EXECUTIVE SUMMARY

With the eIDAS Regulation, the European Union has created a uniform legal framework to enable digital business and administrative processes to be carried out securely and easily. The regulation contains the standardised trust services of the European digital single market, which include the qualified electronic signature (QES), the qualified electronic seal (QSiegel) or qualified website certificates (QWACs). With the help of these tools, electronic communication can be secured. They enable a so-called trust space in digitalisation in which secure interaction between people, software and machines can take place.

QES

Registered and delivery service

The individual digital

The secure digital message as with

signature

the post office or the bailiff

QSiegel

Timestamp

The reliable digital stamp for

The digital stopwatch like electronic

authorities and companies

photo evidence

QWAC

Preservation services

The secure identification of a

The digital eternal archive

website operator

Validation service

The automatic independent auditor

The tools of the digital trust space

In Germany, these tools are still largely unknown and what is even more serious: they have not yet been meaningfully integrated into German law. Consequently, they are hardly used in this country. Yet they have enormous potential. Just as the euro is a European currency, the eIDAS trust services could be used EU-wide for all legal administrative and business processes - and thus speak the same digital language.

To achieve this goal, some legal gaps need to be closed. Existing laws must be expanded where certain eIDAS tools have not yet been implemented. This applies,

for
example, to the eGovernment laws of the Federation and the LÃ¤nder, the
Administrative Court Code, the Code of Civil Procedure or the Social Code. Here,
the
eIDAS tools must be integrated into the legal texts in order to enable digital
and
standardised communication processes. Completely new legal solutions must be
created
where digital processes have not yet been considered. For example, new
regulations for
electronic legal transactions are necessary. This applies, for example, to the
Civil Code,
where a new regulation on digital communication relations must be included, or
to the
professional codes of conduct for lawyers and tax advisors. Last but not least,
a new
understanding of formal requirements is needed. For this, a function of trust
must be
established as a new element in German law.
There are concrete recommendations for action for policymakers: The German
government
should address the deficits in the implementation of the eIDAS Regulation as
quickly as
possible. In particular, new legal regulations are required with regard to the
QSiegel and
QWACs, such as those already in place in the Payment Services Directive 2
(PSD2). In this
context, the Federal Government should see the implementation of the eIDAS
Regulation
as an important contribution to more data and consumer protection in Germany. In
the
context of "digital legislation", there should also be an orientation towards
the "Better
Regulation Toolbox #23" of the European Commission. The "Better Regulation"
project of
the Federal Ministry of the Interior, for Construction and Home Affairs already
exists for this
purpose. This project should be supplemented by an impact assessment of laws for
the digital
transformation, which explicitly takes into account the tools of the eIDAS
Regulation. For
2020, the German EU Presidency will have the opportunity to treat the further
development of the eIDAS Regulation as a priority. For example, the Federal
Government
can take the lead in the negotiations on the revision of the eIDAS Regulation in
order to
introduce new tools (e.g. an eID function for companies) and to achieve greater
binding
force in the use and recognition of trust services. At the same time, further
harmonisation
of the requirements for certification and authorisation of trust services can
also be initiated.

1

INTRODUCTION
The digital transformation is progressing relentlessly and has reached almost
all areas of
private and public life. Nevertheless, Germany is only at the beginning of
profound
upheavals that will permanently change the economy, the state and society. The
associated potential is enormous and yet it is only being exploited to a limited
extent in
this country.

With the Signature Act (SigG), which has since come into force, Germany was a pioneer in secure electronic communication in the 1990s. However, in the course of advancing digitalisation, the prerequisites have changed. Today, the legal framework for digital communication processes is created primarily at the European level. National special paths no longer seem to be expedient and so the motto is: whoever wants to advance digitalisation must think European.

Electronic legal transactions need trust and security

The race for the best digital locations has long since begun in Europe. Germany is in danger of losing out in the European competition if it does not succeed in processing digital business models in a reliable, legally secure and, above all, standardised manner.1 The necessary tools already exist: The European eIDAS Regulation2 contains the trust services of the European Digital Single Market. They are the key to trustworthy and secure electronic legal transactions throughout Europe and can make Germany fit for the digital future. So far, however, they have been insufficiently applied.

This study highlights challenges in the implementation of the eIDAS Regulation in Germany and describes which legal changes are necessary to integrate the trust services of the eIDAS Regulation into German law.3 To this end, we first outline the current legal framework in Germany. We identify regulatory gaps and the need for action. This makes it possible to see which laws need to be changed and how. One of the findings: Consistent implementation of the eIDAS tools in German law can make an enormous contribution to the digitalisation of the administration. In the end, citizens, businesses and not least the administration itself will benefit from this.

Wasted potential

Analogue postcards, letters and contracts will soon be a thing of the past. Communication in administrations and companies and with citizens* will be almost completely digitalised in the next five to ten years. All those involved will have to reposition themselves for this.

Germany currently ranks 21st out of 28 countries in the digitisation of public services.4 So far, only ten percent of the German economy is making use of its digital opportunities. Germany is thus giving away 500 billion euros in potential.5

The next challenge: the digital transformation is advancing at an enormous speed. This particularly affects the very mechanical and organisational German economy with its tendency towards hierarchies and perfection in classic production. This in turn leads to

enormous pressure on politicians to act. It must take on the changing conditions and shape them. After all, German companies can only adapt if the appropriate legal framework is in place. The same applies to the administration: there can only be a digital administration if the use of digital technologies is legally secured.

Reality: Hurdles to digitalisation

Digitisation projects in Germany fail time and again due to a lack of legal requirements. A practical example: In 2005, a pilot project for electronic proceedings began at the Olpe Local Court.6 Divorce proceedings were to be accelerated, made more efficient and more citizen-friendly. It failed because the means of electronic signature were not sufficient. For example, the divorce offices did not accept the divorce decrees signed by the judges with a qualified electronic signature (QES) for lack of secure proof of origin.7 For them, the name and job title of the judge was not sufficient to prove a decree authority. As a result, the judgments were printed out, executed and sent by post.

In this practical example, it becomes clear that the QES is not sufficient to prove with legal certainty that a specific authority has issued a document. With the QES, it is only legally assumed that the document originates from the signing natural person. The question of whether this person is still a judge, has been transferred to another court or is currently on parental leave is not answered with legal certainty by a QES.

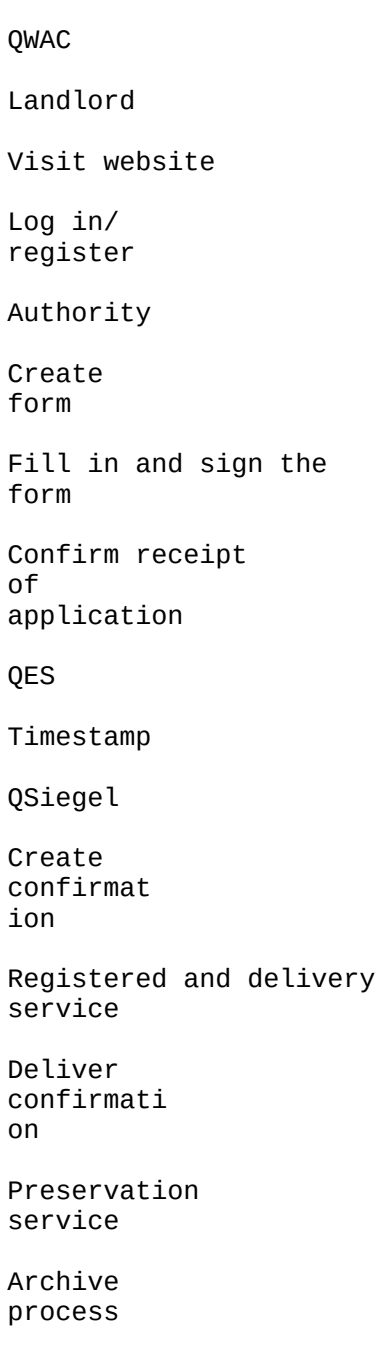
The solution: the qualified electronic seal (QSiegel) of the eIDAS Regulation.8

The eIDAS Regulation has the solution to the problem: the Q seal. It would only have to be affixed to the document in order to provide secure electronic proof of the origin and personal signature of judgments. However, the legal basis for this is still missing in the procedural and court rules. Whether the Q seal will be introduced in Germany and for which processes it is permissible, however, is a matter for the German legislator alone to decide.

The trust space in digitalisation
German legislation is therefore challenged. Only legally secure communication between people, software and machines is reliable communication. The trust services of the eIDAS Regulation can make a valuable contribution to this. If they are used effectively, a trust space will be created in which trusting interaction between all participants is made possible and through which the digitalisation potential in administrative and business processes can be exploited.

Here is another example: If you want to change your place of residence, you have to expect a lot of work and often weeks of waiting time for an appointment at the

competent
authority.9 A digital re-registration would be much easier. For this to work online, the citizen
must be securely identified. The online ID function of the electronic identity card is
suitable for this. The security of the respective website is verified by qualified website
certificates (QWACs)10 . Registration certificate and landlord's declaration are provided with
a QES and a QSiegel. The entire process and the documents receive qualified electronic
time stamps and QSiegels so that the process can be stored and archived for a long time in
a traceable and unchanged manner. This procedure secures the entire communication in
the notification process. In addition, the local offices are relieved of routine tasks. If the
citizen receives a short-term appointment at the office at the same time as the registration
certificate, the new address can be quickly added to the identity card.



The digital trust space using the example of re-registering a flat

eIDAS trust services can be used in many cases: for issuing certificates of good conduct,
certificates of employment or certificates of further education, for delivering election
documents, for re-registering vehicles or for notices or warnings in criminal traffic. All
these communication and service processes need tools so that they can be made secure
and trustworthy in the digital world. The eIDAS Regulation creates the prerequisites for
this with its trust services. It enables a trust space in which completely digitalised
official or corporate workflows are possible, because all the services and products
behind them are certified and a controlled high level is ensured. In addition, this results
in a uniform approach to legal issues, such as liability. Such trust spaces are a necessary
condition for the successful digitisation of the German administration.

