Date	January 26th, 2018
Topic	**Assurance**
Author	Frans HIETBRINK

0. Content

0. CONTENT 1

1. INTRODUCTION 2

1.1. INTRODUCTION OF FACTSHEET 2
1.2. INTRODUCTION OF SBR 2
1.3. INTRODUCTION OF ASSURANCE 3
1.4. ASSURANCE IN A PAPER-BASED PROCESS 3
1.5. ASSURANCE IN A DIGITAL PROCESS 3

2. DOCUMENTATION 4

2.1. DOCUMENTS 4
2.2. WEBSITES 4

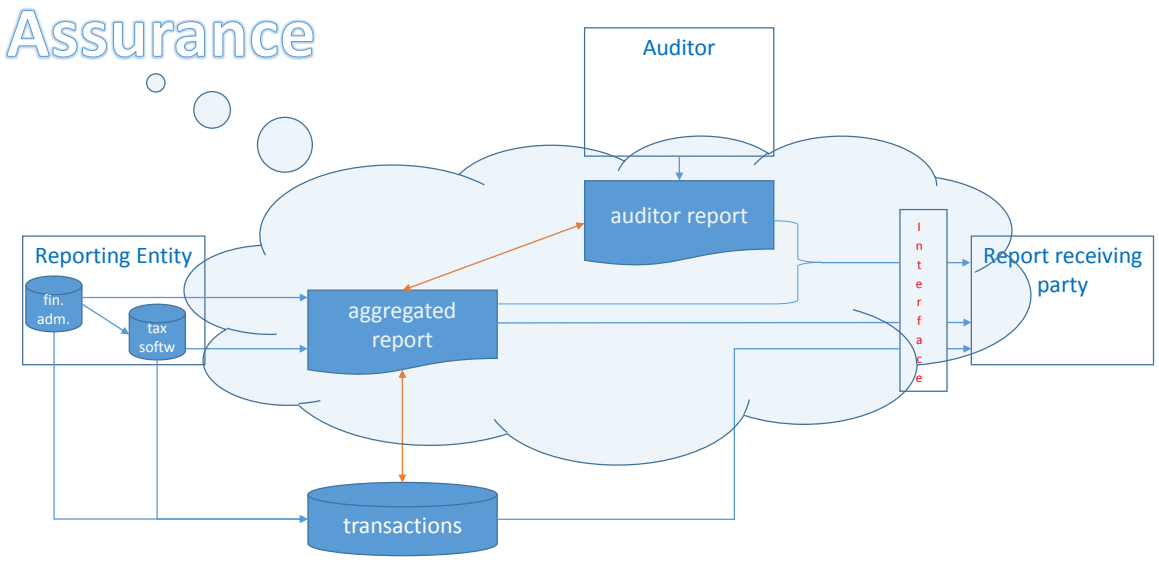
3. DIGITAL PROCESS IN COUNTRIES 4

3.1. DIGITAL PROCESS IN ESTONIA 4
3.1.1. Detailed description of technical infrastructure for assuring validity of annual and monthly reports 4
3.1.2. Detailed description of electronic signing for assuring validity of annual and monthly reports 6
3.1.3. Estonian existing assurance and validity process compared with digital process in Netherlands 6
3.2. DIGITAL PROCESS IN FINLAND 6
3.3. DIGITAL PROCESS IN FRANCE 6
3.4. DIGITAL PROCESS IN THE NETHERLANDS 7
3.4.1. Consistent Presentation 9
3.4.2. Auditors Report Taxonomy 9
3.4.3. SBR Assurance 10
3.4.4. Digital reporting to the banks 11
3.5. DIGITAL PROCESS IN SWEDEN 11
3.6. DIGITAL PROCESS IN UKRAÏNE 11
3.7. DIGITAL PROCESS IN SOUTH AFRICA (DRAFT-TEXT) 11

1. Introduction

1.1. Introduction of Factsheet

The SBR Working Group of XBRL Europe has the objective to share information about e-filing, e-publishing, e-exchange of data and related projects, where XBRL is or may be an adequate solution. To reach this objective the SBR WG publishes a set of factsheets about topics which are relevant to better understand the (relation between) components of a cross domain approach to exchanging business information.



1.2. Introduction of SBR

Standard Business Reporting (SBR) provides governments and businesses with an unequivocal, cost-effective, secure and adaptable method for the exchange of business information between organisations in a reporting chain based on open standards.

The implementation of the SBR approach starts with defining the common data sets between the various domains, a kind of common data dictionary. In a later phase the focus will include IT transformation (implementation of the data definitions in software and implementing secure exchange of data sets).

