DOI: 10.15199/13.2015.1.8

Recapitulation of the electronic signature interoperability tests

(Podsumowanie testów interoperacyjności podpisu elektronicznego)

dr inż. MAREK HOŁYŃSKI, dr inż. prof. ndzw. WOJCIECH NOWAKOWSKI

Instytut Maszyn Matematycznych, Warszawa

The electronic signature was introduced into European law through Directive 99/93/EC, which was enacted in 1999. In Poland the electronic signature was implemented in 2001 with the enactment of the Electronic Signature Act. Legal regulations give special weight to the qualified electronic signature, which is considered legally equivalent to a handwritten one.

The format to be used for a qualified signature was defined by ETSI (*European Telecommunications Standards Institute*) in three separate specifications, which describe the following formats: XAdES, CAdES and PAdES. As the specifications mentioned above are extensive, signatures created on the their basis may differ widely.

The purpose of the first National Electronic Signature Interoperability Test (Narodowy Test Interoperacyjności podpisu elektronicznego – NTIPE, [1, 2]) was to investigate and describe the market of applications used to create and verify the secure electronic signature. Another important consideration was exploration of the problems involved in interactions between different applications, recognition of certificates issued by different certification centers and evaluation of the compliance of signatures thus created with legal requirements.

Ten applications designed by both domestic and foreign entities participated in the 2011 tests.

For the purposes of NTIPE an original development environment was designed, to allow support of test files, and the entering of test results. A certification center was also created, to issue and manage test certificates, and to add test timestamps.

The SD-DSS software, made available by the European Commission, was used to generate test cases requiring an electronic signature. All the results requiring signature verification were checked by means of this application.

To verify that a signature complies with the requirements of Decision 2011/130/EU a custom-designed application was used, which automatically confirmed the presence of required elements, but did not verify the signature's validity.

The applications under testing were installed on workstations provided by their makers. Some of the tests involved the use of qualified certificates. Test certificates were used in cases where it was difficult to obtain a qualified certificate. An example of the latter is the CK04 test, in which the certificate contained a critical extension error.

To reflect various certification paths, three separate certification entities were generated for use during NTIPE:

The first path reflects the infrastructure currently in use in Poland. The other two present two variants of target infrastructure, which may be installed when cryptographic algorithms are changed.

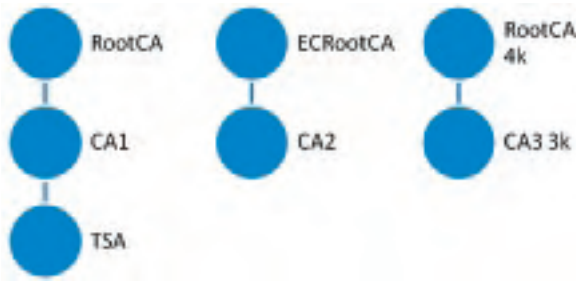

Fig. 1. CA generated for the purposes of the test
Rys. 1. Urzędy CA wygenerowane dla potrzeb testu

The first stage of NTIPE consisted in the so-called pretests which took place from September 26th to October 17th 2011. The test files and results were sent through a WWW portal set up specially for this purpose. In total, 39 test cases were prepared, which can be divided into three groups:

Digital signature creation tests:

ID	Test name
CK06	Capability to create a RSA1024 + SHA1 signature
CK07	Capability to create a RSA 2048 + SHA 256 signature
CK08	Capability to create an ECDSA256 +SHA256 signature
CK09	Capability to create a signature verified with an invalid certificate
DC01	Creating a signature compliant with Decision 2011/130/EC for XAdES
DC02	Creating a signature compliant with Decision 2011/130/EC for CAdES
DC03	Creating a signature compliant with Decision 2011/130/EC for PAdES
DC04	Adding a signature policy identifier to the signature
DC05	Recognizing signature policy in the creation of the signature
DC06	Capability to add a CommitmentType extension to the signature

DC07	Capability to add a time-stamp to the signature
DC08	Capability to add any time-stamp to the signature
DC09	Capability to create an archived version of the signature
DC10	Support of an archived version of the signature with a CRL attached
DC11	Support of an archived version of the signature with OCSP attached

Countersignature tests:

