **C**ertificate **P**olicy*).
NCP	Staðlaðar vottunarkröfur (***N**ormalized **C**ertificate **P**olicy*).
NCP+	Auknar staðlaðar vottunarkröfur (*Extended **N**ormalized **C**ertificate **P**olicy*).
OCSP	OCSP samskiptaháttur (IETF RFC). OCSP er notað til að kalla eftir upplýsingum um stöðu skilríkja yfir nettengingar (***O**nline **C**ertificate **S**tatus **P**rotocol*).
PA	Reglustjórn (***P**olicy **A**uthority*).
PIN	Persónulegt kenninúmer (***P**ersonal **I**dentification **N**umber*).
PKI	Dreifilyklaskipulag (***P**ublic **K**ey **I**nfrastructure*).
PKI-PIN	PIN fyrir beitingu rafrænna skilríkja, til aðgreiningar frá öðrum PIN-númerum.
PKI-PUK	PIN-lausnarlykill, stundum kallað „PUK-númer“, fyrir rafræn skilríki, til aðgreiningar frá öðrum PUK-lyklum.
PUK	PIN-lausnarlykill (***P**IN **U**nblocking **K**ey*).
QCP	Fullgildar vottunarkröfur, fyrir fullgild skilríki (***Q**ualified **C**ertificate **P**olicy*).
SSCD	Öruggur undirskriftarbúnaður (***S**ecure **S**ignature-**C**reation **D**evice*).