Elektronische Signaturen als EFFIZIENZ-BOOSTER für Ihre Prozesse

Nect

INHALTSVERZEICHNIS

01

STATUS QUO

Ein Blick auf die Digitalisierung in deutschen Unternehmen

Um die Relevanz und die Möglichkeiten elektronischer Signaturen besser einordnen zu können, werfen wir zunächst einen Blick auf die Digitalisierung deutscher Unternehmen im Allgemeinen. Die digitale Transformation hat in den letzten Jahren bei einem Großteil der Unternehmen Einzug gehalten. Zahlreiche Organisationen arbeiten daran, ihre Prozesse zu digitalisieren, um effizienter und effektiver zu arbeiten. In vielen Bereichen konnte dabei schon ein klarer Digitalisierungsfortschritt erreicht werden, doch viele Unternehmen sind tagtäglich mit Herausforderungen konfrontiert, die die Digitalisierung ihres Geschäfts blockieren. Schauen wir uns beides einmal genauer an.

Nect

Digitalisierungsfortschritt in deutschen Unternehmen

Deutsche Unternehmen werden digitaler. Dabei liegt der Fokus vor allem auf Investitionen in digitale Technologien, der Nutzung von Cloud-Computing und der Digitalisierung von Geschäftsprozessen. Mit der fortschreitenden Entwicklung innovativer Technologien wie Künstlicher Intelligenz (KI) und Data Science entstehen zusätzliche Potenziale für die digitale Transformation.

Die Studie „Digitalisierung der Wirtschaft 2025“ des Branchenverbands Bitkom zeigt, dass 30 % der deutschen Unternehmen im Jahr 2025 mehr in Digitalisierung investieren als noch im Vorjahr. Dennoch verfügen 72 % der Betriebe über keine zentrale Digitalstrategie, was den Fortschritt hemmt. Gleichzeitig bezeichnen sich 32 % der Unternehmen als digitale Vorreiter, während mehr als die Hälfte (53 %) Schwierigkeiten bei der Umsetzung digitaler Maßnahmen angibt.

Auch die Lünendonk®-Studie 2025 „Der Markt für IT-Dienstleistungen in Deutschland“ verdeutlicht, dass die Digitalisierung für nahezu alle Unternehmen ein zentraler Erfolgsfaktor bleibt. Über 90 % der befragten Unternehmen planen, sich in den kommenden Jahren neu aufzustellen, ihre Geschäftsmodelle stärker zu digitalisieren und Prozesse zu automatisieren. Im Mittelpunkt stehen dabei Produktivitätssteigerung, Effizienz durch neue Technologien sowie eine konsequente Ausrichtung auf Kund:innen und digitale Erlebnisse.

Nect

Herausforderungen in der Digitalisierung

So vielversprechend die aktuellen Entwicklungen sind, so groß sind auch manche Hürden, vor denen Unternehmen im Digitalisierungsprozess stehen. Die folgenden gehören zu den größten Herausforderungen:

REGULIERUNG

Deutschland gilt weltweit oftmals als überreguliert. Bestehende Gesetze und Regulierungen sind nicht auf die neuen Geschäftsmodelle und Technologien der digitalen Welt zugeschnitten. Das hemmt Innovation und schafft Unsicherheiten in den Unternehmen. Eine LinkedIn-Umfrage von Nect ergab, dass fast die Hälfte der Unternehmen regulatorische Hürden als den größten Blocker in der Digitalisierung wahrnehmen.

FACHKRÄFTEMANGEL

Der Fachkräftemangel ist eine der größten Herausforderungen für die Digitalisierung in Deutschland. Es mangelt an spezialisiertem Personal mit den notwendigen Kompetenzen, um die Potenziale der Digitalisierung zu nutzen. Laut Bitkom fehlen in Deutschland aktuell rund 149.000 Fachkräfte im IT-Bereich.

DATENSICHERHEIT

Die zunehmende Digitalisierung und die Weiterentwicklung innovativer Technologien führt zu einem massiven Anstieg der Datenmenge, die gespeichert und verarbeitet wird. Dies macht Unternehmen und Behörden anfälliger für Cyberangriffe und Datenpannen. Bedenken hinsichtlich der Datensicherheit und des Datenschutzes bremsen die Digitalisierung allerdings. Hier bedarf es mehr Aufklärung, um Unternehmen die Risiken zu erklären und sie zu befähigen, entsprechende Entscheidungen zu treffen.

INVESTITIONSKOSTEN

Auch die hohen Kosten, die mit der Einführung neuer digitaler Technologien und automatisierter Tools einhergehen, können vor allem für kleine und mittelständische Unternehmen eine Herausforderung sein und sind oftmals der Grund für Digitalisierungsstopps.

Die Rolle elektronischer Signaturen für den Digitalisierungsfortschritt

Eine der entscheidenden Technologien, die Unternehmen dabei unterstützen können, ihre Digitalisierungsziele zu erreichen, sind elektronische Signaturen. Laut einer forsa-Studie im Auftrag von Tresorit hat knapp die Hälfte (44%) der Unternehmen bereits elektronische Signaturen bei sich integriert. 77% der teilnehmenden Unternehmen gaben an, dass die Bedeutung von E-Signaturen in ihrem Unternehmen in Zukunft steigen wird. In einer Zeit, in der Effizienz, Geschwindigkeit und Sicherheit entscheidend für den Erfolg eines Unternehmens sind, bieten elektronische Signaturen eine effektive Lösung, um traditionelle papierbasierte Prozesse zu optimieren und die Transformation zu digitalen Arbeitsabläufen zu beschleunigen.

