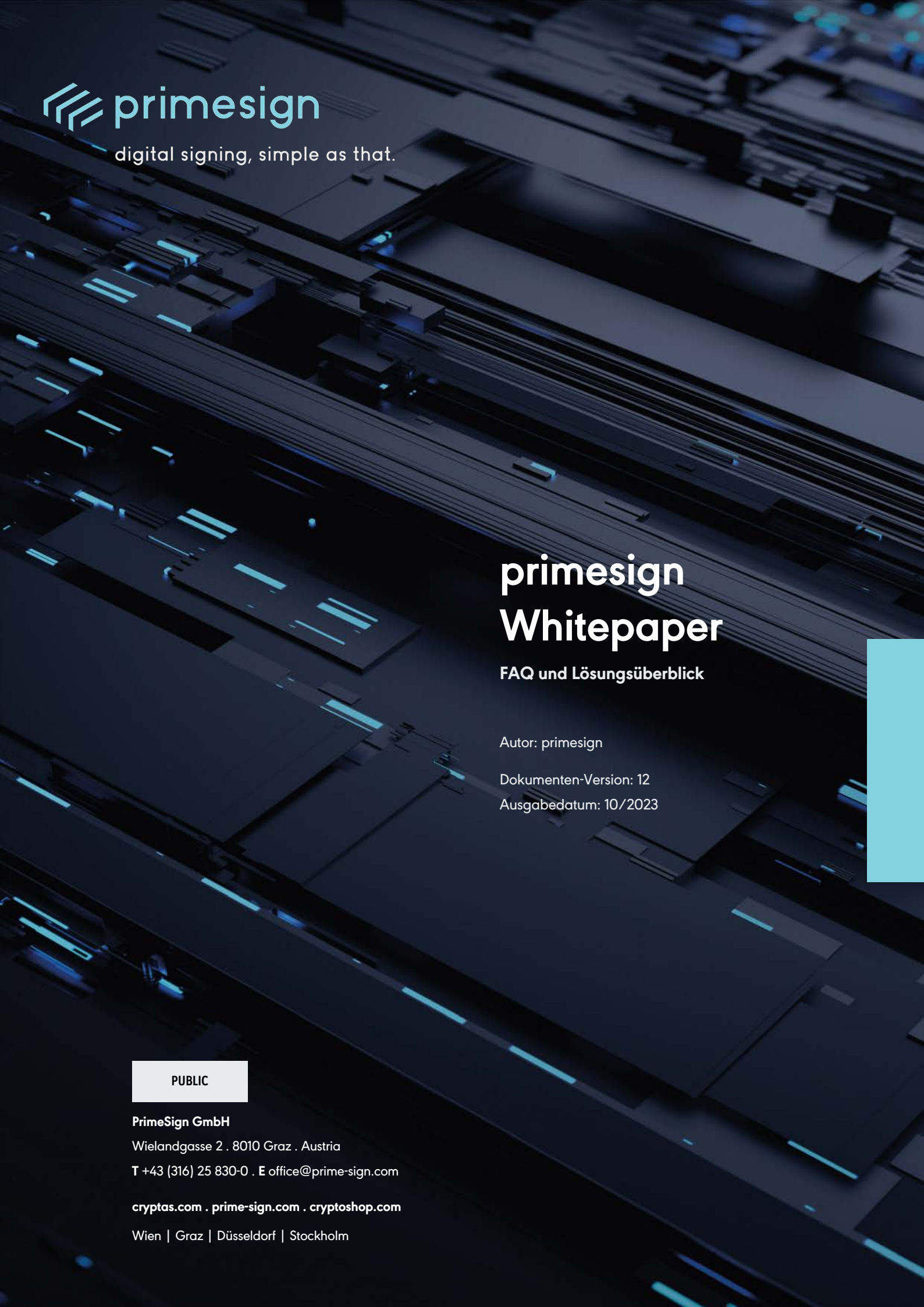

primesign

digital signing, simple as that.

primesign Whitepaper

FAQ und Lösungsüberblick

Autor: primesign

Dokumenten-Version: 12
Ausgabedatum: 10/2023

PUBLIC

PrimeSign GmbH
Wielandgasse 2 . 8010 Graz . Austria
T +43 (316) 25 830-0 . **E** office@prime-sign.com

cryptas.com . prime-sign.com . cryptoshop.com
Wien | Graz | Düsseldorf | Stockholm

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

Dokumenteninformationen

Im Folgenden werden typografische Konventionen und Änderungen bzgl. des Dokumentes bereitgestellt.

Typografische Konventionen

⚠ Warnung – bitte sorgfältig lesen

Weitere Informationen und Tipps

```
Befehl
```

Änderungshistorie

Alle Änderungen des Handbuches werden in der folgenden Historie nachverfolgt.

Datum	Name	Art der Änderung	Version
20.05.2020	Rössler	Entwurf	1 (also 1.0D)
08.06.2020	Rössler	Entwurf	2
10.06.2020	Rössler	Entwurf	3
19.06.2020	Kreuzhuber	Review	4
25.06.2020	Rössler	Erweitert	5
25.06.2020	Rössler	Erweitert & Abschnitt 9 (PrInd) entfernt	6
26.06.2020	Rössler	Freigabe Version 1	7
30.06.2020	Rössler	Editorielle Änderung & Freigabe	8
05.05.2021	Fruhmann	Update Template & Terminologie	8
11.06.2021	Fruhmann	Editorielle Updates	9
01.07.2021	Fruhmann	Editorielle Updates & Grafiken	9
11.03.2022	Kreuzhuber	Erweiterung um primesign WRAPTOR	10
18.05.2022	Fruhmann	Review & editorielle Updates	10
14.06.2022	Fruhmann	Editorielle Updates	10
01.07.2022	Fruhmann, Kreuzhuber, Rössler	Freigabe & Fertigstellung Version 10	10
03.01.2023	Fruhmann	Update primesign MOBILE & Erweiterung Business-Zertifikate	11

25.10.2023	Kreuzhuber	Erweiterung Signieren mit deutschem Online-Ausweis & Qualifizierte Zeitstempel	12

1. Management Summary

Ergänzend zu den bestehenden Produktbeschreibungen des primesign SIGNATURE SERVERs bietet dieses Dokument einen anwendungsorientierten Überblick über typische Lösungsszenarien und liefert Antworten auf zentrale Fragestellungen. Das Dokument ersetzt zwar nicht das Lesen der Detaildokumentationen, soll aber bereits in einer frühen Phase eine praxisbezogene Orientierungshilfe geben, egal ob im Zuge einer Kaufentscheidung oder bereits in Vorbereitung für eine Umsetzung.

Das Dokument gliedert sich wie folgt:

- Kapitel 2 fasst die wesentlichsten Eigenschaften und das umfangreiche Feature-Set des primesign SIGNATURE SERVERs nochmals zusammen. Diese Ausführungen ergänzen und unterstreichen bereits bestehende Produktbeschreibungen des primesign SIGNATURE SERVERs, wie Datenblatt oder Handbuch.
- Im Kapitel 3 werden eine Reihe von oft gestellten Fragen beantwortet und erörtert. Es handelt sich hier nicht nur um rein technische Fragestellungen zum primesign SIGNATURE SERVER und dessen Features, sondern die Fragen gehen auch auf unseren Gesamtlösungsbogen und unterschiedlichste Aspekte eines Signaturprozesses ein. Sie umfassen daher auch Aspekte zu elektronischen Signaturen im Allgemeinen sowie zu unseren primesign Trust-Center-Services im Speziellen.
- Kapitel 4 erörtert wie eine Unternehmenszugehörigkeit und/oder Rollen und Funktionen (Vertretungsbefugnisse, etc.) in elektronischen Signaturen ausgedrückt werden können. Auch qualifizierte Siegelzertifikate (zur Bildung der „Signatur des Unternehmens“) werden behandelt.
- Kapitel 5 erläutert den Weg eines elektronischen Dokumentes im Zuge einer Signaturtransaktion und in Abhängigkeit vom verwendeten Signaturmittel. Beispielsweise können wir bei der Verwendung unseres Remote-Signing-Dienstes primesign MOBILE in Kombination mit einem primesign SIGNATURE SERVER On-Premise-Setup gewährleisten, dass Dokumente auch während des Signaturvorgangs immer vollständig in der IT-Infrastruktur von Kunden verbleiben (auch in Verbindung mit primesign WRAPTOR).
- Im Kapitel 6 werden zwei vereinfachte, aber typische Deployment-Varianten des primesign SIGNATURE SERVERs skizziert. Zum einen eine On-Premise-Architektur; zum anderen die Nutzung des primesign SIGNATURE SERVERs als Managed Service (SaaS).
- Kapitel 7 bietet einen Überblick über die wesentlichsten Hardware- als auch Softwareanforderungen einer typischen primesign SIGNATURE SERVER Infrastruktur.
- Kapitel 8 beschreibt einige Referenzkundenfälle. Weitere Referenzen stehen auf Anfrage zur Verfügung.

- Kapitel 9 referenziert eine Reihe von weiterführenden Dokumenten.

2. Der primesign SIGNATURE SERVER

Unsere Signaturlösung, der primesign SIGNATURE SERVER, ist die zentrale Infrastruktur und Drehscheibe für elektronische Signaturen in Organisationen bzw. Unternehmen. Unabhängig davon, ob der primesign SIGNATURE SERVER in Form einer (physischen oder virtuellen) Appliance vor Ort (On-Premise) betrieben oder als Managed Service (SaaS) genutzt wird, bietet er für die gesamte Bandbreite an Anwendungen von elektronischen Signaturen die richtige Funktionalität.

2.1. Typische Anwendungsfälle

Die Anwendungsfälle von elektronischen Signaturen in Organisationen und Unternehmen sind breit und vielschichtig. Nahezu überall, wo heute Abzeichnungen oder handschriftliche Unterschriften auf Papier gefordert werden, ist die elektronische Signatur mit dem primesign SIGNATURE SERVER das geeignete digitale Äquivalent. Mit dem primesign SIGNATURE SERVER können Digitalisierungsprojekte so durchgängig, umfassend und rechtssicher umgesetzt werden.

Exemplarische Anwendungsfälle:

- Elektronisch unterschreiben von jeglichen Verträgen oder Dokumenten
- Elektronisch unterschreiben von HR-Dokumenten oder Dienstverträgen
- Elektronisch unterschreiben von Bestellungen oder Bestätigungen
- Kündigung von Verträgen
- Elektronisch unterschreiben von Dienstanweisungen oder Formularen
- Elektronisches SIEGELN von ein- oder ausgehenden Dokumenten / Rechnungen

2.2. Installationsfrei für AnwenderInnen

Der primesign SIGNATURE SERVER ist für AnwenderInnen eine installationsfreie Signaturlösung zum Aufbringen von rechtsverbindlichen elektronischen Signaturen. Als Webanwendung (siehe Abbildung 1) ist der primesign SIGNATURE SERVER mit allen gängigen Browsern nutzbar und lässt sich so auch nahtlos in webbasierte Workflows integrieren. Es ist keine lokale Client-Software erforderlich.