Before the introduction of a cross domain approach, which is the basis of the SBR approach, companies were asked by various government agencies to deliver the same information in multiple ways. For the same data definitions, different data sets are used. With the introduction of a cross domain approach, similar data sets are being used for similar data definitions, so companies can deliver the requested information with the proverbial click of the mouse. This leaves them with more time to focus on their business.

In its core, SBR is about the reuse of information. Although different regulators want different sets of data, thanks to SBR, they can all come from the same (financial) administration. With the use of a taxonomy, the basis for the re-use of definitions can be strongly rooted. With Standard Business Reporting it is not only possible for the regulators to return aggregated information. Private parties can use the data (definitions) to supply their stakeholders with relevant information.

The key principle of SBR is to standardize on data definitions, processes and technology. SBR is not tied to a specific technology, but rather adopts proven, widely used, open technologies which support

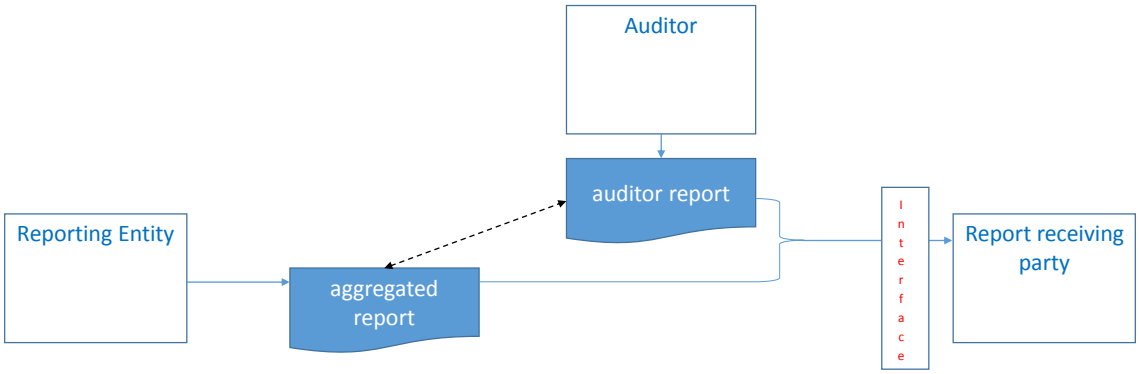
the exchange of structured data, data definitions and enable the unequivocal design and definition of processes.

1.3. Introduction of Assurance

In many countries, law requires annual reports to be audited by a trusted third party (depending on size of the company or other conditions). The stakeholders of the company – creditors, shareholders, regulators – must be able to trust the information in the report before engaging in the company.
In the paper era, a written report and a signature were sufficient. In the digital world, new challenges (and solutions) arise: how do we know whether all parties are seeing the same despite having access to the same digital files, whether the auditors report was not counterfeited, etc

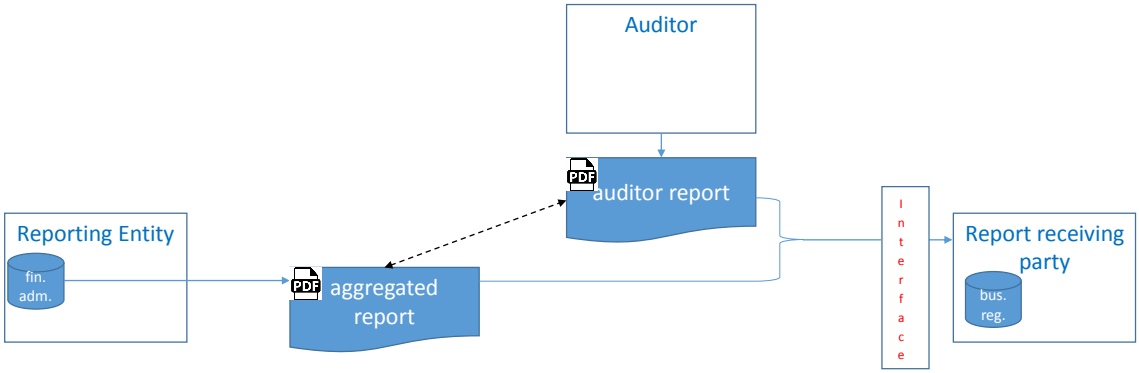
1.4. Assurance in a paper-based process

The paper-based process of filing an annual report is as follows:
1. The business is responsible for preparing their annual report;
2. The auditor performs an audit and provides an opinion in the (signed) auditors report;
3. The business is responsible for filing the annual report (including the auditors report) with the business register;
4. Stakeholders can retrieve the annual report, including the auditors opinion.