Vorteile elektronischer Signaturen

ZEIT- UND KOSTENERSPARNIS

Durch den Einsatz elektronischer Signaturen können Unternehmen langwierige Prozesse beschleunigen, indem Dokumente innerhalb von Sekunden statt Tagen oder Wochen unterzeichnet werden können. Die Zeit, die für den physischen Versand und die händische Unterzeichnung von Dokumenten benötigt wird, entfällt weitgehend. Dies führt zu erheblichen Zeit- und Kostenersparnissen, da Mitarbeitende ihre Zeit für produktivere Aufgaben einsetzen können, anstatt sie in administrative Abläufe zu investieren.

FÖRDERUNG VON NACHHALTIGKEITSZIELEN

Elektronische Signaturen unterstützen auch bei der Erreichung unternehmerischer Nachhaltigkeitsziele. Noch immer werden von deutschen Unternehmen mehr als 10 Milliarden Briefe pro Jahr verschickt. Der Einsatz elektronischer Signaturen kann also eine erhebliche Menge Papier einsparen und so zur Verringerung des ökologischen Fußabdrucks beitragen.

VERBESSERTE KUND:INNENINTERAKTION

Elektronische Signaturen ermöglichen durch die Prozessdigitalisierung eine erhebliche Verbesserung der Kund:inneninteraktion. Verträge, Vereinbarungen und andere wichtige Dokumente können in Echtzeit von überall unterzeichnet werden, was zu einer schnelleren Abwicklung von Geschäftsprozessen und der Verbesserung der Kund:innenerfahrung führt.

EFFIZIENTERES DOKUMENTENMANAGEMENT

Dokumente unterliegen Aufbewahrungspflichten. Die Archivierung und Lagerung in physischer Form sind mit viel Zeit- und Kostenaufwand verbunden. Benötigte Informationen später noch einmal aus Papierstapeln und Aktenhaufen herauszusuchen, kostet in der Regel ebenfalls viel Zeit. Elektronisch signierte Dokumente können ganz einfach digital abgelegt und später schnell wiedergefunden werden.

COMPLIANCE UND RECHTLICHE SICHERHEIT

Ein weiterer entscheidender Aspekt ist die Einhaltung gesetzlicher Vorschriften und Compliance-Standards. Es gibt elektronische Signaturen verschiedener Stärke, die unterschiedliche regulatorische Anforderungen erfüllen. Sie bieten Unternehmen und ihren Kund:innen die Gewissheit, dass ihre digitalen Transaktionen rechtlich bindend und vollständig durchsetzbar sind. Die stärkste Form der elektronischen Unterschrift ist die qualifizierte elektronische Signatur (QES), die rechtlich betrachtet die gleiche Sicherheit wie die händische Unterschrift erfüllt.

02

Deep Dive elektronische Signaturen

Das Feld der elektronischen Signaturen ist groß und komplex. Auf den folgenden Seiten bringen wir Licht ins Dunkel und klären, was eine elektronische Signatur ausmacht, welche Signaturformen es eigentlich gibt und wie der regulatorische Rahmen aussieht. Als sicherste Form der elektronischen Signaturen werden wir einen verstärkten Blick auf die qualifizierte elektronische Signatur (QES), ihre Anwendungsbereiche und das Thema „Identitätsfeststellung“ in diesem Kontext werfen. Außerdem geben wir Ihnen eine Checkliste zur erfolgreichen Implementierung einer QES an die Hand.

Nect

Was ist eine elektronische Signatur?

Eine elektronische Signatur ist ein elektronisches Äquivalent zu einer handschriftlichen Unterschrift auf einem physischen Dokument. Sie dient dazu, die Authentizität und Integrität eines elektronischen Dokuments oder einer elektronischen Nachricht zu gewährleisten. Im Wesentlichen bestätigt eine elektronische Signatur die Zustimmung der unterzeichnenden Person zu den im Dokument enthaltenen Inhalten.

Rechtlicher Rahmen für elektronische Signaturen in Deutschland und Europa

In Deutschland und der Europäischen Union sind elektronische Signaturen rechtlich anerkannt und unterliegen bestimmten Regulierungen und Standards, um ihre Wirksamkeit und Rechtsverbindlichkeit sicherzustellen. Die rechtlichen Rahmenbedingungen für elektronische Signaturen sind im Wesentlichen durch die eIDAS-Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt in der gesamten EU harmonisiert. Die Vorgaben der Verordnung sind für alle EU-Mitgliedsstaaten verpflichtend und gelten vor kollidierenden Gesetzen auf nationaler Ebene.

Die eIDAS-Verordnung stellt sicher, dass die elektronische Signatur vor EU-Gerichten als Beweismittel dient. Die Entscheidung über Einsatz und Wahl der Signaturform für formfreie Dokumente wird jedoch den EU-Ländern überlassen.
In der eIDAS-Verordnung werden drei Signaturtypen hinsichtlich gesetzlicher Schriftformerfordernis und Haftungsrisiko eingeordnet.

