Certifaction

Certifaction Privacy-first eSignature Whitepaper

Einführung

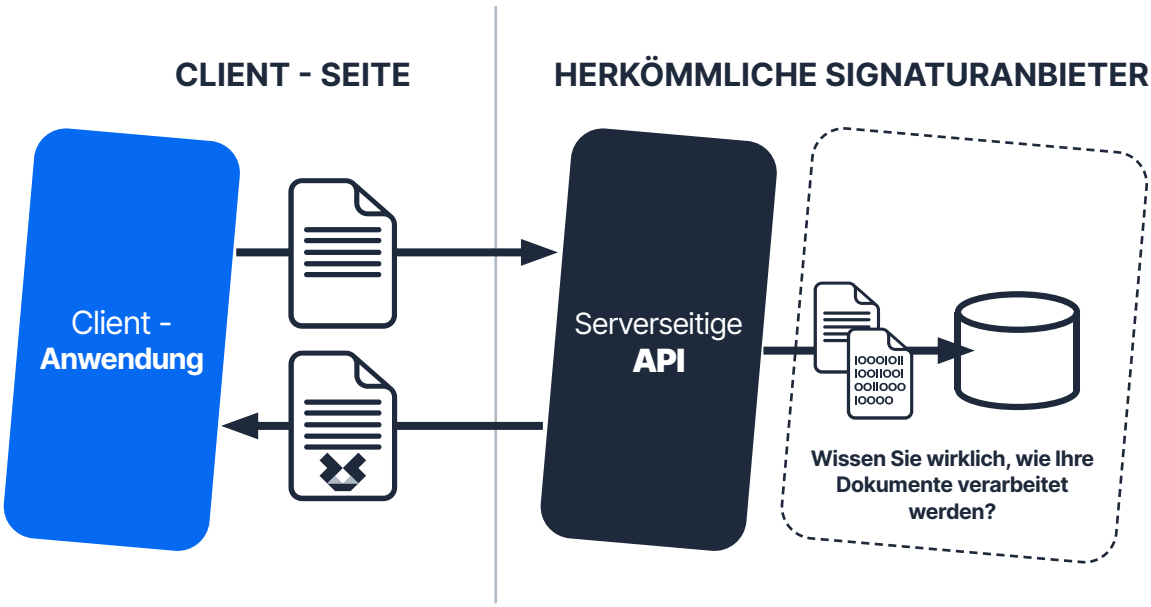
Die elektronische Signatur von Certifaction folgt einem Ansatz, der dem Datenschutz höchste Priorität einräumt. Wir gewährleisten die Vertraulichkeit von Dokumenten, ohne dass dabei dem betreffenden Cloud-Anbieter oder Certifaction selbst vertraut werden muss.

Dies wird durch lokale Dokumentenverarbeitung und Ende-zu-Ende-Verschlüsselung sichergestellt. Je nach erforderlichem Schutzniveau kann der Anwender zwischen höherer Benutzerfreundlichkeit und höherer Vertraulichkeit wählen und die Vorteile einer funktionsreichen elektronischen Signaturlösung nutzen.

Probleme der alten elektronischen Signatur

Die elektronische Unterzeichnung von Dokumenten hat viele Vorteile in Bezug auf Effizienz und Bequemlichkeit mit sich gebracht. Dies ging jedoch meistens auf Kosten der Vertraulichkeit der Dokumente.

Bei herkömmlichen e-Signatur-Lösungen werden die Dokumente vollständig auf den Server geladen, wo sie sich Ihrer Kontrolle entziehen. Sie haben keine andere Wahl, als den Sicherheitsversprechen der Anbieter zu vertrauen.

