HOW DOES A DUTCH AUDITOR SIGN A DIGITAL AUDITOR'S REPORT?

January 2020

Royal Netherlands
Institute of Chartered
Accountants

NBA

INTRODUCTION

In the Netherlands, all annual reports of medium-sized or large companies must be accompanied by an auditor's report. According to the law, the auditor's report must be signed by the auditor. The fact that submissions of these reports to the national register are now digital (based on XBRL) does not change any of these requirements.
This article explains how this is done and how the society can trust the digital signature of an auditor.

SIGNING

When an auditor wants to sign a digital auditor's report, he or she needs four things:

1. a digital annual report;
2. a digital auditor's report;
3. an electronic signing device;
4. and specific software.

THE AUDITOR'S REPORT

In the Netherlands, we have chosen to prepare the auditor's report in the same format as the annual report: XBRL. The professional body for accountants in the Netherlands (NBA) is responsible for the XBRL taxonomy of auditor's reports and supports beside the standard auditor's reports (which conforms to the ISAs) also specific reports from the ISREs standards. The taxonomy in Dutch is freely available at https://www.nba.nl/themas/ict/nba-taxonomie/.

With commercial software, an auditor can create an auditor's report. However, most auditors prefer the web-based solution offered by the NBA. This web-based solution is based on system of questions and answers and is provided with standard text proposals. The web-based tool in Dutch (https://www.nba.nl/generator/) can be used by anyone for free.

SIGNATURE POLICY

According to law the auditor's report needs to be signed. But simply signing a document without any legal substantiation has no meaning. For this in the Netherlands, a signature policy has been created. This signature policy (prepared in four languages: Dutch, English, German and French) is published on the formal website of the Dutch Standard Business Reporting (SBR) Program (http://www.nltaxonomie.nl/sbr/signature_policy_schema/v2.0/SBR-signature-policy-v2.0.xml).

The signature policy identifies the conditions under which electronic signatures are used for SBR in the Netherlands, as well as the conditions for confirming the validity of these signatures. In this regard, the SBR signature policy highlights specific signature-related responsibilities by explaining the various commitments that accompany electronic signatures.

The correct commitments must be selected when signing the auditor's report. In figure 1 the selection is made by selecting the correct commitment type. At this moment there are three commitments available in the signature policy:

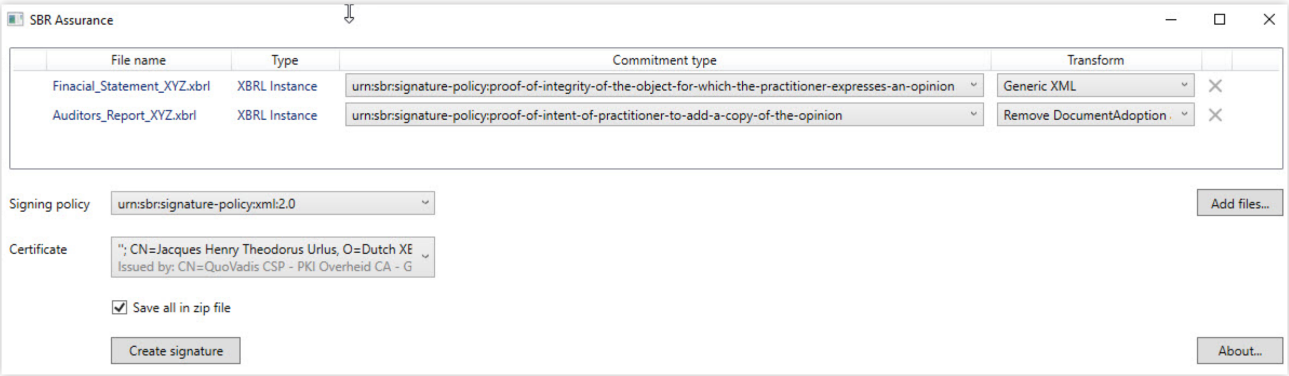
1. proof-of-intent-of-practitioner-to-express-an-opinion;
2. proof-of-intent-of-practitioner-to-add-a-copy-of-the-opinion;
3. proof-of-integrity-of-the-object-for-which-the-practitioner-expresses-an-opinion.

The first commitment means that the auditor has compiled and issued a report and takes responsibility for the content of the report. The second commitment means a confirmation that a (digital) copy of the auditor's report may be accompanied by the (digital) audit object. The last commitment confirms the authenticity of the audit object. Furthermore, an irrefutable relationship is created between the audit object and the issued auditor's report.