In the beginning of digitalisation the reports:

- ➔ are based upon data in information systems
- ➔ are used to enter data in information systems



1.5. Assurance in a digital process

The process for providing assurance on an annual report and filing it is slightly different. In the paper era, people were certain about what they were looking at (rendering of pdf files is considered equivalent).
With a digital XBRL report, stakeholders can't be so sure anymore that they are looking at the information the way it was intended by the business, and the way the auditor was looking at it when preparing the opinion.

Although the XBRL standard evolves and provides ever better ways to ensure consistent presentation of information, the current specifications are not enough for the digital-only annual reporting process.

2. Documentation

2.1. Documents

➔

2.2. Websites

XXXX
- yyy: https://zzzz.html

3. Digital process in countries

3.1. Digital process in Estonia

During the XBRL Europe Week in Frankfurt it was mentioned that Assurance in Estonia is based upon using an independent portal for:

- ➔ filing the report (unchangeable) by automatic upload (machine-to-machine via X-Road) or manual file (XBRL) upload or manual data entry to the state portal (Business Register)
- ➔ adding the auditors statement and needed digital signing
- ➔ Digital container (bdoc-file) formed in the portal Business Register

3.1.1. Detailed description of technical infrastructure for assuring validity of annual and monthly reports

What is X-Road?
X-Road is a system that ensures secure and direct data exchange between its members. During data exchange, X-Road ensures its parties with:

- ➔ Autonomy – an X-Road member defines, which data services it wishes to render and who gains access rights to the services;
- ➔ Confidentiality – information reaches only the authorized parties;
- ➔ Evidential value – using a digital signature enables proving the source of received data;
- ➔ Interoperability – all X-Road members speak the same language, regardless of the technology or architecture a member is using.

X-Road consists of:

- ➔ legal structure;
- ➔ organizational structure;
- ➔ protocol stack;
- ➔ software realizing the protocol stack.

The legal and organizational structure of X-Road regulates the following:

- ➔ who can or must be members of X-Road and how;
- ➔ scope of partial liabilities, rights and obligations.

For whom is X-Road intended?
X-Road guarantees secure Internet-based data exchange that ensures evidential value

- ➔ for the members of X-Road;
- ➔ for the information that is exchanged via X-Road.

Membership of Estonian X-Road is available to legal persons that meet the requirements specified in Regulation No 105 of the Government of the Republic of 23.09.2016 “Data exchange layer for information systems”[1].

What kind of data are forwarded via X-Road?
Messaging via X-Road is only performed within the pre-defined usage templates and data services. Description, development, maintenance and administration of data services is the right and obligation of members. The data format is uniquely predefined with the data service.
X-Road structure:

- ➔ does not determine the necessity of service – that is determined by the provider of data service;
- ➔ does not ensure the richness of content of the data exchanged via services – that is done by the provider of data service.

X-Road gives the provider of data services a universal tool for organizing secure data exchange equably with many parties.

Who can exchange data?
The provider of data services determines who are allowed to exchange data with them through the specific data service. In order to use data services, an X-Road member needs to have:

- ➔ technical readiness – a data service client application;
- ➔ access right given by the provider of data service for using a data service.

The basis for giving access rights is an agreement between the provider and user of the data service.
X-Road does not check the basis for giving access rights. X-Road ensures that:

- ➔ only those members can use the services, who have received access rights from the provider of data services;
- ➔ data exchanged via data services reach the relevant members without leaks and integrally (without deviations and with evidential value).

X-Road enables proving, if and when a specific data exchange took place
The X-Road protocol stack ensures the signing of all messages to be forwarded in the name of the sender by the sender. That means that, in order to prove the correctness of a message retrospectively, a member does not need a confirmation from any third party.
It is important to understand about X-Road that an e-stamp (in simpler terms: a signature) is only valid, if all the following elements exist:

- ➔ a validity confirmation for the message compiler’s certificate (guarantee of the trust service provider that the applied certificate is valid and that the X-Road member is the one they claim to be);
- ➔ the signed data of the message compiler (the message complier identifies their connection with the data to be submitted and shall define the earliest possible time of that connection);
- ➔ the time stamp added to the message (when added, the receiver of the message shall confirm the latest time when the data existed).

Why use the X-Road?
X-Road is the de facto data exchange standard in the public sector of Estonia. X-Road offers a uniform, cost-effective and high security to all exchanged data: confidentiality, uniformity, evidential value and minimum impact on availability.
The software to be created by the Information System Authority in compliance with the X-Road protocol stack is free of charge.
Only one X-Road and member activity is sufficient to be capable of exchanging data with all X-Road members – to save on time and equipment that would be used to develop systems, conclude and maintain bilateral agreements.