Das Ausrollen des primesign SIGNATURE SERVERs in Organisationen und Unternehmen ist daher denkbar einfach. Es werden entsprechende Zugriffsrechte (Accounts) vergeben und entsprechende Zugangsdaten (Links, entweder zur lokalen On-Premise- oder einer SaaS-Instanz) verteilt. Auf diese Weise kann jeder Arbeitsplatz einfach für elektronische Signaturen nachgerüstet werden.

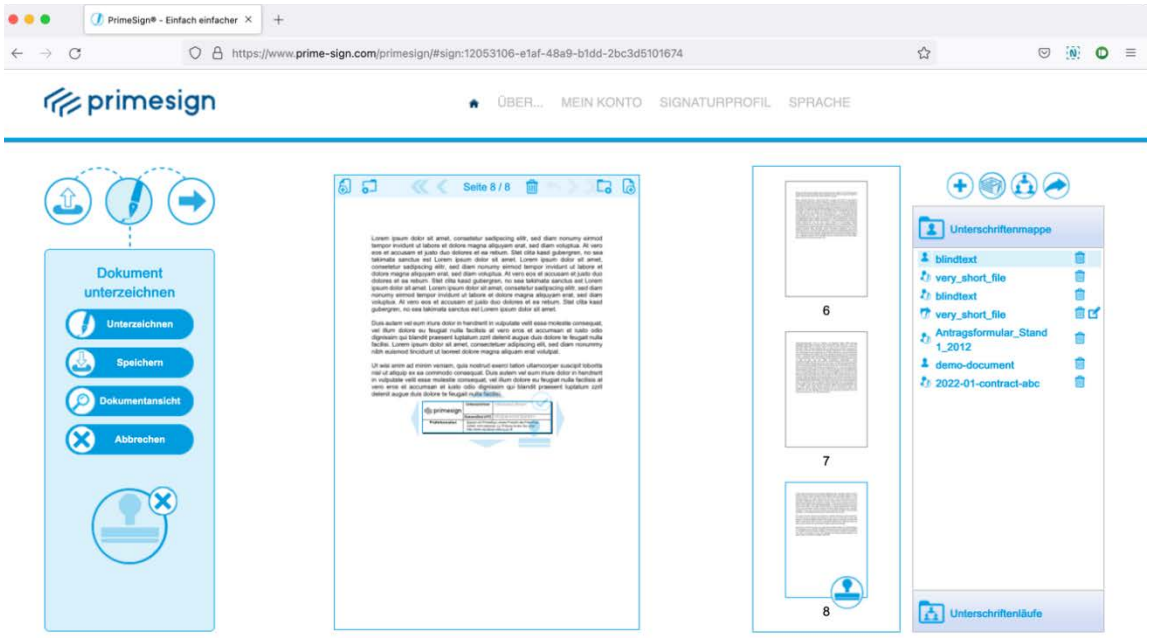

Abbildung 1: Hauptansicht Web-UI primesign SIGNATURE SERVER

2.3. Unterstützte Signaturmittel

Der primesign SIGNATURE SERVER unterstützt eine Vielzahl von Signaturmittel (Signaturzertifikaten) unterschiedlichster Anbieter. Er verfügt auch über Standardintegrationen für einige etablierte Signaturmittel. Auf Anfrage können weitere Signaturmittel, die standardmäßig nicht unterstützt werden, an den primesign SIGNATURE SERVER angebunden werden. Dazu gehören z.B. Signaturkarten anderer Hersteller (siehe Abschnitt 3.1).

Unsere Empfehlung: Signieren Sie mit qualifizierten Signaturzertifikaten (primesign Signaturzertifikaten) unseres eigenen eIDAS-konformen Trust Centers, dem primesign TRUST CENTER. Mit „Signieren mit eID" können auch ausgewählte eIDAS eIDs ohne vorherige Registrierung bei primesign zur sofortigen Signatur mit primesign Zertifikaten genutzt werden.

2.4. Sichtbare Signaturen

Verleihen Sie Ihrer elektronischen Signatur Ausdruck! Mit primesign können Sie Ihr persönliches Signaturbild erstellen und nach Ihrem Wunsch gestalten. primesign bietet hierzu eine Vielzahl an vorgefertigten Templates. Hinterlegen Sie beispielsweise Ihre persönliche handschriftliche Unterschrift als Bild (siehe Abbildung 2) oder lassen Sie das Signaturbild Ihrem Organisations-/Firmenlogo bzw. Ihrem Firmenstempel ähneln. Dadurch erhalten EmpfängerInnen Ihrer elektronisch signierten Dokumente die gewohnte Darstellung einer „konventionellen" Unterschrift oder firmenmäßigen Zeichnung sowie Angaben zur Prüfbarkeit der Signatur. Dies verstärkt die Akzeptanz von elektronisch signierten Dokumenten.

Sie können mit dem primesign SIGNATURE SERVER aber auch „unsichtbar" signieren. Hierbei wird dem Dokument kein sichtbares Element hinzugefügt. Die Signatur ist „nur" in den Dokumenteneigenschaften ersichtlich, entfaltet aber die selbe Sicherheit und Rechtskraft wie eine sichtbare Signatur.

Abbildung 2: Muster eines persönlichen Signaturbildes (Signaturstempel)

2.5. primesign SIGNATURE SERVER – Ihre zentrale Signaturinfrastruktur

Der primesign SIGNATURE SERVER wurde als umfassendes System konzipiert und ist daher für eine Vielzahl von Anwendungsfällen geeignet. Auch kann er als Kernkomponente einer umfassenden Signaturinfrastruktur fungieren (siehe Abbildung 3).

Abbildung 3: primesign SIGNATURE SERVER für viele Anwendungsfälle

INTERNE ANWENDUNGSFÄLLE

Interne Anwendungsfälle sind die naheliegendste Nutzungsform unserer Signaturlösung. Dabei wird der primesign SIGNATURE SERVER zur Abwicklung von persönlichen Signaturen am Arbeitsplatz bzw. im Unternehmen eingesetzt, etwa für interne Unterschriftenläufe, Umlaufbeschlüsse, für das Vorlegen von zu unterschreibenden Dokumenten oder für das rasche Unterschreiben von Einzeldokumenten.

EXTERNE ANWENDUNGSFÄLLE

Hierbei fungiert der primesign SIGNATURE SERVER als Drehscheibe zur Abgabe von Bestellungen und Aufträgen sowie zur Abwicklung von Verträgen mit Kunden oder Partner. Beispielsweise können mit dem primesign SIGNATURE SERVER Unterschriftenläufe mit Externen geteilt werden. Der primesign SIGNATURE SERVER kann dabei auch extern zugänglich gemacht werden, sodass elektronisch signierte Dokumente rechtssicher in Empfang genommen werden können.

MASSENVERFAHREN

Der primesign SIGNATURE SERVER kann auch als zentraler Signaturserver genutzt werden, der effizient und automatisch große Mengen von Dokumenten performant elektronisch signiert (meist per Integrationsschnittstelle an andere Massensysteme angebunden). Beispiele sind elektronische Rechnungen, Vertragsdokumente, Schreiben an Kunden, Bescheide, Angebote, Amtssignaturen oder das Aufbringen von elektronischen Siegeln.

UNTERSCHRIFTENLÄUFE

Mittels des primesign SIGNATURE SERVERs können Unterschriftenläufe mit internen und externen BenutzerInnen automatisch abgewickelt und mit verschiedenen Beteiligten auf unterschiedlichen Ebenen einfach und effizient elektronisch durchgeführt werden.

Beispiel 1: Auf Ebene 1 unterschreiben zwei MitarbeiterInnen; anschließend wird automatisch eine Abteilungsleiterin oder ein Abteilungsleiter zur Gegenzeichnung eingeladen.

Beispiel 2: Die Rechtsabteilung zeichnet die Richtigkeit des Vertrages vorweg ab. Dies kann mit dem primesign SIGNATURE SERVER auch durch Paraphierung erfolgen. Im Zuge des primesign Unterschriftenlaufes wird das Dokument danach automatisch den beiden GeschäftsführerInnen vorgelegt, die parallel unterschreiben.

Beispiel 3: Zunächst eröffnet und initiiert die Assistenz den gesamten Unterschriftenlauf und lädt zuerst UnterzeichnerIn 1 zur Unterschrift ein; danach werden UnterzeichnerIn 2 und 3 parallel aufgefordert zu unterschreiben, etc.

primesign Unterschriftenläufe, abgewickelt mit dem primesign SIGNATURE SERVER, lassen hier beliebige Kombinationen und Ebenen zu (siehe Abbildung 4).

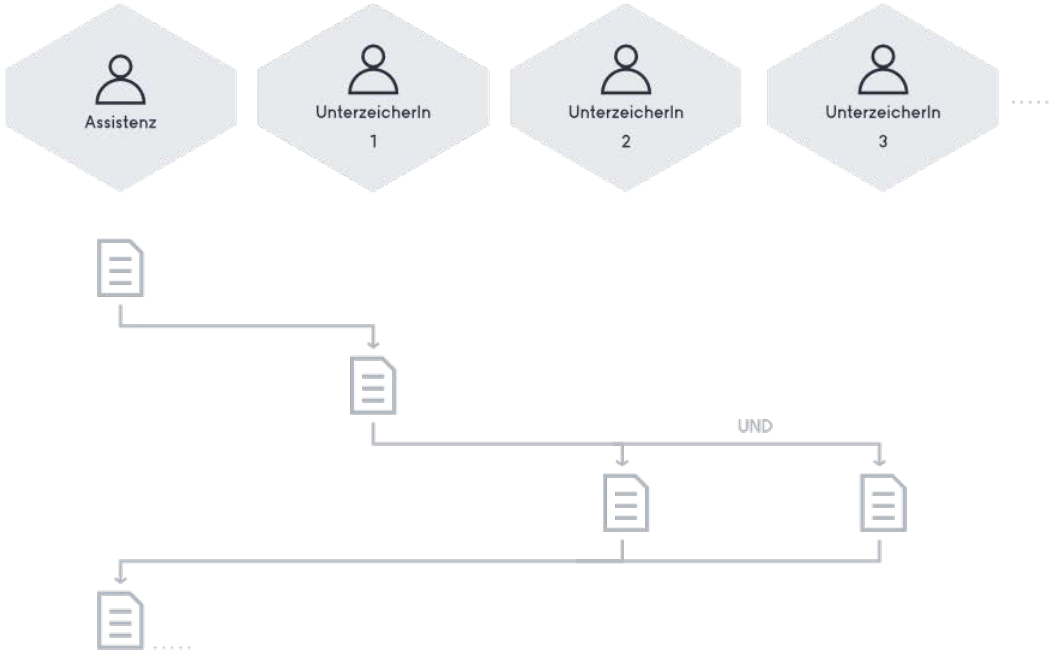

Abbildung 4: Unterschriftenläufe auf verschiedenen Ebenen (Beispiel)

2.6. Wesentliche Eigenschaften des primesign SIGNATURE SERVERs

Der primesign SIGNATURE SERVER zeichnet sich vor allem dadurch aus, dass er mit einer Vielzahl von elektronischen Signaturmitteln (Signaturzertifikaten) verwendet werden kann. Insbesondere im Bereich der persönlichen Signaturen können neben den eigenen primesign Signaturzertifikaten, den primesign MOBILE Signaturzertifikaten, auch weitere Signaturmittel (Signaturzertifikate) von anderen Anbietern verwendet werden.

