XBRL®
THE BUSINESS REPORTING STANDARD

Collaborate | Advocate | Standardise

Digital Signatures in XBRL

XBRL Sweden, 25th June 2024

Paul Warren
Technical Director, XBRL International

@xbrlint

XBRL International

XBRL International is a global **not for profit** operating in the **public interest**. Our purpose is to improve the **accountability** and **transparency** of business performance globally, by providing the **open data exchange standard** for business reporting.

- Membership organisation, supported by a small staff.
- Over 600 members from more than 30 countries.
- Responsible for maintaining the technical specifications that enable digital business reporting.
- Specifications are developed by volunteers in technical working groups
- Published specifications are freely available for royalty-free use

We build the **open standard** that enables a strong, competitive market of **interoperable software**.

Digital Signatures in XBRL

- Applying digital signatures to XBRL is a logical step
- Has been discussed for a number of years
- New working group established in 2022

Digital **S**ignatures **I**n **X**BRL WG

DSIXWG

D6WG

Goal

Develop consistent approaches for applying existing signature technologies to XBRL reports

In the EU, the *AdES family of standards is legally recognised, so D6 *must* interoperate with that

Not invent a new signature standard.

What are Digital Signatures?

Digital signatures provide verifiable proof that a document was signed by the claimed signatory.

- Any modification to the document will invalidate the signature – guarantees that the document is as it was when signed.
- Proves that the signatory had a particular "private key" – ensuring that only the stated person/entity has that key requires PKI (Public Key Infrastructure)

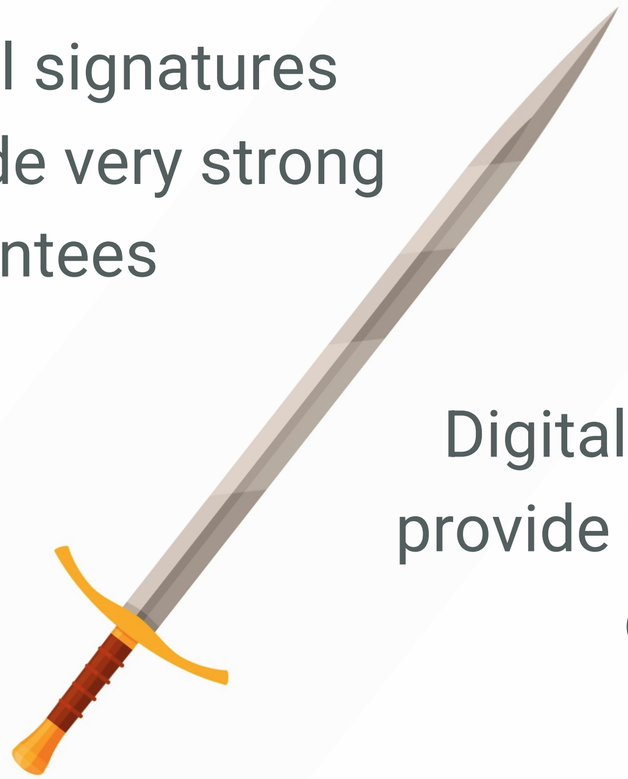
vLEI (Verifiable Legal Entity Identifier) provides a mechanism for tying keys to Legal Entity Identifier, making it a natural solution to this part for many XBRL reporting systems.

Why are signatures needed in XBRL?

- Guarantees that the document was created by the claimed author - and not modified since
- Guarantees that the document was audited by the stated auditor - and not modified since
- Non-repudiation - signatories cannot later deny that they created/reviewed document