[1] https://www.riigiteataja.ee/akt/127092016004 (in Estonian)

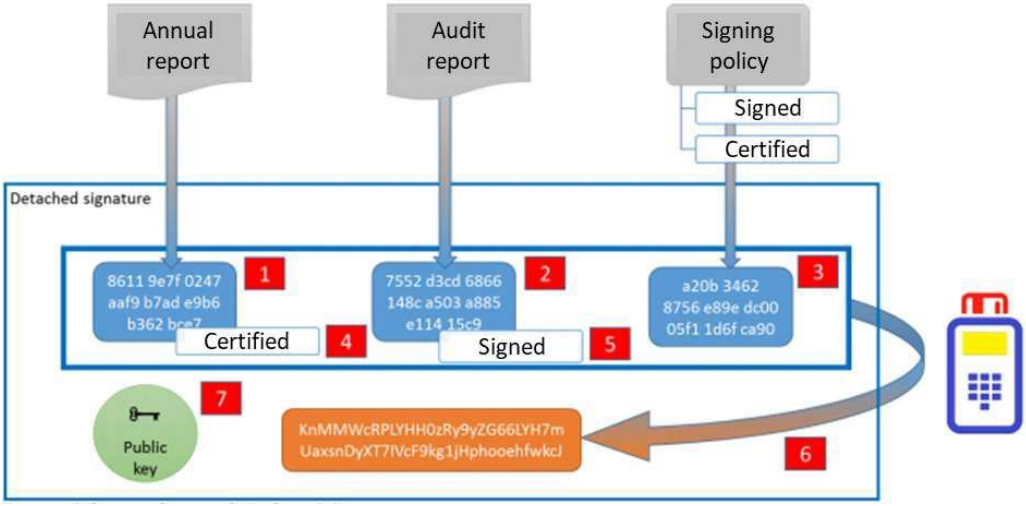
3.1.2. Detailed description of electronic signing for assuring validity of annual and monthly reports

Electronic personal identification
Electronic personal identification with an ID-card (digi-ID) or Mobiil-ID is better and more secure than identification with a user name and password in several ways.

- ➔ Electronic authentication provides assurance regarding the fact that correct data is received from the ID-card, thereby decreasing the risk of users submitting false data for service providers.
- ➔ All service providers are able to directly and securely provide their services to all ID-card holders without prior registration.
- ➔ This is also convenient for the users as they need not remember various user names and passwords – the same card and PIN are valid for all services.

For checking the validity information of certificates in real-time, the validity verification service[2] of AS Sertifitseerimiskeskus should be used. The service ensures secure electronic personal identification and gives digital signatures their legal effect.

3.1.3. Estonian existing assurance and validity process compared with digital process in Netherlands



1. Utilizes existing X-Road
2.– 5. Utilizes existing electronic signing system
6.-7. Digital container (bdoc-file) formed in the portal Business Register than

3.2. Digital process in Finland

In Finland there have been some discussions about the design of “Assurance” in workinggroup-sessions (some years ago). The idea was that:

- ➔ the filer submits the financial statement to the SBR reporting system
- ➔ a hash is created from this report and later attached to the auditors statement
- ➔ the auditor receives the report from the SBR reporting system, completes the audit, submits the auditors report, attaches the hash and digitally signs the auditors report

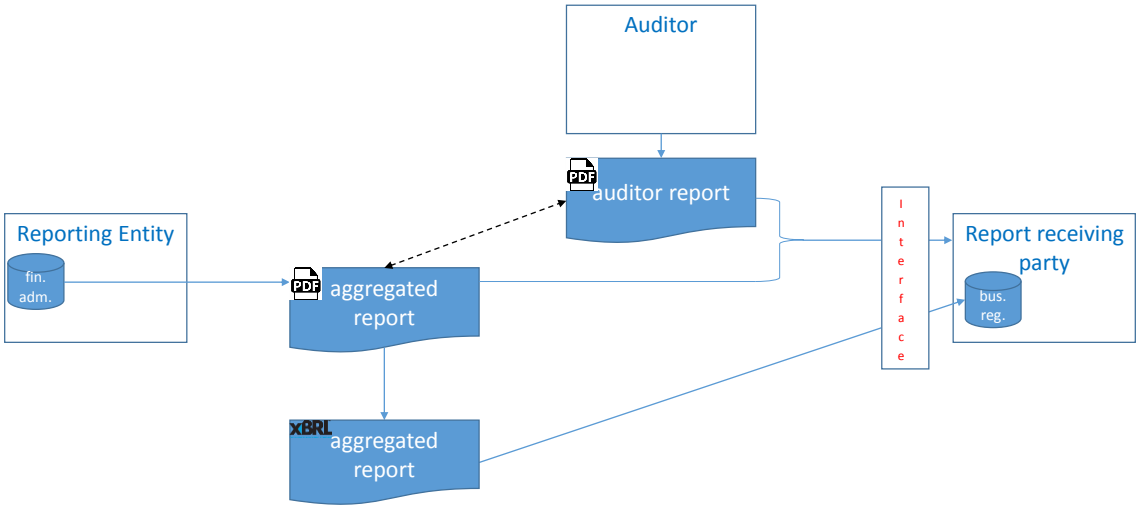
3.3. Digital process in France

There is no digital process for filing Financial reports in France, there is no digital auditors report as well. Digital filing for listed companies will start in 2021. The auditors reports are still based on paper or PDF. Electronic signature is already used for public procurements. There are about 6 French companies which have been filing their financial report in XBRL to the SEC.