Dazu zählen z.B. ID Austria, die Handy-Signatur, Dienstkarten, E-Cards oder andere Signaturmittel oder HSMs. Zudem können auch ausgewählte eIDAS eIDs wie z.B. der deutsche Online-Ausweis, ID Austria oder die Handy-Signatur mittels primesign WRAPTOR ohne vorherige Registrierung bei primesign zur sofortigen Signatur mit primesign Zertifikaten genutzt werden (siehe 3.18).

Als Softwarehersteller und Trust-Center-Betreiber können wir außerdem durchgängig optimierte Gesamtprozesse von der Ausstellung eines Signaturzertifikats bis zu dessen Nutzung mit dem primesign SIGNATURE SERVER – oder in angebundenen Anwendungen anbieten.

Darüber hinaus hebt sich der primesign SIGNATURE SERVER auch durch sein umfangreiches Feature-Set von anderen Signaturlösungen ab. Dieses umfangreiche Feature-Set umfasst beispielsweise die Stapelsignaturfähigkeit, das freie Positionieren des Signaturbildes (inkl. Auswahl mehrerer Signaturbilder), die Paraphierungsfunktion (Paraphe optisch auf jeder Seite), grundlegende PDF-Editierfunktionen, eine einfache Bedienbarkeit sowie die Möglichkeit, sofort, direkt und ohne vorherige Registrierung bei primesign, mittels ausgewählten eIDAS eIDs zu signieren.

Die folgende Liste stellt eine kleine Auswahl der wesentlichen Merkmale des primesign SIGNATURE SERVERs dar:

- Signieren von PDF-Dokumenten ohne Client (Web-Oberfläche)
- Optimal in Verbindung mit unseren primesign MOBILE Signaturzertifikaten und unseren Trust-Center-Leistungen nutzbar
- Unterstützt verschiedenste Signaturmittel wie Signaturkarten, eIDs oder Remote-Signing-Lösungen (wie primesign MOBILE, deutscher Online-Ausweis oder die ID Austria/Handy-Signatur)
- Erstellung von qualifizierten persönlichen Signaturen oder qualifizierten Siegeln (Unternehmen)
- Garantierte Langzeitprüfbarkeit der signierten PDF-Dokumente (PAdES und LTV-konform)
- Unterschriftenläufe, auch mit mehreren Parteien (Intern/Extern)
- Erstellung und Nutzung von Vorlagen für Unterschriftenläufe
- Minimal-UI für optimale Integration in Anwendungen (SOAP-Integrationsschnittstelle)
- primesign WRAPTOR: Nutzung ausgewählter eIDAS eIDs, um eine qualifizierte Signatur mit einem primesign MOBILE Einmalzertifikat zu erstellen - sofortiges signieren, keine vorherige Registrierung mit primesign erforderlich

- Unified Trust: Garantierte Rechtssicherheit und einheitliche Signaturen; immer mit primesign Zertifikaten signieren, unabhängig davon, welches Signaturmittel verwendet wird; ein Rechtsrahmen, ein verantwortlicher Trust-Partner und maximale Rechtssicherheit – primesign WRAPTOR macht es möglich.
- Stapelsignaturfähig (zum Beispiel mit primesign MOBILE oder primesign WRAPTOR): Signieren Sie einen Stapel von PDF-Dokumenten auf einmal; dank des primesign WRAPTORs auch mit eIDAS-Identitäten oder bestehenden Signaturzertifikaten von Drittanbietern
- On-Premise oder als Managed Service (SaaS); im On-Premise-Betrieb des primesign SIGNATURE SERVERs können wir bei der Nutzung von primesign MOBILE (auch in Verbindung mit primesign WRAPTOR) garantieren, dass Dokumente während des Signaturvorgangs immer vollständig in der IT-Infrastruktur von Kunden verbleiben
- Sichtbare Signaturen, Signaturbild manuell oder automatisch platzierbar
- Platzierung von Signaturbildern anhand von Platzhaltern, die bereits bei Dokumenterstellung eingebracht werden können
- Editierfunktionen für PDF-Dokumente und PDF-Konvertierung für viele Office-Formate (PDF/A optional)

Für weitere Merkmale des primesign SIGNATURE SERVERs siehe Produktdatenblatt bzw. Produkthandbuch sowie die nachfolgenden Abschnitte dieses Dokumentes.

3. Frequently Asked Questions

3.1. Welche Signaturqualitäten können erreicht werden?

Mit dem primesign SIGNATURE SERVER können verschiedenste Signaturqualitäten erstellt werden. Dazu zählen auch qualifizierte Signaturen und Siegel, die rechtlich die höchste Beweiskraft erreichen.

Primär entscheidend für die Qualitätsstufe einer elektronischen Signatur ist dabei die Qualität des dem verwendeten Signaturmittels zugrunde liegenden Signaturzertifikats. Wenn das verwendete Signaturmittel sich auf qualifizierte elektronische Signaturzertifikate stützt (z.B. auf ein qualifiziertes primesign MOBILE Signaturzertifikat), so können mit dem primesign SIGNATURE SERVER unter Verwendung dieses Signaturmittels, qualifizierte elektronische Signaturen auf Dokumente aufgebracht werden.

Der primesign SIGNATURE SERVER unterstützt eine Vielzahl von Signaturmittel (Signaturzertifikate) unterschiedlichster Anbieter. Er verfügt auch über Standardintegrationen für einige etablierte Signaturmittel. Auf Anfrage können weitere Signaturmittel, wie z.B. Signaturkarten anderer Hersteller, die standardmäßig nicht unterstützt werden, an den primesign SIGNATURE SERVER angebunden werden.

Folgende Signaturmittel werden vom primesign SIGNATURE SERVER standardmäßig unterstützt:

- **primesign MOBILE** (qualifizierter Remote-Signing-Dienst der PrimeSign GmbH, siehe 3.19)
  - Wird unser Remote-Signing-Dienst primesign MOBILE in Kombination mit einem primesign SIGNATURE SERVER On-Premise-Setup genutzt, können wir gewährleisten, dass Dokumente auch während des Signaturvorgangs immer vollständig am primesign SIGNATURE SERVER und damit in der IT-Infrastruktur von Kunden verbleiben.
- **primesign WRAPTOR** (qualifizierte Signatur mit primesign MOBILE Einmalzertifikat auf Basis vorhandener eIDAS eIDs, z.B. deutscher Online-Ausweis, ID Austria/Handy-Signatur, siehe 3.18)
  - Nutzt man primesign WRAPTOR in Kombination mit einem primesign SIGNATURE SERVER On-Premise-Setup, verbleiben auch hier die Dokumente immer vollständig in der IT-Infrastruktur von Kunden (siehe **primesign MOBILE**).

- **ID Austria/Handy-Signatur (A-Trust)**
  - Kann mit oder ohne der Signatur-Box der A-Trust genutzt werden: Durch den Einsatz der Signatur-Box verbleiben die Dokumente auch bei der ID Austria/Handy-Signatur am primesign SIGNATURE SERVER und damit in der Infrastruktur der Kunden. Die Nutzung der Signatur-Box ist kostenpflichtig.
- **Signaturkarten, die über eine zum primesign SIGNATURE SERVER kompatible, lokale Middleware-Software zur Signatur angesprochen werden können.** Eine kompatible Middleware-Software ist eine lokal auf dem Endgerät – z.B. dem Desktop – installierte Software zur Nutzung der Signaturkarte. Die Software muss das Security-Layer-Protokoll als Signaturschnittstelle bereitstellen (Security-Layer Version 1.2[1]). Beispiele für kompatible Middleware-Clients: A-Trust asign Client, it-Solution trustdesk, MOCCA Middleware, etc. Eine derartige Middleware wird in der Regel vom Kartenanbieter zur Verfügung gestellt. Dies deckt heute fast alle gängigen Bürgerkarten und Dienstkarten der österreichischen Verwaltung ab, wie:
  - Dienstkarte der österreichischen öffentlichen Verwaltung (herausgegeben durch bzw. vorbereitet für Zertifikate der A-Trust).
  - A-Trust Signaturkarten

Zusätzlich kann primesign auch verschiedenste serverseitige Signaturmittel (z.B. Software-Zertifikate/Schlüssel oder in einem HSM gehaltene Signaturschlüssel) anbinden, wie es etwa für das Aufbringen von Amtssignaturen oder von (qualifizierten) Siegeln erforderlich ist. Serverseitige Signaturen erfolgen primär sowohl HSM-basiert (Liste unterstützter HSMs auf Anfrage) als auch auf Basis von Softwarezertifikaten.

[1] siehe https://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/Index.html bzw. auch typische Middleware-Produkte: https://www.buergerkarte.at/downloads-karte.html

3.2. Welche Dokumentenformate werden signiert?

Der primesign SIGNATURE SERVER signiert ausschließlich PDF-Dokumente. Zur Signatur von PDF-Dokumenten wird der internationale Signaturstandard PAdES herangezogen. Die Einhaltung dieses Standards gewährleistet eine langfristige und produktunabhängige Prüfbarkeit der mit dem primesign SIGNATURE SERVER erstellten und signierten PDF-Dokumente. Die signierten PDF-Dokumente sind somit mit gängigen Standard-PDF-Werkzeugen prüfbar.

Obwohl der primesign SIGNATURE SERVER ausschließlich PDF-Signaturen erzeugt, können dem Server auch verschiedenste Office-Dokumente übergeben bzw. mit dem primesign SIGNATURE SERVER zur Signatur geöffnet werden. Diese werden vom primesign SIGNATURE SERVER mittels eines integrierten PDF-Konverters zu einem entsprechenden PDF-Dokument umgewandelt.

3.3. Wie lange ist eine elektronische Signatur prüfbar?

Handelt es sich um eine LTV-konforme Signatur, sind Langzeitprüfinformationen in das signierte Dokument miteingebettet. Dadurch bleibt selbst nach Jahren eine vollständige Prüfung der Signatur ohne externe Abhängigkeiten möglich. Insbesondere Signaturen erstellt mit primesign Signaturzertifikaten (z.B. klassische primesign MOBILE Signaturen oder primesign WRAPTOR Signaturen) erfüllen diesbezüglich alle Anforderungen. Die Verwendung von primesign Signaturzertifikaten in Verbindung mit dem primesign SIGNATURE SERVER garantiert die Langzeitprüfbarkeit elektronischer Signaturen.

primesign setzt hier auf bewährte Standards. primesign Signaturen erfüllen die Anforderungen von Level "LT" gemäß ETSI TS 103 172 V2.2.2.[2]

3.4. Wie kann eine elektronische Signatur geprüft werden?

Unsere Signaturlösung – der primesign SIGNATURE SERVER – bietet eine optionale Signaturprüffunktion. Hierbei verwenden wir im Kern dieselbe Prüfsoftware, die auch bei der österreichischen Aufsichtsstelle für Vertrauensdienste und elektronische Signaturen – der Rundfunk- und Telekom-Regulierungsbehörde (RTR) – zum Einsatz kommt. Diese Prüfsoftware wird auch vom öffentlichen Prüfdienst (www.signaturpruefung.gv.at) verwendet.