2

THE CURRENT LEGAL FRAMEWORK
CONDITIONS OF TRUST SERVICES

The EU Commission's Digital Agenda 2010 came to the conclusion that the heterogeneous
regulations for electronic signatures in the individual countries were an obstacle to the
establishment of a digital single market.11 Although the equality of the QES with the
handwritten signature had been legally established in the EU Signature Directive, among
other things, corresponding communication between the member states was only possible
in exceptional cases. There were simply no uniform legal and technical solutions that were
compatible and mutually recognised.

These problems were solved with the eIDAS Regulation. As a European regulation, it applies
directly in all member states of the European Union and takes precedence over national
law. The SigG, which applied in Germany until then, was replaced by the eIDAS Regulation
on 29 July 2017. In contrast to the SigG, it allows Q seals to be introduced in the member
states. This is made possible in Art. 37 para. 1 (electronic seals in public services).12 In addition,
the Trust Services Act (VDG)13 was created in Germany, which has supplemented the
Regulation since 29 July 2017 and is also intended to regulate areas previously left open in
German law. In conjunction with this, the Trust Services Ordinance (VDV)14 came into force
in February 2019.

2.1

The eIDAS Regulation

The eIDAS Regulation of the European Union has been applicable law in all 28 member states and in the European Economic Area since 17 September 2014. It has been adapted by Iceland, Liechtenstein and Norway. The regulation repeals the EU Signature Directive (1999/93/EC).15 The eIDAS Regulation thus forms the regulatory umbrella for implementing secure and trustworthy electronic business processes in Europe. National regulations are not repealed, but they may not contradict the eIDAS Regulation or must be limited to specific national applications (sovereignty of application). The German SigG was therefore repealed in order to create legal certainty. An evaluation of the regulation by the European Commission is planned for 2020.

2.1.1

The tools of electronic legal communication

Trust services for electronic legal transactions have been around for a long time. However, they have so far been used rather rarely by end users. This was probably mainly due to the complex design of the technical tools on the basis of the formerly valid legal basis (EU Signature Directive [1999] and SigG [1997]). This is because the use of signatures based on certificates from accredited providers of high-security modules with secured application components is a field that is as broad as it is complex.

In principle, a distinction is made between trust services and qualified trust services. Qualified trust services are to be recognised as equivalent in all member states and can thus be applied in a standardised manner in the European Union.

All qualified trust services of the eIDAS Regulation are characterised by two features:

1. Qualified trust services are marked with an EU trust mark. This is intended to enable consumers to recognise and assess the quality of the products at first glance, similar to the EU organic seal. The EU trust mark was introduced by the first Implementing Regulation No. 2015/806 of the eIDAS Regulation.

2. Qualified trust services are included in a national trust list, which contains the qualified trust service providers of a country. The national supervisory authorities are responsible for this. In Germany, these are the Federal Network Agency or the Federal Office for Information Security. They provide the national list in the form of a TLS (structured according to ETSI Technical Specification ETSI TS 119 612) in a machine-readable form

and thus enable an automatic check. The EU Commission provides all national trusted lists centrally in a "List of Trusted Lists". This means that providers of technical components can obtain the list from a central and trustworthy office and check the trustworthiness of certificates.

European standardisation

In order to develop technical norms and standards, there are two standardisation organisations in the European Union: ETSI (European Telecommunications Standards Institute) and CEN (ComitÃ© EuropÃ©en de Normalisation).

Both organisations were commissioned to fundamentally restructure and comprehensively revise the existing interoperability standards. This ensures that eIDAS trust services used in Europe can be used interoperably and across borders.

The EU trust mark

The eIDAS Regulation provides for various qualified trust services, which we explain below and which are all based on an electronic certificate.16

The electronic certificate

The electronic certificate is a basic technology that is used in almost all eIDAS tools. It is a collection of information about the certificate holder, the certificate issuer (trust service provider), information about the certificate itself (purpose of use, validity period, verifiability, underlying issuing guidelines, etc.) and the public key of the certificate (certificate content). These certificate contents are checked for correctness by the trust service provider and in turn electronically signed and thus confirmed by him. This ensures that the certificate details are protected against unnoticed manipulation.

In principle, a certificate is always public. Decisive for the quality, i.e. to a certain extent the validity of the certificate, are the underlying process for identifying the certificate holder, the process of generating the key material and the certificate, as well as the storage location of the private key.

In this context, the eIDAS Regulation and the referenced implementing acts define the framework conditions that must be met in order to achieve the "qualified certificate" level, among other things.

Qualified Electronic Signature (QES) Certificate

A QES is based on a qualified certificate. The QES is linked to the electronic file in such a way that no unnoticed change can be made to the signed document after it has been signed. Furthermore, the certificate makes it possible to see who signed the document. A QES is generated by or on behalf of a natural person. It is often used for declarations of intent by natural persons. A QES is responsible for securing the application level.

Qualified certificate for the electronic seal (QSiegel)

A QSiegel is also based on a qualified certificate. The functioning of the

QSiegel is
comparable to the QES. The decisive difference is that a Q seal is not assigned to a natural
person, but to a legal entity - such as a company. The sealed electronic file receives a
corresponding proof of origin, but not a declaration of intent. Like the QES, the QSiegel is
responsible for securing the application level.

Qualified Website Authentication Certificate (QWAC)
A QWAC (qualified website authentication certificate) is the digital ID for a website or cloud
application. On the basis of QWACs, website operators can be securely identified. This
technology is based on SSL/TLS encryption and is used worldwide. However, in contrast
to "pure" SSL/TLS encryption, where the browser or operating system manufacturers
determine the trustworthiness of the underlying certificates, the trustworthiness is
determined by the EU Trust List. This is particularly important in order to be able to
establish trustworthy, authenticated and encrypted communication relationships, for
example between EU citizens and websites or between IT systems. QWACs can be
used not only on the server side, but also on the client side. This means that a server can
also identify itself to another server as a client. A QWAC is responsible for securing the
transport layer.

Qualified preservation service for QES and QSiegel
Once a QES or Q seal has been generated, it is permanently valid. The verifiability can be
severely limited over the years, as the trustworthiness of the underlying cryptographic
algorithm still depends on technical developments. Therefore, the qualified preservation
service preserves the state of the qualified signed and/or qualified sealed file.
Qualified validation service for QES, QSiegel and qualified preservation services These
services are focused on QES and QSiegel. They enable the independent verification of the
mathematical and legal validity of a QES or a QSiegel. As a result, a special test report is
issued which lists the test steps and results. This test report can be embedded in the
document, if this is technically supported, and thus enables the traceability of the
independent test result over a long period of time.

Qualified service for the delivery of electronic registered mail
The service for the delivery of electronic registered mail brings the postal registered mail
service into the electronic world. Both the sender and the recipient are identified and
the message is protected from unnoticed manipulation by at least one advanced
electronic signature. The date and time of sending, receiving or changing the message is
protected by means of a qualified time stamp. This service is already known in a comparable
form through the De-Mail Act.

Qualified electronic time stamp
The functioning of a qualified electronic time stamp is comparable to the QES. The time stamp preserves the time at which the electronic file was submitted. In this way, it is clearly traceable when the electronic file was available and in what state. No qualified certificate is used here.

The tools of the digital trust space

QES
The individual digital signature

Registered and delivery service
The secure digital message as with the post office or the bailiff

QSiegel
The reliable digital stamp for authorities and companies

Timestamp
The digital stopwatch like electronic photo evidence

QWAC
The secure identification of a website operator

Preservation services
The digital eternal archive

Validation service
The automatic independent auditor

2.2

The Trust Services Act
The Trust Services Act (VDG) is part of the eIDAS Implementation Act.17 At the same time, it repealed the SigG on 29 July 2017. The VDG creates the uniform legal framework for the areas regulated by the SigG and supplements them with the new regulatory areas created by the eIDAS Regulation. In this way, it fills in the areas left open by the directly applicable eIDAS Regulation in German law. In February 2019, the Trust Services Ordinance (VDV) also came into force. In the VDV, requirements for accessibility, the design of the coverage provision of qualified trust service providers, the documentation when issuing certificates, the permanent verifiability of certificates and the display of QES or QSiegel creation units are specified.18

2.3

Formal requirements under German law
Under current German law, many contracts are possible without any form. Only certain contracts require a special form, such as text form, written form, notarised form or the form of closure before a special public body. Against this background, formal requirements define the conditions under which a declaration has legal effect. The system of formal requirements dates back to 1896 and must be changed for the digital world. This is because complex machines or software were not thought of at that

time. In a few years, however, every contract and every legally relevant procedural act in civil or public law will be completed digitally. A trust anchor is needed for the connection between analogue action and digital accumulation. For certain legally relevant acts, it must be certain who said what, when and to whom digitally.

German law has various formal requirements for different legal transactions. In principle, however, there is no prescribed form for contracts and other legal transactions. Therefore, contracts can be concluded in any form. A contract is entered into when two expressed and concurring declarations of intent are made and received by two natural persons. In the case of mutual contracts, this occurs through the offer and acceptance of an offer. Therefore, in principle, contracts can also be concluded by e-mail, messenger or video telephony. Unilateral legal transactions are made known by the accumulation of wills with the respective legal intention and must also be received in order to have the respective effect (e.g. revocation, termination, withdrawal).

Special forms should be provided for certain legal transactions. This is because particularly important legal transactions must be more reliable than other contracts. The legal system also has a special interest in this. For example, an employment contract is concluded in writing because it is an important basis for an employee and also has social significance.

Over the years, the respective formal requirements have been adapted again and again. They are intended to fulfil a specific function that is necessary for the respective legal transaction or the respective protective purpose of the norm. These include the information function, clarification and evidence function, control function, warning function and advisory function.19

The different functions of contracts

An example: The warning function is used to draw attention to the consequences of an onerous legal transaction. This is increasingly done today through the use of the legal institutions of rights of withdrawal and information duties for consumers.20 This is because legal reality shows that the small print requires such a high level of attention and in-depth specialised knowledge that it simply overwhelms most people.