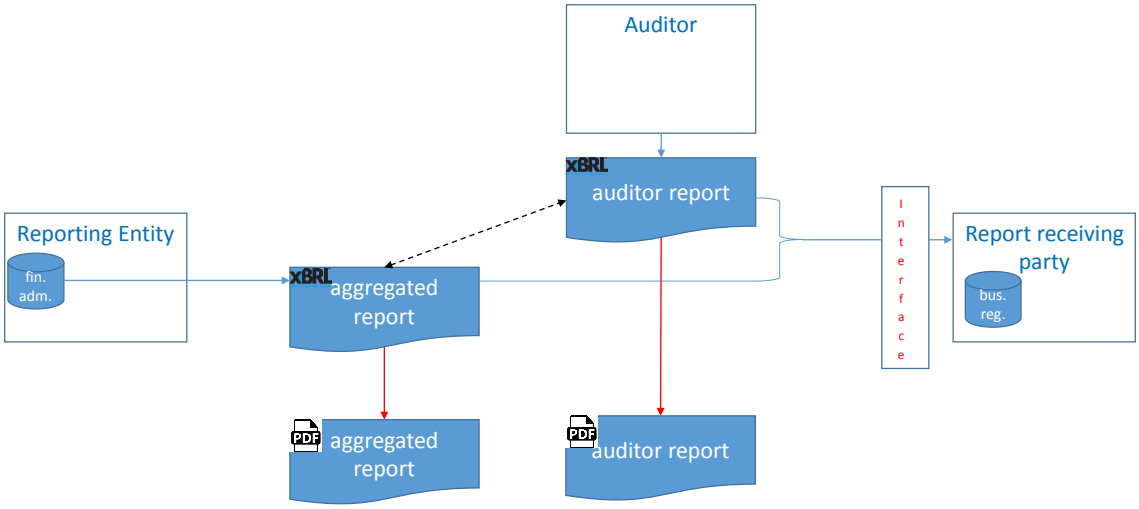
[2] https://www.sk.ee/en/services/validity-confirmation-services/

3.4. Digital process in the Netherlands

The Netherlands noticed that there were XBRL-implementations in which paper business reports were (partially) digitalized, but the auditor report still was based upon the paper version of the business report.



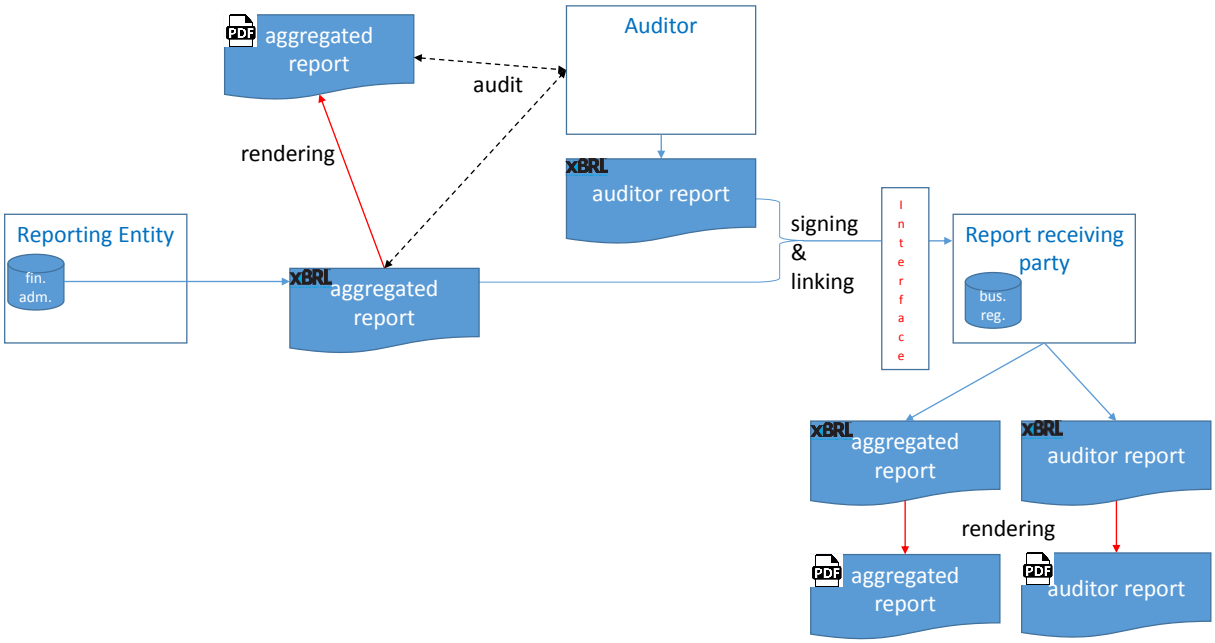
In the vision of the Netherlands it was necessary to design a methodology in which the interaction as a whole would be digital, with the possiblity to create human-readable versions of the digital documents.