AnwenderInnen können so mittels der optionalen Prüffunktion des primesign SIGNATURE SERVERs die Prüfung aller Signaturen (auch Signaturen verschiedenster Quellen) eines Dokumentes

[2] https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

vornehmen. Die Signaturprüffunktion kann in der Benutzeroberfläche des primesign SIGNATURE SERVERs aufgerufen werden.

Alternativ dazu kann auch das seitens EU Kommission bereitgestellte DSS Framework[3] zur Signaturprüfung angebunden werden.

3.5. Qualifizierte Elektronische Zeitstempel

Eine mit primesign erstellte elektronische Unterschrift enthält immer den Zeitpunkt der Signatur. Dieser Zeitpunkt wird durch die lokale Serverzeit des eingesetzten primesign SIGNATURE SERVERs festgelegt und bei Signaturen mit primesign MOBILE und primesign WRAPTOR auch mittels Plausibilitätsprüfung gegen das primesign TRUST CENTER geprüft.

Je nach Use Case kann es aber darüberhinausgehende formale Anforderungen an die Dokumentation des Signaturzeitpunkts eines Dokuments geben. Diese Anforderungen können mit primesign unter Nutzung von qualifizierten Zeitstempeln gemäß eIDAS erfüllt werden.

Ein sogenannter Zeitstempel verbindet ein elektronisches Dokument mit der exakten offiziellen Zeit und garantiert so die Existenz eines Dokuments zu einem bestimmten Zeitpunkt. Vor allem in Anwendungen, wo Abgabe- oder Eingangstermine dokumentiert werden, z.B. bei Vergabeverfahren, ist dies oft erforderlich. In Kombination mit LTV (siehe 3.3) wird somit die maximale Beweiskraft eines elektronisch signierten Dokuments erreicht – und dies auch noch nach vielen Jahren. Weiters erfordern manche Signaturprüfanwendungen Zeitstempel um Signaturen auch nach Ablauf der Zertifikatsgültigkeit als vollständig gültig auszuweisen (dies ist insbesondere in Kombination mit primesign Einmalsignaturen von Vorteil).

Mit dem primesign SIGNATURE SERVER kann im Zuge einer Signatur auch ein qualifizierter Zeitstempel ins Dokument eingebracht werden. Die Steuerung, ob Zeitstempel eingebracht werden, erfolgt per primesign SIGNATURE SERVER Konfiguration. Es ist kein Zutun des Benutzers erforderlich.

Standardmäßig werden vom primesign SIGNATURE SERVER keine Zeitstempel eingebracht. Aktivierung von Zeitstempel auf Anfrage. Nutzung des qualifizierten Zeitstempeldienstes erfordert kommerzielle Abklärung.

[3] https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html

3.6. Elektronische Signaturen am Arbeitsplatz

Der primesign SIGNATURE SERVER verfügt über ein webbasiertes User-Interface, das neben der Signatur von Dokumenten auch eine Vielzahl von Zusatzfunktionen aufweist (z.B. Unterschriftenläufe, PDF-Editor-Funktionen).

Für die persönliche elektronische Signatur greifen AnwenderInnen einfach über einen Web-Browser auf die primesign Benutzeroberfläche zu und wählen das zu signierende PDF-Dokument aus dem Dateisystem aus (oder ziehen es per Drag & Drop in das Anwendungsfenster des primesign SIGNATURE SERVERs). Anschließend können AnwenderInnen das Dokument sofort mit allen Funktionen des primesign SIGNATURE SERVERs signieren oder auch Unterschriftenläufe mit KollegInnen oder Externen (wie KundInnen, BürgerInnen etc.) einleiten. Zur Signatur stehen, je nach Konfiguration, wiederum alle möglichen Signaturmittel zur Verfügung (z.B. primesign MOBILE sowie ausgewählte eIDAS eIDs wie z.B. deutscher Online-Ausweis, ID Austria/Handy-Signatur, Dienstkarte). Am Ende des Signaturprozesses kann das signierte PDF-Dokument wieder am Arbeitsplatz gespeichert werden.

3.7. Integration von elektronischen Signaturen in externen Anwendungen

Die Übergabe der zu signierenden Dokumente aus einer Anwendung heraus erfolgt per SOAP-Schnittstelle, und zwar entweder als Einzeldokument oder als Stapel von Dokumenten.

Entsprechend der SOAP-Schnittstelle können AnwenderInnen Einzeldokumente – oder Stapel von Dokumenten – mit dem entsprechenden Signaturmittel signieren. Stehen mehrere Signaturmittel zur Verfügung (zum Beispiel primesign MOBILE, ausgewählte eIDAS eIDs wie z.B. deutscher Online-Ausweis, ID Austria/Handy-Signatur, Dienstkarte) können UnterzeichnerInnen das Signaturmittel vor dem Auslösen der Signatur wählen.

Auf Wunsch steht AnwenderInnen auch die gesamte Benutzeroberfläche des primesign SIGNATURE SERVERs zur Verfügung, sodass ein Dokument gelesen oder das geeignete Signaturbild ausgewählt und an die richtige Stelle im Dokument platziert werden kann.

Die erfolgreich signierten Dokumente oder eine entsprechende Fehlermeldung werden über unsere SOAP-Schnittstelle an die aufrufende Anwendung zurückübermittelt.

Als Referenz können wir beispielsweise die Integration von primesign beim ELAK-im-Bund nennen. Auf eine detaillierte Beschreibung der SOAP-Schnittstelle wird am Ende des Dokumentes referenziert.

3.8. Wiederholtes bzw. mehrfaches Signieren von Dokumenten

Dokumente können mit dem primesign SIGNATURE SERVER mehrfach signiert werden. Dies gilt auch für Dokumente, die bereits im Vorfeld signiert wurden. Diese können mit dem primesign SIGNATURE SERVER erneut mehrfach signiert werden (z.B. Gegenzeichnen).

Ein Dokument kann also beliebig oft mit dem primesign SIGNATURE SERVER signiert werden, und zwar ungeachtet davon, ob bereits (mehrere) Signaturen mit primesign aufgebracht wurden, oder ob das Dokument bereits andere Signaturen aus anderen (externen) Quellen enthält. Externe Signaturen, die zuvor auf ein Dokument aufgebracht wurden, müssen jedenfalls dem PAdES-Signaturstandard entsprechen und dürfen das PDF-Dokument nicht sperren oder verschlüsseln.

Beim Mehrfachsignieren wird ein bereits zuvor signiertes Dokument erneut in die Benutzeroberfläche des primesign SIGNATURE SERVERs geladen (oder per SOAP-Schnittstelle an den primesign SIGNATURE SERVER übergeben).

Vor dem erneuten Unterzeichnen können die bestehenden Signaturen auf Wunsch der AnwenderInnen auch geprüft werden. So kann die Richtigkeit aller vorab aufgebrachten Signaturen ungeachtet deren Quellen sichergestellt werden. Der übrige Workflow ist identisch zu dem einer Einzelsignatur.

3.9. Stapelsignatur

Der primesign SIGNATURE SERVER unterstützt die Stapelverarbeitung von Signaturen. Das heißt, dass mehrere Signaturen, die auf einen Stapel von Dokumenten aufgebracht werden sollen, mit nur einer Freigabe ausgelöst werden können. Allerdings muss das Signaturmittel (Signaturkarte und Middleware bzw. die entsprechende Remote-Signatur) die Stapelsignaturverarbeitung unterstützen. primesign MOBILE als auch primesign WRAPTOR unterstützen die Stapelsignatur standardmäßig. Bei Nutzung von primesign WRAPTOR ist es somit möglich, dass auch mit eIDAS-Identitäten wie z.B. deutscher Online-Ausweis, ID Austria/Handy-Signatur oder anderen bestehenden Signaturzertifikaten, die von primesign WRAPTOR unterstützt werden, Stapelsignaturen ausgelöst werden können. Mit primesign MOBILE bzw. primesign WRAPTOR ist es möglich bis zu 30 Dokumente mit nur einer Freigabe zu signieren.

Die Stapelsignatur wird auch von den A-Trust Boxen und den in 3.1 genannten Signaturkarten – mit dem entsprechenden a.sign Client oder MOCCA Middleware Komponenten unterstützt.

Eine Stapelsignatur kann über die Benutzeroberfläche des primesign SIGNATURE SERVERs mittels der Unterschriftenmappen-Funktion ausgelöst werden. Alle vorgelegten oder selbst hinzugefügten, noch zu signierenden Dokumente können von AnwenderInnen im Stapel, das heißt in einem Durchgang und mit nur einer Freigabe (zum Beispiel PIN-Eingabe oder SMS-Freigabe) signiert werden. Anschließend können die Dokumente dann im Stapel – als ZIP-Container – oder einzeln weiterverarbeitet werden.

Die Übergabe der zu signierenden Dokumente aus einer externen Anwendung heraus erfolgt per SOAP-Schnittstelle. Die Dokumente werden entweder als Einzeldokument oder, im Falle einer Stapelsignatur, als Stapel übergeben. Entsprechend der SOAP-Schnittstelle kann dann das Einzeldokument – oder der Stapel – unmittelbar mit dem entsprechenden Signaturmittel signiert werden. Stehen mehrere Signaturmittel zur Auswahl, können UnterzeichnerInnen das Signaturmittel vor dem Auslösen der Signatur wählen. Die erfolgreich signierten Dokumente oder eine entsprechende Fehlermeldung werden an die aufrufende Anwendung über unsere SOAP-Schnittstelle zurückübermittelt.

3.10. Zwei-Faktor-Authentifizierung beim Auslösen von Signaturen

Bei qualifizierten Signaturen werden heute ausschließlich 2-Faktor-Authentifikationsprozesse verwendet. In der Regel bedingt hier schon das verwendete Signaturmittel eine Zwei-Faktor-Authentifizierung, wie beispielsweise eine Signaturkarte oder eine auf Mobiltelefonen basierende qualifizierte Remote-Signatur wie z.B. primesign MOBILE Signatur oder ID Austria/Handy-Signatur (2 Faktoren: Entweder durch Besitz der Signaturkarte + Wissen der PIN; oder Wissen des Passworts + Besitz des Mobiltelefons (SMS/App) etc.).

Für derartige Signaturen zugelassene und mit dem primesign SIGNATURE SERVER nutzbare qualifizierte Signaturmittel gewährleisten immer eine derart starke Authentifikation.

3.11. Integrationsschnittstellen

Das Dokument primesign SIGNATURE SERVER – Integration Documentation [3] bietet eine ausführliche Dokumentation der Standard-Integrationsschnittstellen des primesign SIGNATURE SERVERs.

3.12. primesign SIGNATURE SERVER – Mandantenfähigkeit

Es können sowohl mehrere Organisationen (Mandanten) an einem Server angebunden als auch eine Mandanten-Separation über virtuelle Instanzen erreicht werden. Beim ersteren Ansatz (mehrere Organisationen auf einem Server) empfiehlt es sich, die Nutzerverwaltung über ein externes Active Directory vorzunehmen und dieses an primesign anzubinden. Hierbei ist jedoch zu beachten, dass diese Organisationen unter einer Active-Directory-Domäne organisiert sein müssen.