Digital signatures

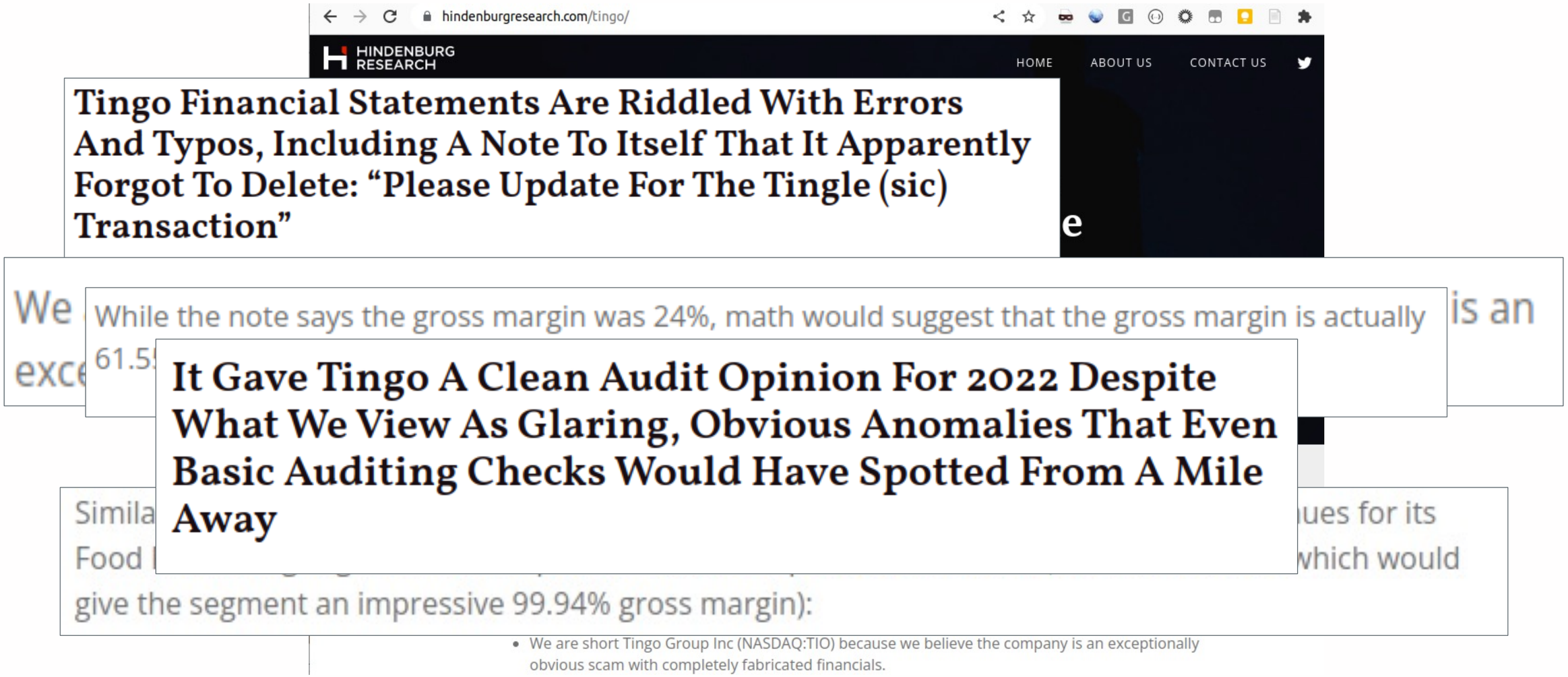
Digital signatures provide very strong guarantees



Digital signatures provide very strong guarantees

Digital signatures don't care whether you added a missing comma, or added three zeros to your reported revenue: a change is a change, and will invalidate a digital signature.

Is this a real problem?



Why are signatures needed in XBRL?

- Guarantees that the document was created by the claimed author - and not modified since
- Guarantees that the document was **audited by the stated auditor** - and **not modified since**
- Non-repudiation - signatories cannot later deny that they created/reviewed document

?

Digital signatures would allow us to trivially check these details, in a way that is just not possible in a non-digital world.

The SEC have now charged Tingo's founder with fraud, and lying to auditors and Tingo have de-listed, but being able to answer these questions immediately would be very valuable.

XBRL/iXBRL-specific challenges

- Dependencies
  - Taxonomies (extension and base)
  - Styling (CSS)
  - Images
- Where to place the signatures
- Partial signatures
  - Ability to create a signature that only relates to part of a report

- Many of these issues also relate to HTML reports
- Solutions applicable even if XBRL tags are out-of-scope for signature purpose

Embedded vs detached signature

- In a paper + ink world, signature forms part of the document
- Adding a signature to a document is a modification
- In a digital world, naïvely inserting a signature into a document would invalidate the signature
- Option 1: detach - keep the signature separate (inconvenient for recipient)
- Option 2: embed - set aside a location to insert the signature and carefully exclude it from the signature process

Embedded signatures

- Embedded signatures are obviously better for the end user, but are inherently more complicated to create and check.
- Signatures are much simpler when you just sign complete files

Embed both signature and report in a container

Put the signature inside another file (e.g. a ZIP file) along with the report, and other signed files.

