procilon GROUP

Digital Transaction Management

Greater safety

for your data management

Secure identification

Secure communication

Secure storage

Introduction

The procilon GROUP → has been specializing in the development of cryptological software and strategic consulting on information security and data protection for more than 20 years.

Today, more than 1500 companies, organizations, and authorities have taken preventive technical and organizational measures to protect their data with the support of procilon.

The present document is intended for institutions and private individuals who need to observe and adhere to compliance guidelines, as well as for anyone interested in the topic of cyber security. The Digital Transaction Management (DTM) guide should be seen as an informative security recommendation. It is designed to familiarize IT-interested readers with security-relevant information and current developments in data management.

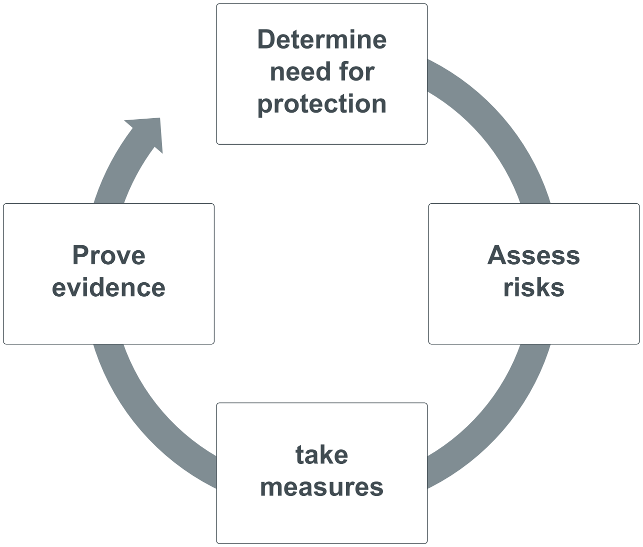


Figure on the right:
Process chart, data protection cycle, copyright by procilon

Following the explanation of the challenges of compliance in Digital Transaction Management, an overview is provided of Basic DTM, Extended DTM, and the main aspects to be considered in DTM. A brief essay will outline the development of DTM, followed by a discussion of cryptography in digitization. In order to sign digitized or digital documents securely and quickly, electronic signatures should be applied. That is why the subsequent chapter explains the different types of electronic signatures, their integration into workflows and the legal force of digital signatures.

The challenge of compliance in DTM

Data protection → The approach is complete only when the aspects of personal data protection, protection of secrets, and the German Trade Secrets Act (GeschGehG) are being included. The GDPR also provides a legal framework for that, and cryptography, with its various encryption methods, makes an important contribution to meeting the necessary requirements.

Compliance → When you observe all these legal principles and tap the full technological potential of DTM, the necessary compliance is created, which ensures reliance for all users.

Security potentials in the digitization process

Simply explained, Digital Transaction Management (DTM) describes the digitization of document processes. However, there is more behind that than simply transferring analog paper processes into the digital world – the strategies for digitizing established, previously analog processes need to be carefully thought through and redesigned in a legally compliant manner using the appropriate technologies.

Digital Transaction Management opens up a broad field of technological possibilities, ranging from the simple transfer of analog paper documents into digital files to the complete automation of the entire process chain of digital document processing.

That results in the need to secure digital processes, especially in case of locally separated work tasks, not only in terms of "classic" IT security, but also to use additional compliance elements. In the end, it is therefore a matter of efficiently selecting and evidently making use of the potential of these trustworthy elements for transactions in the digitization process.

Binding security levels

With all these intentions, DTM focuses on compliance. In automated, digital processes, proof of the origin and integrity of documents can only be generated by applying cryptographic means.

It makes no difference whether only integrity protection is required or whether it is required in conjunction with a digital signature – in both cases, there is no way around the electronic signature. The conditions are uniform and unambiguous, as the eIDAS Regulation has set European standards for electronic signatures and applicable identification procedures in terms of binding security levels.

