bitkom

eIDAS tools and their innovation potential: Promising and Trustworthy

White paper on the Short-Term Goals and Potentials of the eIDAS Regulation

Introduction

With the entry into force of the Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market of the European Union (eIDAS) in 2014, the foundation for a Europe-wide, legally valid electronic communication and secure electronic identification was established. The EU eSignature Directive, the German Electronic Signature Act, and Signature Ordinance became obsolete.

Through the use of trust services (electronic signatures, seals, timestamps, delivery services, and authentication certificates), companies, administrations, and individuals within the European Union can digitally exchange information on a unified legal basis, which is traceable by independent third parties. eIDAS creates new application possibilities within and between all countries of the European Union. This applies to all aspects of life. Contracts can now be securely concluded in electronic form across borders. Patient data and medical communication, such as medical reports, are now digitally protected on a uniform basis throughout Europe. Public registers, such as commercial registers and land registers, now have the option of providing legally valid digital information. Public administration can communicate authoritatively across national borders.

The potential of these new tools and standardization for digitalization is enormous and should urgently be applied in both the economy and administration. The use of trust services must therefore be accompanied and promoted primarily by corresponding national conditions. With this policy paper, Bitkom aims to draw necessary attention to the significance and relevance of electronic trust services. To achieve this, trust services should be strategically promoted through appropriate measures.

This policy paper describes the short-term measures and use scenarios. At the same time, a focus of the document is on the immediate benefits that the use of trust services brings to the German administration and economy. Naturally, existing or presumed obstacles to immediate use are also addressed.

Bitkom considers the following applications to be feasible in the short term and worthy of promotion:

- Qualified electronic remote signature for government use (↗Section 1)
- Qualified electronic seal (Q-seal) for official documents (↗Section 2) as well as electronic certificates (↗Section 3)
- Qualified website authentication certificates (QWACs) for website protection (↗Section 4)
- Remote identification through video identification process (↗Section 5)
- Recommended is the further development of legislation to support digitalization. (↗Section 6)

What’s a Q-Seal anyway?

Digitization Booster: The Electronic Seal

Good to know

In the EU regulation eIDAS, there are three variants of the seal:

- Advanced electronic seal (Art 3 Abs. 26)
- Qualified certificates for electronic seals (Art 3 Abs. 30)
- Qualified electronic seal (Art 3 Abs. 27) (Unterschied: Sichere Siegelerstellungseinheit + qualifiziertes Zertifikat)

However, only for the latter does the eIDAS provide rules of evidence. Therefore, the focus should be on this seal.

The EU-compliant Q-seal provides a convenient and reliable way to subject electronic documents to a quick authenticity check. As a result, one can rely on

- The fact that the legal entity or organization (company, authority, university, etc.) mentend as the sencer actually issued the document (Authenticity);
- The assurance that the data withing the document exactly matches the original, meaning they have not been altered afterwards (Integrity).

A legal entity is granted the Q-seal only if it could be clearly identified by the trust service provider.

Subsequently, the Q-seal of the applying organization is transferred onto a secure medium, such as a seal card, a Hardware Security Module (HSM), or even as a remotely triggered Q-seal.

The qualified electronic seal represents the highest level of sealing, and the identification process is accordingly rigorous. However, the effort is worthwhile: a document sealed with a qualified seal is admissible as evidence in court across Europe.

What’s a qualified website authentication certificate (QWAC) anyway?

TLS certificates for transport security and identity confirmation

The TLS certificate serves two functions: transport security and identity confirmation. A typical TLS certificate includes information about the domain it secures for identity confirmation. Additionally, it may contain details about the organization to which the domain belongs, including address and contact information. These details are verified by a trust service provider that issues the corresponding TLS certificate. For the user, a TLS-encrypted connection is recognizable by a padlock icon in the address bar. The user can view the information stored in the certificate within the browser.

Taking it a step further with the qualified website authentication certificate

The qualified website authentication certificate (QWAC) defined in eIDAS takes a step further than the traditional TLS certificate. The QWAC offers the element of authenticity as a distinctive feature. The EU Commission recognized early on that, in addition to mere encryption, it is necessary to create a tool that provides reliable information to the counterpart of the web server, regardless of whether it's a browser, an app, or a service, about the entity one is communicating with.

This is ensured by allowing only qualified trust service providers (VDA) to issue qualified website authentication certificates. Technically, it's a regular TLS certificate, but all the information in the certificate has been verified for accuracy by the qualified VDA. The applicant must provide the necessary evidence to guarantee that the desired entries can be made.

The profile of a website certificate is defined in the standard ETSI EN 319 412-4.

Qualified website authentication certificates enable the establishment and operation of a secure infrastructure, an aspect that should not be underestimated in today's world: secure and trustworthy communication in insecure networks.