- Complete files can be signed
  - Simple
  - Works with all file types (iXBRL, XBRL, images, CSS, fonts, taxonomies)
- Specific directory can be excluded for placing signatures in.
- We have an existing container format...

Report Packages 1.0

A brief diversion

Why?

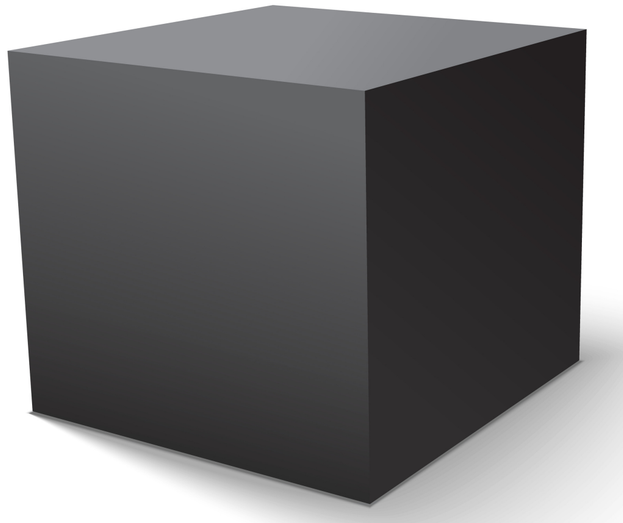
- XBRL reports are often not a single file:
  - Extension taxonomies
  - Images, CSS & fonts for Inline XBRL
  - xBRL-CSV tables + metadata
- Report packages combine report dependencies in a ZIP file
- XBRL tools increasingly take a Report Package as input, making loading reports simpler for users

Status

- Report Packages have been around since 2018, following an informal Working Group Note
- A formal Report Package specification was finalised in 2023
- Implementations such as ESEF and UKSEF are in the process of migrating to the new standard

"Black box" report packages

- Report Packages are specially structured ZIP files
- Report Packages currently use the ".zip" file extension
- Many ESEF report packages are invalid because users don't realise the format is important, and modify the files or file structure
- Report Packages should be a "black box" - end users should neither know nor care what is inside them, just like .docx, .xlsx, .jar, etc.



The new XBRL Report format

.xbri Dedicated file extension for packages containing Inline XBRL reports

.xbr Dedicated file extension for packages containing xBRL-CSV, xBRL-XML, xBRL-JSON and other, non-Inline XBRL reports.

"XBRL is too complicated!"

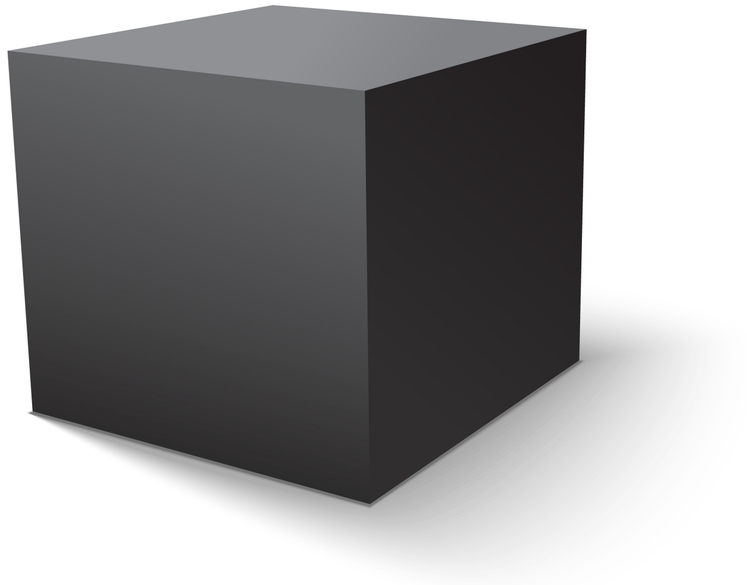
Goal is a change in thinking from:

Report Package contains an XBRL report

to:

signed

*Report Package **is** the XBRL report*



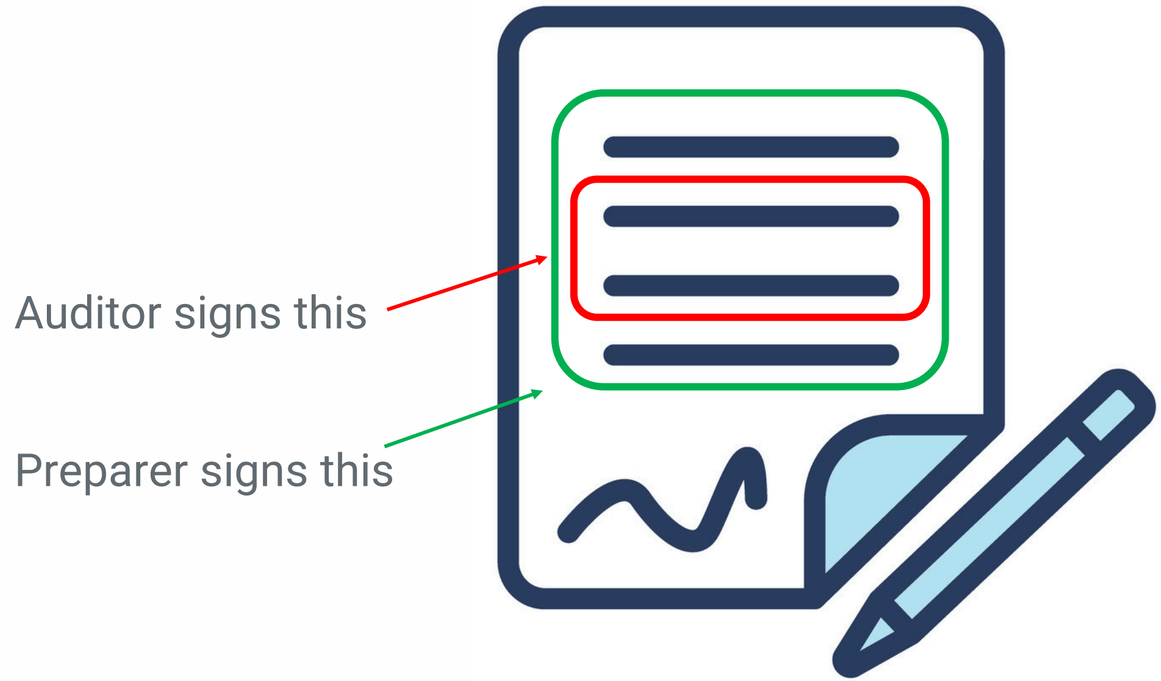
Report Packages provide the perfect mechanism for attaching a signature to an XBRL report.

Back to D6

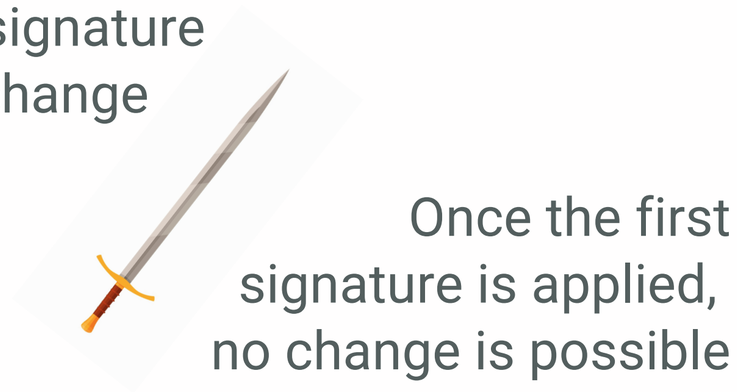
Key features

Partial signatures

- D6 supports "partial signatures"
- Different parties can sign different parts of a report
- Partial signatures can select XBRL facts, visual HTML elements, or both.