Most recently, in addition to the written form - i.e. a declaration with a handwritten signature in ink on paper - the text form was introduced in order to be able to conclude contracts by e-mail, for example, if the informal obligation is not sufficient or there is a special need for information. Around 1900, when the German Civil Code (BGB) was introduced, written form was the most convenient way to conclude significant

contracts.
Until the mid-1950s, contracts were still written by hand and signed by the obligee
himself. Later, contracts were mainly prepared by typewriters. Today, this is done digitally.
Nevertheless, the written form retains its essential function in the law of formal
requirements. At the beginning of the 21st century, the QES was largely equated with the
written form.

These formal requirements also apply to legal persons - such as companies. Legal persons are legal entities that are treated like natural persons under civil law. They are
abstract and therefore cannot incur any criminal liability of their own or bind themselves,
for example, by a marriage contract. Nevertheless, these legal entities must be able to act
and do so through their human, legal representatives. These must sign by hand or by
qualified electronic signature in order to comply with the written form.

Lack of anchoring in German law

With the eIDAS Regulation, the Q seal has now been introduced for these legal entities. A Q
seal can only be used by a legal entity or a public body and has a strong evidentiary function.
However, this means is not found in German law with regard to formal requirements.
Here, the "legal diversions" that a natural legal representative, such as an employee,
must sign for a legal person (i.e. his company) still applies. It would therefore make
sense to legally integrate the QSiegel into electronic business transactions. The aim of a
regulation must be that a company can rely on the legal effect and the recipient on the
origin of the Q seal. In addition to the legal effect of the Q seal, this also requires formal
requirements in national law that make this form binding for businesses.

This does not mean that the Q seal is equivalent in content to the written form of a
declaration of intent. This is not intended in accordance with the eIDAS Regulation.
Rather, the goal must be to enable companies to use a new, electronic and binding form.

Negative and positive publicity means that the entries in the commercial register may be assumed to be correct and complete, even if they do not correspond to the actual circumstances. This is regulated in Â§ 15 of the Commercial Code.

In legal transactions, the counterparty can only rely on the fictitious truth from the commercial register (negative and positive publicity). The representative indicated there is authorised to sign. A verification for legal transactions, which is to be protected by formal requirements, is therefore only possible via this control diversions. With the Q seal, on the other hand, this is no longer necessary, because the verification of the authenticity of the Q seal is

electronically automated by the system of trust services happens.
The actual legal representative therefore does not have
to act himself every time, but can delegate.

In companies, it is possible for the legal representatives to issue powers of attorney and
thus also allow other persons to sign with legal effect. This is also possible with the Q
seal. However, the legal circle enjoys more protection of confidence with the Q seal
because the origin of the declaration can be assumed as legally presumed.21 This is not
the case with a letterhead or an e-mail.

Another form requirement is the electronic text form. It was adopted into German law by
the European Consumer Protection Directive (Directive 2011/83/EU) in 2014 with the new
version of Section 126b of the German Civil Code (BGB). There it is regulated that the
text form is also complied with if the recipient of the declaration made in text form can
recognise the sender and permanently store the declaration. This is also assumed for email messages.
This is still unclear for messenger services such as Skype, WhatsApp,
Snapchat, Facebook or Instagram.

The situation is different with De-Mail: It does not replace the written form, as is the case
with the QES pursuant to Art.
Â§ 126a of the German Civil Code (BGB), but can nevertheless be used equivalently for
communication between citizens and the state within the framework of the
EGovernment Act (EGovG). The reason for this is that with the De-Mail standard, in
principle only the service provider applies the QES in its own name to sign the message
transactions. If documents are to be processed electronically, the written form in private
law can be replaced by electronic form (Â§ 126 para. 3 BGB). Correspondingly, in the area of
administrative procedural law, according to section 3a, paragraph 2, sentences 1 and 2 of
the Administrative Procedure Act (VwVfG), the written form can be replaced by
electronic form "unless otherwise provided by law. Electronic form is satisfied by an
electronic document bearing a qualified electronic signature." To replace the written form,
the user would have to do this himself with his own signature. The written form
requirement applies, for example, to building applications, building permits, tax
assessments, objections to administrative acts pursuant to section 70 VwGO
(Administrative Court Code) or applications in formal administrative proceedings pursuant
to section 64 VwVfG. Comparable regulations can be found in the General Part of the
Social Code (SGB I) and in the Fiscal Code (AO). According to Â§ 36a SGB I and Â§ 87a AO,
the handwritten signature can also be replaced by the QES in these areas.

2.4

Rules of evidence under German law
Rules of form and rules of evidence are two sides of the same coin. The rules of

form
deal with the creation of legal effects, the rules of evidence with the probative value of the
means used. The advantage of an effective contract is that the rights and obligations can be
enforced before a court. Formal and evidentiary rules intertwine and create a space of trust
in which legally relevant action can take place safely for the parties involved. Without this
space of trust in law, no economic development is possible. Against this background, this
section deals with the treatment of the trust services of the eIDAS Regulation in the
evidence procedure. The eIDAS Regulation provides that certain trust services are to be
given legal effect.

and admissibility as evidence in court proceedings may not be denied solely because they
are in electronic form or because they do not meet the requirements for the respective
qualified electronic trust service. They are thus in principle evidence in court proceedings.
This applies, for example, to QES, QSiegel, qualified electronic time stamps and qualified
electronic registered mail services.

The most secure means of evidence in German procedural law is documentary evidence by
means of a public or private deed.22 The content of the deed declaration is deemed to have
been made by the issuer (formal and material probative force) and restricts the judge's free
assessment of evidence pursuant to section 286 of the Code of Civil Procedure (ZPO).23
However, this only applies to physical, hand-signed documents. For electronic documents,
even the qualified electronic certificate of a qualified trust service for an electronic
signature pursuant to section 371a ZPO only effects the prima facie evidence for private
electronic documents or the statutory presumption for public electronic documents
pursuant to sections 371a (3), 437 ZPO.24 Nevertheless, the provisions on the probative
value of documents pursuant to section 371a (1) sentence 1 and (3) sentence 1 of the Code
of Civil Procedure are applied accordingly to electronic documents signed in this way.

The evidential value for the tools of the eIDAS Regulation is not regulated in German law (with the exception of QES, because it was already provided for in the SigG). The VDG has not made any changes here either. Contrary to its wording in the German translation, the eIDAS Regulation itself is not intended to create a legal "presumption" for the evidential value of the Q seal, but also to mean prima facie evidence of the integrity of the data and the correctness of the indication of the origin of the data.25 The eIDAS Regulation applies directly in German procedural law, as it would itself require treatment as prima facie evidence according to the German system. This means that the person contesting an electronic document would have to present facts that

make an atypical course of events appear probable.
These connecting facts must then be proven.

Irrespective of its lack of dogmatic derivation, the prima facie evidence is customary.
The principle of causation is legally recognised in German law and is indispensable in court
practice. According to case law, it permits proof of a causal connection or culpable
conduct in the case of typical sequences of events without an exact factual basis, but
on the basis of empirical principles. 26

This leads to the situation that electronic documents bearing the technically permissible Q seal of a company or another legal entity such as an association (for
example, donation receipts) are prima facie evidence of the existence of a legal entity.

Art. 35 eIDAS Regulation Legal effect of electronic seals

(1) An electronic seal may not be denied legal
effect and admissibility as evidence in legal
proceedings solely because it is in an
electronic form or does not meet the
requirements of qualified
electronic seal fulfilled.

(2) A qualified electronic seal is subject to the
presumption of the integrity of the data and
the accuracy of the indication of origin of the
data to which the qualified electronic seal is
linked.

The issuer is entitled to claim for the integrity and correctness of the indication of the
origin of the data. In addition, however, the rules of evidence for private documents do
not apply here because this requires a handwritten (or signed) signature of the issuer.
The Q seal does not offer this because no individualisation of the declarant is permitted.27

On the other hand, under section 371a (3) in conjunction with sections 415 and 437 of
the Code of Civil Procedure, the Q seal on electronic documents from public authorities
creates a presumption of authenticity of the deed or electronic document if it also has
the appearance of a public deed. This is because section 371a (3) of the Code of Civil
Procedure is not limited to the deed, which must show the individualised issuer, but
refers to all public electronic documents and is correspondingly broader. From this
perspective of the law of evidence, the Q seal is therefore already fully usable for public
authorities.

Â§ 371a para. 3 ZPO
The evidential value of electronic documents

Electronic documents that are stored by a public authority within the limits of its official powers or by a person with public trust within the scope of

business assigned to him or her in
If the document has been created in the prescribed form (public electronic documents), the provisions on the probative force of public documents shall apply mutatis mutandis. If the document has been provided with a qualified electronic signature by the public authority that created it or by the person having public trust, the following shall apply Â§ 437 accordingly.

3 REGULATORY GAPS IN GERMAN LAW

The European legal framework outlined in chapter two provides a uniform set of rules
for the use of trust services in the European Digital Single Market. This makes it possible
to map complex digital applications with corresponding services in a legally secure
manner and to use a secure digital infrastructure.

However, there are numerous regulatory gaps for successful digitisation. This is not
surprising given the historical background of the legal system of declarations of intent
and rules of evidence. Therefore, the corresponding gaps should be identified and the
means for secure digital communication in the European single market should be enshrined in law. The eIDAS Regulation has been created to make this possible in a
uniform manner throughout Europe.

Just as the euro is the European currency, the new eIDAS tools
could be used EU-wide for all legal administrative and business
processes - and thus speak the same digital language.

For example, the use of QWACs allows a website to communicate securely. However, this
has not yet been included in the Telemedia Act (TMG), which was amended by the IT
Security Act and requires encryption of website communication as the current state of
the art. Here, websites whose communication is in the public interest should additionally
be required to use QWACs so that the user can safely identify the operator of a website.
Websites are thus always secured according to the current state of the art, because the
technical security of the certificates can always adapt to it. Finally, the cryptoalgorithms
of the certificates can be further developed and improved.

Both the formal requirements and the evidentiary requirements allow private and public bodies to use the QSiegel without restriction. This is advantageous, because in
official cooperation or in communication between courts and authorities, it is often decisive
that the competent authority seals and not the employee signs. The indication of origin can
only be proven by the Q seal and not by the issuer or an attribute in the certificate that
existed at the time of issue. Thus, the QSiegel complements the QES in a meaningful way to
ensure the origin and authenticity of a digital declaration, depending on the intended use.