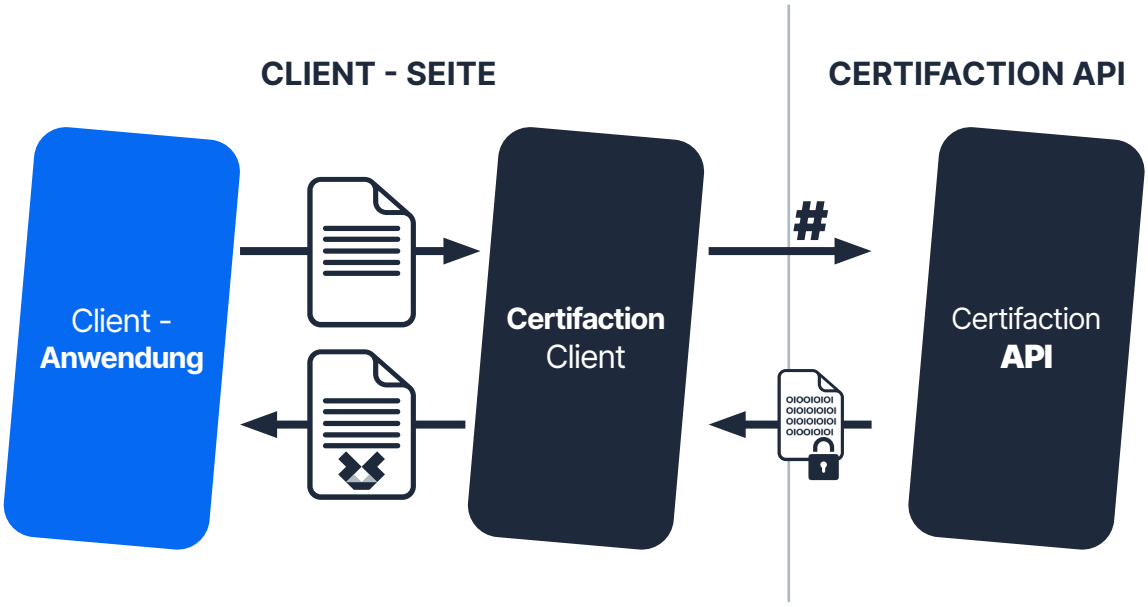


Obwohl die Anbieter von elektronischen Signaturen stolz auf ihre Compliance-Zertifizierungen und sicheren Prozesse verweisen, sind sie nicht vor versehentlichen oder böswilligen Datenlecks gefeit.

Unsere Lösung:

lokale Dokumente-verarbeitung

Um die Vertraulichkeit Ihrer Dokumente zu gewährleisten, verarbeitet Certifaction Ihre Dokumente lokal und stellt sicher, dass Inhalte Ihre kontrollierte IT-Umgebung zu keiner Zeit verlassen.



Certifaction bietet verschiedene Client-Technologien, die

- **die relevanten PDF-Signaturfelder hinzufügen,**
- **den zu signierenden Dokumenten-Hash berechnen und**
- **den Hash an die Certifaction API senden.**

Das daraus resultierende PAdES-Signaturzertifikat wird dann an den Certifaction-Client zurückgegeben und dem Dokument hinzugefügt.

Die Vorteile von On-Premise ohne die üblichen Kosten

Die lokale Verarbeitungslösung von Certifaction kann als zustandslose lokale API in Ihrem Rechenzentrum eingesetzt werden oder einfach in den Benutzer-Browsern (SaaS) laufen.

Die lokale API wird verwendet, um elektronische Dokumentensignaturen zu Ihren bestehenden Prozessen hinzuzufügen, wobei eine einfache HTTP-API genutzt wird.

Dieser hybride Ansatz mit lokalem Client und Remote-API bietet die Vorteile einer On-Premise-Lösung ohne den damit verbundenen Aufwand und die Kosten eines herkömmlichen elektronischen Signaturdienstes in der eigenen IT-Infrastruktur.

	Certifaction	Traditionelle On-Premise-Lösung
Modell	Hybride Bereitstellung. Lokale Dokumentenverarbeitung, Signatur via API	Vollständige Bereitstellung vor Ort
Infrastruktur	Beliebige ODER überhaupt keine	Hardware-Anwendung
Komponenten	Einzelne zustandslose interne Komponente	Verschiedene Komponenten. Zu pflegende und zu schützende Internet-bezogene Anwendung (öffentlich zugänglich)
Datenbanken / Speicher	Keine. Speicherkomponente optional	Erforderlich: Datenbank & zu pflegende Datenspeicher
Schlüssel-speicher/HSM	Keine. Keine Dokumente, vertrauliche Informationen oder Schlüssel gespeichert	Empfohlen. Komplexe Einrichtung und Wartung erforderlich

Im Weiteren beschreiben wir in diesem Dokument, wie die Certifaction-Funktionen zusammenwirken, um unser Versprechen einer elektronischen Signatur, bei welcher der Schutz des Dokuments an erster Stelle steht, zu erfüllen.