Demgegenüber werden strikt zu trennende Mandanten jeweils über eigene virtuelle Instanzen des primesign SIGNATURE SERVERs abgebildet. Damit wird auch eine komplette Trennung auf Basis von eigenständigem Schlüsselmaterial zur Verschlüsselung der auf den Servern jeweils verarbeiteten Dokumente und Daten erreicht.

Die Art der Abbildung von Mandanten wird letztlich durch die kundenseitigen Anforderungen bestimmt.

3.13. Wie ist die Definition "Nutzer-Lizenz" zu verstehen?

Der Begriff „Nutzer-Lizenz" bezieht sich nicht auf Mandanten oder Rechenzentren. „Nutzer-Lizenzen" beziehen sich auf die Anzahl der sogenannten Named-User (das sind die signierenden Personen mit einem eigenen User-Account und somit Signaturprofil) pro Serverinstanz. Named-User können den vollen Funktionsumfang eines primesign SIGNATURE SERVERs nutzen. Dies umfasst u.a. die Unterschriftenmappe, die Möglichkeit zum Starten eines Unterschriftenlaufs oder die Nutzung von Vorlagen für Unterschriftenläufe. Weiters kann für Named-User eine unlimitierte Anzahl persönlicher Signaturprofile erstellt werden.

3.14. Wie kommt man rasch zu einem Signaturzertifikat?

Ist noch kein Signaturzertifikat vorhanden, so bietet das primesign TRUST CENTER über einen Online-Registrierungsprozess (Onboarding) eine einfache und sofort umsetzbare Möglichkeit, sich per Remote-Identifikation wie Video oder eID (z.B. deutscher Online-Ausweis, ID Austria/Handy-Signatur) ein qualifiziertes primesign MOBILE Signaturzertifikat ausstellen zu lassen. Die Ausstellung kann rund um die Uhr von zu Hause oder dem Büro gestartet werden und nimmt nur wenige Minuten in Anspruch. Eine Identifikation per Video ist täglich von 07:00 bis 22:00 (CET) möglich.

3.15. Welche Videoidentifikationsdienste bietet primesign als Vertrauensdienst an?

Die PrimeSign GmbH hat als Vertrauensdiensteanbieter mehrere Videolegitimationsdienste von etablierten Anbietern zur Ausstellung von qualifizierten Signaturzertifikaten angebunden. Die PrimeSign GmbH hat auch die entsprechende Zulassung, diese Dienste zur Legitimation heranzuziehen und demnach anzubieten.

Unter anderem werden der Videolegitimationsdienst der Kapsch, der österreichischen Staatsdruckerei oder der WebID Solutions GmbH angeboten (Reihung in alphabetischer Folge).

Eine Anbindung anderer eIDAS-konformer Videoidentifikationsdienstleister ist auf Wunsch und Anfrage möglich.

Alternativ zur Videoidentifikation kann für die Ausstellung eines primesign MOBILE Signaturzertifikats auch eine bestehende eIDAS eID zur Identifikation herangezogen werden (siehe 3.16).

3.16. Welche eIDs unterstützt primesign zur Zertifikatsausstellung bzw. zur Signatur?

Folgende eIDs werden bei der Signatur mit primesign WRAPTOR (siehe 3.18) sowie als Alternative zur Videoidentifikation bei der Zertifikatsaustellung mittels primesign OnBoarding-System unterstützt:

- ID Austria
- Handy-Signatur
- Deutscher Online-Ausweis
- Weitere eIDs folgen in Kürze

3.17. Was wird benötigt, um den deutschen Online-Ausweis zur Zertifikatsausstellung bzw. zur Signatur nutzen zu können?

Zur Nutzung des deutschen Online-Ausweises sind folgende Voraussetzungen zu erfüllen:

- Online-Ausweis (Online-Ausweisfunktion muss aktiviert sein. Folgende Ausweise können genutzt werden: Personalausweis, Unionsbürgerkarte, Elektronischer Aufenthaltstitel)
- Installation und Öffnen der AusweisApp (oder vergleichbare Anwendungen)
- Kartenleser zur Auslesung des Ausweises. Ihr Mobiltelefon kann ebenso als Kartenleser genutzt werden, sofern dies NFC unterstützt.
- Gesetzter PIN. Sie haben einen selbstgewählten, sechsstellige PIN gesetzt.

3.18. Was ist primesign WRAPTOR?

Als neues Service unseres Trust Centers ermöglicht primesign WRAPTOR die einfache, schnelle und sofortige Erstellung von qualifizierten elektronischen Signaturen mittels ausgewählten eIDAS eIDs Technisch wird dabei die bestehende eID von AnwenderInnen zur Identifikation herangezogen und im Anschluss „on-the-fly" ein primesign Einmalzertifikat ausgestellt, das sofort und nur für diese eine Signatur genutzt wird. In der Praxis entscheiden sich AnwenderInnen in der Benutzeroberfläche des primesign SIGNATURE SERVERs einfach dafür, eine Signatur per bestehender eID zu autorisieren. So kann sofort, direkt und ohne vorherige Registrierung bei primesign mit primesign Einmalzertifikaten signiert werden. primesign WRAPTOR wird vom primesign SIGNATURE SERVER standardmäßig unterstützt.

Für Kunden ergeben sich folgende Vorteile:

- **Keine Registrierung bei primesign:** AnwenderInnen nutzen Ihre bestehende eID zur Signatur. Keine Registrierung bei primesign erforderlich und daher ideal für gelegentliche Nutzung.

- **Signieren mit eIDAS eID:** Ideal für multinationale Unternehmen, die MitarbeiterInnen und KundInnen einen schnellen Weg zur qualifizierten elektronischen Signatur ermöglichen wollen. Die Liste an europäischen eIDAS IDs, die primesign zur Signatur unterstützt, wird dabei stetig erweitert.
- **Stapelsignatur:** Mit primesign WRAPTOR können mehrere Dokumente (maximal 30) auch mit eIDAS-Identitäten oder bestehenden Signaturzertifikaten von Drittanbietern auf einmal im Stapel und mit nur einer Freigabe unterzeichnet werden.
- **Vertraulichkeit:** Bei Nutzung des primesign WRAPTORs in Kombination mit einem primesign SIGNATURE SERVER On-Premise-Setup verbleiben Dokumente auch während des Signaturvorgangs immer vollständig in der IT-Infrastruktur von Kunden.
- **Unified Trust & Einheitliche Haftung:** Immer mit primesign Signaturzertifikaten signieren, unabhängig davon, welches Signaturmittel verwendet wird; ein Rechtsrahmen, ein verantwortlicher Trust Partner – primesign TRUST CENTER.
- **Unified Trust & Langzeitprüfbarkeit:** Unabhängig von der verwendeten eID werden langzeitprüfbare und rechtsverbindliche qualifizierte Signaturen mit einem primesign Einmalzertifikat erstellt. primesign gewährleistet, dass die Signaturen auch noch in 30+ Jahren prüfbar sind.

Auch bei Nutzung des primesign OnBoarding-System profitieren AnwenderInnen von der Möglichkeit, sich alternativ zur Videoidentifikation per bestehender eID zu identifizieren und für primesign MOBILE zu registrieren. AnwenderInnen können sich so rund um die Uhr und innerhalb kürzester Zeit ein persistentes primesign MOBILE Signaturzertifikat (Gültigkeit von bis zu 5 Jahren, siehe 3.20) ausstellen lassen.

3.19. Was ist primesign MOBILE?

primesign MOBILE ist der qualifizierte Remote-Signing-Dienst der PrimeSign GmbH. Mit primesign MOBILE signieren Sie unkompliziert qualifiziert. Sie geben Signaturen bequem mit Ihrem Handy frei und das ohne zusätzliche Installation einer App. Um mit primesign MOBILE qualifiziert zu signieren, benötigen Sie ein sogenanntes qualifiziertes Signaturzertifikat (primesign MOBILE Zertifikat). Hierbei unterscheidet man zwischen Einmalsignaturzertifikaten und persistenten Signaturzertifikaten (siehe 3.20). primesign MOBILE wird vom primesign SIGNATURE SERVER standardmäßig unterstützt.

3.20. primesign MOBILE Zertifikate – welche Typen gibt es?

Die PrimeSign GmbH bietet auf Basis ihres qualifizierten Remote-Signing-Dientes primesign MOBILE sowohl Einmalsignaturzertifikate als auch klassische persistente Signaturzertifikate an. Zur Ausstellung der Signaturzertifikate ist unser eigenes eIDAS-konformes Trust Center berechtigt.

Das qualifizierte Einmalsignaturzertifikat wird „on-the-fly" ausgestellt, hat eine Gültigkeit von wenigen Minuten und ist so nur einmalig für eine Signaturtransaktion nutzbar. Es eignet sich optimal für Online-Vertragsabschlüsse (ermöglicht über unsere Integrationsschnittstellen und eng gekoppelt mit einer unmittelbar vorangegangenen Videolegitimation oder Identifikation per eID). Auch bei der Signatur mit primesign WRAPTOR wird ein primesign MOBILE Einmalzertifikat ausgestellt (siehe 3.18).

Das persistente Signaturzertifikat hat derzeit eine Gültigkeit von bis zu 5 Jahren. Es eignet sich daher für Anwendungsfälle und UserInnen, die wiederkehrend Signaturen leisten müssen, wie z.B. MitarbeiterInnen oder Business-KundInnen. Ein persistentes Signaturzertifikat können Sie sich mittels unseres OnBoarding-Systems online und in nur wenigen Minuten ausstellen lassen (siehe 3.14).

Beide Signaturzertifikatstypen bieten natürlich dieselben funktionellen (z.B. Stapelsignaturverarbeitung) und rechtlichen Merkmale und entfalten dieselbe höchste Rechtswirkung und Sicherheit. Bei der Auswahl der geeigneten Ausprägung sind ausschließlich die Kundenanforderungen und der Use-Case entscheidend.

3.21. primesign in Adobe Acrobat Sign

primesign MOBILE ist der Remote-Signing-Dienst von primesign, der auch für qualifizierte elektronische Signaturen in Adobe Acrobat Sign verwendet werden kann. primesign MOBILE kann dabei direkt aus Adobe Acrobat Sign genutzt werden, um Dokumentensignaturen einfach und schnell freizugeben. Weitere Informationen zu primesign MOBILE für Adobe Acrobat Sign finden Sie auf unserer Website: www.prime-sign.com/adobe. primesign MOBILE für Adobe Acrobat Sign kann auch direkt in unserem Online Shop erworben werden.

Mittels „Signieren mit eID" (primesign WRAPTOR) können BenutzerInnen aus Adobe Acrobat Sign sofort und ohne Registrierung mit primesign eine bestehende eIDAS eID (z.B. deutscher Online-Ausweis, ID Austria oder österreichische Handy-Signatur) zur Signatur verwenden.

3.22. primesign in der Fabasoft eGov Suite

primesign ist als Standard-Signaturanbieter in der Fabasoft eGov Suite integriert. Die Fabasoft eGov Suite nutzt nahtlos und medienbruchfrei die primesign Webanwendung, um persönliche elektronische Signaturen auf Dokumente aufzubringen.