Once the first signature is applied, no change is possible



Once the first signature is applied, no change is possible

Signature coverage: taxonomies

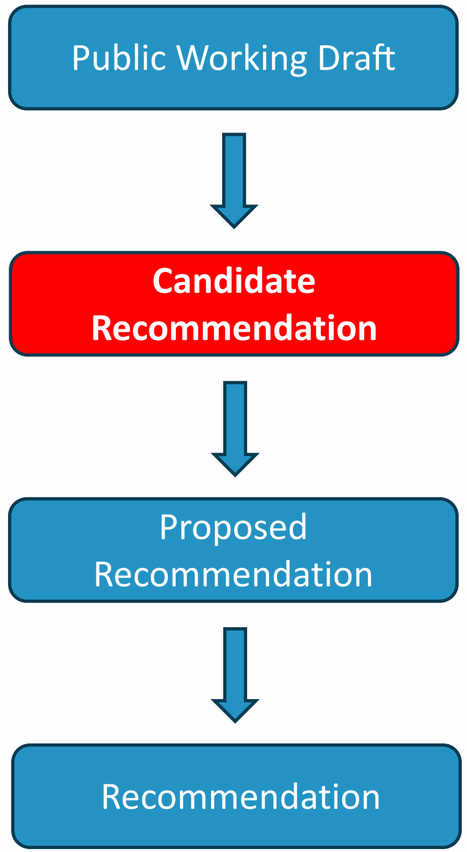
Signature will include the extension taxonomy (if any)
Signature will include URLs to base taxonomy
Signature will *optionally* include the base taxonomy

1. A change to the base taxonomy could invalidate or change the meaning of a report that depends on it, so any change to the base taxonomy should invalidate the report signature.

2. Base taxonomies are managed by trusted authorities who will ensure that any changes do not invalidate or change the meaning of a report. Including the content in the signature would make it unnecessarily difficult to correct errors in a base taxonomy.

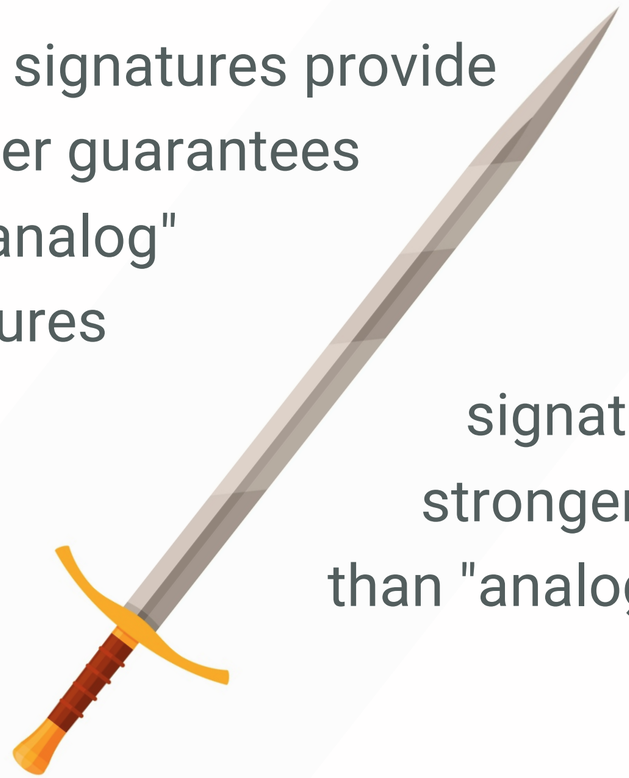
D6 Status

- Requirements published
- Candidate Recommendation specification published
  - Feedback needed on these and other issues
- Initial Conformance Suite published
- Software needed...
- Get involved!
  - Provide feedback on published requirements (specifications.xbrl.org)
  - Join the working group and contribute directly



How will D6 affect your processes?

Digital signatures provide stronger guarantees than "analog" signatures



Digital signatures provide stronger guarantees than "analog" signatures

- Digitisation rarely means:

"Do what you did before, but on a computer"

- Digital signatures are *not* "signatures, but on a computer"
- Processes need to change to work with, and to benefit from, the technology

Software needed

- User experience is often the weak link in digital signatures/cryptography
- For D6 to be successful, we need *good* software that makes it easy for end-users to sign reports, and verify signatures
- Call to vendors:
  - Start looking at the D6 conformance suite
  - Starting thinking about the user experience for applying digital signatures
  - Consider helping D6 effort with Proof-of-Concept demonstrations