1 Securing the operational capability of authorities during a pandemic situation

Initial Situation »Pandemic«

The COVID-19 pandemic acts as a magnifying glass, highlighting where digital services in the economy and administration fall short. Both administrative staff and citizens often lack the means to engage in legally binding electronic communication.

In the current situation, it is crucial that administrative and corporate services function seamlessly online, without the need for manual intervention. They are facing several central challenges in digitalization, such as:

- Government agencies must be able to provide their services continuously, even with limited opening hours and access options, both at the national and European levels.
- Consistent digital workflows need to be established, functioning even when government offices are closed. This also leads to cost-efficiency in the employed specialized processes.

The pandemic has underscored the importance of robust digital infrastructure, not only for convenience but also for maintaining essential services and ensuring business continuity during challenging times.

Solution „Utilization of Qualified Remote Signature”

The eIDAS qualified remote signature trust service has a significant impact on digitization. The qualified electronic signature holds the same legal effect as a handwritten signature. With the qualified electronic remote signature, electronic signatures can also be triggered remotely online. Documents signed with a qualified electronic signature clearly identify the signatory and simultaneously protect the document from tampering.

In Duty: Administration and Politics
To further establish the qualified remote signature in the digital realm, it must be user-friendly and easily integrable. Important steps have already been taken in this direction: Remote signature services are already available on the market. These solutions are cloud-based services that enable electronic signatures through a web application. Additionally, the remote signature service can be easily integrated into an existing workflow in compliance with GDPR through an API.

There is already a wide range of commercially available German signature solutions that can be immediately utilized. This allows for electronic signatures to be seamlessly executed directly from the signature application. As a result, a seamless digital administrative process becomes easily achievable.

2 Official Seal with Q-Seal

Initial Situation: „Paper is patient”

Although many citizens, businesses, and administrations wish for it, most administrative procedures still rely on paper-based notifications, even though electronic forms are equally permissible (§ 37 Administrative Procedures Act) and would simplify processes and reduce waiting times. Digital methods could also reduce the occurrence of forgeries of such documents.

This is particularly evident in the following example: How can one determine the authenticity of an official document? When documents are presented on paper, authenticity often stems from the letterhead, an official seal, and the envelope in which they are contained. However, both letterhead stamps and corresponding envelopes can be skillfully replicated with little effort.

Thus, as early as 2003, qualified electronic signatures were introduced in administrative law to protect electronic documents from unnoticed manipulation and provide information about the signatory. However, authorities never fully capitalized on the benefits of the qualified electronic signature because, in most applications in the past, many employees had to be equipped with signature cards instead of a central digital signature service similar to an official seal. In cases where signature cards were used, including in external-facing situations, documents were marked with a personal qualified signature of the processor. Any change in position, such as departure, transfer, or renaming of the department, necessitated the blocking of the certificate, followed by reapplication and reissuance.

Since many notifications did not require a personal signature, the "old" practice of stamping paper was simply more convenient.

Solution »Electronic Government Seal«

The Q-seal could enable a significantly higher number of official notifications to be provided or sent electronically compared to the current practice. This is because one of the key requirements of administrative acts is that they must clearly indicate the issuing authority. This has the potential to save a substantial amount of money for public administrations, especially in mass processes like tax or pension notifications.

For instance, the recipient can open a sealed PDF document using software like Adobe Reader or other freely available tools, such as the digiSeal reader, and immediately

receive a reliable verification result ("Green Checkmark" or "Red Exclamation Mark"). This approach enhances efficiency and reliability in processes, streamlining administrative workflows while providing recipients with a user-friendly and trustworthy experience.

3 Digital Certificates / Records / Protocols with Q-Seal

Initial Situation »Paper Documents«

An elaborately presented or even framed and hung certificate might fill someone with pride, but when it comes to presenting one's qualifications to a new employer, what truly matters is simple and secure means of transmission. Unfortunately, fake certificates are not uncommon in everyday job application practices. There are even internet portals where one can order a certificate of their choice – without any actual achievement, of course, for a certain fee.

News reports about cases of job application fraud or individuals falsely claiming academic titles in public highlight the practical consequences. This phenomenon applies across all groups of applicants, whether it's a candidate for an apprenticeship or a college dropout who fabricates their own university degrees and doctoral certificate. Not all cases are as sensational as someone illegitimately practicing as a doctor, teacher, or pilot, but it is a criminal offense regardless and involves the act of misrepresentation.

All these documents share the characteristic of being originally created on paper. At first glance, it's often difficult to detect full forgery. Nowadays, copies are frequently submitted, for instance, in online applications, and prospective employers often forego the presentation of originals. Only inquiries with the document-issuing authority can lead to uncovering the fraud.