Signaturtypen laut eIDAS

1.EINFACHE ELEKTRONISCHE SIGNATUR (EES):

Die einfache elektronische Signatur ist die grundlegendste Form der elektronischen Unterschrift. Sie kann in Form eines eingescannten Bildes einer handschriftlichen Signatur oder einer digitalen Eingabe, zum Beispiel durch Klicken auf „Akzeptieren“ in einem digitalen Dokument, vorliegen. Diese Art von Signatur bietet die geringste Sicherheit, da sie relativ einfach durch Fälschung verändert werden kann.

Beispiele für Anwendungsgebiete der EES:

- Kostenvoranschläge
- Interne Dokumente wie Urlaubsanträge oder Spesenabrechnungen
- Datenschutzerklärungen
- Kaufverträge beweglicher Güter oder Dienstleistungen

2. FORTGESCHRITTENE ELEKTRONISCHE SIGNATUR (FES):

Die fortgeschrittene elektronische Signatur bietet ein höheres Maß an Sicherheit und Vertrauen als die EES. Sie erfordert spezielle Technologien, die sicherstellen, dass die Signatur eindeutig mit dem Unterzeichner verbunden ist und Veränderungen am Dokument nach der Unterzeichnung nachvollziehbar sind. Eine FES kann beispielsweise durch kryptografische Techniken wie Public-Key-Infrastruktur (PKI) erstellt werden.

Beispiele für Anwendungsgebiete der FES:

- Unbefristete Mietverträge
- Personenversicherungen wie Unfallversicherung
- Kooperationsvereinbarungen
- Bescheinigungen wie Gesundheitszeugnisse

Haben Sie das gewusst?

Die fortgeschrittene elektronische Signatur (FES) ist die zweitstärkste Form der elektronischen Signaturen gemäß eIDAS. Laut Artikel 26 der eIDAS-Verordnung muss eine FES die folgenden Anforderungen erfüllen:

(a) Sie ist eindeutig dem Unterzeichner zugeordnet.
(b) Sie ermöglicht die Identifizierung des Unterzeichners.
(c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.
(d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Viele Signaturanbieter erfüllen diese Bedingungen, indem das Zertifikat für die FES im Namen des Anbieters und nicht der unterzeichnenden Person ausgestellt wird. Der "visuell" sichtbare Name in der Unterschrift weicht vom Namen im Zertifikat ab. So ist zwar der Anbieter identifizierbar, nicht aber die eigentlich unterschreibende Person. Diese wird häufig lediglich per E-Mail "identifiziert".

Dieses Vorgehen ist angreifbar, da durch eine E-Mail-Adresse nicht uneingeschränkt sichergestellt werden kann, dass die berechtigte Person die Signatur auslöst. Muss man zu einem späteren Zeitpunkt beweisen, dass wirklich die richtige Person unterschrieben hat, muss der Weg über den Anbieter gehen, sofern dieser, z. B. nach einigen Jahren, noch existiert. Der Anbieter trägt dann die Beweislast und kann versuchen zu beweisen, welche Person wirklich unterschrieben hat. Insofern sollte auch bei einer FES eine niederschwellige Identitätsfeststellung vorgenommen werden und darauf geachtet werden, dass das Zertifikat für die FES für den:die Nutzer:in und nicht für den Anbieter ausgestellt wird.

Wir empfehlen daher, für alle Anwendungsfälle die qualifizierte elektronische Signatur (QES), auf die wir im Folgenden eingehen, einzusetzen. Diese bietet die höchste Beweiskraft und belegt eindeutig die unterschreibende Person. Darüber hinaus ist die QES bei einigen Anbietern ebenso kostengünstig und nutzungsfreundlich wie die FES.

3. Qualifizierte elektronische Signatur (QES):

Die qualifizierte elektronische Signatur ist die höchste Stufe der elektronischen Signatur und gemäß eIDAS der einzige elektronische Signaturtyp, der rechtlich die gleichwertige Sicherheit zur händischen Unterschrift aufweist. Eine QES wird durch einen qualifizierten Anbieter von Vertrauensdiensten ausgestellt und basiert auf einem qualifizierten Zertifikat, das die Identität der unterzeichnenden Person eindeutig bestätigt. Somit ist eine QES sehr schwierig zu fälschen und bietet das höchste Maß an Sicherheit und Vertrauen in einem elektronischen Dokument.

Beispiele für Anwendungsgebiete der QES:

- Arbeitsverträge
- Verbraucherdarlehensverträge
- Befristete Mietverträge
- Patientenverfügungen

Bürokratieentlastungsgesetz IV – mehr Raum für elektronische Signaturen

Im Januar 2024 wurde der Referentenentwurf des Bundesministeriums der Justiz über das Bürokratienenlastungsgesetzt IV (BEG IV) veröffentlicht. Das BEG IV soll die administrative Belastung für Bürger:innen, Unternehmen und die öffentliche Verwaltung reduzieren. Das BEG IV ist Teil eines größeren Pakets zur Bürokratieabrechnung der Bundesregierung. Das Gesamtpaket zielt darauf ab, die Bürokratiekosten in Deutschland bis zum Jahr 2025 um 10 Milliarden Euro zu senken.