Digital Transaction Management (DTM)

Advantages for enterprises →

- *Reduced time to revenue*
- *Improved profitability*
- *Improved and simplified customer experience*
- *Saves paper and storage space*

Advantages for authorities →

- *Faster action through digital processes*
- *Reduced need of communication with citizens*
- *Secure digital storage of documents*
- *Simple management of documents*
- *Saves paper and storage space*

Process design → Nowadays, the aim is to simplify digital communication and document-based customer and employee processes. That is why WCA is seen as a strategic part of this digital process design.

Basic DTM

The introduction of DTM may start with the digitization of simple paper processes, thus opening up a quick path to success. Examples include co-signing or releases in administrations or contractual agreements. With the help of digital documents and electronic signatures, the time required to sign contracts is significantly reduced. For example, DTM can be applied to supplier contracts, non-disclosure agreements as well as mergers and acquisitions.

Digitization simplifies processes by drastically reducing the time it takes to exchange documents – which is needed to conclude a contract, for example – and thus the time it takes to achieve a result. That could also accelerate the company‘s booked sales, and it saves paper and shipping costs. Consequently, companies that use DTM develop a significant competitive advantage and administrations increase their efficiency.

Extended DTM

Extended DTM includes the digitization and automation of the entire document creation process – Workflow and Content Automation (WCA). For example, complex document processes are realized, such as the compilation and routing of documents, integration with other applications, and work processes that precede and follow the decision between approval or signature.

Connectivity and integration with document management systems (DMS) and archiving systems also play a crucial role in keeping documents structured, legally compliant, and secure.

However, when archiving signed electronic data – especially over longer periods of time – various specific features must be considered, above all the minimization of risks for the legal value of signed documents.

Digital Transaction Management (DTM)

Market segmentation for digital transaction management →

- *E-signature*
- *Authentication*
- *Document archiving*
- *Workflow automation*

Main aspects in DTM

Using various types of cloud services for the digital management of a large number of document-centered business processes is one of the most important aspects of DTM. However, within the field of electronic signatures, DTM not only includes content management, but also covers the aspects of authentication, non-repudiation, document transfer and certification, workflow, data integration and form integration, data management, secure archiving, and some meta-processes related to the management of electronic transactions.

Figure on the right:
Photo by tippapatt, Adobe Stock

Primary requirements for user DTM

- Creation of electronic signatures is the core function
- Possibility of document compilation
- Forwarding of documents and workflow automation
- Basic and extended analyses based on the organizational level
- Integration with leading content management systems and other Line of Business platforms (LOB)
- Mobile apps (remote, personal, and offline signing, administration)

Secondary requirements for DTM

- Asset Management, including transaction management and trust services
- Workflow and Content Automation (WCA)

Intelligent contracts and blockchain → Blockchains enable so-called smart contracts. That way, an enforceable contract can be developed and automatically processed with the help of software, provided that all parties involved fulfill the previously defined conditions. At best, the software itself checks whether all parties have met the conditions. A smart contract can therefore control, monitor, document, or effect a legally relevant process.

APIs, mobile apps, cloud, and transactions

Application Programming Interfaces (APIs) are the gears of the programming interface in order to modernize enterprises and they provide the foundation for integration and interoperability. That means that an increasing number of digital transaction management platforms are being created on the market, enabling the integration of other necessary applications and thus creating further interfaces, which then facilitates faster and more effective automation of common business and administrative processes.

In many cases, a mobile application is provided for digital signing. However, the new approach for digital process design is to use a customer-owned mobile app for DTM. As a result, the signing functions must be integrated via an application programming interface to provide a unique and personalized user experience.

The integration of transactions that trigger one-time and recurrent payments is also possible. It is therefore expected that new financial technology providers (FinTech) will embed themselves as partners in the DTM. Thus, transactions and payments can be completed within the native DTM app.

Intelligent Content Analytics (ICA)

For the past twenty-five years, companies have been focusing on data management and, of course, data retention. Today, the companies' focus has broadened to include two aspects: quick access to the information they store and its analysis.