Why the QSiegel should be included in the ZPO

However, it seems to contradict the eIDAS Regulation that the QSiegel has not been included in the BGB or the ZPO, leaving it up to the legal practitioner to interpret the European implications. This situation of ambiguity about the procedural effects of the Q seal is particularly unsatisfactory because prima facie evidence is also not legally defined and the specific reference to the Q seal is not explicitly regulated in German procedural law.

The legal concept of prima facie evidence is intended to facilitate the presentation of evidence of causality and fault in the case of a typical course of events that corresponds to life experience. However, there are neither special empirical values on the Q seal nor can the legal practitioner find its instrument of digital communication in the legal text on rules of evidence. Against this background, it makes sense to include the Q seal in the Code of Civil Procedure and to anchor it in section 371a.

The machine moves close to the right

In the century before last, the system of declarations of intent and the rules of evidence for legal transactions based on them assumed that only human beings could act in a legally relevant way. Machines were naturally not seen as agents in the legal sense.

Today, however, the digital transformation means that more and more machines and software are carrying out the economic exchange of goods and services as well as administrative activities.

Accordingly, the idea that every legally relevant act must be attributed to a person is now considered outdated. This notion is followed if it continues to be assumed that the Q seal can have no or less probative value because it cannot be directly attributed to a person.28

In fact, it is not necessary to be reliably assigned to a certain person, the assignment to a legal person is sufficient. In civil law, attribution always refers to liability for a legally relevant act. However, liability affects not only natural persons, but also legal persons. And in legal reality, the recipient of the declaration of intent or legally relevant act always wants something from the person acting (for example, to enforce a claim such as liability for damages). The formal requirements cover precisely this interest through the warning function, evidentiary function, etc.

The Q seal user is the person against whom a claim is made, the debtor, in the situations that are relevant to the proceedings. Since only a legal person can stand behind the Q seal, the claim is directed against a legal person. Only if the legal person wants to

exculpate itself,
i.e. exonerate itself from liability, must it prove that the person acting was not actually
authorised to act on behalf of the legal person and that there was no prima facie power of
attorney. The Q seal therefore offers more legal certainty for legal transactions, because this
exculpation is more difficult for a legal person in the relationship between the parties. The
consumer or the other party either uses a QES and is therefore identifiable as a creditor or
also uses the QSiegel and is a claimant as a creditor anyway, who can use the fiction of the
QES for himself.

Â§ Section 184 (1) of the German Civil Code (BGB). Accordingly, subsequently authorised
legal transactions have retroactive effect to the time when the legal transaction was
carried out and the lack of power of representation is no longer a problem.

This is easy to understand with an example: A company uses a Q seal to conclude a
contract on its own side or to fulfil information obligations towards the customer. In a
legally disturbed legal relationship, the customer or other party can claim that the Q seal
is from the company and that the company is liable from the legal relationship (for
example, if the customer wants to have the loan proceeds paid out or the information
obligations were not fulfilled and therefore wants to revoke the contract later). In civil
proceedings about this, each party must now prove the facts that are favourable to
them, unless a rule on the burden of proof outlined above applies that determines
otherwise, such as a reversal of the burden of proof, a presumption or prima facie
evidence. The use of the Q seal leads to at least prima facie evidence of the origin of
the declaration from the company. The company cannot simply claim that the Q seal was
not used by it, but by an unauthorised third party (as in the case of a QES). The customer
can claim prima facie evidence for the fact that the declaration came from the company
and does not have to prove it with a document, a witness, an expert opinion or by
inspection. The company now has to explain how it could have happened otherwise and
prove the relevant connecting facts by means of the special rule of evidence of prima facie
evidence. It must therefore explain how the Q seal could be used by an unauthorised
person and prove that this could also work in the abstract. It is conceivable, for example,
that the former employee could take the seal data with him and trigger a Q seal for the
company. The company must then prove that remote sealing with two-factor
authentication with the company data is possible at all (whereby liability for negligence
in handling the Q seal data would also be conceivable here). This proof will be very

difficult because the security requirements for the use of the QSiegel are very high. It
therefore leads to a similar dilemma of proof as the current signature solution or the proxy
regime for paper-based communication. The only difference is that the burden of proof
rules are interpreted here in favour of the recipient of the declaration. The interest in
proof is thus better distributed. In the case of former employees, the company must
prove that it was possible to use stationery or templates after the end of the
employment relationship. If the company has not established a prima facie case, i.e. the
person did not work for the company, the protective effect of the prima facie case is lost
and the claimant must prove that the declaration came from the company.

Use of the QES:
In case of doubt, the recipient must prove that the QES
holder was employed by the company.

Use of the Q seal:
In case of doubt, it must be proven to the user that the Q seal has been
lost by the company.

The evidentiary interests of the QES and the QSiegel

If one compares this with the QES of the declaration, one comes to a less
purposeful result. Here, the legal presumption applies that the declaration originates from
the person stated in it. However, in the example, the customer must prove that the person
making the declaration was authorised to represent the company or that the company
allowed this person to act on its behalf for a long time and thus made a legal appearance.
This is an unfair result.

Every legal person or public authority can also log the use of the QSiegel data itself in such
a way that it can trace who sealed which declaration and when. This is also accessible to
evidence. If these possibilities are not used, for example for cost reasons, this is the
responsibility of the seal creator. Under German law, no one is forced to secure
evidence themselves if they do not wish to do so. The decision to bear the risk in legal
proceedings must be made economically and can also be accepted depending on the
amount of damage. A company does not have to log transactions worth a few euros if it is
clear that the evidence will never be needed in proceedings.

Another circumstance arises for the public authorities. Here, liability for sovereign acts of
the individual civil servant for the citizen is largely excluded. Article 34 sentence 1 GG does
not provide for individual liability for state liability anyway. Here, therefore, there is no
interest for the recipient of the declaration to know the certain identity of the individual
declaring, but to attribute the origin of the declaration to the state. The Q seal provides this
secure legal assignment. The previous QES, on the other hand, only refers to the acting

person.

As a result, the Q seal, because it forces compliance with certain technical procedures,
represents a higher level of security and better protects the legal circle because the
person who has an interest in the determinable origin of a declaration is better protected
by prima facie evidence. All constructions of the chain of authority of legal persons
ultimately serve this protection of legal transactions (publicity of the commercial
register, sub-authorisation in the company and the prima facie power of attorney). Through
the trust services of the eIDAS Regulation, this diversions is no longer necessary for the
first time. They make it possible to automatically store the origin in the QSiegel, query it,
check it and use it in the process.

As a result, it can be stated that whenever an act of legal persons is performed digitally,
there is a regulatory gap because a link from the physical act to digital accumulation is
only legally regulated for natural persons with the QES. However, the QSiegel offers the
possibility to close this gap by law.

4

CURRENT NEED FOR ACTION AND REGULATION

The existing regulations should be expanded where certain eIDAS tools have not been implemented and where only the gap between the old SigG and the new European Single Market needs to be closed. New laws should be created where digital
processes have not yet been considered. In addition, a new understanding of formal
requirements is needed if all contracts and legal relationships have a digital component.
The Federal Republic promised this in the Tallinn Declaration on eGovernment 2017 for
the eIDAS tools and should be implemented with the following measures.

Ministerial Declaration on eGovernment - the Tallinn Declaration

(...) The Member States reaffirmed their commitment to progress in linking up their public eServices and implement the eIDAS regulation and the once-only principle in order to provide efficient and secure digital public services that will make citizens and businesses lives easier.

4.1

The trust function in electronic legal transactions

If consumers are overwhelmed by excessively long contract texts and licence conditions
and sign them without reading them, the written form can no longer adequately fulfil its
warning function. Especially in digital business processes, a new type of warning
function would make sense. This could look like this: companies could provide their
contract template with a Q-seal and the consumer would have to sign it with his

or her
own electronic signature. In this way, the consumer can directly check whether the
contract or the information sheet really comes from the issuing company. By signing
their own signature (even if it is only the remote signature with PIN and smartphone),
the consumer can see that their own actions are legally relevant.
In addition, a stronger link should be established between digital action and the actual
effects in the physical world. This is because legal spaces extend to new levels of action. In
order to enable a legally secure connection of the levels, the identities must be translated
from the physical level into the digital level. This bridge from the digital to the physical
world should create the necessary trust in the origin of the action. This is a function that
is not present in the canon of functions of formality. It is true that there were so-called
transactions between absentees, which were made possible by the written form, for
example, over great distances. But they always remained on the physical plane. The
recipient could always identify the signatory by the writing or the print on the paper.
There was therefore a physical link between declaration and form. In contrast, there is
no longer a physical connection between the keystroke and the written character
representation or the speech spoken into an app and the digital text output in the
dictation function. Data can be changed and lose any reference to the origin.

The trust function

The bridge from the digital to the physical world can now be created by the trust
services of the eIDAS Regulation. This bridge is the trust function, which is to be
established as a new element in German law. This is a new function for formal
requirements of legal transactions. Unlike the identity, authenticity and verification
function within the already recognised clarification and proof function, the trust
function is added for the connection of the physical and the digital when it comes to
identifying the originator and verifying whether the declaration is genuine. It thus
creates trust in the origin of an act.

Where do we need to be sure that everyone involved is who they say they are?

The legislature must ask itself which legal transactions and which eGovernment processes
are based on particular trust and therefore require protection through the trust function.
The identified processes must be secured by appropriate means. The trust services of the
eIDAS Regulation are suitable for all processes involving European member states or EU
foreigners.

Other methods could also be chosen for purely German situations. However, this

would
lead to double standards with significantly increased costs. The decisive advantage of
interoperability with uniform standards throughout Europe would be given up and the use
of existing systems could not be dynamically expanded.

Three characteristics form the basis for the new trust function:

1. The trust function must always be present when it comes to digital business or
administrative processes that have a lasting impact in the physical world.

2. The trust function must always be given when it comes to the traceability of the
identity of the parties involved.

3. The trust function must always be given if an increased level of security is to be
guaranteed. Security describes the protection goals of availability, integrity and
confidentiality of the business or administrative process.