The forgery of maintenance protocols for technical infrastructures or transportation means can carry significant potential for damage. In the scandal involving fake maintenance records in the Berlin S-Bahn, Deutsche Bahn estimated potential damages of up to 200 million euros at the beginning of the affair.

However, it's not only about certificates or protocols. Especially during the pandemic, the need to digitize and seal even seemingly simple documents such as "listener certificates" at universities became apparent. This would provide students with a straightforward yet secure and reliable way to obtain proof of their achievements.

Solution »Sealed PDF-Certificate«

An electronic seal from the institution that issued the certificate (such as a school, university, or company) can help guard against the alteration of an electronic document (such as a certificate or protocol) and vouch for its authenticity.

In the field of education, the following scenarios are conceivable: Vocational certificates issued by chambers of commerce or trade could be secured electronically with the chamber's seal. The same procedure could be applied to certificates of expertise issued by chambers of commerce. Not only could electronically sealed certificates enhance trustworthiness in application processes, but it could also facilitate entirely electronic admissions procedures at universities. Cumbersome parallel procedures, like having to authenticate a high school diploma after online enrollment and submitting it in paper form, would become a thing of the past. Official authentication is essentially integrated into the electronically sealed certificate, and there would be no need for further authenticity checks at the issuer in the future.

These procedures can be applied to all sectors in business and administration where some form of certification is required. The recipient or independent third parties can easily verify the sealed certificate using software like Adobe Reader or other available tools.

Required measures and success factors

To establish Q-seals in the German public and corporate sector, the groundwork is laid on a Europe-wide scale. Thanks to the eIDAS regulation and the preparations of trust service providers, there are no obstacles to the dissemination of new organization-based certificates. However, the attractiveness of this new product for German users does not automatically follow: Not everything conceivable for the use of electronic seals is already legally permissible today. For this reason, the German legislature must also play its part. This is not only about a symbolic "endorsement," but also about declaring electronic seals suitable, permissible, or perhaps even mandatory for specific administrative acts in individual laws and regulations.

Official Notifications and Documents

- **Federal E-Government Act** (§ 2, § 6, § 7): Authorities should be obligated to accept electronic documents with an electronic seal (not just a qualified electronic signature).
- **Administratives Procedures Act** (§ 3a): Authorities should be allowed to use the qualified seal in addition to the qualified electronic signature.
- **Administrative Procedures Act** (§ 33): In its current form, the law already stipulates that every authority, which has produced documents itself, should be able to issue electronic documents and electronic certifications. What could be more appropriate than to require such a copy/certification to be secured with a qualified electronic seal?
- **Administrative Procedures Act** (§ 37): Explicitly, it is already established that an electronic administrative act must indicate the issuing authority. The electronic seal perfectly fulfills this requirement and should therefore logically be mentioned in this context.

Certificates

Incorporation in all relevant regulations for issuers or at a central point (Civil Code and Administrative Procedures Act): Issuers of digital certificates and attestations must apply a qualified electronic signature or seal to these documents, provided they are intended for use in legal transactions.

4 Secure Government Websites in an Insecure Network

Initial Situation „Fake Websites, e.g. Corona Aid Application Pages"

In April 2020, the state of North Rhine-Westphalia had to abruptly halt online applications for COVID-19 emergency aid. Fraudsters had created fake websites and redirected applicants there. Unaware, many applicants disclosed their information, including their company registration number, tax identification numbers, ID card details, and bank account information. Using this data, cybercriminals submitted applications on the legitimate websites and collected funds. The West German Broadcasting Corporation (WDR) reported over 90 fake websites, affecting between 3,500 and 4,000 applicants with data misuse.

What lessons can be learned from this incident? Only when individuals can be electronically identified without a doubt and a website is unmistakably genuine, a trust environment for electronic interactions and transactions can be established.

Solution „Securing Websites with Qualified Web Server Certificates (QWACs)"

1. Securing Government Websites
Anyone who has prepared for a trip outside the EU and needed a visa for their destination country will be familiar with the problem. Which website is actually the official one for preparing the visa application? Often, alongside the legitimate website, there are many agency websites or fake websites solely interested in collecting fees.

But even within the EU, it's often not clear whether the accessed domain truly represents the official government website. A prime example of this is the COVID-19 aid application pages. Here, a Qualified Web Server Certificate (QWAC) serves as an important anchor that not only provides encryption but also reveals the true identity of the website owner, thereby establishing trust. This benefits all residents of Germany and the EU.