Mit Beschluss des BEG IV sollen auch Unterschriftsprozesse digitalisiert und vereinfacht werden. Unter anderem soll die Schriftformerfordernis, je nach Anwendungsfall, aufgehoben oder herabgesetzt werden. Dokumente, die bisher händisch unterzeichnet werden mussten, z. B. unbefristete Arbeitsverträge, können somit dann per qualifizierter elektronischer Signatur unterschrieben werden.

Fortgeschrittene vs. qualifizierte elektronische Signatur

Die fortgeschrittene und die qualifizierte elektronische Signatur bieten ein höheres Maß an Sicherheit und Vertrauen als eine einfache elektronische Signatur. Doch was unterscheidet die beiden Signaturtypen?

Vorteile	FES	QES
Beweiskraft	hoch	maximal
Rechtsgültigkeit	✓	✓
Beweislastumkehr*	✗	✓
Ausgabe von zertifizierten Anbietern von Vertrauensdiensten	✗	✓
Erfüllt Anforderung an Schriftform	✗	✓
Risikominimierung	✗	✓

*Wenn die Gültigkeit einer FES in Frage gestellt wird, liegt die Beweislast beim Signierer. Die Beweislast der QES liegt bei der Partei, die die Gültigkeit der qualifizierten Signatur anzweifelt.

Die QES als Rundum-Versicherung

Für einige Anwendungsfälle, wie Arbeitsverträge oder Kreditabschlüsse, ist eine qualifizierte elektronische Signatur schon von Rechtswegen erforderlich. Doch auch für andere Branchen und Use Cases ist sie aufgrund der hohen Sicherheit empfehlenswert. Denn: Die Beweislast liegt bei der Partei, die die Gültigkeit der Unterschrift anzweifelt. Damit sind Sie, egal bei welchem Dokument oder für welche Transaktion, immer auf der sicheren Seite und sichern sich mit dem elektronischen Pendant zur händischen Unterschrift bestmöglich ab. Aufgrund der Stärke und der breiten Einsatzmöglichkeit der QES werden wir im weiteren Verlauf des Whitepapers einen Fokus auf die QES legen.

Beeinträchtigt eine QES das Kund:innenerlebnis?

Eine QES erfüllt ein sehr hohes Sicherheitsniveau und umfasst daher mehrere Sicherheitsprüfungen im Prozess. Dennoch kann dieser absolut nutzer:innenfreundlich gestaltet werden. Durch den Einsatz von künstlicher Intelligenz beispielsweise können der Identifizierungs- und Signaturprozess vollautomatisiert werden, sodass Kund:innen den Vorgang intuitiv und in wenigen Minuten durchlaufen können – bei höchster Sicherheit.

Anwendungsbereiche für QES nach Branchen

Banken	• Kreditverträge • Kontoeröffnungsformulare • Investmentverträge
Versicherungen	• Versicherungspolicen • Schadensmeldungen • Verträge für Lebensversicherungen
Personalabteilungen & HR Dienstleister	• Befristete und unbefristete Arbeitsverträge • Vereinbarung zur Elternzeit • Aufhebungsverträge
Verwaltung	• Steuererklärungen • Anträge • KFZ An- und Ummeldungen
Vermietungssektor	• Mietverträge • Zustimmung zur Bonitätsprüfung • Autovermietungsverträge

Identitätsfeststellung bei der QES

Die Personenidentifizierung ist ein integraler Bestandteil der qualifizierten elektronischen Signatur und stellt sicher, dass die Signatur tatsächlich von der Person stammt, die sie vorgibt zu sein. Nur durch diese Identifizierung kann die QES ihr hohes Maß an Sicherheit und den rechtskonformen Ersatz der händischen Unterschrift gewährleisten.

Wichtig: Jede:r Nutzer:in hat individuelle Bedürfnisse, Hintergründe und Ausweisdokumente. Um die QES möglichst vielen Menschen zugänglich zu machen, sollte bei der Wahl der Identifizierungslösung darauf geachtet werden, dass Nutzer:innen eine möglichst große Bandbreite an Identifizierungsverfahren zur Verfügung gestellt wird.

Welche Verfahren können zur Identitätsprüfung genutzt werden?

- **Automatisiertes Video-Ident:** vollautomatisierte Identifizierung mit Selfie-Video, z. B. per App
- **Video-Ident mit Call-Service-Agent:in:** Identifizierung per Video-Chat mit einem Mitarbeitenden des Vertrauensdienstanbieters
- **Online-Ausweis:** Identifizierung mit der Onlineausweis-Funktion des deutschen Personalausweises (eID) via NFC-Chip und PIN
- **ePass-Funktion:** Identifizierung mit der international verfügbaren ePass-Funktion per NFC-Chip und Selfie-Video

Einsatz von qualifizierten elektronischen Signaturen für juristische Personen

Neben der Nutzung durch natürliche Personen ermöglicht die eIDAS-Verordnung auch juristischen Personen, wie Unternehmen und Behörden, die Vorteile qualifizierter elektronischer Signaturen (QES) zu nutzen.

Vorgaben für die qualifizierte elektronische Signatur von juristischen Personen

Verantwortliche Person: Die Nutzung der QES durch juristische Personen erfordert die Benennung einer verantwortlichen Person, die für die Verwaltung der Zertifikate und die Sicherstellung der Einhaltung der Sicherheitsanforderungen zuständig ist.