Ende-zu-Ende verschlüsseltes digitales Archiv

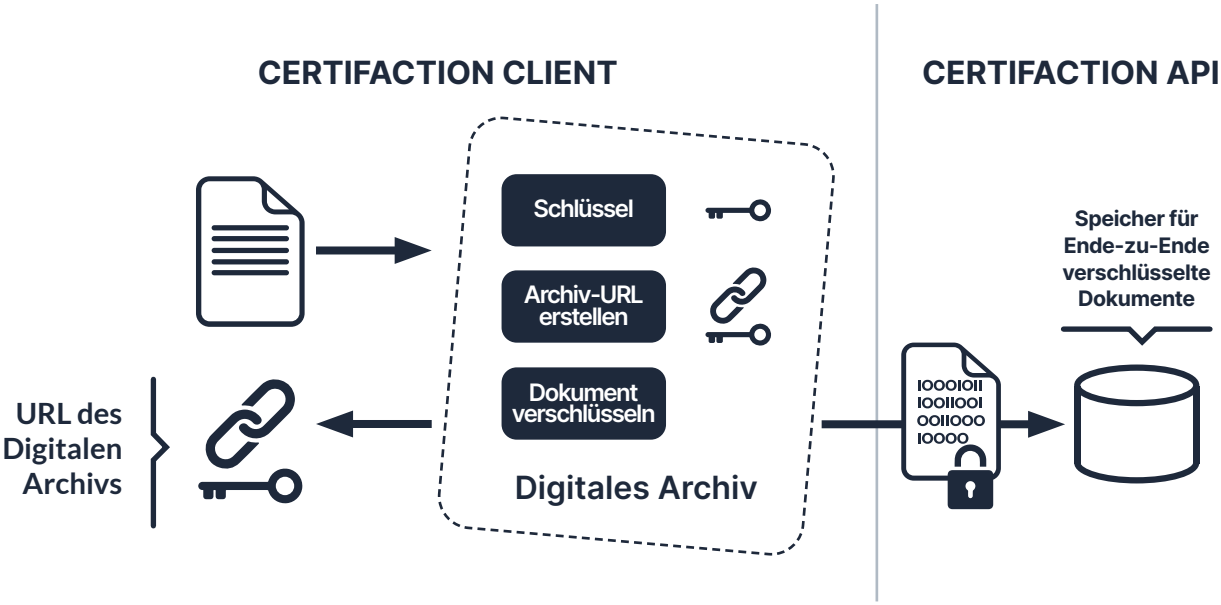
Auch wenn Certifaction nicht auf den Inhalt Ihrer Dokumente im Klartext zugreifen kann, können Sie dennoch Dokumente freigeben und andere Personen einladen, diese zu signieren.

Ermöglicht wird dies durch das Ende-zu-Ende-verschlüsselte digitale Archiv von Certifaction, das Dokumente sicher speichern und abrufen kann.

Speicherung von Dokumenten

Das digitale Archiv von Certifaction speichert Dokumente sicher ab durch

- Generierung eines symmetrischen Kodierungsschlüssels,
- Erstellung einer eindeutigen Speicher-URL, die den Kodierungsschlüssel als URL-Fragment enthält,
- Verschlüsselung des Dokuments unter Verwendung des Schlüssels auf der Client-Seite mit NaCl Secretbox,
- das Hochladen des verschlüsselten Dokuments an einen externen Speicher sowie
- Schutz des Kodierungsschlüssels der Speicher-URL durch ein kryptographisch starkes Passwort.

