Ensuring Trust and Integrity in Corporate Reporting: A New Global Standard for Digital Signatures

By John Turner, LLB

John Turner is the Chief Executive Officer of XBRL International, (https://www.xbrl.org/) where he leads the ongoing development and global adoption of XBRL, the standard for digital reporting. He has been involved in the XBRL community from its outset, previously serving as the CEO of a software company, heading XBRL activities at a big four firm, and managing data collection at a prudential regulator. He is a passionate advocate for the pragmatic use of standards to enhance reporting, data availability and corporate transparency worldwide.

Corporate reports provide vital information on business performance, governing a wide range of decisions by investors, regulators, creditors, customers and other stakeholders. Reports can have an enormous impact on an organization's value and reputation. It is essential that users can trust in their integrity, with full confidence that corporate data is reliable and that audit reports are genuine. But just how solid are the foundations of that trust?

Today, users of reported financial information often lack a provable connection between a regulatory filing and its issuer or auditor. This connection is historically based on assertions by the company. Users must take reports on trust, which can leave room for manipulation by bad actors and doubt by users. To address this issue, there is a growing need to establish a higher level of digital trust in corporate reporting.

Users must take corporate reports on trust, which can leave room for manipulation by bad actors and doubt by users.

While we might reasonably consider that the risk of management manipulating an audit report before submitting it to a regulator is remote, such incidents – while rare – can have significant impact. Further, with the rise of digitization in every walk of life comes a concomitant increase in cybersecurity concerns. The risk that a corporate report (or related audit report) is manipulated by a bad actor is also relatively low, but is rising as cybercrime become more sophisticated. The impact of such a bad actor's actions, both in terms of potential loss to the issuer and on broader trust in a regulated market, could be extremely severe. It is now time, therefore, for regulators and policy makers to consider additional layers of protection.

With digital reporting now the norm in the vast majority of major markets, a digital solution to the risk of impaired trust over disclosures provided to regulators and exchanges is required. In a world where information is exchanged and utilized on a global scale, we need a global standard for authentication. And with reporting becoming more complex and diverse – including, for example, sustainability disclosures alongside financial statements – a granular approach to authentication is increasingly important.

In this article I will discuss the need for a digital trust solution, particularly in terms of fraud prevention, and will introduce the new standard for digital signatures that is currently being finalized by XBRL International's Digital Signatures in XBRL Working Group (D6WG).

The Need for Digital Trust

The need for a digital approach to trust in corporate reporting is pressing worldwide, both to discourage and to detect fraud, as well as to ensure user confidence. The examples that follow show how fraud can occur; they are drawn from the US, but similar cases can be found in other jurisdictions. Ultimately, it is important to prevent fraudulent activities from happening in the first place, requiring a more robust and reliable connection between filings, issuers and auditors.

Here are two examples of fraud discovered by the US Securities and Exchange Commission (SEC):

1. The SEC announced that on August 6, 2001, Mark S. Jakob had been sentenced to 44 months in prison for the Emulex stock hoax and his role in disseminating a false press release that wreaked havoc with the stock price of Emulex.

   Mr. Jakob was facing a loss of almost $100,000 as a result of short-selling stock in the Emulex Corporation and wrote the fake release in an attempt to cover his losses. The press release appeared to come from Emulex and falsely stated that the SEC was investigating Emulex, that the company's CEO had resigned and that the company was revising and lowering its earnings for the preceding quarter. The next day, on August 25, 2000, several news organizations republished the press release. In a 16-minute period following the republication of the fake press release, 2.3 million shares of Emulex stock were traded, and the price plummeted almost $61.00, from $103.94 to $43.00, resulting in Emulex losing $2.2 billion in market capitalization. Following a trading halt by Nasdaq, Emulex resumed trading later that day, after the hoax was discovered, and the price rebounded to close at $105.75.