ID	Test name
IK01	Application's interoperability with regard to countersignature
IK02	Interoperability with ePUAP with regard to countersignature

Digital signature verification tests:

ID	Test name
CK01	Building a certification path for certificates issued domestically
CK02	Recognition of a qualified certificate on the basis of a given certification policy
CK03	Recognition of a qualified certificate by means of the QCStatement extension
CK04	Recognition of the invalidity of a qualified certificate
CK05	Building a certification path for certificates issued abroad
DC12	Recognizing the addition of a signature policy
DC13	Recognition of the restrictions defined in signature policies
DC14	Verification of time-stamped signatures
DC15	Verification of an archived version of a signature for a valid certificate
DC16	Verification of an archived version of a signature for a suspended certificate
DC17	Verification of a signature in the BES format for a suspended certificate
DC18	Verification of a signature with a revoked time-stamp
DC19	Verification of a signature with an invalid digest
DC20	Verification of a modified file
DC21	Verification of detached signatures
DC22	Verification of enveloped signatures
DC23	Verification of enveloping signatures
DC24	Verification of a signature containing in its hierarchy the following certificates: RSA 4k+SHA512 i RSA3k + SHA256
DC25	Verification of a signature containing in its hierarchy the following certificates: ECDSA 256 +SHA256 i RSA2k + SHA256
IK03	Application's interoperability with regard to verification
IK04	Interoperability with ePUAP with regard to verification
IK05	Verification of a signature compliant with Decision 2011/130/EC created by applications taking part in the test

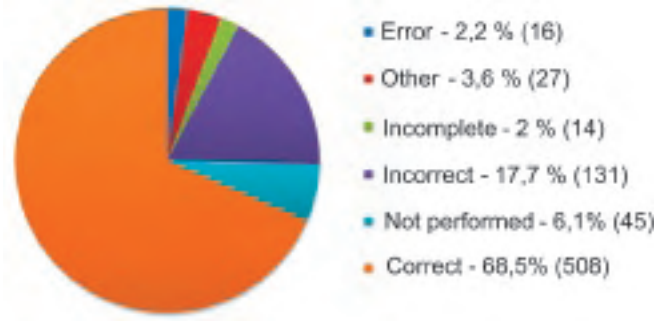

Fig. 2. Pre-test results. Rys. 2. Wyniki pretestów

In total, 742 tests were carried out at the pre-test stage. The diagram below shows results as percentage values, and, in brackets, the number of tests with a given result.

Because the workshops took place at the same time as a conference (October 26–27), it was not possible to conduct as many tests as in the pre-test stage. For this reason the organizers decided to carry out three tests to verify the pre-test results, and five additional tests intended specifically for the workshop participants.

Verification of pre-test results:

ID	Test name
CK04	Recognizing that the signer's certificate contains invalid critical extensions
CK05	Verification of the use of a TSL by the application to establish trust for qualified certificates issued abroad
DC24	Verification of readiness for the introduction of new certification paths containing the SHA2 and RSA algorithms with a length of more than 2048 bits

Tests for the workshop participants:

ID	Test name
DC1	Verification of the application's capability to create a signature conforming with the reference format for XAdES
DC02	Verification of the application's capability to create a signature conforming with the reference format for CAdES
DC03	Verification of the application's capability to create a signature conforming with the reference format for XAdES
IK5	Verification of a signature compliant with Decision 2011/130/EC created by applications taking part in the test
IK6	Creation of a qualified signature based on any qualified certificate issued in Poland

As part of the workshops 264 tests were carried out. The diagram below presents the results as percentage values, and, in brackets, the number of tests with a given result.

