

NATIONAL SECURITY AUTHORITY
Information Security and Electronic Signature Department
Budatinska 30, 850 07 Bratislava 57

Annex 1 to No. 3679/2006/IBEP-001

4 October 2006, Bratislava

Guideline on assessment of certified SW applications for QES with the usage of signature policies being valid to 31 December 2006

Introduction

In signature verification the Qualified Electronic Signature (QES) is valid, among others, if the signature policy approved by the National Security Authority (NSA) was used for its creation.

1. Analysis of approved signature policies in certified applications for QES

Some certified applications for QES use the following approved signature policies:

- **ES** Signature Policy for Qualified Electronic Signature (policyEs.der);
- **ES-T** Signature Policy for Qualified Electronic Signature with Time Stamp (policyEsT.der);
- **ES-C** Signature Policy for Qualified Electronic Signature with complete validation data (policyEsC.der);
- **ES-A** Signature Policy for Archival Qualified Electronic Signature (policyEsA.der);
- **ES-T-UTF8** Signature Policy for Qualified Electronic Signature with Time Stamp of textual data in ASCII and UTF8 coding (policyEsTUtf8.der);

whose **validity ends on 31 December 2006**. After the validity end of signature policies mentioned above, the qualified electronic signature created pursuant to signature policies mentioned above shall be considered to be invalid because of the usage of invalid signature policy. The application for QES certified by the NSA which can **only** operate with signature policies mentioned above shall be incapable for QES signing and verification since 1 January 2007, because the validity of policies in question shall end up on 31 December 2006. Upon that fact the NSA is entitled to revoke the certificate validity because after its issuance may occur circumstances under which the certified product does not meet conditions of the usage (e.g. the annex of the certificate contains that “the application for QES may be used only with a given signature policy together with OID of the policy”).

2. Signature policy “Qualified Electronic Signature in accordance with the legislation of the Slovak Republic”

The NSA issued a new signature policy “**Qualified Electronic Signature in accordance with the legislation of the Slovak Republic (policyQES.der)**” with the validity period from 20 March 2006 to 1 January 2008. This signature policy substitutes all signature policies mentioned above and deals with other requirements of international standards and the Slovak legislation.

In future application certifications for QES the auditor shall verify which fields and values of signature policy fields can be processed by the application. These fields shall be mentioned in the audit report and the application certificate shall not be limited to particular signature policy but while importing the signature policy, the application shall check if it can recognize all fields of the signature policy. In case there are present unknown fields the application shall declare that it is not possible to operate with the signature policy and therefore it is not possible to determine the correct result of verification according to this signature policy. The life cycle of the signature policy shall follow the document "Signature Policy Management" (updated as Trusted List Management) in valid and the NSA-approved version.

3. Procedure for removal of status that has occurred

The meeting of the "Working group with regard to the issue of certification of SW applications for QES" which was dealing with the issue of the validity end of signature policies mentioned above was held in the premises of the NSA on 25 July 2006. The manufacturer representatives of applications that only use the signature policies mentioned in point 1, also participated at the meeting.

The conclusion of the meeting was:

Affected companies shall make an agreement with the NSA on joint action to remove the problem that has occurred. At individual meetings it shall be necessary to analyse whether:

- the application is capable to operate with a new all-purpose approved signature policy QES;
- the change of the signature policy means the interference in the application code;
- it is required to conduct a new audit.

Following the analysis the manufacturers whose application is incapable to operate with the NSA-approved signature policies being valid after 1 January 2007 must submit a request for a new application certification for QES. In the certification process the NSA shall consider already known facts and the certification process shall be performed as soon as possible.

Conclusion

The implementation of the new all-purpose signature policy "Qualified Electronic Signature in accordance with the legislation of the Slovak Republic" and its management according to the document "Signature Policy Management" (updated as Trusted List Management) in valid and the NSA-approved version shall resolve the problem of the signature policy usage in the applications for QES creation and verification.

Action Officers: Ivan Chrenko
Anton Lachky