The characteristics of the digital trust function

Example "digital reporting process

An illustrative example of the digital trust function would again be the re-registration of
residence according to the registration laws in Berlin.
The digital re-registration has effects in the physical world in that there is a new
residential address to which, for example, documents such as election papers, tax
notices or administrative acts are sent. In addition, the re-registration is carried out by a
real person, the real landlord confirms the residential use and the real authority issues
a registration confirmation. The identity of the parties involved must therefore be
verifiable. Furthermore, it is important that the communication is secured, as personal data
is transmitted. Unauthorised intervention by auften also carries the risk that a registration
certificate could be fraudulently obtained. It is also essential for the authority that the
documents attached by the citizen do not contain any malware. The process itself must be
archived for a long time in order to remain traceable. There is therefore an increased
need for security in the communication process.

This would be different, for example, with the online reservation of a theatre ticket. If
you don't show up on time, the reservation expires and the seat is given to someone else.
The process has no effect in the physical world and the identity of the visitor is not relevant
to the theatre either. No personal data is stored or files exchanged that need to be
auditable for a long time.

Back to the re-registration example. The trust space for the digital registration process

would look like this: The citizen submits his application and signs it with a forgery-proof
QES. Communication via the internet would be secured with QWACs. The landlord could
provide the confirmation with the QES or, in the case of housing associations, with the
QSiegel. The authority would process the registration process automatically and provide the registration certificate with its QSiegel. The registration certificate could be
securely delivered via De-Mail or other electronic registration and delivery services.
Alternatively, citizens could download it from a website secured with a QWAC using their
QES. Authorised third parties could also trigger these processes with their own signatures. These third parties could also be located in other EU countries, since the
eIDAS trust infrastructure functions uniformly throughout Europe.

Such a room of trust would also be conceivable in other cases. For example, prisons could
re-register inmates or refugee shelters or care facilities could register residents. A
notification and placement system for free kindergarten places would also be conceivable.

4.2

Examples of regulatory gaps in the use of trust services

The trust function results in enormous savings potential. The above-mentioned example of re-registration already shows how a digital process saves public resources,
creates trust in one's own actions and is extremely efficient. The authorities are relieved
and citizens can register their homes promptly. The savings potential also applies to the
economy in particular. After all, businesses have to come into contact with authorities
much more often than citizens. Thus, a digital administration can make a major contribution to improving the competitiveness of German companies. To do this, the
administration must offer its most important services digitally. This process is currently
underway: according to the Online Access Act (OZG), 575 administrative services must be offered online by 2022.

As a general rule, it should be noted: Individual solutions, such as the special electronic
lawyer's mailbox, are not worthwhile. Different standards, closed user systems and limited
use cases do not lead to expandable solutions and save effort. In the case of the lawyer's
mailbox, for example, not only lawyers and courts are possible communication partners,
but also professional parties to proceedings such as authorities, notaries, bailiffs, tax
advisors, experts, guardians ad litem, youth welfare offices and professional guardians,
witnesses or employers. In addition, there needs to be a
cross-border communication. Such communication should therefore include all groups and
enable a media-free interface to all participants.

4.2.1

Digital communication in the justice system

If courts and authorities were to introduce the QSiegel in their electronic legal transactions, this would result in significant financial and personnel relief. Cases could be processed and concluded more quickly.

The physical service of certified electronic transcripts alone can take two to three weeks.
If they were served digitally, paper, printer ink, labour time and time in court proceedings
could be saved. The QSiegel can be built into the delivery process in such a way that only
authorised persons can access it. For example, this could be triggered by remote sealing in a central cloud service. This way, court staff can deliver the documents within a
few seconds. At the courts for civil and family matters in North Rhine-Westphalia, there
were 3,103,752 service of documents in the course of proceedings in 2015 (eight service
per proceeding conducted by lawyers). If these figures are taken as a basis, this would
result in 646 saved working days of eight hours each in the service area alone with
automated electronic sealing.29

Another advantage of the QSiegel over the QES is that the QSiegel can be assigned to a
court in a legally secure manner. And this is without the recipient having to trace whether
the person who issued the signature actually works at that court and had jurisdiction. In
the European context, court decisions can also be served in a legally secure manner
and decisions under the Convention on Jurisdiction and the Enforcement of Judgments
in Civil and Commercial Matters can be carried out more straightforwardly.

The QSiegel can be used in a variety of ways. It can be used where the legal written
form is not required. It is ideal to use it when it is crucial that the creator can be assigned
to an organisation or authority. This is in line with the legal idea of section 169 (3) of the
Code of Civil Procedure, which permits machine certification. It cannot be used if there
is a personal signature requirement, such as when a judge signs judgments and orders.30

In 2018, the special electronic lawyer's mailbox was introduced for lawyers to communicate with each other or with courts. However, this isolated solution has disadvantages for future-proof communication: third parties and interfaces to the outside
cannot be integrated. As soon as messages, documents or files have to be transferred
from one system to another (intersectoral communication), the advantages of the closed
system, and thus in particular authenticity and integrity, are lost. As shown above, there
is a whole range of possible emp-

The documents in question may include professional parties to the proceedings,

authorities,
notaries, professional advisors, witnesses, employers or the client.

In judicial communication, the three characteristics for the trust function are present:
1. The physical impact refers to actual procedural actions.
2. The identity of the recipients and senders is essential to ensure professional
confidentiality.
3. An increased level of security must be guaranteed. The documents must be tamper-proof.

It would make sense - as described in the example of the notification process - to enable the
tools of the eIDAS Regulation for the communication of all parties involved. These include
the QES or a Q seal for authorities and legal entities. Websites with QWACs or electronic
registration and delivery services (e.g. De-Mail) could be used as communication infrastructure.

To this end, the respective laws (BRAO, GVG, BOStB, VwVfG, VwGO) must be amended accordingly. It would have to be stated that the obligation to professional secrecy is
satisfied if state-of-the-art encryption technologies are used. In addition, it would have to
be stipulated that the digital disclosure of confidential information is only permissible if
all parties involved can be reliably identified. The identification of the parties involved is
ensured if QES, QSiegel, the online ID function of the electronic ID card or De-Mail are
used.

4.2.2

Digital communication in the authority

With Q seals, significantly more official notices can be sent out. Especially in mass procedures such as tax or pension notices, there is a huge savings potential.

Authorities use the following text module for many letters sent conventionally by post:
"This letter was produced by machine and is therefore valid without a signature". This
results from Â§ 37 para. 5 sentence 1 VwVfG, which defines the written, oral or electronic
form for administrative acts and thus makes the reproduction of names and signatures in an
automated procedure dispensable. Against this background, with a QSiegel, many more
official notices can be sent digitally than before, because paper, costs and above all time are
saved. In the case of administrative acts, it is essential that the issuing authority can be
identified (Â§ 44 para. 2 no. 1 VwVfG). Curiously, this text module may be used for letters on
easily forged recycled paper - but not for the much more secure electronically sealed documents.

The E-Government Act (EGovG) came into force on 1 August 2013 and is intended to promote the dissemination of electronic administrative services. Previously, a major

obstacle to e-government offerings by the public administration was that only the QES was permitted as the electronic equivalent of the written form and that this was not sufficiently widespread. With the EGovG, therefore, in addition to the QES, De-Mail and the online ID function (eID function), for example of the electronic identity card, were approved as further secure technologies to electronically replace the written form in administrative procedures. In addition, a statutory order authorising the Federal Government, with the consent of the Bundesrat, allows for rapid adaptation to technological developments throughout Germany and Europe (section 3a (2) sentence 4 no. 4 VwVfG). The statutory order can be used to establish further sufficiently secure procedures as a substitute for written form.

The QSiegel must also be anchored at this point. It technically fulfils the same security level as the QES. In addition, the personal signature of the legal representative is not necessarily required for administrative procedures. It can be granted by means of a power of attorney. The QSiegel assumes this power of attorney in accordance with Â§Â§ 164 para. 1 sentence 2, 167 para. 1 2nd alt. BGB or according to the principles of prima facie power of attorney in connection with Art. 35 eIDAS Regulation. This is because a declaration made to the third party according to the circumstances must be accepted by the represented party - in this case the seal user. This is comparable to a company giving stationery and company stamps into the hands of its employees. The company must also accept a declaration made in this way. However, the Q seal offers a much higher level of security than a company stamp, which can be quickly stolen. Incidentally, the authentication methods mentioned above only apply to natural persons. Legal entities cannot use the online ID function, QES or De-Mail for legally secure identification. Companies or even associations require a reliable authentication method with the QSiegel. Therefore, it must be enshrined - by law or in the legal ordinance of the Federal Government according to Â§ 3a para. 2 sentence 4 no. 4 VwVfG - that the Q seal sufficiently identifies legal persons and that authorities can use it.

Public administrations can already use remote signature for all processes where the applicant's signature is required by law. This includes, for example, applications for subsidies, building permits, waste permits and documentation for the acquisition of certificates in emissions trading.31

Q seals not only ensure the origin but also the integrity of electronic data - an important feature of official certifications. That is why they can be used to deliver documents of all kinds (birth, marriage and death certificates) and testimonials electronically. They are also suitable for legally effective public announcements on the internet, which must

be
protected against deletion and falsification. In addition, the eIDAS Implementation Act
explicitly provides that Q seals are permitted in public administration award procedures
alongside the QES.32

4.2.3

Digital communication in the health sector

eIDAS trust services enable negotiable documents for
intersectoral communication in the health sector. The use of trust
services saves bureaucratic effort and ensures efficient and
secure handling of information about treatments and patients.
This can improve patient care enormously.

The healthcare sector has a particularly high potential for making work easier through
digital processes. The bureaucratic documentation effort can be automated as far as
possible and information about treatments and patients can be used more efficiently.
These processes must be designed to be legally secure and technically flawless. The trust
services of the eIDAS Regulation make this possible throughout Europe.

The Q seal could, for example, be usefully applied to the discharge letter. This is
because the hospital, rather than the doctor, is necessarily liable in the case of
hospitalisation. This also applies to specialists, laboratories and medical care centres:
laboratory reports and specialist examination results could be automatically marked with
the Q seal instead of with a doctor's signature, as is currently the case. This must be
anchored in law. The current solution with a local signature card is too complicated for
many hospitals. However, discharge letters must be able to be issued on any device by the
responsible doctor and then sent by mobile phone.