Considering the results it is possible to dispose of the myth about the supposed difficulties associated with interaction between applications used to create and verify electronic signatures. Furthermore, the participation of foreign entities makes it apparent that successful interaction with foreign applications does not pose any major problems, either. However, despite

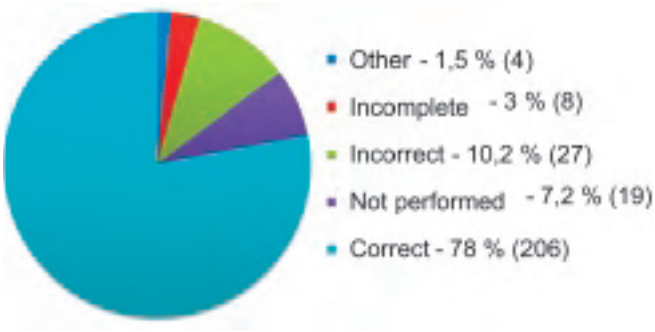

Fig. 3. Workshop results. Rys. 3. Wyniki warsztatów

a relatively high level of interoperability between the applications in question, it should be noted that where a tool such as the electronic signature is concerned the users' expectations are much higher. The average user will expect operational accuracy at a level close to 100%. To use the mobile phone as an analogy: the user expects to be able to call any phone, of any model, not just a chosen few. This indicates that there is still a lot of work to be done on the electronic signatures market.

The first National Electronic Signature Interoperability Test that took place in October 2011 was a big success. The participants, both domestic and foreign, made very good use of the chance to test applications for the creation and verification of electronic signatures designed by various companies and organizations. Their favourable comments led to the decision to conduct another edition of the test in 2012.

This event was held under a new name – Electronic Signature Interoperability Summit, CommonSign. The high standard of the previous year's edition was maintained. Its cyclical character created another opportunity to verify progress in application development and adaptation to the constantly changing norms and requirements. To achieve this, three groups of tests were prepared: new, repeated from the previous edition, and regular. In that way, it will be possible to draw meaningful comparisons, using the results of future editions.

The tests were accompanied by a two-day conference on electronic signature interoperability, during which much attention was devoted to the regulation of the European Parliament and the Council on electronic identification and trust services for transactions in the internal market. The purpose of the National Electronic Signature Interoperability Test was to verify the feasibility of successful interactions between various applications used to create electronic signatures and investigate the current state of the electronic signatures market. Another important goal was to gather information about the market's evolution.

The ongoing rationalization of electronic signature standards creates the need to test applications with regard to accurate support of the changes that are being introduced.

There were 5 applications that took part in the Electronic Signature Interoperability Summit, CommonSign 2012. The applications performed a series of specialized tests. Their scope was divided into three major areas, as depicted in the diagram below:

The regular set of tests makes it possible to gather information about the evolution of the electronic signature.

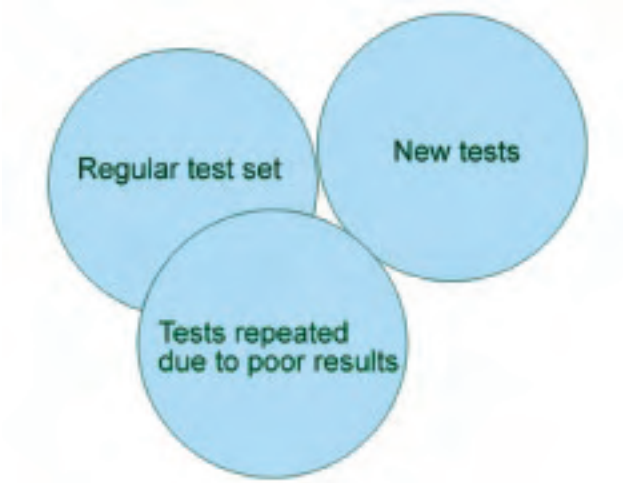

Fig. 4. Scope of tests. Rys. 4. Zakresy testów

This kind of data enables investigation of long-time trends in electronic signatures.

Test subject matter	Subject matter description
Signature interoperability with regard to verification	The test involves the creation of electronic signatures by the applications under testing, and mutual verification of the signatures thus created
Building a certification path for certificates issued abroad	The test involves the verification of a signature created on the basis of a qualified certificate issued by a foreign entity. The entity in question is included on the TSL

The tests repeated from the previous edition of CommonSign make it possible to assess the quality of introduced improvements. These tests relate to specific elements of the application, or the signature format.