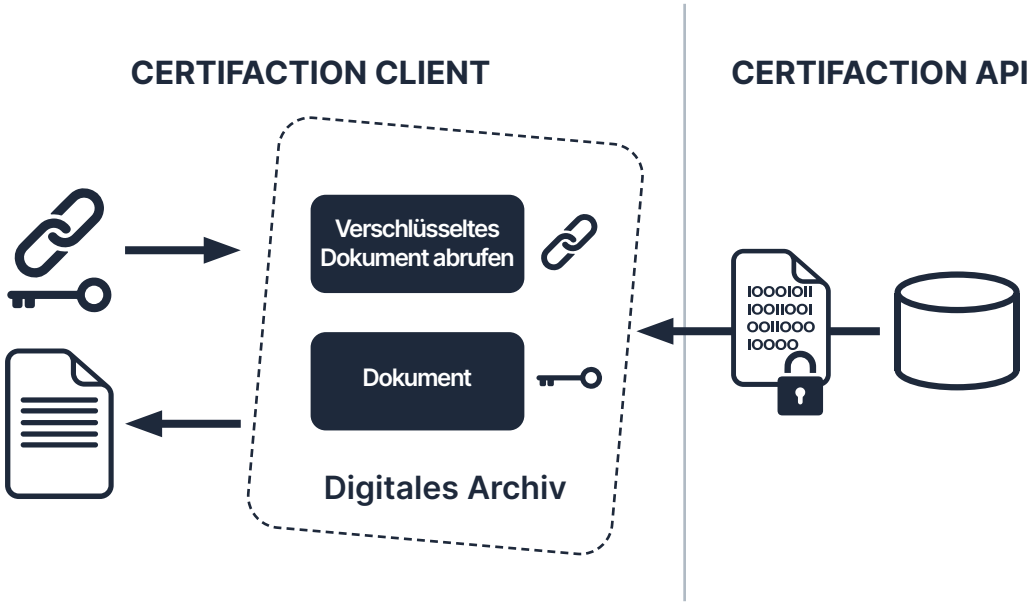


Geheime Kodierungsschlüssel bleiben immer auf dem Client und werden als Teil der URL des digitalen Archivs zurückgegeben. Da die URLs des digitalen Archivs die zur Entschlüsselung der Dokumente erforderlichen geheimen Informationen enthalten, müssen die URLs sicher übertragen und gespeichert werden. Dies kann durch den Schutz der geheimen Informationen mit einem kryptographisch starken Passwort erreicht werden.

Abrufen von Dokumenten

Benutzer können Dokumente mit den URLs des digitalen Archivs einfach herunterladen und entschlüsseln, indem sie

- die URLs zum Abrufen der verschlüsselten Dokumente verwenden und
- die verschlüsselten Dokumente mit Hilfe des geheimen Verschlüsselungscodes unter Verwendung von NaCl Secretbox in den URL-Fragmenten entschlüsseln.

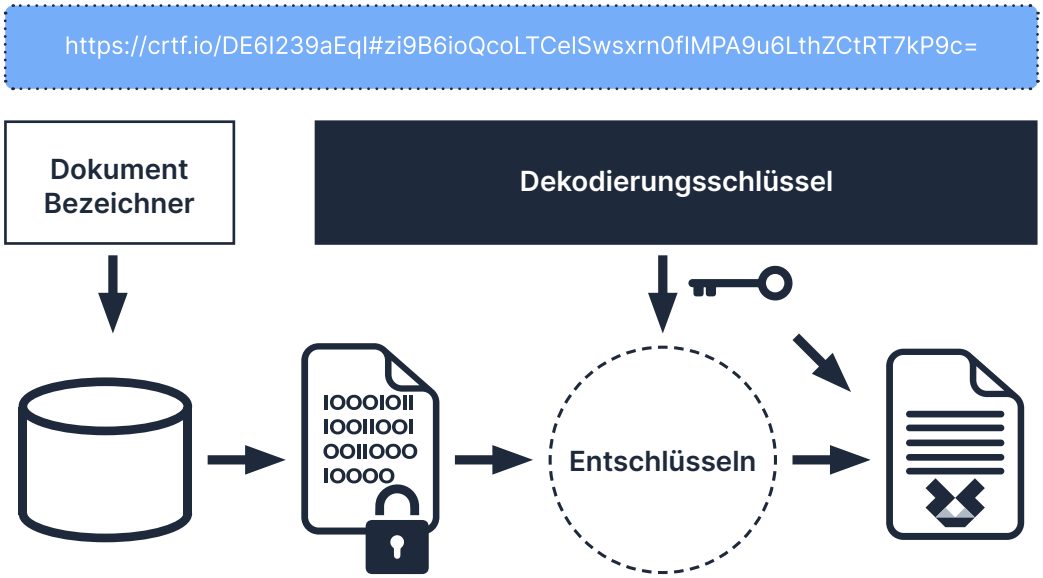


Ablaufdaten von Dokumenten

Die Aufbewahrungsdauer verschlüsselter Dokumente kann konfiguriert werden. Nach Ablauf der Frist wird das verschlüsselte Dokument dauerhaft aus dem Speicher gelöscht und kann nicht mehr abgerufen werden, auch nicht über die URL des digitalen Archivs.

