



Dátueffirlitið

Tórshavn, tann 18. februar 2021

Samskipti umvegis teldupost

Á fundi 11. februar 2021 umrøddi Dáturáðið teldupostsamskipti, og hvussu dátuábyrgdarar o.o. kunnu tryggja, at trygdin er nøktandi, tá persónupplýsingar verða sendar umvegis teldupost.

Niðurstøðan hjá Dáturáðnum var, at tann, sum sendir persónupplýsingar umvegis teldupost eigur at tryggja sær, at teldupostsamskiptið er bronglað. Verða viðkvæmar persónupplýsingar og persónupplýsingar, sum eru fevndir av trúnaðarásetingum, sendar við telduposti, eigur sendarin at vera serliga varin.

Dáturáðið var samt um, at tað til eina og hvørja tíð er upp til tann einstaka dátuábyrgdaran at meta um, hvørji trygdartiltøk eru hóskandi at seta í verk, og at meta um, m.a. hvat slag av brongling skal nýtast.

Dáturáðið var tó samt um, at TLS-brongling (versión 1.2.) ella annað slag av brongling, sum er á sama støði, er eitt lágmark fyri trygd, tá ið viðkvæmar persónupplýsingar verða sendar umvegis teldupost.

Í summum førum er kanska best at nýta ein annan miðil til trygt samskipti enn teldupost sum til dømis Mínboks.

Dáturáðið umrøddi hesi sløg av brongling:

- Brongling í flutninginum (“Kryptering på transportlaget” – TLS-brongling)
- End-to-end brongling

Brongling í flutninginum (“Kryptering på transportlaget”) (TLS-brongling)

TLS (Transport Layer Security) brongling bronglar teldupostar undir flutninginum frá sendara til móttakara. Telduposturin verður í útgangsstøðinum goymdur óbronglaður og atkomuligur á teldupostservingum hjá bæði sendara og móttakara.

End-to-end brongling

Við end-to-end brongling verður innihaldið í teldupostinum bronglað. Hetta merkir, at upplýsingarnar verða læstar við einum lykli, áðrenn tær verða sendar, og ikki kunnu lesast, fyrr enn móttakarinn letur teldupostin upp við rætta lyklinum.



Dátueffirlitið

Dømi um end-to-end brongling eru hesi:

- *PGP*
Við Pretty Good Privacy (PGP), sum fylgir tí sonevndu OpenPGP, kann ein og hvør fáa eitt lyklapar (ein almennan og ein privatan lykil), sum eru knýttir til eina ávísa teldupostadressu. Almenni lykilin kann almannakunngerast í netbornum uppslagi, sum virkar til deiling av lyklum. PGP kann tengjast saman við m.a. Outlook og Thunderbird.
- *S/MIME*
Á sama hátt sum við PGP hava sendari og móttakari hvør sín almenna og privata lykil. Við S/MIME eru almennu lyklarnir hjá pørtunum partur av einum ‘certifikati’, sum er útgivið av einum sonevndum CA (Certificate Authority), sum knýtir virðið á tí almenna lyklinum til ein likamligan persón. Tá ið ein teldupostur verður sendur, verður certifikatið hjá móttakaranum góðkent grundað á tøkni, sum vanliga er innbygd í einum teldupostklienti, og sum er ósjónlig fyri brúkaran.