Care services have considerable documentation obligations in order to be able to invoice
their services. The documentation could be done digitally on mobile devices and sealed
automatically - as long as no personal signature or QES is required. This would be much
faster and the nursing staff would have more time for patient care. Therefore, the legal
prerequisite would have to be created that all documents that require a qualified proof of
the sending institution and were previously sent by paper could also be made available
electronically with QSiegel.

An automated electronic sealing procedure is always suitable where it is important to
document the process and not the personal responsibility. This could possibly include
notifications for outpatient care services as well as notifications to and from chambers,
associations of panel doctors and payers. In order for the QSiegel to be used

interoperably,
asynchronous electronic communication based on the specifications for electronic registration and delivery services must also be anchored in law. With so-called certified
gateways, these services can be used in and out of a secure network. This enables secure
communication, for example with patients, carers or lawyers.

One trend is that communication in networks, such as specialised applications from doctors,
the medical service or laboratories, is automated. Then it is no longer the human being
who triggers the exchange of information, but the laboratory system can contact the
doctor's patient information system directly and transmit necessary patient data. This
type of communication should be secured by QWACs. This way, authorised persons can
communicate with each other confidentially. For this purpose, the respective IT systems
use unique identities to identify themselves. All communication partners can bindingly
check with whom they are ultimately communicating. Unauthorised persons cannot establish
communication. The technology used is not proprietary, but can be obtained throughout
Europe from any trust service provider.

4.2.4

Certificates and attestations

Documents such as management, training or work certificates as
well as diplomas and master craftsman's certificates become
forgery-proof through the eIDAS trust services. This increases
trust in the digital world.

Fake certificates are often submitted with job applications. There are even portals where
you can order a certificate of your choice for a fee.33 Because the certificate provides proof
that can, for example, help to get a job, there is an immediate connection between
the analogue and the digital world. Companies or other organisations to which a certificate
is presented want to be sure that the identity of the certificate issuer and recipient is
genuine and that the certificate has not been forged. The eIDAS trust services can be
used very usefully for this purpose.

The regulatory content is as follows: Digital certificates and attestations used in legal
transactions must make the issuer identifiable with sufficient security. This security can be
ensured by ensuring that the services are always state of the art. The security requirements can be guaranteed by the QES of the signatory or the Q seal of the issuing
legal entity. The eIDAS trust infrastructure would make it possible to check automatically
throughout Europe whether the certificate is genuine. There would be no need for the
issuer to conduct its own authenticity searches.34 This regulatory content can be

anchored either in a central place or in all corresponding standards for the respective
issuers. The German Civil Code (BGB) and the Administrative Procedure Act (VwVfG) would
be suitable here, as a generally valid regulation can be made for both the civil and public
spheres.

4.2.5

Certification of copies by authorities

The QSiegel can be used for the certification of transcripts by authorities. The electronic process eliminates the need to go to the authorities.

The certification of documents is one of the most sought-after official services. This involves
creating a copy of an already existing official document, for example a certificate or a birth
certificate. However, the document may not simply be copied, but binding proof is required
that the duplicate matches the original. Such official certifications can be made by public
authorities - both for documents they have issued themselves and for documents that
originate from other bodies. In the digital age, such certifications are increasingly requested
in electronic form.

This is a tailor-made application for the QSie- gel. However, it presupposes that the VwVfG and the Social Code also permit this.35 In this regard, Â§ 33 para. 4 no. 4 and para. 5 VwVfG only regulates the use of the QES, but not of Q seals. In this case, the VwVfG requires exactly the same information in addition to the signature that is verified in a QSiegel. In the case of certification by the authority, however, it is more important for legal transactions that the identity of the authority has been verified and not that of the employee whose name the signature contains. The attribute in the authority's certificate no longer has any direct legal effect.

Â§ Section 33 (5) no. 2 VwVfG Authentication of electronic documents: In addition to the information pursuant to subsection 3 sentence 2, the certification note shall contain the name of the official responsible for the certification and the designation of the authority performing the certification in the case of the certification of an electronic document.

4.2.6

Replacing scanning in companies and public authorities

Scanning processes can be greatly simplified with the help of the QSiegel. Even large files can be scanned efficiently and securely.

In the course of the digital transformation, companies and administrations are gradually
transferring their analogue documents into the digital world. This requires a legally
compliant process in which it is comprehensible that the scanned document

replaces the
original or that already scanned documents are given the status of the original. The
scanning process can dramatically save storage and administrative capacity. Public
authorities, companies, hospitals, lawyers, tax advisors and other institutions across
Germany spend enormous costs on renting archive rooms and on staff to manage the
paper archive. Many of the files have to be stored for 30 years or longer. Replacing
scanning is made legally secure by the eIDAS trust services - in conjunction with the
technical guideline for legally secure replacing scanning of the Federal Office for
Information Security (BSI, TR RESISCAN).

For a long time, the idea prevailed that public documents
had to be scanned by hand and signed individually with
the signature card. This is also regulated in Â§ 371b ZPO.
However, only processes that allow the efficient and
automated digitisation of large volumes of files are
future-proof. And without an employee having to enter
his or her signature card and PIN many times in succession.
The QSiegel should be applicable here and this service
should also be permitted by specialised third parties in order
to spare the already burdened judiciary and administration.

The Q seal may generally be used at this point. The BSI
technically attributes to the Q seal the ability to provide the necessary integrity
protection and authenticity. Even if the European priority of application of the eIDAS
Regulation does not apply to a purely German solution, the technical permissibility of using
the QSiegel remains. Although a purely German solution or a closed circle of users may
set their own standards, the Q seal nevertheless always remains a legitimate means of
trust services. So far, there is no German regulation to the contrary. The argument that it
is not possible to draw conclusions about the scanning natural person from the use of
the Q seal does not apply here either.

TR RESISCAN provides for procedural documentation in 4.2.1.36 In the sample
procedure documentation, the service provider or scanner is obliged to name the
respective personnel responsible.37 This always ensures who is responsible for the
process. A QES therefore offers no advantage over the Q seal. On the contrary, the QES
is likely to be even more time-consuming because many signature cards or remote
signature accounts would have to be used here compared to a few seal cards.

The Q seal in TR RESISCAN

The TR RESISCAN mentions the Q seal in A.AM.
IN.H.1: "An advanced electronic signature
(...) or an electronic seal in accordance with Art.
3 No. 25 of Regulation (EU) No. 910/2014 can be
used to ensure not only the integrity but also the
authenticity of the corresponding data objects
(e.g. scan product, transfer note)".

4.2.7

Cloud services and applications

There is a public interest in a secure public digital infrastructure. For example, data centres can be secured or interconnected through the eIDAS trust services.

Currently, there are no legally binding specifications for the use of cloud services.
Accordingly, network services that offer computing power on servers in data centres are
not yet regulated. Nevertheless, the BSI has included various international standards and
their summary in the BSI requirements catalogue Cloud Computing or Cloud Computing
Compliance Controls Catalogue (C5). In order to be allowed to use cloud services,
however, they need to be enabled by regulation: framework conditions and legal bases
are required.

The trust services enable a legally binding and secure trust infrastructure. For example,
the communication channel between the application and the computing centre can be secured by QWACs in accordance with Art. 45 of the eIDAS Regulation. The identity of
the application software itself or the databases as well as the users can be protected by QES
or a QSiegel. With the open-technology trust services - and supplemented by C5 - the data
centre can be secured physically and electronically and the quality of the application can
be increased.

In this way, joint data centres for mass police data analysis could be operated securely.
In recent years, the public has been called upon from time to time - for example after
terrorist attacks - to send in private smartphone pictures and videos of the events to
the authorities. This results in gigantic amounts of data and thousands of hours of image
material that can no longer be analysed promptly by police officers. Automated high
performance computers and special software are needed here, which can be operated
together as a cloud application. These systems must not be infected with malware under
any circumstances and it must be ensured that unauthorised persons cannot access them. Here, trust services can secure access management. For example, QWACs could
enable the unique identification of communication partners and an encrypted connection. With their help, secure networking of different data centres would also be
possible.

4.2.8

Technical monitoring of tachometer readings

With the tools of the eIDAS Regulation and the tacho database, the odometer readings of used cars can be traced throughout Europe
in a court-proof manner for the first time.

The last example on regulatory gaps in trust services deals with the the Germans' "favourite child": the car. In European law, there is an obligation to monitor the speedometer readings of used cars. The speedometer readings are to be entered into a Europe-wide database. This should make the mileage of used cars traceable and combat fraud through manipulation.38 The entries could ideally be secured with the Q seal. To this end, Article 16 of Directive 2014/45/EU of the European Parliament and of the Council of 3 April 2014 must be implemented uniformly across Europe.

4.3 Proposals of necessary amendments to the law

There are numerous examples of how digitalisation in Germany is being delayed by a lack of legal certainty. As shown in this study, there are also some German laws in which the digital dimension has not even been considered. The EU's second Payment Services Directive (PSD2) shows how to do things better with new regulations. Here, digitalisation was taken into account in the legislative process.

The positive example of Payment Services Directive 2 (PSD2)
PSD2 regulates online payment transactions between market participants within the EU. Among other things, PSD2 obliges banks to with business activities in the European Union to grant third-party providers access to customer accounts. In order for the third-party providers to be able to access the bank account automatically, they must identify themselves with one or more certificates. Banks also identify themselves to the accessing payment service providers by means of a certificate. The certificate is considered a "company ID" in electronic business transactions. Article 34 of Delegated Regulation (EU) 2018/389 stipulates that QWACs or Qseals must be used. This secure process enables new business models between companies that originally had no contractual relationship with each other. The inclusion of the eIDAS trust services in the PSD2 thus opens up completely new and secure possibilities for communication.

Basically, new laws are about regulatory enabling and not restrictive regulation. A model for this is the "Better Regulation Toolbox"39 of the European Commission. On 17 pages, the Toolbox#23 provides valuable assistance in regulating digital processes, preventing superfluous regulation and promoting consistency. Consideration also reduces the risk of possible sanctions of EU infringement proceedings due to lack of implementation of the eIDAS Regulation.