Test subject matter	Subject matter description
Recognizing that the certificate contains an unknown critical extension	Test CK4 from the previous edition of NTIPE. It consists in the verification of a signature by means of a test certificate. The certificate contains an unknown critical extension, which should result in its being rejected
Capability to add a CommitmentType extension in the signature	Test DC6 from the previous edition of NTIPE. It involves the creation of a signature by the application undergoing testing. The application should add the CommitmentType attribute to the signature.
Support for an archived version of a signature with a CRL attached	Test DC10 from the previous edition of NTIPE
Support for an archived version of the signature with OCSP attached	Test DC11 from the previous edition of NTIPE
Verification of an archived version of a signature for a suspended certificate	Test DC16 from the previous edition of NTIPE

The introduction of new tests makes it possible to emphasize a specific area of the electronic signature, which can then be tested more thoroughly. In this way the attention of application makers may be drawn to a specific area of the electronic signature, which, in consequence, leads to improvement in the quality of their products in this regard.

Test subject matter	Subject matter description
Interaction of the application with the ePUAP function Trusted Profile	Verification of a secure signature prepared on the ePUAP portal, Verification of a signature confirmed with a trusted profile prepared on the ePUAP portal, Verification of a secure signature created with the application undergoing testing on ePUAP, Verification on ePUAP of a signature confirmed with a ZP profile created by the application in question Verification on ePUAP of a signature confirmed with a trusted profile and archived by the application being tested, Verification on ePUAP of a qualified signature archived by the application being tested
Specifying a certificate profile for a natural person	Verification of correct interaction with a certificate issued according to the profile defined in TS 119 412-2 V 1.1.1

Signature creation seals	Awarding requirements
Signature Creation SEAL XAdES	at least 70% of correct results in XAdES signature creation tests
Signature Creation SEAL CAdES	at least 70% of correct results in CAdES signature creation tests
Signature Creation SEAL PAdES	at least 70% of correct results in PAdES signature creation tests

Signature verification seals	Awarding requirements
Signature Verification SEAL XAdES	at least 70% of correct results in XAdES signature verification tests
Signature Verification SEAL CAdES	at least 70% of correct results in CAdES signature verification tests
Signature Verification SEAL PAdES	at least 70% of correct results in PAdES signature verification tests
Golden SEAL	The application has received all the three basic signature verification seals

ePUAP Seal	Awarding requirements
ePUAP SEAL	at least 70% of correct results in ePUAP tests

The results of CommonSign 2012 encourage an optimistic view of the electronic signature market in Poland. The results achieved by the applications in the tests repeated from last year's edition confirmed the conclusions which had been presented at the time. The majority of the errors that came up in 2011 were minor faults, easy to correct, as this year's results confirmed.

The 2012 tests were prepared with a greater focus on investigating real-life issues and the needs of electronic signature users, and less emphasis on specific problems, including technical ones.

Furthermore, from the diagram above it is apparent that the percentage of correctly completed tests was 90%. This represents a tremendous improvement in quality, for the results obtained during NTIPE 2011 were in the range of 75% of correct results for the workshop, and below 70% for the pre-tests. 100% accuracy has not yet been achieved, but the upward trend is evident, and the degree of improvement significant.

Concurrent with the workshop sessions there was a conference on the subject of electronic signature interoperability. During this two-day event presentations were made by representatives of public administration, certification centres, and companies active in the field of electronic signatures.

During the discussions many interesting points were raised about the progress and organization of CommonSign 2012. There were suggestions that the future editions should move beyond the issue of norms and standards, and focus on application interoperability instead. According to the participants it is essential to widen the scope of future tests, by including elements related to public administration – such as the ePUAP system or electronic inboxes.

The seals/marks of quality awarded to applications for high results in the tests were very well received.

It is important that the Ministries of Economy as well as Administration and Digitization become involved in the popularization of the CommonSign seals of quality, for it is largely their responsibility to popularize and promote the use of electronic tools in the economic sphere.

References

[1] Szacki K., Poznański R., Wachnik D., Stroiński Ł.: Podsumowanie testu interoperacyjności podpisu CommonSign 2012, Elektronika – konstrukcje, technologie, zastosowania, nr 2/2013, str. 72–74.

[2] Poznański R., Szacki K., Stroiński Ł.: Podsumowanie Narodowego Testu Interoperacyjności Podpisu Elektronicznego, Elektronika – konstrukcje, technologie, zastosowania, nr 6/2012, str. 74–76.