SIGNING SOFTWARE

The software for signing can be integrated in commercial software or the auditor can use open source software. It should be noted that a lot of commercial software vendors have incorporated the open source solution in their own software.

The open source software (https://opensbr.org) is available as source code on GitHub, but a compiled version is also provided by the organization behind OpenSBR. In the tool, an auditor needs to select the annual report, the auditor's report and the specific commitments according to the signature policy. When for example an SSCD (see box 1 for clarification) is inserted (via the USB port) in the computer and after clicking on the 'Create signature' button, a password Pop-Up appears on the screen. If the entered password is correct, a detached signature (see box 2 for clarification) file is being created.



SBR Assurance

File name	Type	Commitment type	Transform
Finacial_Statement_XYZ.xbrl	XBRL Instance	urn:sbr:signature-policy:proof-of-integrity-of-the-object-for-which-the-practitioner-expresses-an-opinion	Generic XML
Auditors_Report_XYZ.xbrl	XBRL Instance	urn:sbr:signature-policy:proof-of-intent-of-practitioner-to-add-a-copy-of-the-opinion	Remove DocumentAdoption

Signing policy: urn:sbr:signature-policy:xml:2.0

Certificate: "; CN=Jacques Henry Theodorus Urlus, O=Dutch XE
Issued by: CN=QuoVadis CSP - PKI Overheid CA - G

☑ Save all in zip file

Figure 1: A screenshot of the open source program for signing auditor’s reports

THE PROCESS OF FILING

If the company wants to submit its annual report, it must submit three files via the Dutch Government Digital Gateway (Digipoort) to the Dutch Chamber of Commerce. These files are the annual report, the auditor’s report and the detached signature. When Digipoort receives these files, it will start to check the validity of the signature value. First, it will check if the three hashes in the detached signature are the same as the hashes calculated by themselves. If this is the case, then we know for certain that the files (annual report, auditor’s report and signature policy) have not been changed after signing. Secondly, Digipoort checks with the information of the public key if the certificate is still valid (not on the blacklist) and whether the certificate contains the correct profession (Registeraccountant or Accountant-Administratieconsulent). The final check is the check of the signature value. This is done by combining the information (hashes, the signature value and other information like the date and time of signing) in the detached signature and to verify this with the available public key. If all goes well, the process of filing will continue. If something is incorrect, the filing process will stop immediately. The Annual report will not reach the Chamber of Commerce.
With these validations in Digipoort society can trust that all filings received by the Chamber of Commerce have not been altered and have been signed by an auditor who was entitled to do so.

DISCLAIMER

Although the auditor’s digital signing process is covered in this article, not all nitty-gritty details have been covered for clarity of this article. For example, it is possible to exclude certain parts from the hash calculation. After all, after the auditor’s report has been issued by an auditor, the annual report needs to be approved by the owners or shareholders. The date of adoption is added after the digital signature of the auditor, but before submission.

BOX 1:
ELECTRONIC SIGNING DEVICE

To sign electronically, an electronic singing device must be available. An example of such an electronic singing device is a Secure Signing Creation Device (SSCD). An SSCD is a hardware token that is used by the auditor to create the digital signature. An SSCD can only be obtained from a Trusted Service Provider (TSP). TSP's are under constant supervision of the Dutch government.

The SSCD adheres to the highest security level available. This means that the person who becomes the owner of the SSCD must be identified in person, must have sole control and the private key for creating the digital signature cannot be copied to any other device. In this case, we are talking about qualified certificates. In the Netherlands an electronic signature created with a qualified certificate has the same legal value as a hand-written signature.

In case of an auditor we go one-step beyond these requirements. Before an auditor receives a certificate, the TSP verifies with the professional body for accountants in the Netherlands (NBA) whether the auditor is included in the formal register of auditors. Only after a positive reaction, the auditor receives his or her SSCD. The profession (Registeraccountant or Accountant-Administratieconsulent) is included in the certificate, which is stored on the SSCD. If the auditor is being removed as an active member from the formal register of auditors (for example due to retirement or a disciplinary action), the NBA notifies the TSP about this. The TSP will then add the certificate to the Certificate Revocation List (CRL) or the Online Certificate Status Protocol (OCSP); both could be referred as the so-called blacklist. From this moment, all signatures which are created after inclusion on the blacklist, are legally invalid. And any attempt to nevertheless sign an auditor's report will automatically result in a blockade of the filling process. Digital signatures created before the moment that the certificate has being added to a CRL or OCSP, will remain valid.

