Dear All,

Attacks have occurred, where a false content of the signed PDF file was displayed or used.

The attacks occurred on ASiC were based on using different document than the one that the signer has signed, by including more documents, namely unsigned document(s) or document(s) signed by somebody else, all seemingly having been signed by the assumed signer.

I would like to inform you about the procedures which (SK NSA) electronic filing office has implemented for security reasons in case mentioned attacks on PDF as well as on ASiC are included in files sent to us, e.g. to the electronic registry.

It might be of interest to you, as well.

See the last figure on the last page of the document:

<https://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/Navod.pdf>

You can test it by using attached document “hideQF1.pdf”.

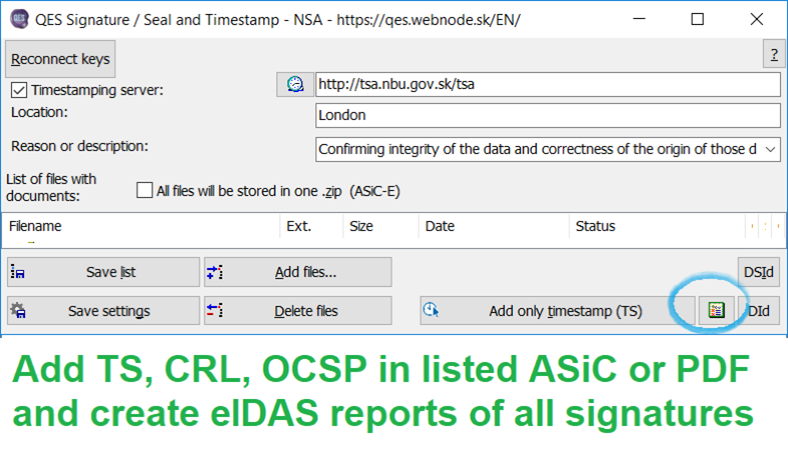
What is included in the above-mentioned one click, please see here in more detail, how I have implemented it in the application created by me:

1.      Any received PDF or ASiC are included in the list of files in the QES application (all are stored on disc/USB with writing allowed). The application is available in these two ways:

                 I.          Free QES application can be installed from the Microsoft Store which contains version only for Windows 10 - [Get QES 32](http://www.microsoft.com/store/apps/9PH7C2FV4SSX)-bits from the [Microsoft Store](https://www.microsoft.com/store/apps/9PH7C2FV4SSX) or [Get QES 64](http://www.microsoft.com/store/apps/9P8XFT775N53)-bits from the [Microsoft Store](https://www.microsoft.com/store/apps/9P8XFT775N53).

               II.          Free QES application [qes.webnode.sk/en/](https://www.nbu.gov.sk/en/trust-services/trusted-list/tl-and-qes-applications/index.html)  does not require installing, just download it from the NSA web page and run it in Windows without installation, after extracting it from the Zip which contains version for any Windows ([Unblock App in Windows](https://www.tenforums.com/tutorials/5357-unblock-file-windows-10-a.html#option3) Defender SmartScreen). Get [QES.zip](http://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/QES.zip) (32-bit, SHA-256, zip, 3.9 MB) or Get [QES64.zip](http://www.nbu.gov.sk/wp-content/uploads/doveryhodne-sluzby/QES64.zip) (64-bit, SHA-512, zip, 5.0 MB).

2.      Click on the button in the blue circle:



3.      For all signatures in PDF (for all revisions) and for all signatures in ASiC (including nested ASiC and nested PDF) will be created validation reports stored in the separately created ZIP files for each signature (usage of short file names is recommended, not above 130 characters).

4.      If the timestamp service is available at entered address, the timestamp of PDF document will be included and if signatures in ASiC on the first level of nesting does not contain signature timestamp, the signature timestamp will be included.

5.      Created ZIP file contains only signed version/revision of PDF of the one respective signer’s signature or all documents signed in ASiC with the one respective signer’s signature. The TXT validation report of that one particular signature will be created by using the trusted list and stored in this ZIP.

6.      At the end, all used OCSP responses or CRLs will be included in listed PDF files or ASiC containers to be able to validate them also on off-line computers or later.

7.     Individuals, e.g. officials according to the subject fields mentioned in the validation reports, stored in ZIP, select the expected signer (the respective ZIP) and will use only files included in such a ZIP which contains only files signed by the selected signer.

8.      The incorrect version of PDF or unsigned files from ASiC (modified through attack) will not be used or displayed.

9.      Try it with the attached document.

Kind regards,

Deputy Director **COL Peter Rybár**

Regulation and Supervision Department | NSA

Budatínska 30 |851 06 Bratislava |Slovak Republic

tel.: +421 2 6869 2163|fax: +421 2 6869 1700

[peter.rybar@nbu.gov.sk](mailto:peter.rybar@nbu.gov.sk) |[www.nbu.gov.sk](http://www.nbu.gov.sk/)

Free QES application [qes.webnode.sk/en/](https://www.nbu.gov.sk/en/trust-services/trusted-list/tl-and-qes-applications/index.html)