

Integrität trifft Effizienz.

T-TeleSec Public Key Service – die rechtsverbindliche elektronische Signatur von T-Systems.



Elektronisch besser unterzeichnen.

Unternehmen wie auch öffentliche Institutionen setzen vermehrt auf elektronische, automatisierte Abläufe. Doch was geschieht beim Umgang mit elektronisch erstellten Bescheiden, Genehmigungen, Verträgen, Nachweisen oder rechtsverbindlicher Korrespondenz? Überall, wo der Gesetzgeber die handschriftliche Unterschrift auf einem Papierdokument vorsieht, wird der Arbeitsfluss unterbrochen. Das kostet Zeit und Geld – von den Produktivitätseinbußen ganz zu schweigen. Die qualifizierte elektronische Signatur nach dem Deutschen Signaturgesetz (SigG) ersetzt den manuellen Vorgang und wirkt sich messbar auf die Prozesseffizienz aus. Denn die elektronische Signatur ist nicht nur der manuellen Unterschrift rechtlich gleichgestellt, sondern sie ist ihr auch in vielen Punkten überlegen. Vorausgesetzt, Ihr Unternehmen hat den richtigen Partner mit einem Ende-zu-Ende-Angebot – vom Trustcenter bis zur individuellen Prozessintegration: T-Systems.

Ihr T-TeleSec Public Key.

Mit dem zunehmenden Einsatz von Informationstechnologie im Unternehmensalltag wachsen auch die Sicherheitsrisiken. Jeglicher Datenaustausch in internen und öffentlichen Netzen ist gefährdet. Ist der vermeintliche Absender auch der, für den er sich ausgibt? Wer garantiert, dass die Daten unterwegs nicht manipuliert werden? T-TeleSec Public Key Service schafft Rechts- und Beweissicherheit bei der papierlosen Kommunikation in jeder Branche. Denn mit Hilfe der elektronischen Signatur ist zweifelsfrei feststellbar, wer ein Dokument erstellt hat und dass dieses Dokument danach nicht verändert wurde. Darüber hinaus können Sie Bezahlvorgänge im E-Commerce absichern.

Ihre Vorteile.

- Unterschrift für die rechtsgültige Übertragung und Archivierung von elektronischen Dokumenten, z. B. von Verträgen
- Durchgängige elektronische Bearbeitung von Bestellvorgängen
- Stellt dauerhaft die Datenintegrität sicher
- Sorgt für Manipulationssicherheit
- Für alle Branchen geeignet
- Steigerung der Effizienz in Prozessen
- Einsparung von Kopie- und Portogebühren
- Prüfung von Zertifikaten
- 24-h-Sperrservice für die Chipkarte
- Nach dreimaliger Falscheingabe der PIN Entsperrung über PIN2

Die Unterschrift, die alles kann: Verträge unterzeichnen, Bezahlvorgänge im E-Commerce sichern oder Datensätze vor Manipulation schützen – T-TeleSec Public Key Service!

Alles komplett: Ihr Chip, PIN und Zertifikat.

Ihre elektronische Signatur erzeugen Sie mit Ihrer persönlichen Chip-Karte (Krypto-Chip-Karte) plus PIN. Damit die Signatur auch zweifelsfrei Ihrer Person zugeordnet werden kann, brauchen Sie zusätzlich einen digitalen Ausweis (Zertifikat). Diesen beantragen Sie einfach, z. B. über das Online-Portal bei T-Systems oder über einen firmeninternen Sammelvorgang. Anschließend lassen Sie sich in einer Postfiliale, in einer unserer Registrierungsstellen oder beim Notar mit Ihrem gültigen Personalausweis registrieren. Nur natürliche Personen können diesen Antrag stellen. Das Trust Center der Deutschen Telekom stellt daraufhin das Zertifikat, die persönliche Chip-Karte und den Kartenleser bereit. Vorher werden im Trust Center die geheimen Signaturdaten generiert, im Karten-Chip unlesbar gespeichert und mit Ihren persönlichen Daten zum Zertifikat verbunden. Dieses wird entweder auf der Chip-Karte gespeichert und Ihnen per Post zugestellt oder per E-Mail zum Nachladen auf schon ausgelieferte Chip-Karten bereitgestellt. Mit Ihrer Signatur-Chip-Karte, einem PC, Chip-Kartenleser und der entsprechenden Software sind jetzt alle Voraussetzungen gegeben, Daten elektronisch zu signieren und auf Wunsch zusätzlich zu verschlüsseln. Je nach Bedarf bestellen Sie den Chip-Kartenleser und die Software mit – oder nutzen die in der Geschäftsanwendung Ihres Unternehmens integrierte Software.