Figure 2: Sole control of an SSCD; attached to a key ring

BOX 2:
DETACHED SIGNATURE

What happens under the hood? When the auditor clicks on the 'Create signature' button as seen in figure 1, three hashes are being created. A hash from the annual report, the auditor's report and from the signature policy. If none of these files is being modified, every time you create the hashes, they are the same. If only one bit does change, you will end up with a different hash. With this technique, anyone can determine that the files have not been changed after signing.

The three hashes and other information (like the date and time of signing) are the basis for the digital signature. All this information is passed through the SSCD where the private key resides (as stated before, the private key cannot leave the SSCD) and a signature value is being created. This signature value and the public key (for verification of the owner of the SSCD) is returned to the signing software. The signing software subsequently adds the hashes, the signature value and the public key to the detached signature file. The content of the signature value can be considered as the signature.

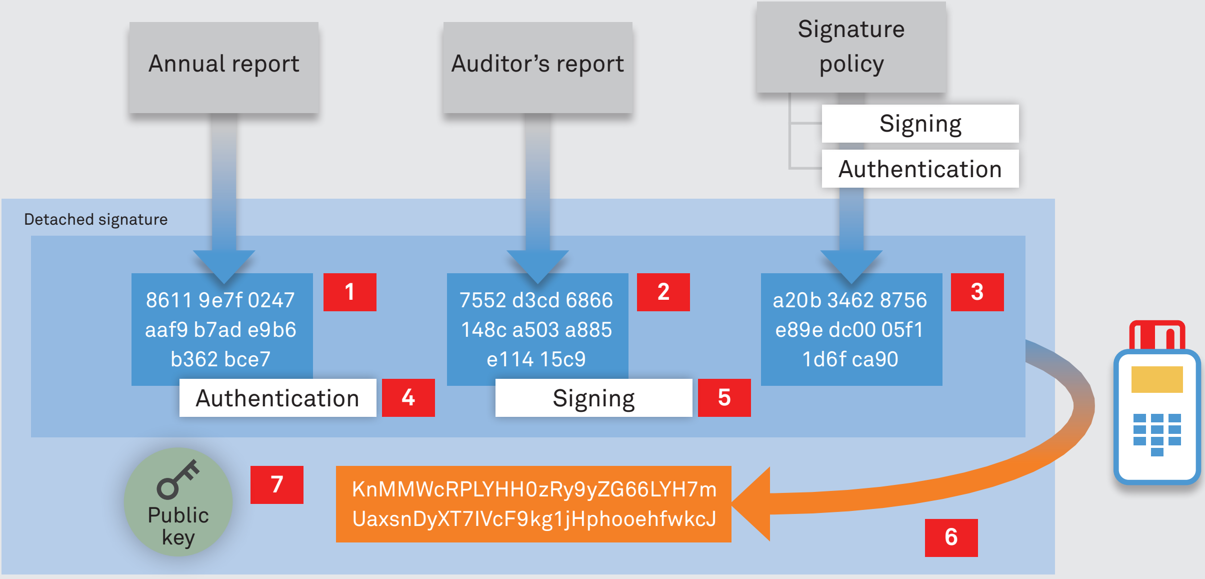

Annual report
Auditor's report
Signature policy
Signing
Authentication
Detached signature
8611 9e7f 0247 aaf9 b7ad e9b6 b362 bce7
1
7552 d3cd 6866 148c a503 a885 e114 15c9
2
a20b 3462 8756 e89e dc00 05f1 1d6f ca90
3
Authentication
4
Signing
5
Public key
7
KnMMWcRPLYHH0zRy9yZG66LYH7m UaxsnDyXT7IVcF9kg1jHphooehfwkcJ
6

Figure 3: Digital signing process under the hood

In the figure above 7 steps can be distinguished. The first three steps consist of calculating the hashes from the files. In steps 4 and 5 the correct commitments from the signature policy are selected and linked to the hashes. Step 6 illustrates the creation of the digital signature. The final step is to include the public key from the SSCD in the detached signature.

Royal Netherlands
Institute of Chartered
Accountants

NBA

The NBA's membership comprises a broad, diverse occupational group of over 21,000 professionals working in public accountancy practice, at government agencies, as internal accountants or in organisational management. Integrity, objectivity, professional competence and due care, confidentiality and professional behaviour are fundamental principles for every accountant. The NBA assists accountants to fulfil their crucial role in society, now and in the future.

Further information

If you have any questions, please send an e-mail to:
sbr@nba.nl

Royal Netherlands
Institute of Chartered
Accountants

NBA

Antonio Vivaldistraat 2
NL-1083 HP Amsterdam
P.O. BOX 7984
NL-1008 AD Amsterdam

T +31 20 301 03 01
E nba@nba.nl
I www.nba.nl