> **Frauds, turbo-charged by the convincing inventions of Large Language Models, could be perpetrated today in all kinds of markets, and risks around cybercrime and artificial intelligence are growing.**

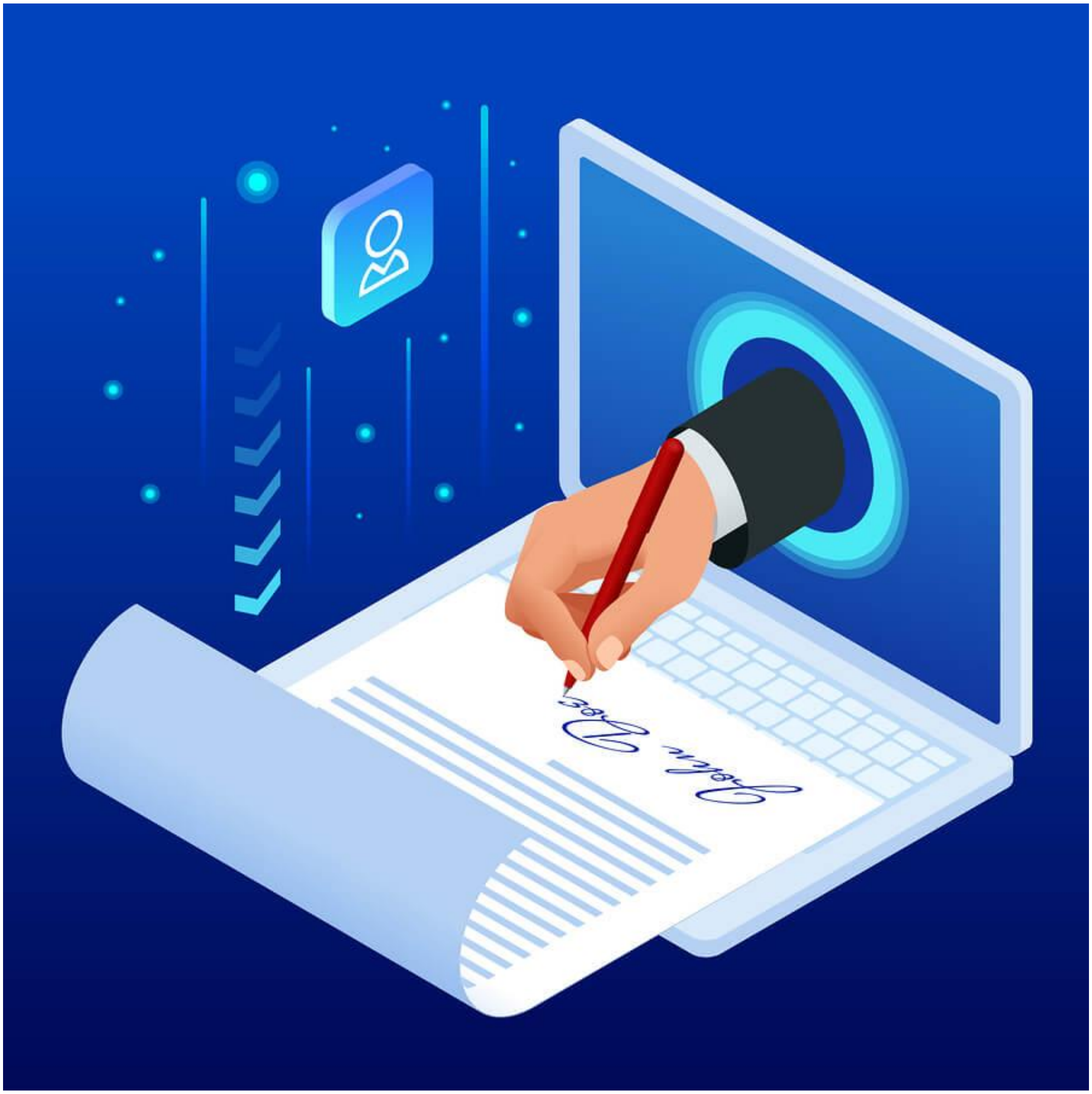
2. The SEC filed a civil injunctive action on January 26, 2010, against Tsukuda-America Inc., an Indiana corporation, and Mr. John W. Petros, alleging fraud in connection with a $600,000 offering of Tsukuda common stock. Petros, the sole officer, director and shareholder of Tsukuda, prepared and submitted Tsukuda's Form S-1 registration statement for the offering, incorporating false and misleading statements and forged documents.