Intelligent Content Analytics can help organizations not only manage the stored information from documents, but also filter, process, and analyze the information, as well as use these functions to help them make more informed decisions faster.

Cryptography in digitization

History of cryptography

Cryptography → contributes significantly to the applicable standards of information security and the protection goals defined therein.

In the past, cryptography – or more broadly, cryptology – was primarily applied to protect confidential information. The methods used for encryption can be traced back to antiquity.

The basic operating principle has not changed much to this day: Information is encrypted using a key and an associated procedure and can be made readable again using a fitting key.

The principle of encryption applied at that time → is now being utilized in the digital world by using these methods to protect against manipulation and to prove origin.

Figure on the right: Evolution of encryption, copyright by procilon

The original use of cryptological procedures to prevent unauthorized reading – i.e., "classic" encryption – does not play the main role for the issues of the following explanations. The focus is on tamper-proof, digital information.

The elementary building block → to achieve the protection goals is the electronic signature, which must be used in the end to create trustworthy and completely digital processes that also meet the requirements of automated processing. The possible applications range from the simple protection of the integrity of digital information or e-mails to replacing handwritten signatures.

Information security and cryptography

Protection of integrity: Unauthorized manipulation of digital information (for example, insertion, modification, deletion, substitution of parts) is to be detected.

Proof of authenticity with regard to proof of identity: Party A (for example, a user of an IT system or an IT system itself) must be able to prove its digital identity to party B beyond doubt.

Figure on the right:
Photo by Sashkin, Adobe Stock

Proof of authenticity related to proof of origin: Party A must be able to prove to party B that a piece of digital information originates from party A and has not been altered or manipulated.

Secrecy: No unauthorized third party should be able to access the contents of the message or the file itself.

Binding force (non-repudiation: The focus is on provability to third parties – from a legal perspective, another very advantageous and effective effect.

Electronic signatures

Electronic signatures → Protect the integrity of data and make manipulations detectable.

The categorization of electronic signatures → results from the trustworthiness of the signature keys, the signature certificate, and the associated signature processes. A qualified signature certificate is required for the electronic signature to replace the written form (QES). A trust service provider (TSP) generates the signature certificate. The TSP must first identify the person or, in the case of seal certificates, the institution in conformity with eIDAS and document the whole process in a verifiable manner. That means that the signature certificate is clearly associated with o the certificate holder – a natural or legal person. That explains why qualified signatures require specially protected and verified signature processes.

Protection of integrity

Depending on their design, electronic signatures may fulfill two basic tasks. On the one hand, they provide proof of authorship, comparable to a handwritten signature on paper. On the other hand, they can be used to detect changes to digital information (manipulation) after the signature was made, especially in the case of cryptographic forms.

The different types of signatures have different probative value and security in order to protect files and documents. The simple, the advanced and the qualified signature are being distinguished. The legal framework was standardized in the European eIDAS Regulation for the internal market and implemented in national law with the German Act on Trust Services.

The basic cryptographic procedure is the same for advanced and qualified signatures. The signers require a pair of keys consisting of a private (secret) signature key and a public verification key, which is disclosed together with a digital certificate and authenticated or certified by a certificate authority (CA). A mathematical process is used to create a unique image (fingerprint, hash value) of the document to be signed. That image is encrypted using private signature key of the signature certificate used.

Types of electronic signatures

The value or quality of the signature depends on the status of the issuers of the certificates. For example, users can generate advanced certificates themselves from various locations. However, for the highest form of security, you have to turn to so-called trust service providers or TSPs, which, in accordance with the eIDAS Regulation, generate the certificates in a security-checked process and additionally store them on secure hardware (HSM).

Electronic signatures

Simple electronic signature

A simple signature is easy and quick to use. It may, for example, consist of a textual name in an e-mail or a scanned signature. The simple electronic signature is the weakest form of signature because it can be executed without identity verification. That means it cannot be clearly assigned to a person or one of the signers and does not provide any protection against manipulation. Therefore, that type of signature should be used only when there is a low legal risk, for example, for the documents listed on the left.