Identitätsprüfung: Wie bei der QES für natürliche Personen, muss auch bei juristischen Personen vorab die Identität überprüft werden. In diesem Fall muss hierbei sichergestellt werden, dass die Person, die im Namen des Unternehmens unterschriftsberechtigt ist, tatsächlich auch im Handelregister steht. Daher wird während des Identifizierungsvorgangs zusätzlich ein Handelsregisterabgleich durchgeführt.

Technische Anforderungen: Die QES für juristische Personen muss, ebenso wie die für natürliche Personen, den technischen Anforderungen der eIDAS-Verordnung entsprechen. Dazu gehört die Verwendung von sicheren Signaturerstellungseinheiten (z.B. Signaturkarten) und die Einhaltung von kryptographischen Standards.

Implementierung elektronischer Signaturen

Die Implementierung elektronischer Signaturen in Unternehmensprozesse kann auf verschiedene Weise erfolgen, abhängig von den individuellen Anforderungen und der IT-Infrastruktur des Unternehmens sowie dem Signaturtyp. Wir schauen uns nachfolgend die Integration der qualifizierten elektronischen Signatur genauer an. Da die qualifizierte elektronische Signatur eine Reihe an Sicherheitsanforderungen erfüllen muss, ist die Integration etwas komplexer als z. B. die der einfachen elektronischen Signatur. Es gibt verschiedene Optionen, um eine QES in die Unternehmensprozesse zu integrieren.

Eigenimplementierung

Die Eigenimplementierung einer QES bietet Unternehmen die maximale Flexibilität und Kontrolle. Sie erfordert jedoch umfangreiches technisches Know-how, Ressourcen und die Bereitschaft, Verantwortung für die Sicherheit und Zertifizierung der Lösung zu tragen. Um eine QES-Lösung selbst zu implementieren, ist tiefgreifendes Wissen in den Bereichen Kryptografie, PKI (Public Key Infrastructure) und Softwaredesign nötig. Darüber hinaus sind Zeit, Budget und personelle Ressourcen für die Entwicklung, Wartung und Weiterentwicklung der Lösung erforderlich.

PROZESSÜBERBLICK

1. Anforderungsanalyse

Klare Definition der Anwendungsfälle, Nutzergruppen, Sicherheitsanforderungen und Integrationsszenarien

2. Komponentenauswahl

Auswahl geeigneter QES-Komponenten von Drittanbietern (z.B. Signaturbibliothek, TSP-Anbindung)

3. Entwicklung

Implementierung der Signaturfunktionalität unter Berücksichtigung der spezifischen Anforderungen des Unternehmens

4. Integration

Anbindung der QES-Lösung an bestehende Dokumenten- und Workflow-Systeme

5. Sicherheit und Compliance

Implementierung umfassender Sicherheitsmaßnahmen und Sicherstellen der Einhaltung rechtlicher Vorgaben

6. Zertifizierung

Beantragung und Erlangung einer QES-Zertifizierung durch eine anerkannte Zertifizierungsstelle

7. Test und Wartung

Durchführung umfassender Tests und Sicherstellen der kontinuierlichen Wartung und Aktualisierung der Lösung

Implementierung mit Signatur-Dienstleister

Die Implementierung elektronischer Signaturen über einen Signatur-Dienstleister bietet Unternehmen eine komfortable und kostengünstige Möglichkeit, die Vorteile der elektronischen Signatur in ihre Prozesse zu integrieren. Wichtig ist, dass das Unternehmen, dass die QES implementieren möchte, die entsprechenden technischen Voraussetzungen, z. B. eine API (Application Programming Interface), erfüllt und Ressourcen wie eigene Entwickler:innen, die die Schnittstelle des Signatur-Dienstleisters im eigenen System integrieren können, zur Verfügung stellen kann.

PROZESSÜBERBLICK

1. Dienstleister-Auswahl

Recherche und Vergleich verschiedener Anbieter, um einen Dienstleister zu finden, der zu den Anforderungen des Unternehmens passt

2. Technische Anbindung

Implementierung der Schnittstelle zwischen den Systemen des Unternehmens und dem Dienstleister (z. B. über eine API).

3. Prozessaufbau

Definition durch Umsetzung von prozessualen Schnittstellen zu den Nutzer:innen (z. B. Aufbau von Fallback-Prozessen)

4. Test und Einführung

Durchführung von Testanwendungen, bevor die QES-Lösung im produktiven Umfeld eingeführt wird.

Exkurs

Was ist eine API?

Die API (Application Programming Interface) ist eine Schnittstelle, die es unabhängigen Anwendungen ermöglicht, in Echtzeit miteinander zu kommunizieren und den Austausch von Daten beschleunigt und vereinfacht. Eine API besteht aus einem Satz von Definitionen und Protokollen, die Entwickler:innen zur Erstellung einer Anwendungssoftware oder zur Interaktion mit einem externen System verwenden können. Die API dient also dem Datenaustausch zwischen dem Backend des Signatur-Dienstleisters und dem System des Auftraggebers.