   Tsukuda's registration statement contained a forged audit report, falsely identified a stock transfer agent company as the transfer agent for Tsukuda, included a bogus legal opinion and geologist's report, as well as sham consents from an attorney and a geologist who do not exist, and contained fictitious financial information.

Both of these real-life examples occurred some time ago, perhaps a testament to the work carried out by regulators in terms of authentication. It is not hard to imagine, however, that frauds of this sort, turbo-charged by the convincing inventions of Large Language Models, could be perpetrated today at scale in all kinds of markets – and that risks around cybercrime and artificial intelligence are growing.

Different regulatory environments worldwide have taken different approaches to authenticating reports. Some regulators employ only minimal security measures, while others maintain complex, multi-layered systems. A number of countries have implemented linkages between audit reports and financial statements using Adobe signatures. A rethink is needed, however, as reporting goes digital. The widespread shift to Inline XBRL, which has the huge advantage of making reports computer-readable, also means that relying on PDF signature mechanisms is no longer feasible. The world needs an international standard for signing digital reports prepared in XBRL.

Digital signatures, applied in a standardized manner, provide the well-proven solution that regulators need. They offer verifiable proof that a document was signed by the claimed signatory, ensuring legal non-repudiation and certainty that it has not been manipulated. The cases above illustrate the ability of motivated bad actors to falsify information. The use of digital signatures could ensure that only a genuine company officer can sign a press release, only an auditor can sign an audit report, and so on, providing a clear and traceable link to each signatory. It seems highly probable that digital signatures would have prevented these cases of fraud, or ensured their detection at the time of filing.



A New Global Standard for Digital Signatures

The Digital Signatures in XBRL Working Group, or D6WG – yes, we are aware we are terrible at naming things! – brings together experts from a number of countries and is chaired by Mohini Singh of PwC. It was formed to address the global need to establish trust in XBRL-based digital reporting. The group aims to provide a standardized approach to applying digital signatures to XBRL reports.

The use of digital signatures offers essential non-repudiation, authentication and integrity in a digital reporting context. For many years, XBRL International did not have a digital signature standard on its roadmap, as it was felt there were too many national solutions, often governed by legislation unique to that jurisdiction. Cyber risks are increasing, however, and the addition of specific assurance requirements over Inline XBRL tagging decisions in the EU and elsewhere brought this question to the fore.

The focus of the D6WG is not to create a new digital signature technology. Numerous technologies already exist, including some that are legally mandated at a national or regional level. Rather, the D6WG seeks to develop consistent approaches for applying these existing signature technologies to XBRL reports.

So, what exactly are digital signatures and what do they provide? At its core, a cryptographic digital signature provides verifiable proof that a document was signed by the claimed signatory, using pairs of “keys.” A private key is held by the signatory and a public one is published or otherwise made available by the signatory in a controlled manner. Thanks to the verification processes involved in the issuance of these key pairs, digital signatures prove the identity of the person signing the report by demonstrating that they possess a specific private key.

In other words, if I sign a document with my private key, then you can be confident that it was me that did so, as you can check my signature with my public key.

The proposed standard will enable companies, auditors, regulators, and other stakeholders to affirm their signoffs over a report in a digital and permanent manner.

The signing process takes as input the document and the private key, creating a very large number, which is the signature. Anyone who has the document and the public key can verify that the signature is valid – that is, that it was created using the paired private key from exactly the same document. If the document has changed in any way, the verification process will fail. Anyone who has the public key can check a digital signature, but creating a new signature requires the private key. These basic processes are 50 years old and underpin the operation of the internet, ATMs and your banking applications, as well as many other systems.