Mittels „Signieren mit eID" (primesign WRAPTOR) können BenutzerInnen mit der Fabasoft eGov Suite sofort und ohne Registrierung mit primesign eine bestehende eIDAS eID (z.B. deutscher Online-Ausweis, ID Austria oder österreichische Handy-Signatur) zur Signatur verwenden.

3.23. CSC-Unterstützung

primesign ist Mitglied des Cloud Signature Consortium[4]. Das Cloud Signature Consortium ist ein internationaler Zusammenschluss von Experten aus dem universitären Umfeld und der Industrie zur Schaffung eines neuen Standards für cloudbasierte digitale Signaturen (CSC-Standard). Unser Remote-Signing-Dienst primesign MOBILE ist CSC-konform und so via CSC-API einfach in eine Vielzahl von Signaturanwendungen integrierbar. Somit kann sowohl die Signatur mit primesign MOBILE Signaturaccounts als auch „Signieren mit eID" (primesign WRAPTOR) leicht in CSC-konforme Signaturanwendungen integriert werden.

Siehe [6] für mehr Informationen zur Integration via CSC-API.

[4] https://cloudsignatureconsortium.org/

4. Darstellung der Unternehmenszugehörigkeit und Funktion in elektronischen Signaturen

⚠ Für eine rechtsverbindliche digitale Signatur – rechtsverbindlich auf dem Niveau einer handschriftlichen Unterschrift – benötigt eine natürliche Person ein qualifiziertes Signaturzertifikat. Dieses Zertifikat ist an die natürliche Person gebunden. Alle Berechtigungen und Vertretungsbefugnisse die eine Person bereits besitzt, können so auch im elektronischen Umfeld ausgeübt werden. Diese Berechtigungen und Rollen sind rechtlich etabliert und können somit auch auf konventionellen Wege außerhalb der Signatur nachgewiesen werden.

Es gibt verschiedene Möglichkeiten, Unternehmenszugehörigkeit, Rollen und Funktionen in elektronischen Signaturen darzustellen. Sie können z.B. in das Zertifikat eingebettet UND im visuellen Signaturbild angezeigt werden oder auch „nur" im visuellen Signaturbild angezeigt und nicht ins Zertifikat aufgenommen werden.

AUFNAHME INS SIGNATURZERTIFIKAT UND ANZEIGE IM SIGNATURBILD

Alle Daten, die in ein qualifiziertes Signaturzertifikat eingebettet werden, müssen von der Zertifizierungsstelle, die das Zertifikat ausstellt, strengstens überprüft werden. Eine solche Zertifizierungsstelle ist ein staatlich beaufsichtigter und nach EU-Recht agierender so genannter Vertrauensdiensteanbieter wie z.B. die PrimeSign GmbH. Im einfachsten Fall enthält ein Zertifikat die Personendaten, die über anerkannte (amtliche) Ausweise oder vergleichbare Dokumente verifiziert werden. Personendaten, die in primesign Signaturzertifikate eingebettet werden, werden dabei entweder via Video-Identifikation durch Verifizierung des Ausweises geprüft oder von der zur Registrierung verwendeten eID (z.B. ID Austria/Handy-Signatur) übernommen.

Im Rahmen von primesign Business Zertifikaten können zudem aber auch zusätzliche Attribute, wie etwa die Zugehörigkeit zu einer Organisation, Funktionen und Rollen innerhalb dieser Organisation (z.B. GeschäftsführerIn, ProkuristIn) oder auch die E-Mail-Adresse in das Zertifikat aufgenommen werden. Alle EmpfängerInnen eines mit einem solchen Zertifikat signierten Dokumentes können diese Zusatzinformationen durch Prüfung der Signatur sehen. Eine Person, die eine Funktionsbezeichnung (Rolle) beansprucht, signiert elektronisch rechtsverbindlich durch Angabe dieser Funktion. primesign überträgt die Pflichten zur Bereitstellung, Prüfung bzw. Sicherstellung dieser Attribute auf die jeweiligen Organisationen. Für die Ausstellung von Business-Zertifikaten müssen Organisationen daher eine Vertragsbeziehung mit primesign eingehen.

In dieser Vertragsbeziehung werden folgende Punkte vereinbart:

- Die Organisation ist Inhaberin der Domain *.musterorganisation.at und die Vergabe von E-Mail-Adressen an MitarbeiterInnen erfolgt unter ihrer alleinigen Kontrolle
- InhaberInnen von Organisations-E-Mail-Adressen (z.B. max.mustermann@musterorganisation.at) dürfen die Organisationszugehörigkeit im Zertifikat führen (der im Firmenbuch eingetragene offizielle Organisationsname muss als Attribut „O" im Feld Antragsteller/in erfasst sein)
- Wird eine Rolle innerhalb der Organisation eingebracht, gilt folgendes: Die Organisation muss primesign einen Datensatz zur Verfügung stellen, der die E-Mail-Adresse der Person mit der Rolle verknüpft sowie primesign notwendige Nachweise übermitteln, die dies belegen (z.B. max.mustermann@musterorganisation.at enthält die Rolle Geschäftsführer)
- Gemäß der Bedingungen zur Nutzung für qualifizierte Zertifikate der PrimeSign GmbH besteht eine Widerrufspflicht, wenn sich bescheinigte Umstände im qualifizierten Zertifikat ändern. Dies gilt auch für die Organisationszugehörigkeit, Rolle und die E-Mail-Adresse. Sollte eine Berechtigung erlöschen, so muss die Organisation einen Zertifikatswiderruf initiieren.

Auch wenn die Pflichten zur Bereitstellung, Prüfung bzw. Sicherstellung von Attributen an die jeweiligen Organisationen übertragen werden, bleibt rechtlich normativ natürlich – wie im konventionellen Fall – die entsprechende Quelle für solche Berechtigungen, wie bei GeschäftsführerInnen das Firmenbuch, etc.

Vorteil gegenüber der Papierwelt: Durch die in ein elektronisches Zertifikat eingebetteten personenbezogenen Daten lässt sich jederzeit zweifelsfrei nachvollziehen, wer entsprechende Angaben – auch fälschlicherweise – gemacht und per Signatur bestätigt hat. Die in einem Zertifikat eingebetteten Funktionen und Rollen können zusätzlich auch im visuellen Signaturbild angezeigt und somit für EmpfängerInnen beim Öffnen eines Dokumentes sofort sichtbar gemacht werden.

ANZEIGE NUR IM SIGNATURBILD

Mit dem primesign SIGNATURE SERVER kann eine Funktionsbezeichnung (Rolle) auch „nur" im visuellen Signaturbild angezeigt und nicht in das Signaturzertifikat aufgenommen werden. Wird eine Rolle oder Funktion „nur" im Signaturbild angezeigt aber nicht im Zertifikat eingebettet, entspricht das eher dem konventionellen Umgang, bei dem die Unterzeichnerin oder der Unterzeichner selbst – z.B. ein Prokuristin oder ein Prokurist durch das Hinzufügen von "p.p.a." – ihr/sein Vertretungsbefugnis zum Ausdruck bringt. Hierfür eignen sich insbesondere verschiedene Vertretungsbefugnisse die im Innenverhältnis eines Unternehmens, etwa durch Geschäftsordnung und Organigramm, begründet werden, jedoch nicht unbedingt Einzug ins Firmenbuch finden (z.B. EinkäuferIn, VerkäuferIn) oder die einer gewissen Dynamik unterliegen.

Die Darstellung der Unternehmenszugehörigkeit in einer elektronische Signatur ist ähnlich der Darstellung von Funktionsbezeichnungen oder Rollen. Auch hier kann und soll der Name der juristischen Person, für die die natürliche Person agiert, als geprüftes und belegtes Attribut in das qualifizierte Signaturzertifikat aufgenommen werden. Auf diese Weise hätte die Person alle relevanten Merkmale als verifiziertes Attribut in ihrem persönlichen Signaturzertifikat erkennbar (z.B. Name + Rolle der Geschäftsführerin oder des Geschäftsführers + Firma + FB-Nummer). Aber auch die Unternehmenszugehörigkeit kann alternativ „nur" über Textelemente im Signaturbild abgebildet und nicht ins Signaturzertifikat aufgenommen werden (siehe vorherige Absätze).

Ergänzend dazu gibt es auch die „elektronische Signatur eines Unternehmens": das sogenannte elektronische Siegel. Ein elektronisches qualifiziertes Siegel ist EU-weit rechtlich akzeptiert, basiert wie die qualifizierte Signatur auf der eIDAS-Verordnung und ist technisch vergleichbar mit der qualifizierten elektronischen Signatur natürlicher Personen. Rechtlich entspricht das Siegel dem „digitalen Unternehmensstempel", sprich es dient der "Ursprungsfeststellung" (d.h. das Dokument stammt aus dem Unternehmen, das im Siegelzertifikat ausgewiesen wird) und zur Prüfung der Unversehrtheit (d.h. das Dokument wurde nachträglich nicht verändert). Der einzige bedeutsame rechtliche Unterschied zur qualifizierten Signatur der natürlichen Person ist, dass das Siegel keine Willenserklärung darstellt. Dazu braucht es, wie im Papierfall, immer die handelnde/n Person/en und so eben auch die persönliche/n elektronische/n Signatur/en der handlungsbefugten Person/en.

Die Siegelsignatur des Unternehmens kann auch mit einer qualifizierten Signatur der handelnden Person kombiniert und gemeinsam auf die Dokumente eines Unternehmens aufgebracht werden. Enthält aber bereits das qualifizierte Signaturzertifikat der handelnden Person den Firmenbezug als geprüftes Attribut im Zertifikat, so wäre ein zusätzliches Siegel an sich nicht notwendig. Das Unternehmenssiegel hingegen kann allein ebenfalls verwendet werden, etwa um Rechnungen, ausgehende Dokumente, AGBs etc., in Massenprozessen zu signieren, um so auch bei Massendokumenten den Bezug zum Unternehmen herzustellen.

Einige offizielle EU-weite Anwendungen, wie z.B. das European Product Registry for Energy Labelling (EPREL), erfordern bei der Registrierung eine elektronische Verifizierung mittels eines qualifizierten elektronischen Siegels. Mit dem primesign MOBILE SEAL bieten wir die perfekte Lösung, um Unternehmen schnell und einfach in der EPREL-Datenbank zu registrieren. Wir bieten das primesign MOBILE SEAL in einem Jahrespaket an. Im Angebot enthalten sind:

- Die Ausstellung eines qualifizierten primesign MOBILE SEAL Zertifikats (lautend auf den Namen des Unternehmens)
- Ein primesign PREMIUM Signatur-Service-Account für unser Online-Signaturservice (www.prime-sign.com)
- Eine unlimitierte Anzahl von Siegeltransaktionen pro Jahr (Fair-Use-Prinzip)

Im Zuge der Beantragung wird zudem ein persönliches primesign MOBILE Signaturzertifikat (qualifiziertes Signaturzertifikat gem. eIDAS) für persönliche elektronische Signaturen ausgestellt. Das Signaturzertifikat kann von der antragstellenden Person zusätzlich zum Siegel genutzt werden (Zertifikation und Transaktionen sind im Preis enthalten).