API vs. Signaturplattform

Ein Signaturdienstleister kann nicht nur über eine Backend-Schnittstelle, also eine API, sondern auch in Form einer Signaturplattform integriert werden. Während die Signaturplattform ein externes Angebot darstellt, das nicht direkt in die IT-Umgebung des Unternehmens eingebunden werden kann, ermöglicht die Integration einer QES über eine API die direkte Implementierung in der eigenen IT-Infrastruktur. Mitarbeitende können so in der gewohnten IT-Umgebung arbeiten, ohne für eine QES in ein externes Interface wechseln zu müssen. Darüber hinaus hat die API-Integration weitere Vorteile.

Ein Vergleich

Vorteile	API-Integration	Signaturplattform
Flexibilität	Bietet hohe Flexibilität bei der Integration in vorhandene Systeme und Workflows. Entwickler:innen können die Signaturlösung direkt in die Unternehmensanwendungen einbetten.	Bietet weniger Flexibilität, da die Plattform in ihrer eigenen Infrastruktur läuft. Einige Plattformen bieten (begrenzte) Möglichkeiten, auf das System des Unternehmens angepasst zu werden.
Integration mit bestehenden Systemen	Ermöglicht eine nahtlose Integration in vorhandene Unternehmenssysteme, wie z. B. CRM, ERP usw.	Erfordert die Nutzung eines externen Tools, das interne Prozesse untebricht.
Zugriff auf Daten	Datenzugriff funktioniert über das gewohnte Dokumententool des Unternehmens.	Damit auf Daten zugegriffen werden kann, ist eine weitere, externe Accountverwaltung notwendig.
Kosten	Ist potenziell kosteneffizienter sein, da nur die tatsächlich genutzten Funktionen bezahlt werden müssen.	Plattformen arbeiten meist mit einem Abonnementmodell. Die Kosten hierbei können stark variieren und es können zusätzliche Gebühren für spezielle Funktionen anfallen.
Entwicklungszeit	Die Entwicklungszeit kann je nach Komplexität der Integration variieren, bietet jedoch die Möglichkeit, schnell eine maßgeschneiderte Lösung bereitzustellen.	Die Implementierung funktioniert in der Regel recht schnell, da viele Funktionen bereits vorgefertigt, dadurch aber auch weniger flexibel sind.

Vorteile der QES-Implementierung über einen Signatur-Dienstleister

Neben den besser kalkulierbaren Kosten und der flexiblen Skalierung sind vor allem der geringe IT- und Wartungsaufwand sowie die Sicherstellung der rechtlichen Anforderungen die größten Vorteile bei der Zusammenarbeit mit einem Signatur-Dienstleister. Rechtliche Grundlagen wie Zertifizierungen, Audits und die Integration von Vertrauensdiensteanbietern werden vom Dienstleister sichergestellt und regelmäßig geupdatet. Bei einer Eigenimplementierung müssen Unternehmen diese Parameter selbst erarbeiten und dafür erhebliche finanzielle und zeitliche Ressourcen aufwenden.

Checkliste: Implementierung einer QES

- [ ] Definition von Anwendungsfällen und Nutzer:innengruppen
- [ ] Bestimmung des zu erfüllenden rechtlichen Rahmens
- [ ] Definition benötigter Identifizierungsverfahren, um die bestimmten Nutzer:innengruppen abzuholen
- [ ] Entscheidung für eine Eigenimplementierung oder einen Signatur-Dienstleister
- [ ] Bestimmung benötigter und zur Verfügung stehender Ressourcen
- [ ] Prüfung der eigenen IT-Systeme auf Kompatibilität
- [ ] Aufsetzen der Test-Umgebung
- [ ] Adaption in die produktive Umgebung

Zusätzlich bei Eigenimplementierung:

- [ ] Anpassung der IT-Infrastruktur für die Einbindung der QES
- [ ] Prüfung benötigter Zertifikate und Audits und entsprechende Anpassung interner Prozesse
- [ ] Recherche und Bestimmung eines Vertrauensdiensteanbieters
- [ ] Aufsetzen eines Support Centers/Help Desks für Nutzer:innen
- [ ] Sicherstellung einer Langzeitarchivierung signierter Dokumente
- [ ] Prüfung, Etablierung und Umsetzung regelmäßiger Wartungen und Sicherheitsaudits