Simple electronic signature for:

- *General business relationships*
- *Documentations*
- *Internal reports*
- *PDF including scanned signature*
- *Informal agreements*

Advanced electronic signature

The advanced electronic signature enables the signer to be identified and is uniquely assigned to the signer. It must be created using a unique, secret signature key to which only the holder has access. The advanced signature therefore offers a higher level of evidential value and security than the simple signature and provides very good protection against manipulation, for example for the documents listed on the left.

Advanced electronic signature for:

- *Privacy statements*
- *Insurance applications*
- *SEPA mandates*
- *Powers of attorney*
- *Non-disclosure agreements*

Qualified electronic signature

The qualified electronic signature has the highest probative value among digital signatures and is legally on a par with a handwritten signature. That level of security requires the identity of the signer to be verified by the issuer of the certificate. Such identity checks can be performed, for example, via video or bank ident. After successful verification, a certified trust service provider creates an electronic certificate with the name of the signing person. Using the certificate in conjunction with a secure signature creation device, the person signing can trigger a qualified signature. The qualified signature can thus legally replace a handwritten signature and be used for documents for which a written form requirement is mandatory, for example the documents listed on the left.

Qualified electronic signature for:

- *Clause to limit the term of employment contracts (fixed-term employment contracts)*
- *Unlimited employment contracts*
- *Securities*
- *Life insurances*

Electronic signatures

Integration of electronic signatures

In the past, using cryptography in everyday life has usually been complicated and not user-friendly. For example, a qualified electronic signature required a signature card, a suitable reading device, and additional software. As a general rule, the higher the security requirement, the greater the effort, but the lower the acceptance.

The eIDAS regulation and the introduction of the so-called remote signing have created the possibilities for achieving user-friendly embedding in existing processes in addition to the use of special cloud solutions. The integration of security technologies in applications reduces the additional cryptographic effort and relieves the user.

Other user-friendly criteria:

- *Mobile and trusted usage from the cloud*
- *One-time registration of secure identities*
- *Mostly no need for additional hardware*
- *Corresponding software already includes necessary verification components (e.g., whether electronic consent has the same value as a signature on a paper form for an online contract)*

Probative value of electronic signatures

The types of electronic signatures have different probative values and only the qualified signature can replace the handwritten signature if the written for is required. That also creates a so-called reversal of the burden of proof – i.e., the plaintiff has to prove that the qualified signature is invalid.

All types of signatures → are legally valid and enforceable according to the eIDAS Regulation. The acceptable level of signature is agreed by the users among themselves.

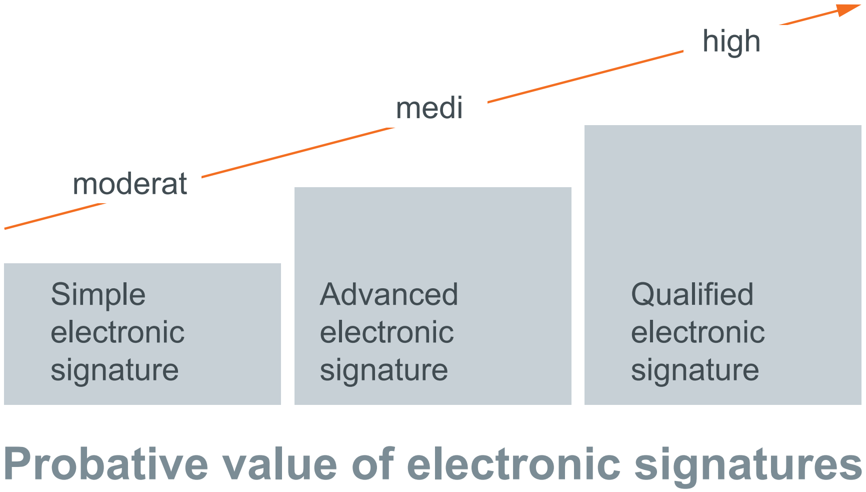

high
medi
moderat
Simple electronic signature
Advanced electronic signature
Qualified electronic signature
Probative value of electronic signatures

Figure on the right:
Process chart, Probative value of electronic signatures, copyright by procilon

Validity of electronic signatures

Legal retention periods → for documents must be observed. For example, commercial and business letters must be kept for six years, while annual and consolidated financial statements must be kept for ten years.