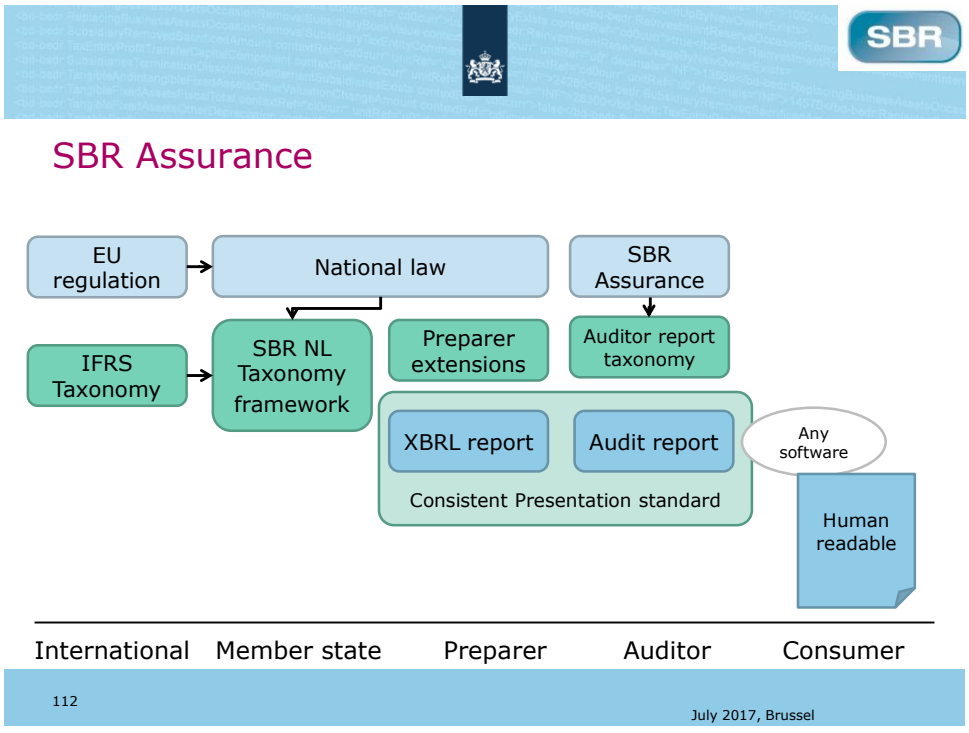
The Dutch SBR Project[3] devised a set of standards that provides a solution for digital assurance on digital information:

- ➔ A set of rules which provide certainty about the rendering of an XBRL report. This is called **Consistent Presentation**.
- ➔ **An XBRL taxonomy for the auditor report**, provided by The Royal Netherlands Institute of Chartered Accountants[4].
- ➔ A digital signature policy, called **SBR Assurance**, which ensures that the auditor report is created by the signing auditor and linked to the annual report. The policy[5] is based on the digital fingerprints (hash) of the files and the digital certificate of the auditor.

[3] More information about SBR is available on https://www.sbr-nl.nl/english-site/
[4] Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA)
[5] The Signing Policy is available in Dutch and in English http://www.nltaxonomie.nl/sbr/signature_policy_schema/v1.0/SBR-signature-policy-v1.0.xml



The annual report is based upon a National Taxonomy[6] and sometimes an Entity Specific Disclosure[7].
The auditors report is based upon the Auditors Report Taxonomy
The presentation is based upon a Consistent Presentation Standard
A human readable presentation will be provided by any software.