Noch sicherer: mit dem Teilnehmerverzeichnis.

Alle digitalen Ausweise (Zertifikate) nehmen wir in ein öffentliches und für jedermann online zugängliches Verzeichnis auf – derzeit befinden sich rund 24.000 Zertifikate im Verzeichnis. Damit erhalten Sie zusätzliche Sicherheit: Jeder Empfänger kann prüfen, ob das zur Unterschrift benutzte Zertifikat noch gültig ist. Falls die Chip-Karte verloren geht, können Sie Ihr Zertifikat sofort über unseren 24-Stunden-Service sperren. Gleichzeitig ist es mit dem digitalen Ausweis möglich, ein Dokument so zu verschlüsseln, dass es nur der Besitzer der zugehörigen Chip-Karte öffnen und lesen kann. Der Schlüssel für diesen Besitzer steht ebenfalls im zentralen Verzeichnis zum Abruf bereit.

Kontakt:

T-Systems International GmbH
Günter Oppold
E-Mail: security@t-systems.com
Internet: www.telesec.de

Alles integriert: von Nachweis bis Kantine.

Mit der elektronischen Signatur und Ihrem Full-Service-Partner T-Systems erhalten Sie vielfältige Möglichkeiten, den Unterzeichnungsvorgang gleich in Ihre Arbeitsabläufe einzubinden. Als Systemintegrator sorgen wir dafür, dass Sie z. B. Nachweise oder Mahnungen aus der Applikation heraus automatisch elektronisch versenden und diese anschließend archivieren können. Wir binden den Signaturvorgang nahtlos in Ihre Geschäftsanwendungen ein. Gerne realisieren wir individuelle branchenspezifische Funktionalitäten. Darüber hinaus können wir Ihre Chip-Karte so gestalten, dass Sie diese zusätzlich für andere Abläufe verwenden können, z. B. für das Erfassen von Arbeitszeiten oder das Bezahlen in der Kantine. Sie sehen, T-TeleSec Public Key Service lässt sich mit anderen Lösungen ideal kombinieren. Auch im Rahmen einer Custom-PKI, die entsprechend den Unternehmensanforderungen erstellt wurde. Unsere Spezialisten beraten Sie gerne.

Langjährige Kompetenz: das Trust Center der Deutschen Telekom.

Seit 1994 betreibt die Deutsche Telekom AG ein Trust Center, das 1998 als erstes Trust Center bundesweit die Genehmigung zur Ausgabe von Zertifikaten für die elektronische Signatur gemäß dem Deutschen Signaturgesetz (SigG) durch die Regulierungsbehörde für Telekommunikation und Post (heute Bundesnetzagentur) erhielt. Mit dieser Genehmigung wurde Anfang 1999 der Public Key Service (PKS), ein Service im Sinne des SigG von 1997 etabliert. T-Systems betreibt seit 2001 das akkreditierte Trust Center in einem Hochsicherheitsrechenzentrum.

Wichtige technische Daten.

- Qualifizierte elektronische Signatur mit Anbieterakkreditierung nach deutschem Signaturgesetz (SigG)
- Zertifikate nach X.509v3
- Common PKI
- Trust-Center-Sicherheitskonzept, Chip-Kartenbetriebssystem und Schlüsselgenerator nach Signaturgesetz evaluiert und bestätigt

Infos und Anmeldung unter: www.telesec.de