The time limit on the validity of electronic certificates is primarily due to further technological development, which could be exploited by cybercriminals, for example. That is the reason why cryptographic algorithms are constantly checked and renewed with regard to their effectiveness in order to avoid risks to the legal value of signed documents. It is therefore advisable to check the certificates used and to update them if necessary.

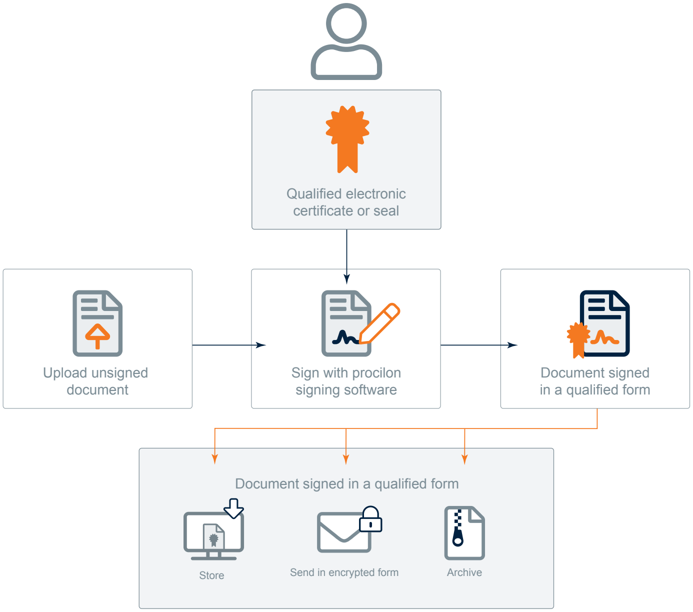

Qualified electronic certificate or seal
Upload unsigned document
Sign with procilon signing software
Document signed in a qualified form
Document signed in a qualified form
Store
Send in encrypted form
Archive

Figure on the right: Process of a qualified electronic signature, copyright by procilon

Retention periods of signed electronic data

A few special considerations must be taken into account when archiving signed electronic data, especially over long periods of time. Important documents that have been signed in a qualified manner must be managed with the same level of care during storage as paper documents.

Long-term archiving – preservation of evidence

Extended DTM → *Examining the extended DTM results in a complete cycle – from document generation to preservation in electronic archives.*

When archiving digital documents, not only must fast access and non-appealability be ensured for possible evidence in court, but also the security suitability of the required cryptographic algorithms and their certificates, together with their directories, must always correspond to the currently required security status in terms of preserving the probative value.

Figure on the right:
Photo by tiero, Adobe Stock

Especially when you archive signed electronic data over long periods of time, the use of IT solutions that preserve the probative value is necessary. The standard defined for that purpose by the German Federal Office for Information Security (BSI) is defined in a differentiated catalog of mandatory and optional requirements for technical software solutions and is associated with the technical guideline TR-ESOR (TR 031259).
TR-ESOR: https://www.bsi.bund.de/tr-esor

When you integrate such a software solution carefully into the digital archives, all signed data retains its legal value for the required retention periods.