[6] As of today the IFRS taxonomy is not an EU regulation. It is an IASB / IFRS Foundation taxonomy. ESMA has chosen to base its taxonomy on it. The ITS ("implementing technical standards") has not yet been published. Within the SBR NL Taxonomy framework there are entrypoints for reports based upon Dutch Gaap and reports based upon IFRS. To support the IFRS entry points the Dutch Taxonomy has 3 schema's (and reference linkbases and label linkbases). To be able to work according the Netherlands Taxonomy Architecture some small changes have been made regarding the names of the schema's, label linkbase and reference linkbase. There are no changes regarding the namespaces, prefixes, elementnames,

[7] In the Netherlands often called: "Preparer Extension"

3.4.1. Consistent Presentation

The Consistent Presentation provides a set of rules which provide guidance on how to present (render) an XBRL report. This should provide enough certainty to all stakeholders that they are looking at the same information which is stored in the provided XBRL file.
The rules cover areas such as the table linkbase, dimensions, labels, rounding, etc.
Some examples are:

- ➔ The Consistent Presentation MAY render units as symbols if these are available in the UTR [Unit Type Registry]
- ➔ The Consistent Presentation MAY convert the value of dates from the ISO 8601 format (YYYY-MM-DD) to the local format
- ➔ The Consistent Presentation MUST apply the tables as included in the table linkbases within the DTS [Discoverable Taxonomy Set]

The full Consistent Presentation document is available in English.

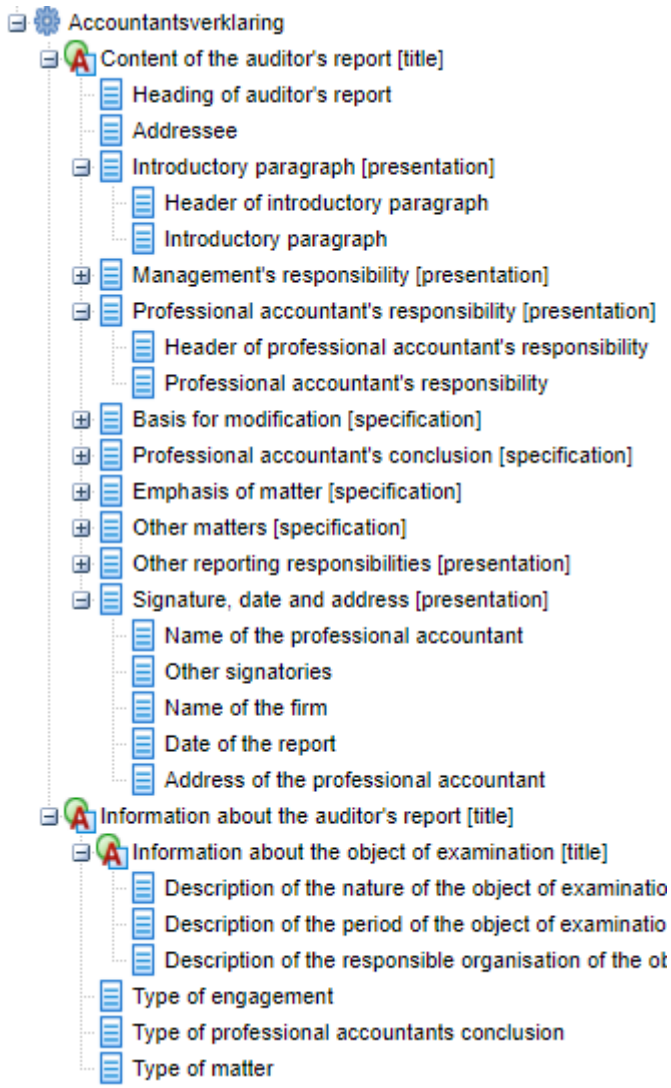
3.4.2. Auditors Report Taxonomy

The Royal Netherlands Institute of Chartered Accountants (or NBA) created the NBA Taxonomy (NBAT)[8].
The taxonomy contains a number of reports which can be issued, depending on the engagement type, e.g.:

- Auditors report[9]
- Compilation report
- Review report

The taxonomy is built according to the Dutch Taxonomy Architecture (NTA), which helps software vendors to incorporate the functionality in auditors-software.

[8] The NBAT, and more information, can be found at https://www.nba.nl/themas/ict/nba-taxonomie/
The NBAT 1.1 is a final version as of January 19th 2015. The documentation is available in Dutch and in English.
The NBAT 2.0 is a final version as of October 20th 2017. The documentation is only available in Dutch.
[9] The texts of the Audit statements are available in Dutch, English, German and French.
https://www.nba.nl/globalassets/tools-en-voorbeelden/voorbeeldteksten-en-passages/engelstalige-teksten/eng_controleverklaringen_1_1_serie.pdf