Applying this technology to XBRL, the proposed D6 standard will enable companies, auditors, regulators, and other stakeholders to affirm their signoffs over a report in a digital and permanent manner. In remaining neutral regarding the type of digital signature used, it accommodates various business and regulatory requirements. A critical feature of the standard is that it uses the fact that signatures are invalidated if any subsequent modifications are made to the document. This ensures data integrity and facilitates data provenance, allowing users to trace the origin and history of reported information. This, in turn, enhances transparency and accountability in corporate reporting.

Another benefit of the new standard lies in its granularity. It allows for multiple signatures, linking each one to all or part of an XBRL report. A digital signature might apply to the report document as a whole, a section, a table or even an individual fact. Signatures in Inline XBRL can apply to parts of the human-readable document, specific digitally tagged facts or a combination of the two. This granularity enables multi-layered approvals, with all relevant stakeholders signing off on the appropriate parts of a report.

For example, a company CEO may sign the full annual report, while the CFO and auditor sign off on the financial report, a specialist company signs the sustainability section, the company secretary signs off the earnings release and the regulator indicates that it received the digitally signed copy at a specific time and date. This provides non-repudiation, making it difficult for any party to deny their involvement. It also makes it clear exactly where the limits of responsibility lie for each section of a complex report, and means that each signatory can put their name to just the specific content they have themselves produced or audited.

The D6WG's first deliverable was a requirements document, which outlines the necessary criteria for implementing digital signatures in XBRL reports. This was followed by a new XBRL specification, currently available as a candidate recommendation draft. One of the questions addressed by the working group was where digital signatures should be located. The specification enables signatures to be stored within an XBRL report package, so that it is securely retained alongside the report files and connected to them, without modifying the files themselves. For more on the work of D6WG, and how the new standard works with the Report Packages specification to provide a consistent solution to digital signatures in XBRL, this presentation from back in November 2023 by XBRL International's Technical Director Paul Warren is worth watching.

Digital signatures are invaluable in verifying the authenticity and integrity of a financial report and its auditors.

Furthermore, the specification allows for the use of digital signatures based on the controlled issue of "digital certificates." This requires a public key infrastructure (PKI) to issue certificates. The PKI verifies the identity of individuals receiving these certificates (strictly, private/public key pairs) ensuring that they are who they claim to be. Typically, this involves the production of an identity document like a passport or driver's license, together with a range of supporting documentation. Thus, the digital signature not only proves that the signatory had a particular key, but also that the key belongs to a verified person or entity.

In this context, the launch of the verifiable LEI (vLEI) by the Global Legal Entity Identifier Foundation (GLEIF) is expected to prove a significant development in facilitating the global adoption of digital proof of identity in corporate transactions of all kinds, including corporate reporting. The LEI is an established legal entity identifier used by companies around the world to identify themselves, including in many existing XBRL reporting systems. The vLEI is its digital counterpart, designed for digital authentication and verification. It provides a mechanism for linking private keys to the LEI, via specific corporate roles. The vLEI is designed to permit digital proof that a specific individual holds a specific role on behalf of a specific legal entity, at a specific point in time. For example, it shows that Jane Wong is the CFO of Acme Pte Ltd, or Rohan Kumar is an audit partner at LWQH LLP.

The use of private keys that are tied to an identifier such as the vLEI makes it possible to guarantee that the document was created by the authors, audited by the stated auditors, and has not been modified since. As well as enabling traceability, this concept of "non-repudiation" ensures that the signatory cannot later deny their involvement, as the private key and signature can be verified. The only claim they can make is that their private key was stolen or accessed by someone else, something that is increasingly difficult with the application of appropriate cybersecurity measures.