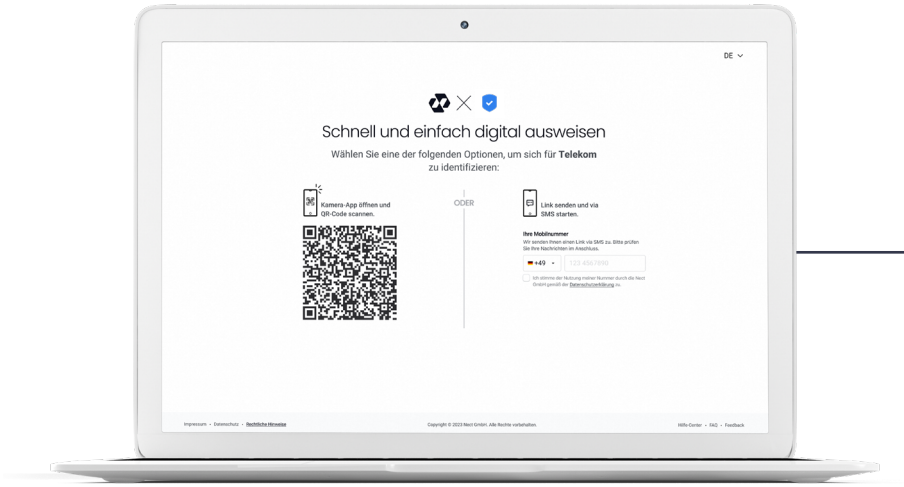
03

Die qualifizierte elektronische Signatur in der Praxis

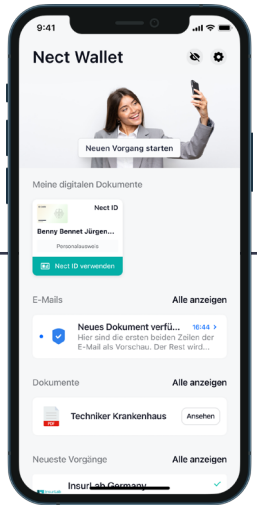
Wie kann die QES nun also im Gebrauch aussehen?
Da eine QES eine eindeutige Identifizierung der unterzeichnenden Person erfordert, ist die Identifizierung immer der erste Schritt. Diese kann separat vom eigentlichen Signaturprozess umgesetzt werden, wird aber im besten Fall in den Signaturprozess integriert, sodass für Nutzer:innen kein Medienbruch entsteht.

Nect

Beispiel für eine QES mit vollautomatisiertem Video-Ident

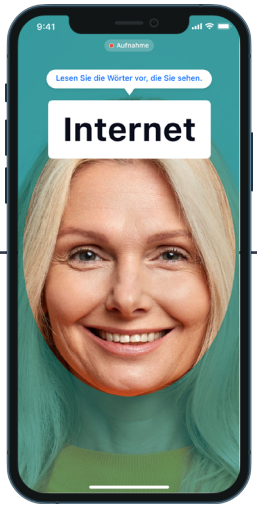


1. Einstieg in den Prozess über QR-Code oder Link per SMS



2. Start des Prozesses in der Nect Wallet App

3. Video des Ausweisdokuments



4. Selfie-Video und zwei Wörter vorlesen

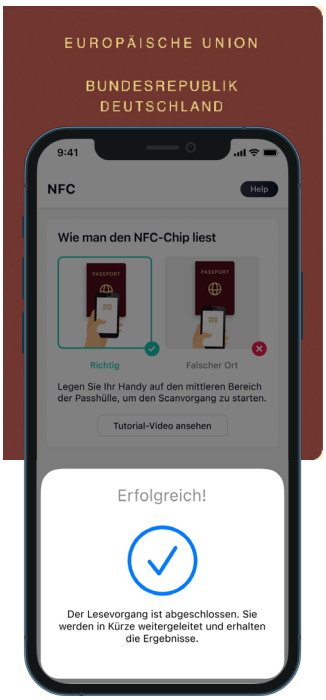
5. Dokument mit einem Klick elektronisch unterzeichnen

Zielgruppenreichweite der QES steigern

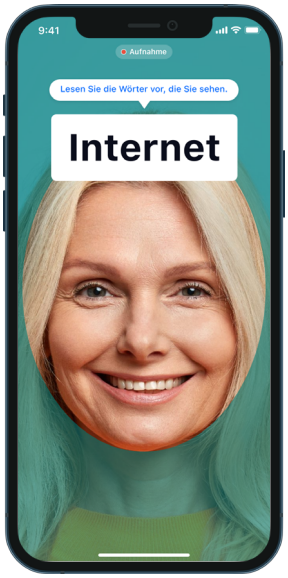
Nutzer:innen haben unterschiedliche Bedürfnisse, diverse Hintergründe und somit auch verschiedene Ausweisdokumente. Um möglichst vielen Menschen den Zugang zu einer QES zu ermöglichen, ist es wichtig, im Prozess eine möglichst große Bandbreite an Ausweisdokumenten auslesen zu können. Dazu gehören u. a. Personalausweise, Reisepässe und Aufenthaltstitel.

Eine besonders sichere und komfortable Ausweisoption ist die ePass-Funktion. Sie ist seit 2021 für alle EU-Länder verpflichtend und automatisch auf europäischen Personalausweisen, weltweiten elektronischen Reisepässen sowie Aufenthaltstiteln integriert. Mit der ePass-Funktion können sich also Menschen zahlreicher Staatsangehörigkeiten durch das Auslesen der NFC-Schnittstelle ausweisen und so eine QES durchführen.