URL des digitalen Archivs

Die URLs des digitalen Archivs setzen sich aus einer eindeutigen Dokumentenkennung und einem geheimen Kodierungsschlüsselfragment zusammen. Da URL-Fragmente bei HTTP-Anfragen nie übertragen werden, bleiben alle vertraulichen Informationen immer auf der Client-Seite.



Solange sie über einen entsprechend sicheren Kanal ausgetauscht werden, können digitale Archiv-URLs verwendet werden, um vertrauliche Dokumente bequem zwischen Parteien auszutauschen.

Wir verwenden NaCl Secretbox XSalsa20 und Poly1305, um das Dokument mit Geheimschlüssel-Kryptografie zu verschlüsseln und zu authentifizieren. Die Schlüssellänge beträgt 256 Bit.

Digitaler Zwilling

Ein sichtbarer QR-Code für die URL des digitalen Archivs kann zu Dokumenten hinzugefügt werden. Wenn ein Dokument gedruckt wird, kann der scanbare QR-Code verwendet werden, um einen digitalen Zwilling der Papierkopie sicher abzurufen.

QR-Codes des Digitalen Zwillings enthalten geheime Informationen und müssen entsprechend geschützt werden.

Digital Twin URLs enthalten Dokumentenkennungen und geheime Kodierungsschlüssel. Dokumente können durch Scannen geladen und entschlüsselt werden, auch wenn Certifaction niemals auf den Inhalt des Dokuments im Klartext zugreifen kann.

Signaturanfrage

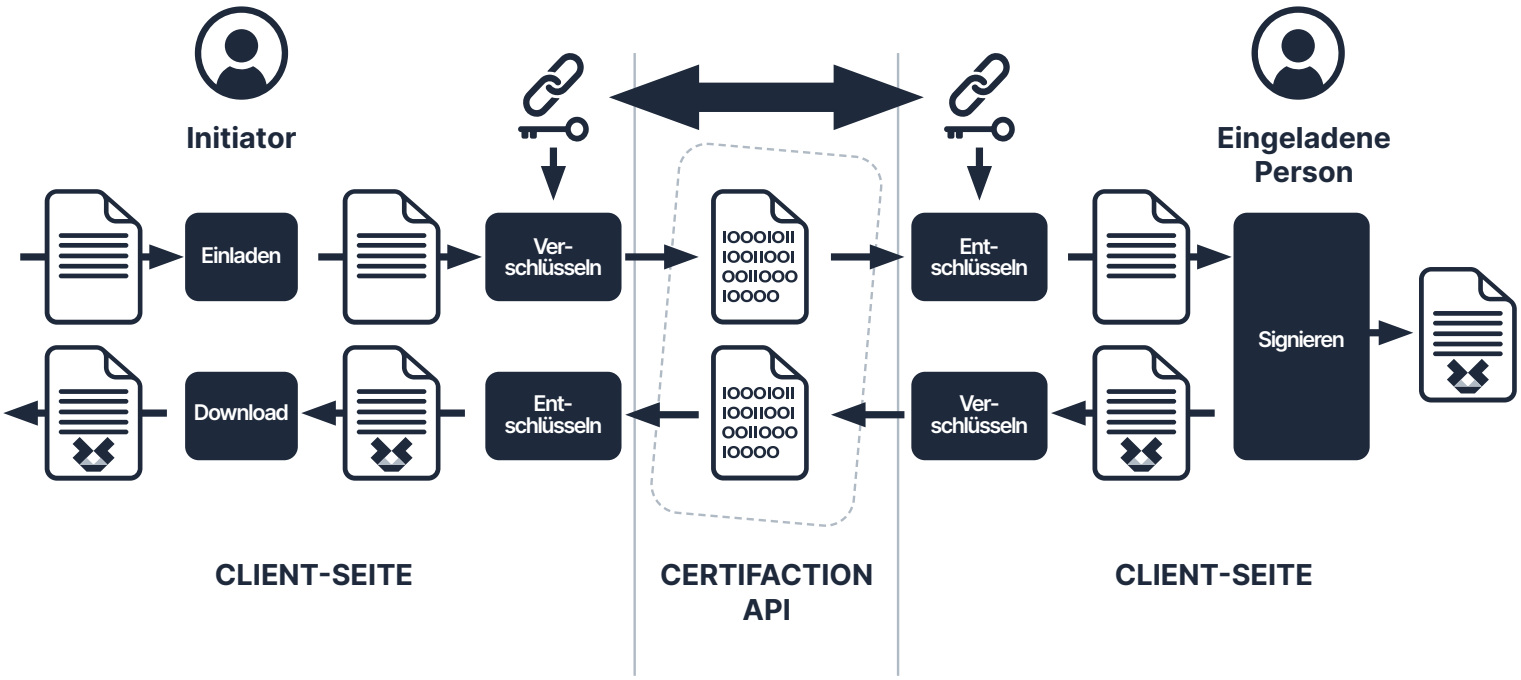
Benutzer können andere Personen einladen, Dokumente zu signieren, indem sie Signaturanfragen erstellen und versenden.