There is also the project "Better Lawmaking" of the Federal Ministry of the Interior, for Construction and Home Affairs. This project should be supplemented by an impact assessment of laws for the digital transformation, which recognises the consideration of eIDAS trust services as an important means of digitisation-friendly legislation, as is the case at EU level.

Need for regulation in eleven application examples according to current legislation

4.3.1

Introduction of the trust services

It has become clear so far that a future-proof communications infrastructure must be established on the basis of the European single market regulation. First and foremost, this involves the introduction of the QSiegel and QWACs into German legislation. The e-government laws of the Federation and the LÃ¤nder must be adapted accordingly. To this end, a uniform federal framework must be created, but it must also be implemented in the LÃ¤nder. This will enable authorities, municipalities and other public bodies to use the trust services of the eIDAS Regulation in a legally secure manner.

E-Government Act (EGovG)
The EGovG of the Federation (Â§ Â§ 2, 6, 7) should contain an obligation that the instruments of the eIDAS Regulation must be used. Public authorities should be obliged to accept electronic documents with QSiegel (not only with QES). On top of this, the EGovG of the Federation (Â§ Â§ 6, 7) should also be expanded to include the regulations on electronic records: The QSiegel could function as a suitable technical-organisational measure to safeguard electronic file management and the destruction of paper originals when electronic archives are introduced. Although the TR RESISCAN contains a reference to this, the legal anchoring creates more legal certainty for public users than the outdated reference exclusively to the signature.

German Civil Code (BGB)
The example of digital certificates makes it clear that the BGB must also be adapted. As described in the example, QES and QSiegel would have to be introduced. The regulations could either be added to the general part of the BGB or to the respective specific legal regulations (educational institutions, employment relationships, etc.). Furthermore, it would make sense to introduce a new form requirement for the QSiegel for legal entities.
Similar to how the text form found its way into the BGB with the increasing spread of the computer, the QSiegel should be anchored as a "written form for companies". This would make sense, for example, when issuing electronic certificates.

Administrative Procedure Act (VwVfG)
The implementation of the QSiegel in the VwVfG is not only about a symbolic "accolade", but also to declare the Q seals in individual laws and ordinances as suitable, permissible or perhaps even binding for specific administrative acts.40
40 Cf: Floren, Annette/Entschew,

Certificates and attestations can also occur in public law and be issued by

universities,
authorities and chambers. Here, a regulation with the above content is required, whereby a
Q seal must also be found here.

The QSiegel should be anchored in Â§ 3a VwVfG and supplement the QES. In this way,
costs for signature cards and infrastructure can be saved in the future and at the same
time old signature cards can be used until they expire.

The VwVfG must also be amended so that public authorities accept Q seals from companies. Then companies, associations, foundations and other European legal entities will also be able to communicate securely with the administration electronically.

The draft of the "Act on the Elimination of Waivable Written Form Orders in Federal
Administrative Law" lists 586 federal legal provisions for which the written form can be
waived. They can either be deleted without replacement or replaced by simple electronic procedures.41 The law finally came into force with 464 amendments on 30
March 2017. The Q seal could be used here because the stricter written form is not
required. Nevertheless, an explicit legal clarification is needed to enable the authorities
to use it in a legally secure manner. In this case, the focus is not on the binding nature of
the origin or, in the case of the signature, the declaration of intent, but on integrity
protection (protection against unnoticed modification).

Â§ Section 33 of the Administrative Procedure Act (VwVfG) already stipulates that every
authority must be able to issue electronic documents and electronic certifications of
documents that it has produced itself. These electronic copies and certifications must
also be possible with a Q seal so that the legal community can rely on them and there is
proof that the document originates from this authority.

In Â§ 37 VwVfG, it must be expressly stipulated that the issuing authority must also be
recognisable by a Q seal in the case of an electronic administrative act. This requirement
is fulfilled by the Q seal in contrast to the attribute certificate and should therefore be
mentioned logically.

Code of Civil Procedure (ZPO)
The presentation of the rules of evidence has shown that the Q seal can be used without
restrictions as long as it is not intended to replace the written form. Nevertheless, it is not
mentioned by the ZPO and thus cannot become significant for legal transactions. The
German courts and legal practitioners must also familiarise themselves with the European

because it will be increasingly used in the European digital single market in the future.
Against this background, it seems reasonable to include the Q seal in section

371a of the Code
of Civil Procedure. The content of the regulation could be to treat the Q seal as evidence in
the same way as the QES. Thus, for an electronic message or an electronic document, the
prima facie case of authenticity can only be shaken by facts that give rise to serious doubts
that the message was sent by this legal person with this content. Problems concerning the
power of representation can also be solved in accordance with these provisions and the
principles of representation.

Furthermore, a problem arises with the probative value according to Â§ 371b ZPO. This
provides that a formerly physical public document only becomes an electronic public
document with the presumption of authenticity if the scanning person is identical to the
confirming person and had a public function or is provided with public faith and also affixes
their personal QES. However, large archival collections cannot be digitised efficiently in this
way because the person at the scanner must affix his or her signature to each document.
For efficient and yet secure digitisation processes, the QSiegel must also be possible
here. This bridge between the paper-based and the digital world is what makes future-oriented
action possible in the first place.

In addition, section 169 (4) of the Code of Civil Procedure would have to be amended to
include the use of the Q seal so that the certification and authentication of service of
pleadings can be automated and efficient use can be made of the technological possibilities.

Administrative Court Rules (VwGO)
Just as in the ZPO, the eIDAS trust services must also be anchored in the VwGO and the
other court systems. Only in this way are uniform, interoperable and future-proof IT
solutions possible. Section 55a VwGO already regulates electronic transmission - in
particular the replacement by the QES in the case of the previous written form
requirement. The QSiegel has not yet been taken into account here. However, in addition to
the QES, another secure procedure that ensures the authenticity and integrity of the
transmitted electronic document may be permitted. This should be determined by a new
legal ordinance of the Federal Government. For a future-proof procedure, the QSiegel must
also be introduced here, as it is based on the same technology of the certificates for
QES.

Telemedia Act (TMG)
In the TMG, it would have to be made possible for websites with a public interest these include, for example, the websites of public authorities and future citizens'
accounts, employment offices, the Foreign Office, hospitals, the fire brigade or the

police - to be securely assigned to the actual operator. The user must be able to
automatically check that it is a website or internet application originating from the issuer.
To this end, the use of QWACs should become a mandatory safeguard. This is already
stipulated in Section 13 (7) of the German Telemedia Act (TMG) for the encryption of
website communication and can also be carried out for the reliable operator origin in a
technology-open manner.

Social Code (SGB) I, IV, V, X, XI
The existing eIDAS standards should be used for the exchange of data and documents in the health sector. This requires a number of changes in the SGB. In general, a screening of standards is advisable here in order to obtain a complete overview
of the need for adaptation and to establish a stronger eIDAS reference in the SGB.

In the First Social Code, the Q seal should be included as an electronic means in Â§ 36a
(electronic communication), for example by adding a new paragraph:

Proposal for an addition to SGB I Â§ 36a

(1) The transmission of electronic documents is permissible if the recipient opens access for this purpose.

(2) (new) The intersectoral communication and data transmission in the health care system is defined as the electronic data exchange of personal treatment and health care data beyond the boundaries of the traditional sectors, such as physicians in private practice, clinics, aftercare and rehabilitation areas, the self-governing bodies, health insurance funds/replacement funds, authorities and public health care institutions, via infrastructures approved by the legislator (telematics infrastructure, KV-SafeNet, etc.).), the use of standardised transmission technologies to ensure data protection and data security as required by law, as well as the use of suitable standardised methods for identification, authentication and integrity in accordance with Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).
For transport security in the exchange of data between the primary systems in the healthcare sector and for the identification of the participants or participating systems in the communication, QWACs in accordance with the above-mentioned regulation shall be used. For securing the authenticity of medical documents and data (application levels), qualified seals in accordance with the above-mentioned regulation shall be used, unless the written form must be maintained.

The Fourth Social Code (Â§ 110, SGB IV) stipulates the storage obligation for social
security institutions. Here, the electronic form of storage should also be explicitly
secured with the help of Q seals. This enables automated filing systems. In the Fifth
Social Code (Â§ 291a ff. SGB V), the "gematik Gesellschaft fÃ¼r Telematikanwendungen der
Gesundheitskarte mbH" (Society for Telematics Applications of the Health Card) defines
the standards for the use of the telematics infrastructure in agreement with the BSI. The
QSiegel can also be applied there.

In the Tenth Social Code (Â§Â§ 25, 33 SGB X), electronic excerpts or transcripts from files for which file inspection is to be granted should also be secured with the Q seal. This is because in the case of the transcript, it is not the person who initiates or sends the transcript that is important, but the authenticity of the document from which the transcript is requested.

Furthermore, it should be examined whether QWACs and QSiegels can be used in the Eleventh Social Code on Long-Term Care Insurance (Â§Â§ 7, 105 SGB XI) for the billing and documentation systems as well as for other communications. Currently, Â§ 105 (2) SGB XI stipulates that for the transmission of electronic documents, in addition to the QES, another secure procedure must be provided that authenticates the sender and guarantees the integrity of the data record. An anchoring of the QSiegel is always appropriate here if the documentation of the process is important and not personal liability.

4.3.2

New regulations for secure electronic legal transactions

Some areas of legal transactions require entirely new regulations in order to be able to introduce digital business processes.

The BGB and the challenge of completely new forms of communication

A regulation on new communication relationships that emerge in the course of digitalisation must be included in the BGB. Creating a separate body of law would not do justice to the importance of digitisation. By including it in the BGB, the numerous references in specialised laws can be used sensibly.

For example, the self-driving vehicle will autonomously drive to a charging station and fill up with electricity there or rent a parking space in the automated car park and drive to a workshop for repairs. If the smart household appliance places an order, automated internet retailers react to it and also automatically order a transport service, which may be carried out by an automated delivery robot, it must be possible to design these contractual relationships in a tamper-proof way and document them in a comprehensible way.

In terms of content, the regulation would have to cover various areas: (1) What definition is to be found for machine communication. (2) The form that a machine or software must adhere to in order to be humanly comprehensible in retrospect. (3) Who is liable for the actions of the machine. (4) Who becomes entitled to claim.