2. Securing Government Services
Currently, intensive efforts are underway to realize the essential digital interconnection of registries. One possible implementation of this interconnection can be achieved through Qualified Web Server Certificates (QWACs), as they provide clear information about the registry they represent. QWACs can enable registries to exchange data with each other that have never communicated before. In practice, each registry would possess its own QWAC, identifying it as a registry. When two registries need to exchange data, they would mutually identify each other using their QWACs and then communicate through pre-defined protocols. A service that is not a registry would never receive a QWAC with the designation of being a registry.

The same concept can apply to services that provide Open Data. In this way, applications can trust their sources of information, and data quality and origin can be verified. The use of QWACs would also allow government-provided services to be usable not only in Germany but throughout Europe.

3. Payment Service Directive 2 (PSD2)
A very specific and well-advanced example of how QWACs will be used across Europe in the future is demonstrated by the requirements of the PSD 2 (Payment Services Directive 2). Since September 2019, account-holding banks and fintech companies (known as Third Party Payment Providers - TPPs) are mandated across Europe to use QWACs to secure their data exchange among each other. This empowers fintechs across Europe with new GDPR-compliant business models and improved service for banking customers. Expanding this concept to the insurance sector would be easily achievable, providing a boost to emerging InsureTechs and enabling them to develop new business models as well.

5 Harmonization of Recognition of Video Identification Procedures as Remote Identification Methods

Initial Situation „Need for more modern Identification Methods”

By applying the regulations from Chapter III of the eIDAS Regulation, the video identification procedure can be used for the application of qualified certificates in accordance with Article 24(1)(d)(1) of Regulation (EU) No. 910/2014. Some of the first trust service providers in Germany started utilizing these possibilities as early as 2017. Nowadays, video identification procedures using "Artificial Intelligence" (AI) for the application of qualified certificates are being implemented in several EU member states. At the national, German level, video identification procedures with AI are also being used under exceptional authorization. As a result, disparities in the requirements of video identification procedures have already been established, not only on a European but even on a national level, leading to competitive disadvantages for trust service providers.

Under these circumstances, ensuring comparability of the quality of trust service provider offerings becomes questionable, which contradicts the principles of eIDAS. For instance, being located in Germany has become a significant competitive disadvantage for a qualified trust service provider.

Solution „Harmonization of Video Identification Procedures”

Harmonization of the recognition of video identification procedures as remote identification methods must be carried out at the European level. It has been demonstrated that existing regulations at the national level lead to a significant imbalance in the potential service offerings of national trust service providers.

Standardization organizations such as ETSI are well-suited to define common European technical frameworks. This approach can also be applied to video identification procedures.

These measures ensure that the use of video identification procedures is uniformly possible across Europe, and differentiation is based on service offerings and quality of service provision rather than location.

6 Necessary legal adjustments

Initial Situation „Impediment of digitalization due to lack of support for eIDAS tools”

The Tools for this Digitalization are Available. The same applies to the necessary legal framework. This framework is equally effective in all member states through the EU Regulation. However, the eIDAS tools defined in the regulation are not yet widely utilized.

Solution „Utilizing evaluation and Presidency to enhance legislative consideration of eIDAS tools”

The rapid implementation of the EU regulation is a crucial step in mitigating the impacts of any future crises. The upcoming eIDAS evaluation by the EU Commission is expected to draw attention to this matter. Additionally, the German presidency of the EU Council in the second half of 2020 presents an excellent opportunity to elevate eIDAS on the political agenda. For all stakeholders - market providers, authorities, and policymakers - the motto should be: Dare to embrace more eIDAS!

Of paramount importance now is to foster the use of eIDAS tools across various sectors and ensure their widespread deployment not only in the public sector but also in the private sector. It is essential to emphasize the broad range of applications and the added value for daily use. Another significant impetus could come from promoting eIDAS as a framework for Single-Sign-On (SSO) procedures. Greater market reach and harmonization across the European market could be achieved by introducing mandatory acceptance and integration of eIDAS into services and applications. This approach aims to establish the European ID system and create relevance for users by expanding the daily use of identification and authentication across all trust levels.

Public administrations play a pivotal role in resolving the "chicken-and-egg" challenge. Significant progress could be made if authorities widely accepted eIDAS tools and the online identification function of the national ID card. The government can also provide substantial support in this regard. A recent study by the Federal Printing Office highlights the need to give stronger legal consideration to eIDAS trust services. For instance, expanding the current provisions in the Administrative Procedures Act to encompass qualified electronic seals in addition to qualified electronic signatures would simplify the issuance of document certifications by authorities. The study further suggests amending the E-Government Act to mandate the use of eIDAS tools by government entities. Ministries, agencies, and other bodies could then not only accept electronic documents with qualified electronic signatures but also with seals.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact person
Rebekka Weiß | Head of Trust & Security
T 030 27576-161 | r.weiss@bitkom.org

Cover photo
© mbbirdy – istockphoto.com