Signaturanfragen werden mit sicheren URLs verknüpft, die geheime Fragmente enthalten, und zwar nach dem gleichen Prinzip wie bei den URLs des digitalen Archivs.

Die URLs für Signaturanfragen können über einen entsprechend sicheren Kanal Ihrer Wahl oder über die Einladungs-E-Mails von Certifaction versendet werden.

Weitergabe von URLs für sichere Out-of-band-Signaturanfragen

Wenn Sie bereits über einen sicheren Kanal verfügen, können Sie diesen nutzen, um URLs für Signaturanfragen zu versenden. Verschlüsselungscodes in den URL-Fragmenten entschlüsseln.

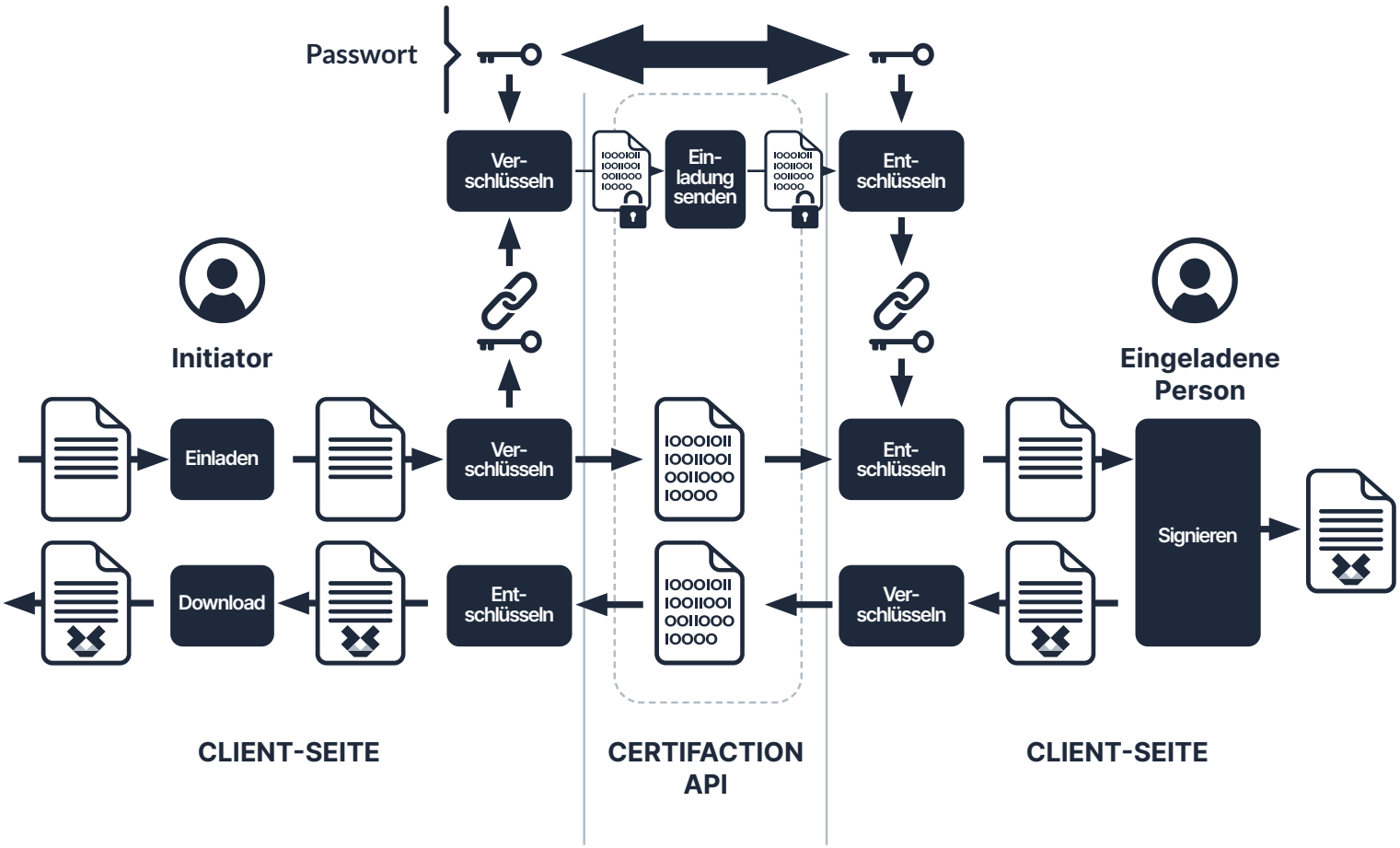


Initiatoren erstellen eine Signaturanfrage mit einem oder mehreren Dokumenten und erhalten eine sichere Signaturanfrage-URL zurück. Die Initiatoren übernehmen die Verantwortung für die Weitergabe der URL an Dritte.

Diese Lösung ist geeignet, wenn Personen Zugang zu einer Anwendung haben, die Sie kontrollieren. In diesem Fall ist es einfach, die URLs der Signaturanfragen sicher an die Anwendung zu übertragen und die Signatur-Anwendung in einer Web View Komponente zu öffnen.