The results of the study on the trust function can be used for the form of communication. A formal requirement must apply whenever there is a lasting effect

from the machine's action, there is an interest in identifying the machine and the legal
entity behind it, and there is a need for security in the communication relationship.

The Q seal is the appropriate form here. It identifies a legal person who stands behind the
machine and software as the legal entity. In addition, the machine communicates in case
of doubt as its own, likewise virtual entity. Another argument in favour of the Q seal is the
need to distinguish it from human communication. It offers the necessary manipulation
security and documentation capability. In this way, it can be avoided that such processes
are triggered by "false" machines or that the communication is manipulated. In addition to
the identity of the machine, the communication path must also be secured. This can be
done by QWACs. They ensure that data encrypted by a machine or software reaches the
correct server or communication platform. Electronic time stamps can be used to record the causal sequence.

The same can apply to human-to-machine communication. Principles have already
been developed for the use of mechanical machines. However, for the first time, there
is also legally relevant communication in the other direction (open-ended software
with humans), for example in chatbots, telephone hotlines or when the software orders
a human supplier to provide a service or a care robot provides services. Here, the human
must also know which machine or software is ordering or providing something.

Professional secrecy holders: BRAO and BOStB

There is a need to extend Section 42 BRAO and Section 5 BOStB. The current regulations
only concern the obligation of the service provider, but not client contact. Here, the
professions are still on their own. It would be beneficial to support digital processes through
a legal framework. It should be regulated that state-of-the-art encryption
technologies are sufficient to fulfil the obligation of professional secrecy. In addition, it
should be regulated that the disclosure, transfer or inspection of confidential information
digitally is only permissible with secure identification of the parties involved in the
communication. These requirements are in particular
in the use of eIDAS trust services. It is to be welcomed that with the reform of Â§ 203
StGB and Â§ 2 BORA the service providers have already been included and here the
problem of the confidentiality of the digital service providers is to be solved. However, this
only includes communication and the receipt or disclosure of documents to the groups
listed above in exceptional cases. These are precisely not service providers of the lawyer
but, in case of doubt, participants in the proceedings. Therefore, a trust infrastructure
that is open to technology and standardised throughout Europe is needed.

EU Directive on roadworthiness tests for motor vehicles
Art. 16 of Directive 2014/45/EU of the European Parliament and of the Council of 3 April 2014 must be implemented uniformly throughout Europe. The database can be secured against manipulation by QWACs and access by authorised users (workshops and TÃ‍V test locations) can be confirmed with Q seals. The retrieval of mileage information can be usefully provided by the means of the EGovG and the eIDAS Regulation (for example De-Mail, QES and QSiegel for insurance companies).

Regulatory enabling of public cloud services
The public sector will become more efficient through cloud services and will be able to better manage digital processes in the future. However, such services and applications require the necessary legal certainty for the users and manufacturers of these solutions. So far, a framework for the regulatory enabling of these services is missing.
To this end, the eIDAS trust services must be used for communication. Here, too, the features of the trust function take effect. This must nevertheless be combined with the previous considerations of the BSI requirements catalogue C5. This ensures the physical security and quality of the service. In addition, the communicative security of users and applications is ensured in a legally binding manner through the use of qualified trust services. A federally binding regulatory solution is needed to allow municipalities, states and the federal authorities to use cloud services efficiently.

5

OUTLOOK

Digitalisation poses major challenges for the German economy and administration. of the changes. It is imperative to adapt German laws, regulations and guidelines to respond to the changes.

The proposed legal changes and the introduction of eIDAS trust services can put Germany back at the forefront of the competition for the best digital locations. At the same time, they can strengthen citizens' trust in the state, as partially or fully automated administrative processes show them the functioning of the public administration.

In spite of all the legal considerations, the factual changes in society must not be ignored.
Digital threats, such as cyber attacks on companies or individuals, are increasing and becoming more serious. Germany must counter these new digital threats with increased resilience. It is essential to introduce and promote digital security mechanisms. This is where the added value of the eIDAS Regulation lies: with its trust services, it can protect against digital threats - be it in the health sector, in digital legal transactions or in administration. For example, official servers can be protected against overload

failures by only allowing forgery-proof certificates to pass through the filter mechanisms. At the same time, software protection could also be improved. The use of trustworthy software is extremely important due to the extensive threats from malware, spying and blackmail programmes. Already today, there are test mechanisms based on QES for the protection of software programmes. In the future, Q seals could be used to protect against malicious manipulation. Before the software is installed or executed, the publisher would be identified by means of the Q seal. If the check is successful, the software can be used. In addition, QSiegels could also be used in combination with QWACs for automated electronic communication processes (for example, machine-to-machine communication), for device authentication or for asynchronous proof of integrity.

6

RECOMMENDATIONS FOR ACTION

The eIDAS Regulation enables uniform digital business and administrative processes in the European Union. However, the trust services contained therein have not yet been meaningfully integrated into German law and therefore do not yet have a major impact.

This results in concrete recommendations for policy action:

1. The German government should address the deficits in the implementation of the eIDAS Regulation as quickly as possible. Especially with regard to the qualified electronic seal and qualified website certificates, new legal regulations are needed, such as those already in place in the Payment Services Directive 2 (PSD2). The PSD2 can serve as a model to open up further fields of application and to adopt similar regulations there. The legal amendment proposals of this study provide orientation in this regard. The first concrete steps should be visible by the first half of 2020 - when the European Commission conducts an evaluation of the eIDAS Regulation. The Federal Government should also see the implementation of the eIDAS Regulation and the use of the trust services standardised in it as an important contribution to more data and consumer protection in Germany.

2. In the context of "digital legislation", orientation should be based on the "Better Regulation Toolbox #23" of the European Commission. The "Better Regulation" project of the Federal Ministry of the Interior, for Construction and Home Affairs already exists for this purpose. This project should be supplemented by an impact assessment of laws for the digital transformation, which recognises the consideration of eIDAS trust services as an important means of digitisation-friendly legislation, as

is the case at EU level.

3. Within the framework of the German EU Council Presidency in 2020, the Federal Government should treat the further development of the eIDAS Regulation as a priority and use the presidency to take the lead in negotiations in the Council on the
revision of the Regulation. The main issues here are the introduction of new instruments (e.g. an eID function for businesses), greater binding force in the use and recognition of trust services, and further harmonisation of the requirements for the certification and authorisation of eIDAS trust services.

The following list contains examples of legislative measures to integrate eIDAS trust
services into German law in a meaningful way:

Law

Extension of the trust service

Application examples

Responsibility Ministry

ZPO

QSiegel, timestamp

Service of pleadings,

BMJV

certification, evidence

StVZO

QSeal, time stamp, delivery

Tachometer reading

services

database for TÃ✍V and car

BMVI

workshops
VwVfG

QSiegel

Applications and declarations to

IT Planning Council, BMJV

authorities by companies,
Â§ 3a VwVfG
QSiegel

Electronic equivalent for certifications

IT Planning Council, BMJV

and official seals,

Â§ Sections 3a, 33 (5), 37 VwVfG

EGovG Federal Government

QES, QSiegel

Certificates of good conduct

BMJV

Anchoring of all standards of the

Basis for the introduction in the

IT Planning Council, BMI

eIDAS Regulation

E-government: obligation to deliver and receive, e-file with Q seals

EGovG Countries

Anchoring of all standards of the

Basis for the introduction in the

eIDAS Regulation

E-government: obligation to

IT Planning Council, IMK

deliver and receive, e-file with Q seals
BGB

QSiegel

Digital company information

BMJV

QES, QSiegel

IHK certificates, employer

BMJV

references, diplomas, master craftsman c e r t i f i c a t e s
QSeals, QWACs, timestamps

Human-to-machine communication

BMJV

and human-to-human communication
TMG

QSiegel, QWACs

Secure communication,

BMI, BMVI

Â§ 13 Para. 7
BRAO, BOStB

EStG

QSeal, time stamp, delivery

Use of the eIDAS trust services for

services

procedural communication

QSiegel

Use of the QSiegel for banks,

BMF, BMJV

BMF

Â§ 45a para. 2 EStG
Eu-RiLi roadworthiness tests for

QSiegel, QWACs

Database Creation and Use Act

BMVI

SGB I

QSiegel

Securing electronic communication

BMG

SGB XI (Nursing)

QSiegel, QWACs

Communications, accounting,

BMG

motor vehicles

documentation in care
SGB IV, X (e-health)

QSiegel, QWACs

Notification of carriers, storage and
transcripts

BMG

LIST OF ABBREVIATIONS

AO	Tax code
BGB	Civil Code
BMG	Federal Ministry of Health
BMI	Federal Ministry of the Interior, for
BMVI	Federal Ministries
	Conference of Interior Ministers
	Consumer Protection
PSD2	Payment Services Directive 2
	Federal Ministry of Transport and
QES	Qualified
QSiegel	Qualified
	Federal Ministry of Justice and
	Professional code of conduct for lawyers
BOStB	Professional Code of Conduct of the Federal Chamber of Tax Consultants
BRAO	Federal Lawyers' Act
EGovG	Act on the Promotion of Electronic Administration (E-Government Act)
eIDASRegulation	(EU) No. 910/2014 of the European Parliament and of the Council of 23 July
	electronic
	electronic

signature
seal

SGB

Social Code (with Roman numerals)
Number designation)
SigG

Signature Act (entered into force)

StGB

Criminal Code

StVZO

Road Traffic Licensing Regulations

TMG

Telemedia Act

TR
RESISCAN Technical Guideline for Legally Compliant

2014 on electronic

Replacing Scanning of the German Federal

Identification and trust services for

Office for Information Security (BSI)

electronic transactions in the
Internal Market and repealing Directive
1999/93/EC
ERVAct on the Promotion of Electronic Legal
Relations with the Courts

47

Joint Rules of Procedure of the

Judicature Act

BORA

EStG

Germany
GGO

IMK

Digital Infrastructure

Law

Basic Law for the Federal Republic of

GVG

Building and Home Affairs

BMJV

GG

Income Tax Act

VDG

Trust Services Act

VDV

Ordinance on Confidential Services

VwGO

Administrative Court Code VwVfG
Administrative Procedure Act ZPO
Code of Civil Procedure