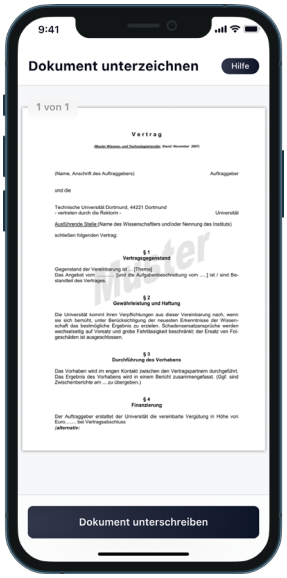
1. Video des Ausweisdokuments



2. Auslesen der NFC-Schnittstelle



3. Selfie-Video und zwei Wörter vorlesen

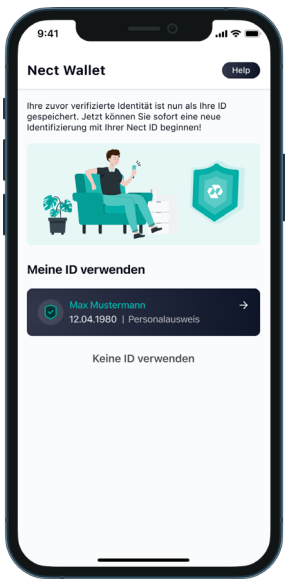


4. Dokument mit einem Klick elektronisch unterzeichnen

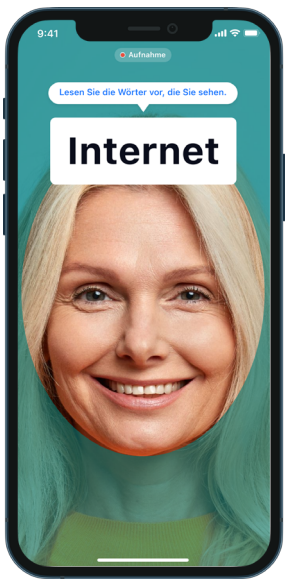
QES mit bester Usability durch ID Wallet

Die eIDAS 2.0-Verordnung soll die EU-Mitgliedsstaaten zukünftig dazu verpflichten ihren Bürger:innen eine Europa weit gültige ID Wallet für die digitale Identität bereitzustellen. ID Wallets haben einen entscheidenden Vorteil: Sie ermöglichen die sichere Ablage und die Wiederverwendung des abgelegten Ausweisdokuments. Dadurch wird das digitale Ausweisen und Unterzeichnen noch einfacher und schneller.

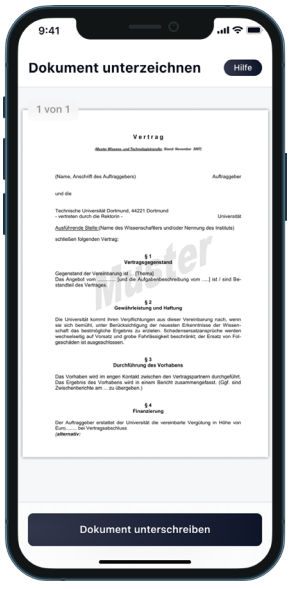
In der Nect Wallet z. B. kann die digitale Identität durch ein simples Selfie-Video, also per Gesichtserkennung, wiederverwendet werden. So dauert die Identifizierung für die QES nur wenige Sekunden und das Dokument ist noch schneller unterzeichnet.



1. Auswählen der abgelegten Identität



2. Selfie-Video und zwei Wörter vorlesen



3. Dokument mit einem Klick elektronisch unterzeichnen

Zusammenfassung

Elektronische Signaturen können einen wertvollen Beitrag zur Prozessdigitalisierung in Unternehmen leisten. Vor allem die qualifizierte elektronische Signatur bietet ein sehr hohes Maß an Sicherheit, das sie zur besten Wahl unter den elektronischen Signaturen macht. Dank regulatorischer Anpassungen, z. B. durch das Bürokratieentlastungsgesetz IV, werden qualifizierte elektronische Signaturen für immer mehr Anwendungsfälle zulässig.

Nutzen Sie elektronische Signaturen als Effizienz-Booster für Ihre Prozesse und profitieren Sie von Kosten- und Zeiteinsparungen, einer erhöhten Zufriedenheitsrate bei Ihren Kund:innen und der Verbesserung Ihrer Nachhaltigkeitsziele.

Sie suchen einen passenden Signatur-Dienstleister, um elekronische Signaturen in Ihre Prozesse zu integrieren? Mit Nect setzen Sie auf eine All-in-One-Lösung für die qualifizierte elektronische Signatur, die die Identifizierung und die Signatur in einem Prozess abbildet. Um möglichst vielen Menschen die QES über die Nect Wallet zugänglich zu machen, stellt Nect alle gängigen Identifizierungsmethoden zur Verfügung. Darüber hinaus können bereits identifizierte Nutzer:innen ihre abgelegte Identität per Gesichtserkennung wiederverwenden und so Dokumente binnen Sekunden digital unterschreiben. Die QES von Nect ist ebenso kostengünstig und nutzungsfreundlich wie eine fortgeschrittene elektronische Signatur (FES), bietet aber das höchste Maß an Sicherheit.

Sie möchten die QES in der Nect Wallet kennenlernen und persönlich testen? Vereinbaren Sie noch heute Ihren Demo-Termin unter sales@nect.com oder nect.com.

Quellenverzeichnis

Digitalisierung der Wirtschaft, Bitkom e.V., 2025
Lünendonk®-Studie, Lünendonk® und Telekom, 2025
Forsa Studie, im Auftrag von Tresorit, 2023

Über Nect

Nect ist einer der führenden Anbieter für digitale, KI-basierte Identifizierungs- und Signaturlösungen in Deutschland. Die patentierte Nect Technologie zeichnet sich durch die Verbindung sehr hoher Sicherheitsvorgaben mit intuitiver Nutzungsfreundlichkeit aus. Alle Lösungen des Unternehmens werden über die unternehmenseigene App, die Nect Wallet, zur Verfügung gestellt, die bis heute rund vierzehn Millionen Nutzende zählt.