Versenden von E-Mails mit Signaturanfragen mit Hilfe von Certifaction

Wenn kein sicherer Kanal verfügbar ist, können Sie die Einladungs-E-Mails von Certifaction verwenden. Certifaction übernimmt die Verantwortung für die Übermittlung der URLs für die Signaturanforderung und schützt sie optional mit einem kryptographisch starken Passwort.



Bitte beachten Sie, dass die Sicherung der Signaturanforderungs-URL mit einem Passwort optional ist, damit die Benutzer fallbasiert zwischen maximaler Vertraulichkeit und besserer Benutzerfreundlichkeit wählen können.

Diese Option ist in allen Certifaction-Clients verfügbar.

Ökosystem von Certifaction

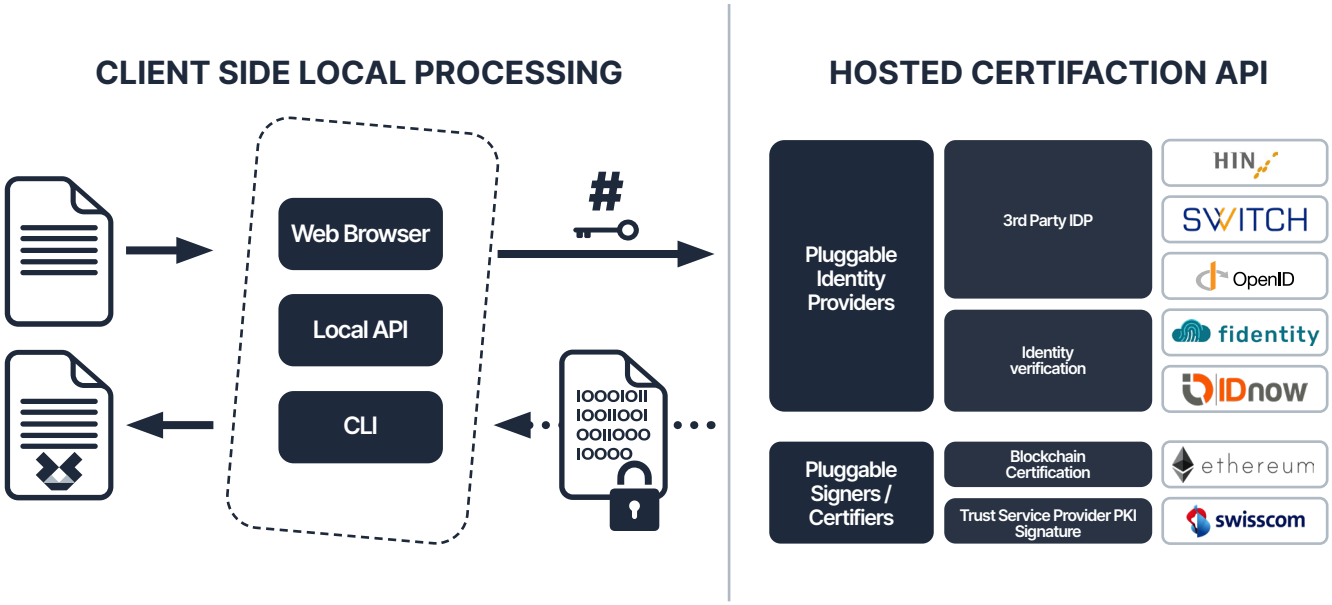
Die Architektur von Certifaction ist modular, sicher und skalierbar. Dokumente werden immer Client-seitig verarbeitet und nie im Klartext an die Cloud gesendet.