Electronic signatures

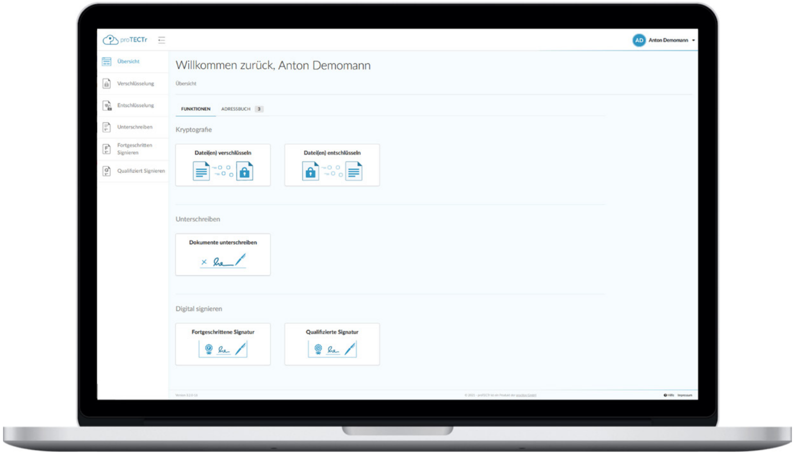
Documents for review and signing → can be sent to customers without lengthy email communication by a team can send. Quotations, confidentiality agreements, contracts, meeting minutes and more can be digitally signed, encrypted, and sent via a platform, automating and shortening processes.

Practical example

There are various browser-based web applications for DTM, especially for encryption and the creation of electronic signatures. Individual components are bundled into useful functions and integrated into workflows.

They can be used usually by individuals as well as by organizations. For organizations, the advantage is that managing all members of the organization can be controlled independently and in a targeted way through appropriate assignment. That opens up the possibility of being able to use compliance elements in terms of digital transaction management in a very short time without having to invest in costly implementations and user training.