Die Ausstellung des primesign MOBILE SEAL Zertifikats erfolgt online und erfordert eine Identifikation per Video. Diese ist zwingend von einer für die Organisation vertretungsbefugten Person durchzuführen. Zudem sind weiterführende Nachweise, wie z.B. Firmenbuchauszug vorzulegen. Weitere Informationen zu unserem Angebot und zum Ausstellungsprozess finden Sie auf unserer Website: www.cryptas.com/trust-center. primesign MOBILE SEAL kann auch direkt in unserem Online-Shop erworben werden.

5. Dokumentensicherheit und Signaturtransaktionen

Eine oft wiederkehrende Fragestellung bezieht sich auf den Verbleib eines zu signierenden Dokumentes während einer Signaturtransaktion (Signaturvorgang, Aufbringen der Signatur auf ein Dokument), wenn ein Dokument die IT-Infrastruktur des Kunden nicht verlassen soll. Wie kann sichergestellt werden, dass sensible Dokumente während einer Signaturtransaktion in der IT-Infrastruktur von Kunden verbleiben?

Um zu gewährleisten, dass ein Dokument die IT-Infrastruktur von Kunden nicht verlässt, muss der primesign SIGNATURE SERVER zum einem vor Ort (On-Premise) betrieben werden. Zum anderen spielt auch das verwendete Signaturmittel eine entscheidende Rolle.

Wird der primesign SIGNATURE SERVER On-Premise betrieben, verbleibt ein Dokument bis zum eigentlichen Auslösen der Signatur immer in der IT-Infrastruktur von Kunden. Der Server kann dabei sowohl als virtuelle Appliance oder optional als Hardware-Appliance in Betrieb genommen werden. Das verwendete Signaturmittel (Zertifikat) hingegen ist entscheidend, ob im Anschluss ein Dokument auch während der Signaturtransaktion (Signaturvorgang, Aufbringen der Signatur) in der IT-Infrastruktur von Kunden verbleibt.

> Unser Portfolio umfasst sowohl die On-Premise-Installation des primesign SIGNATURE SERVERs als auch die Bereitstellung eines virtuellen Servers im Rahmen unserer Betriebsinfrastruktur (SaaS in Rahmen unserer Private Cloud). In Saas-Betriebsmodellen verlässt das zu signierende Dokument jedoch zwangsläufig die IT-Infrastruktur von Kunden, unabhängig vom verwendeten Signaturmittel.

Wird der primesign SIGNATURE SERVER On-Premise betrieben und ein geeignetes Signaturmittel verwendet, so kann jedenfalls sichergestellt werden, dass ein Dokument während des gesamten Signaturprozesses (Dokument-Upload, Signaturvorgang, Dokumentablage) in der IT-Infrastruktur von Kunden verbleibt.

Zum Beispiel kann zum Aufbringen der Signatur eine Signaturkarte verwendet werden. In diesem Fall ist immer gewährleistet, dass ein Dokument ohne weitere Infrastruktur oder Komponenten in der IT-Infrastruktur des primesign SIGNATURE SERVERs und am Arbeitsplatz von UnterzeichnerInnen verbleibt. Konkret: Die Signatur wird über den On-Premise betriebenen primesign SIGNATURE SERVER und über die lokal am PC-Arbeitsplatz angebundene Signaturkarte von UnterzeichnerInnen erstellt – das Dokument verlässt diese Bereiche nicht.

Auch wenn unser Remote-Signing-Dienst primesign MOBILE oder primesign WRAPTOR (siehe 3.19 und 3.18) in Kombination mit einem primesign SIGNATURE SERVER On-Premise-Setup genutzt wird, können wir gewährleisten, dass Dokumente während des gesamten Signaturprozesses immer

vollständig in der IT-Infrastruktur von Kunden verbleiben. Zu signierende Dokumente werden hier nicht an primesign übermittelt. primesign erhält lediglich den sogenannten Hash-Wert (Fingerabdruck) der zu signierenden Dokumente. Daraus lässt sich der Dokumenteninhalt nicht ableiten.

Bei Remote-Signaturen mit ID Austria oder der Handy-Signatur (sofern nicht in Verbindung mit primesign WRAPTOR genutzt) hingegen, müssen besondere Vorkehrungen getroffen werden, um sicherzustellen, dass Dokumente während eines Signaturprozesses die IT-Infrastruktur von Kunden nicht verlassen. Damit hier nicht das gesamte Dokument an die Remote-Signing-Infrastruktur der A-Trust übermittelt wird und somit der Schutz von sensiblen Inhalten gewährleistet werden kann, bietet die A-Trust eine zusätzliche Hardware-Komponente (Signatur-Box), die das Aufbereiten des Dokumentes zur Signatur lokal vornimmt.

Der primesign SIGNATURE SERVER kann mit der Signatur-Box der A-Trust out of the box verbunden werden und nutzt diese als „Gateway" zur A-Trust.

Die nachfolgende Tabelle zeigt nochmals den Zusammenhang zwischen der jeweiligen Deployment-Architektur und dem verwendeten Signaturmittel. Die Tabelle gibt auch Aufschluss über den Verbleib der zu signierenden Dokumente während einer Signaturtransaktion.

Tabelle 1: Dokumentensicherheit in Abhängigkeit von Deployment-Architektur und Signaturmittel

Zu signierende Dokumente verbleiben in der Infrastruktur von Kunden			
		Deployment-Architektur primesign SIGNATURE SERVER	
		On-Premise	*SaaS (Private Cloud der CRYPTAS)*
Signaturmittel samt allfälliger Zusatzanforderungen	***Serverseitige Signaturerstellung*** *mit SW-Schlüssel/-Zertifikat oder mit in einem HSM gehaltenen Signaturschlüssel/-zertifikat direkt am primesign SIGNATURE SERVER angebunden bzw. konfiguriert*	**Ja**	Nein
	Signaturkarte *zum Beispiel Dienstkarte, Bürgerkarte. Unabhängig vom Zertifizierungsdiensteanbieter (Vertrauensdienst)*	**Ja**	Nein
	ID Austria/Handy-Signatur (A-Trust) ohne lokaler Komponente und nicht in Verbindung mit primesign WRAPTOR genutzt	Nein	Nein
	ID Austria/Handy-Signatur (A-Trust) mit lokaler Komponente (A-Trust Signatur-Box On-Premise)	**Ja**	Nein
	primesign MOBILE	**Ja**	Nein
	primesign WRAPTOR	**Ja**	Nein

6. Exemplarische Deployment-Architekturen

Das folgende Kapitel beschreibt und skizziert zwei typische Deployment-Architekturen: ein einfache On-Premise-Architektur und dessen äquivalent als Managed Service (SaaS).

⚠ Die schematischen Skizzen der Deployment-Architekturen zeigen die Wechselwirkungen und Zusammenhänge wichtigster Kernelemente. Weiterführende Aspekte, wie z.B. Redundanzen, Single-Sign-On (Domain-Authentifikation), LDAP-Anbindungen, Ausfallsicherheit und Backup etc. werden aus Gründen der Vereinfachung nicht dargestellt.

6.1. On-Premise

Die in

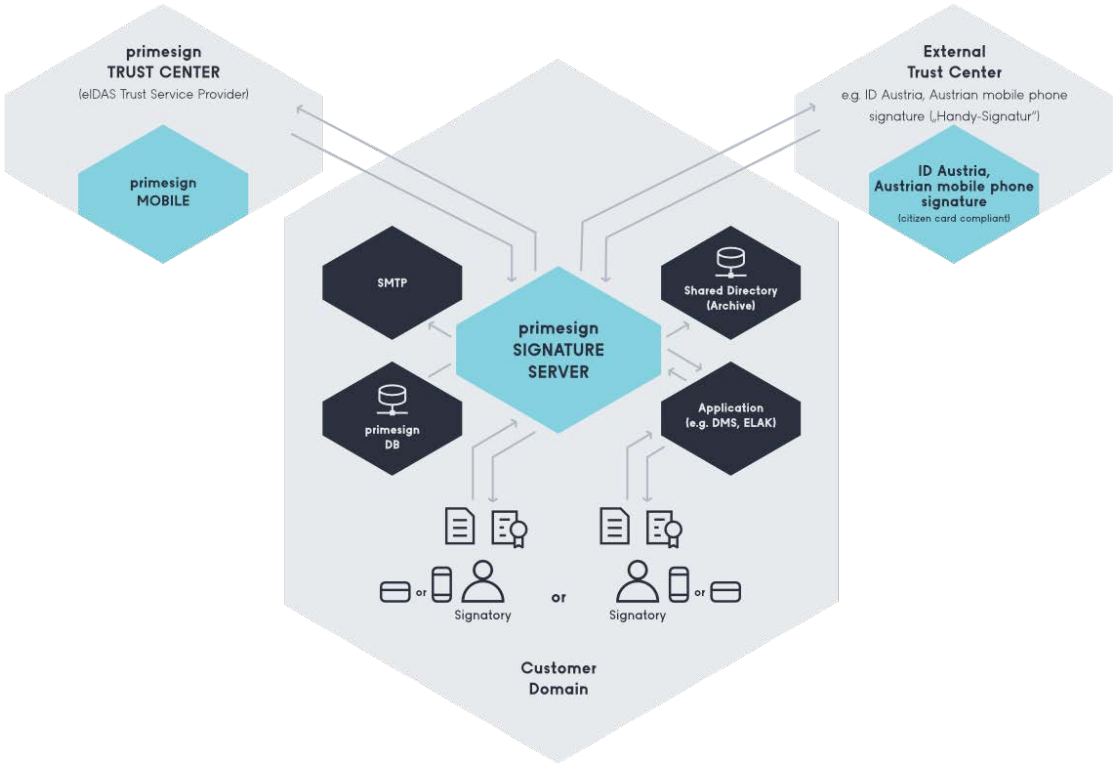

Abbildung 5 skizzierte exemplarische Architektur liefert einen Überblick über die wichtigsten Komponenten einer On-Premise-Architektur sowie über Abhängigkeiten zwischen den einzelnen

Systemelementen.