Certifaction bietet verschiedene Client-Implementierungen:

- eine Webanwendung für die manuelle einfache Signatur von Dokumenten,
- eine lokale API für die Integration in Kunden-Rechenzentren und
- eine CLI für Intensivnutzer, Skripting und Integration in eigenständige Anwendungen.

Jeder Client verarbeitet PDF-Dokumente und versieht sie lokal mit elektronischen Signaturen, ohne dass das gesamte Dokument im Klartext an die Certifaction API gesendet werden muss, wie dies bei herkömmlichen Anbietern elektronischer Signaturen der Fall ist, die auf den Inhalt der Dokumente in ihren Rechenzentren zugreifen können.

Certifaction arbeitet mit renommierten, europäisch akkreditierten Vertrauensdienste- und Identifikationsanbietern zusammen. Wir sind stets auf der Suche nach neuen Lösungen am Markt und integrieren diese in unsere modulare Architektur.



Zusammenfassung

Herkömmliche Lösungen für die elektronische Signatur von Dokumenten können die Vertraulichkeit der Dokumente nicht garantieren, da der Inhalt der Dokumente zwecks Verarbeitung an die Rechenzentren der Anbieter gesendet wird.

Die datengeschützte elektronische Signatur von Certifaction löst dieses Problem, indem sie Dokumente lokal verarbeitet und ihren Inhalt niemals im Klartext außerhalb Ihrer vertrauenswürdigen IT-Umgebung verbreitet.

Certifaction bietet eine Webanwendung, eine lokale API und eine CLI, um Dokumente sicher zu signieren und zu speichern, Signaturen anzufordern und auf einfache Weise digitale Zwillinge zu erstellen. Der Inhalt der Dokumente bleibt dabei vertraulich.

Mit der Hybrid-Lösung von Certifaction können Sie die Vertraulichkeit von Dokumenten gewährleisten, ohne die Kosten und die Komplexität herkömmlicher On-Premise-Lösungen in Kauf nehmen zu müssen.

Certifaction

Weitere Informationen

Bitte besuchen Sie unsere certifaction.com-Webseite, um sich über unsere Dienstleistungen und Nutzungsbedingungen zu informieren.

Bitte besuchen Sie unser Entwicklerportal unter **developers.certifaction.com,** um die datengeschützte Signatur von Certifaction in Ihre Produkte und Services zu integrieren.

Über Certifaction

Certifaction ist der führende Anbieter für sichere, datenschutzfreundliche eSignaturen. Mit seinen Privacy-first-Lösungen hilft der Schweizer Anbieter Unternehmen dabei, die Abwicklung von Geschäften einfacher, schneller und effizienter zu gestalten. Zudem treiben Sie Ihre Digitalisierung voran: Certifaction macht den Unterschriftsprozess von Unternehmen zukunftssicher. Datenschutz und Nutzerfreundlichkeit stehen dabei an erster Stelle und sind fest in der Unternehmensphilosophie verankert. Dank eigenem eSignatur-Standard PES (Professionelle eSignatur) können Nutzer innerhalb kürzester Zeit überall sichere, rechtsgültige eSignaturen leisten. Unternehmen sparen durch die Verwendung digitaler Unterschriften Zeit, Budget und Ressourcen und leisten zugleich auch einen Beitrag zur Nachhaltigkeit. Certifaction wurde 2020 in Zürich gegründet und zählt Unternehmen wie HIN, SWITCH, Swisscard, H&B/Savills und emonitor zu seinen Kunden und Partnern.