Dear Anneli and experts,

According to Commission Decision 2011/130/EU of 25 February 2011 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:0072:EN:PDF we have created the draft of interoperability profile according to which we plan to update our national requirement and also signature creation and verification applications which are or will be used in the public administration. We hope that it will be useful as a technical input for the developers of open source software developed e.g. by EU Commission (ARHS).

Dear experts, in case that we have our own applications which will be probably used for communication with your public administration, **we need to know whether** this draft of profile is also in the intersection with your national requirement for communication with your public administration according to Commission Decision 2011/130/EU.

We appreciate any comments to this draft of profile to achieve the interoperability based on Commission Decision 2011/130/EU.

For the testing of qualified certificates, in the attachment there is a set of signatures created in LockIt application, where qualified, non-qualified and expired qualified certificates were used.

For the testing purposes the requirements of this profile are also implemented in Lock-It application http://lockitin.webnode.sk/products/produkt-1/ which can be used e.g. for the signature creation and validation and ASN.1 dump view in development of interoperable applications. The Lock-It supports the signature creation with hash algorithms SHA256 and signature algorithms RSA or ECDSA.

Best regards,

Peter Rybar

National Security Authority
Information Security and Electronic Signature Department
Budatinska 30, 850 07 Bratislava 57, Slovak Republic
tel.: +421 2 6869 2163
mob.: +421 902 891 155
fax: +421 2 6869 1701
e-mail: peter.rybar@nbusr.sk

e-mail: peterryb@gmail.com