Stopping Fraud in Its Tracks

Let us explore a recent example where digital signatures would have answered key questions and led to very different outcomes. A report published by Hindenburg Research in 2023 raised serious concerns about Tingo Group, a company filing with the SEC. Hindenburg Research stated that they were shorting Tingo Group because they believed the company was an obvious scam with fabricated financials. The report further highlighted that the financial statements provided by Tingo Group were riddled with errors.

Per the SEC, Tingo Group's Form 10-K for the 2022 fiscal year, filed in March 2023, reported a cash and cash-equivalent balance of $461.7 million in its subsidiary Tingo Mobile's Nigerian bank accounts. In reality, those same bank accounts had a combined balance of less than $50 at the end of the fiscal year.

What makes this situation even more intriguing is that the financial report was audited, and the auditors provided Tingo Group with a clean audit opinion. Hindenburg Research raised doubts as to whether the auditors conducted a thorough audit.

This raises two important questions: Was the report truly audited by the auditors who apparently claimed to have audited it? If it was audited, was the document the auditors saw the same as the document that was filed with the SEC, or was the report modified following the audit? Digital signatures could answer these questions effortlessly. They would have been invaluable in verifying the authenticity and integrity of the financial report and its auditors.

Digital signatures provide extremely strong guarantees that a document has not been modified in any way since it was signed.

Furthermore, the integration of the D6 standard into the report submissions process would make it highly unlikely for fabricated reports to be successfully submitted in the first place. The need for valid private keys means that it is not practically possible to generate fraudulent digital signatures or, in other words, to put a person's name to disclosures they have not willingly signed off on. At the same time, any modifications or tampering with the document after signing would be immediately detected and cause the signatures to be invalidated, preventing submission.

dreamstime.com

ID 183290429 © Ernest Akayeu

What’s Next?
The application of digital signatures to digital reports is a necessary step in ensuring their integrity and authenticity, and so in preventing fraud and fostering trust across today’s reporting landscape. By standardizing the use of digital signatures and leveraging existing technologies, we can establish a consistent global approach to signing XBRL reports. Numerous regulators and policymakers have expressed a strong interest in the D6 specification. Once it is finalized, we anticipate that many regulators will be eager to utilize the standard.

Widespread uptake of the specification will also, however, depend on the user experience developed by software vendors, and will require user-friendly and cost-effective signing. We encourage vendors and other stakeholders to review the specification, provide feedback, and start laying the groundwork for implementing the digital signatures standard.

It is also time for a range of actors within the information supply chain to consider whether existing workflows need to be upgraded.

- Should regulators, in addition to seeking digital signatures from management and auditors over relevant sections of reports being submitted to them, *add their own digital signatures to the report?* This would provide a further guard against later tampering by a bad actor that had gained access to their systems, as well as providing another layer of certainty about the authenticity of each corporate filing that could be relied on by investors, as well as in the course of litigation.

- Do auditors need to think about redesigning some common practices? There are situations today, in some parts of the world, in which a signed set of audited accounts are later altered by management, with the knowledge of the audit team, but not re-signed by the audit firm, not least because it might oblige the audit team to consider subsequent events. The use of digital signatures over XBRL materials would make these kinds of processes impossible.
- More broadly, we all need to consider how digital signatures will disrupt existing processes. Digital signatures provide extremely strong guarantees that a document has not been modified in any way since it was signed – and this makes it impossible to rely on being able to make minor, immaterial changes at a late stage. Digital signatures don't care whether you tripled your reported revenue or simply added a missing comma: any change will invalidate the signature. What does that mean for your practice?

We expect to see broad global adoption of the new D6 standard, ensuring trust in business data for the digital age. In a world of changing and increasingly sophisticated risks, it provides a fully digital, traceable and granular solution for report authentication and non-repudiation, facilitating fraud prevention and fostering user confidence.

We continue to seek broad inputs in order to further improve and finalize the proposed specification, which can be found here. Get in touch with us at XBRL International if you would like to be part of this process, and let’s start these conversations about deploying digital signatures now.