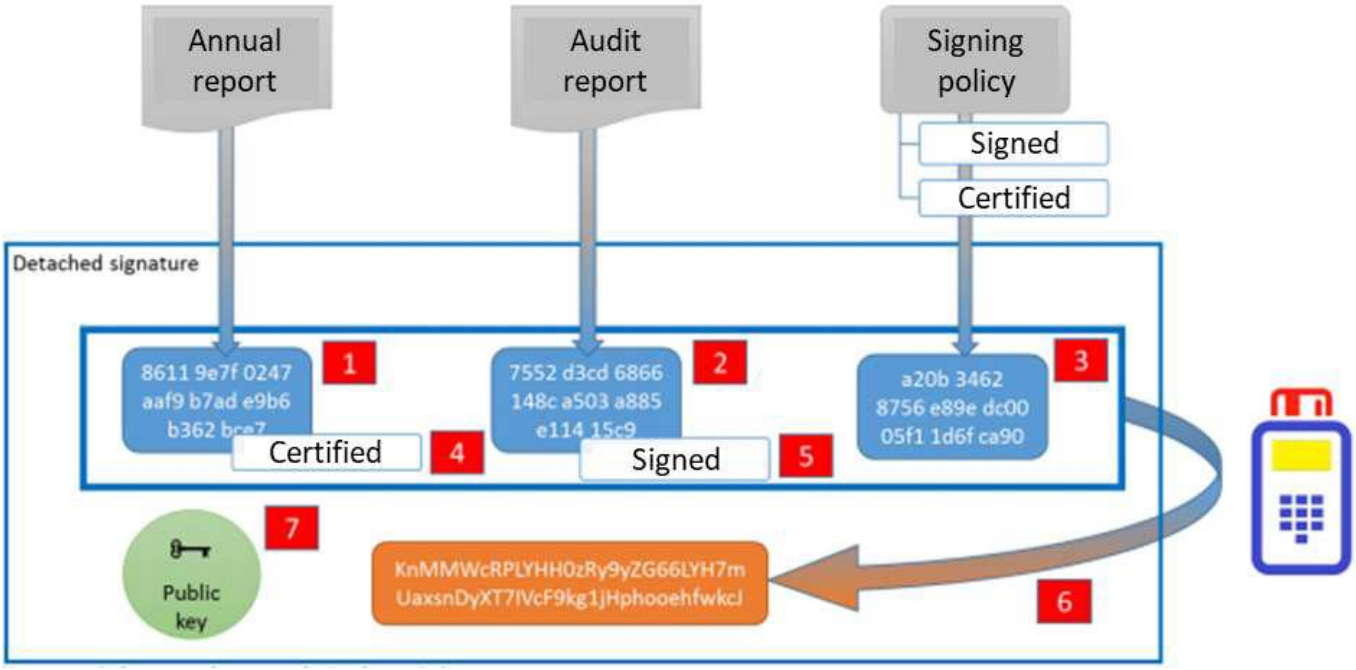
3.4.3. SBR Assurance

With SBR Assurance, any recipient will be able to validate that the signature, annual report and audit report were not changed[10] since signed by the auditor.
Digital fingerprints (hashes) are calculated for all the annual report files (the annual report itself and possible extension taxonomy files), the auditors report, and the selected SBR signing policy file.
The hash values are then combined and signed with the private key of the auditors nationally approved PKI[11] certificate. Together with the public key, the information is stored in a separate detached signature file. Anyone can verify the auditors identity, and whether the files were unchanged.
https://www.nba.nl/themas/ict/beroepscertificaat/

OpenSource-solution in the NL:

- ➔ http://opensbr.org --> Projecten --> SBR Assurance 2.0 -->
- ➔ http://opensbr.org/download/OpenSBR_Assurance_manual_20171118.pdf

[10] SBR Assurance does provide advanced methods to allow certain information to be added after signing. This memo does not focus on these technical details.
[11] A Public Key Infrastructure certificate consists of a private and a public key. Information encrypted with one key can be unencrypted with the other key.



3.4.4. Digital reporting to the banks

A compony can file a a credit revisioning report in XBRL. In this report the company reports that the Annual Accounts have been audited. The auditor does not give assurance on the digital filing of the credit revisioning report.

3.5. Digital process in Sweden

The development of Assurance is in the project phase.

3.6. Digital process in Ukraïne

The digital report and auditors report will[12] be electronically signed.

3.7. Digital process in South Africa (draft-text)

In South Africa the annual accounts are still prepared on paper. A compony can file a digital version in XBRL in a portal. In this digital version the company reports that the original (paper) version has been audited. The auditor does not give assurance on the digital filing.

[12] The UA approach will most probably be conceptually coherent with the NL case. It might even be relevant to replicate it , rather than reinventing the wheel. This has been decided after informally discussing the approach with NBA (february 2017, Amsterdam). As of January 2018, the UA IFRS Taxonomy draft audit report already follows the NBA taxonomy 2.0 as a model.