*Figure on the right:
Dashboard user interface proTECTr,
copyright by procilon*

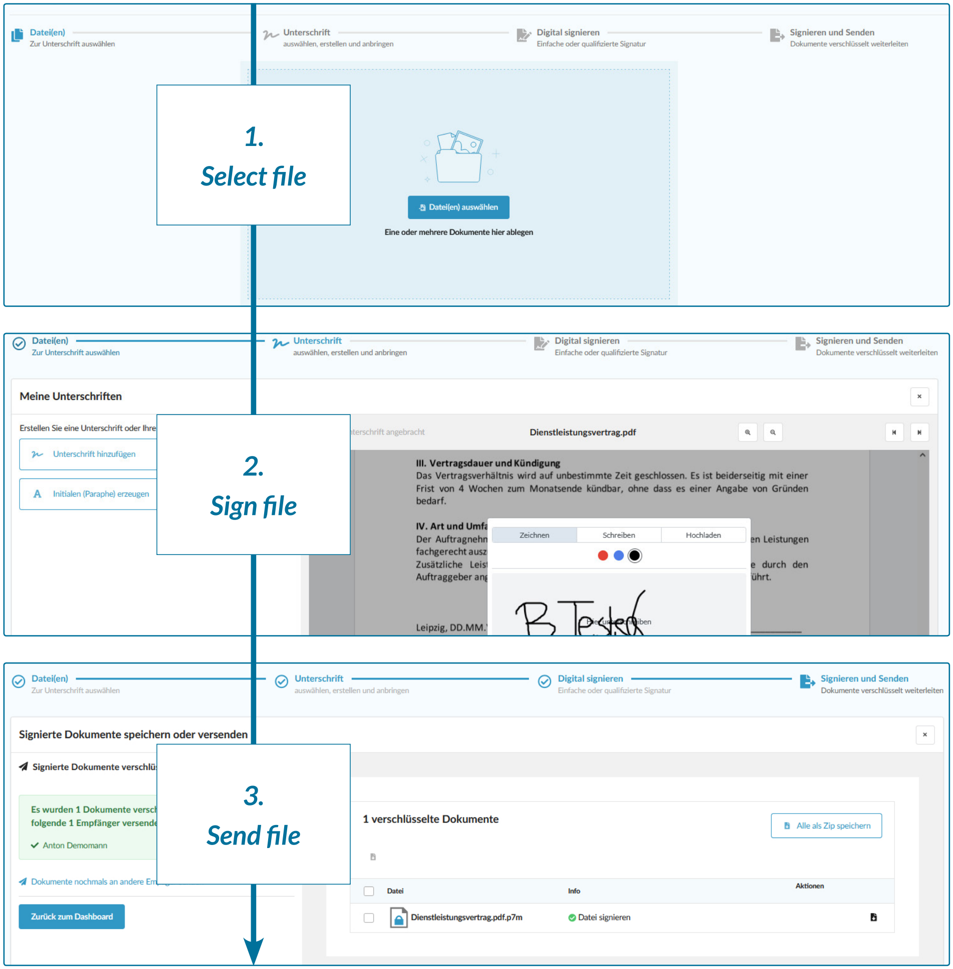


Willkommen zurück, Anton Demomann

Some platforms provide a basic service for spontaneous and strong encryption of files, which meets the requirements of the GDPR for electronic communication. End-to-end digitized processes are enabled by the simple creation and application of a qualified or advanced electronic signature with highest probative value. Both the confirmation of the user's identity and the signature types must be compliant to eIDAS.

Signing workflow in three steps

Files can be electronically signed, encrypted, and saved locally or sent by e-mail in three self-explanatory steps.


1.
Select file
2.
Sign file
3.
Send file
Datei(en)
Zur Unterschrift auswählen
Unterschrift
auswählen, erstellen und anbringen
Digital signieren
Einfache oder qualifizierte Signatur
Signieren und Senden
Dokumente verschlüsselt weiterleiten
Datei(en) auswählen
Meine Unterschriften
Unterschrift hinzufügen
Initialen (Paraphe) erzeugen
Dienstleistungsvertrag.pdf
Zeichnen
Schreiben
Hochladen
Signierte Dokumente speichern oder versenden
Alle als Zip speichern
Zurück zum Dashboard

Eine oder mehrere Dokumente hier ablegen

Erstellen Sie eine Unterschrift oder Ihre

terschrift angebracht

III. Vertragsdauer und Kündigung
Das Vertragsverhältnis wird auf unbestimmte Zeit geschlossen. Es ist beiderseitig mit einer Frist von 4 Wochen zum Monatsende kündbar, ohne dass es einer Angabe von Gründen bedarf.

IV. Art und Umfa
Der Auftragnehm … en Leistungen
fachgerecht ausz
Zusätzliche Leis … e durch den
Auftraggeber ang … führt.

Leipzig, DD.MM.

Signierte Dokumente verschlü

Es wurden 1 Dokumente versch
folgende 1 Empfänger versende
✓ Anton Demomann

Dokumente nochmals an andere Em

1 verschlüsselte Dokumente

	Datei	Info	Aktionen
□	Dienstleistungsvertrag.pdf.p7m	✓ Datei signieren	

Figure on the right: Screenshots of proTECTr user interface, browser-based selection, signing, and sending of a file in three steps, copyright by procilon

Conclusion

Digital Transaction Management facilitates the workflow of paper processes and describes the digitization of workflows. Such digitization helps companies to save time and costs and remain competitive in the future.

The ways to DTM are cleared with the help of the introduction of digital signatures, secure transmission paths, and protected long-term archiving of documents, among other things. The most important aspects of DTM therefore include the use of various forms of cloud services for the digital management of document-centered business processes and the integration of these processes into existing workflows.

Businesses and organizations may use DTM to create greater security for their data management through encrypted delivery, electronic signatures including required identity checks, and secure long-term storage.

About procilon

procilon is one of the leading full-service providers of self-developed public key infrastructure solutions, focusing on the generation, administration, and application of electronic certificates as well as on signatures and encryption.

The unique product spectrum ranges from simple file encryption in browsers to signing applications, identity and access management (IAM), and complete infrastructures for trust service providers according to the EU eIDAS regulation. Varied secure services from the cloud complete procilon‘s portfolio. procilon is a long-standing member and partner of the Alliance for Cyber Security.

procilon.de

procilon
GROUP

procilon GROUP | Leipziger Straße 110 | Taucha | Germany | +49 34298 48 78 - 31 | anfrage@procilon.de