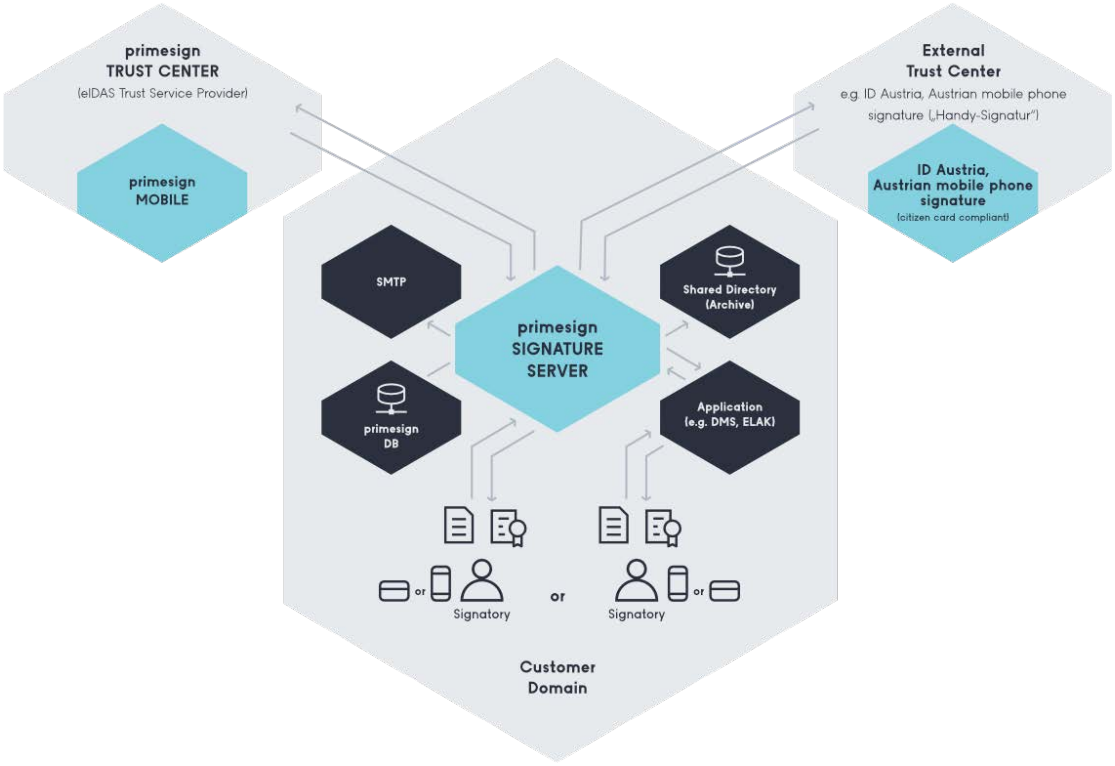

Abbildung 5 zeigt auch exemplarisch die Anbindung von Remote-Signing-Lösungen, wie z.B. primesign MOBILE oder ID Austria/Handy-Signatur (A-Trust). Bei der Verwendung von primesign MOBILE in Kombination mit einem primesign SIGNATURE SERVER On-Premise-Setup, können wir gewährleisten, dass Dokumente während des gesamten Signaturprozesses immer vollständig in der IT-Infrastruktur von Kunden verbleiben (auch in Verbindung mit primesign WRAPTOR). Bei der Verwendung von ID Austria/der Handy-Signatur (wenn nicht in Verbindung mit primesign WRAPTOR genutzt) sind zusätzliche Komponenten erforderlich, wenn der Dokumenteninhalt der zu signierenden Dokumente die IT-Infrastruktur von Kunden nicht verlassen darf (in Abbildung 5 nicht dargestellt, siehe Kapitel 5).

Werden elektronische Signaturen mit Signaturkarten bzw. Dienstkarten erstellt, so entfallen außerdem sämtliche Verbindungen zu Remote-Signing-Diensten bzw. deren Betreibern und die Abbildung kann auf den Bereich „Customer Domain" reduziert werden.

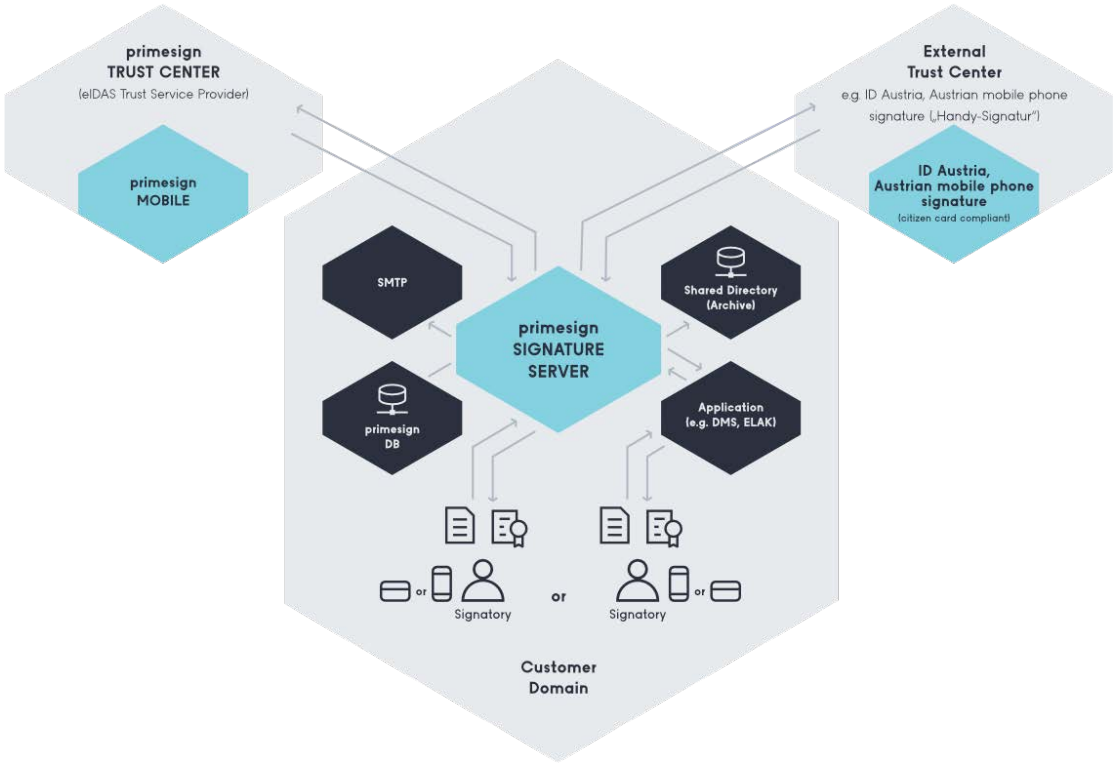

Abbildung 5: Vereinfachte, exemplarische Darstellung: Deployment-Variante On-Premise

Kundendomäne (Customer Domain)

Hauptelemente der kundenseitigen Infrastruktur:

- **primesign SIGNATURE SERVER:** Eine (oder mehrere) primesign SIGNATURE SERVER Appliances (Nodes), die einzeln oder optional in einem Fail-Over-Setup betrieben werden können.
- **primesign Datenbank (primesign DB):** Die primesign Datenbank bildet das Rückgrat unseres Services. Sie enthält alle relevanten Einstellungen unserer Lösung und verwaltet z.B. Unterschriftenläufe. Es wird eine breite Palette an verfügbaren Datenbanksystemen unterstützt (siehe 7.2 und 7.3).
- **UnterzeichnerIn (Signatory):** Es sind zwei beispielhafte UnterzeichnerInnen innerhalb der Domäne des Kunden dargestellt. Zum Signieren kann entweder unser Remote-Signing-Dienst primesign MOBILE, ID Austria oder die Handy-Signatur (A-Trust), der deutsche Online-Ausweis sowie eine Signaturkarte (z.B. Dienstkarte) genutzt werden.

- **SMTP-Server (optional):** SMTP wird zum Senden von E-Mails für Einladungen oder Erinnerungen (Unterschriftenläufe) verwendet. Um diese E-Mails von der Domäne des Kunden zu versenden, muss der Kunde Zugriff auf seinen SMTP-Server gewähren.
- **Shared Directory - Archive (optional):** Der primesign SIGNATURE SERVER unterstützt das automatische Schreiben signierter Dokumente auf einen externen Datenspeicher. Die Standardschnittstelle für diese automatische Exportfunktion ist ein freigegebener Ordner.
- **Application (optional):** Application steht für jede Art von verbundener Anwendung, wie z.B. der Elektronische Akt (ELAK), DMS, die unsere Webservice-Schnittstellen (oder andere Integrationsschnittstellen) zum Signieren von Dokumenten verwenden.

primesign Trust Service Provider

Wird primesign MOBILE oder primesign WRAPTOR zum Signieren von Dokumenten verwendet, wird die PrimeSign GmbH als Vertrauensdiensteanbieter (Trust Service Provider) an die kundenseitige Infrastruktur angebunden.

Hauptelement des primesign qualifizierten Remote-Signing-Services:

primesign MOBILE: Unser Remote-Signing-Dienst verwendet Mobiltelefone, um UnterzeichnerInnen während des Signierens zu authentifizieren und erstellt eIDAS-konforme PAdES-Signaturen. Bei der Verwendung von primesign MOBILE in Kombination mit einem primesign SIGNATURE SERVER On-Premise-Setup ist zudem sichergestellt, dass Dokumente nicht vollständig an das Trust Center übertragen werden müssen (auch in Verbindung mit primesign WRAPTOR). Bei Verwendung von primesign WRAPTOR erfolgt eine Identifizierung mittels ausgewählter eIDAS eIDs auf Basis derer ein primesign MOBILE Einmalzertifikat erstellt und zur Signatur genutzt wird.

Externes Trust Center z.B. ID Austria/Handy-Signatur (A-Trust)

Werden Dokumente mit dem Remote-Signing-Dienst eines externen Trust Centers signiert, wird das externe Trust Center als Vertrauensdiensteanbieter (Trust Service Provider) an die kundenseitige Infrastruktur angebunden. In diesem Beispiel wird die ID Austria bzw. Handy-Signatur (A-Trust) exemplarisch als externes Signatur-Service herangezogen.

ID Austria bzw. Handy-Signatur: Serverseitige Infrastruktur der ID Austria / Handy-Signatur (derzeit von A-Trust betrieben).

Weitere Aspekte

Allgemeine Anmerkungen zur vereinfachten Skizze:

- **End-to-End-Verschlüsselung über SSL / TLS oder IPSec:** Alle Verbindungen werden mit SSL / TLS oder IPSec verschlüsselt und authentifiziert.
- **Interne, externe und anonyme UnterzeichnerInnen**: Obwohl die Skizze nur interne UnterzeichnerInnen abbildet, unterstützt die vorgeschlagene Lösungsinfrastruktur auch externe BenutzerInnen, die sich außerhalb der Domäne des Kunden befinden sowie anonyme BenutzerInnen.
- **Unterstützte Signaturmittel:** Obwohl in der Skizze ausschließlich die Verwendung von Remote-Signing-Diensten (primesign MOBILE, ID Austria, Handy-Signatur) abgebildet wird, werden auch weitere Signaturmittel wie beispielsweise Smart Cards und andere Signatur-Token unterstützt.
- **Bei der Skizze handelt es sich um eine vereinfachte Darstellung der Lösungsinfrastruktur – nicht alle Verbindungen sind abgebildet:** Um die Skizze einfach und übersichtlich zu halten, sind einige bestehende Verbindungen nicht dargestellt. So sind z.B. Verbindungen zu externen Verifizierungsdiensten (OCSP, CRL, etc.) und andere Abhängigkeiten (optional: Active Directory) nicht abgebildet. Welche weiteren Verbindungen innerhalb einer Lösungsinfrastruktur vorkommen ist abhängig von den jeweiligen konkreten Anwendungsfällen und Integrationsszenarien.

6.2. SaaS

Abbildung 6 skizziert den Aufbau der primesign SIGNATURE SERVER Infrastruktur als Managed Service (SaaS). Sie zeigt vereinfacht die entsprechende, exemplarische Architektur und die einzelnen Komponenten eines SaaS-Setup.

In einem SaaS-Setup werden die zu signierenden Dokumente immer an das Managed-Service übergeben. Somit ist es nicht möglich, Dokumenteninhalte innerhalb der IT-Infrastruktur des Kunden zu halten.

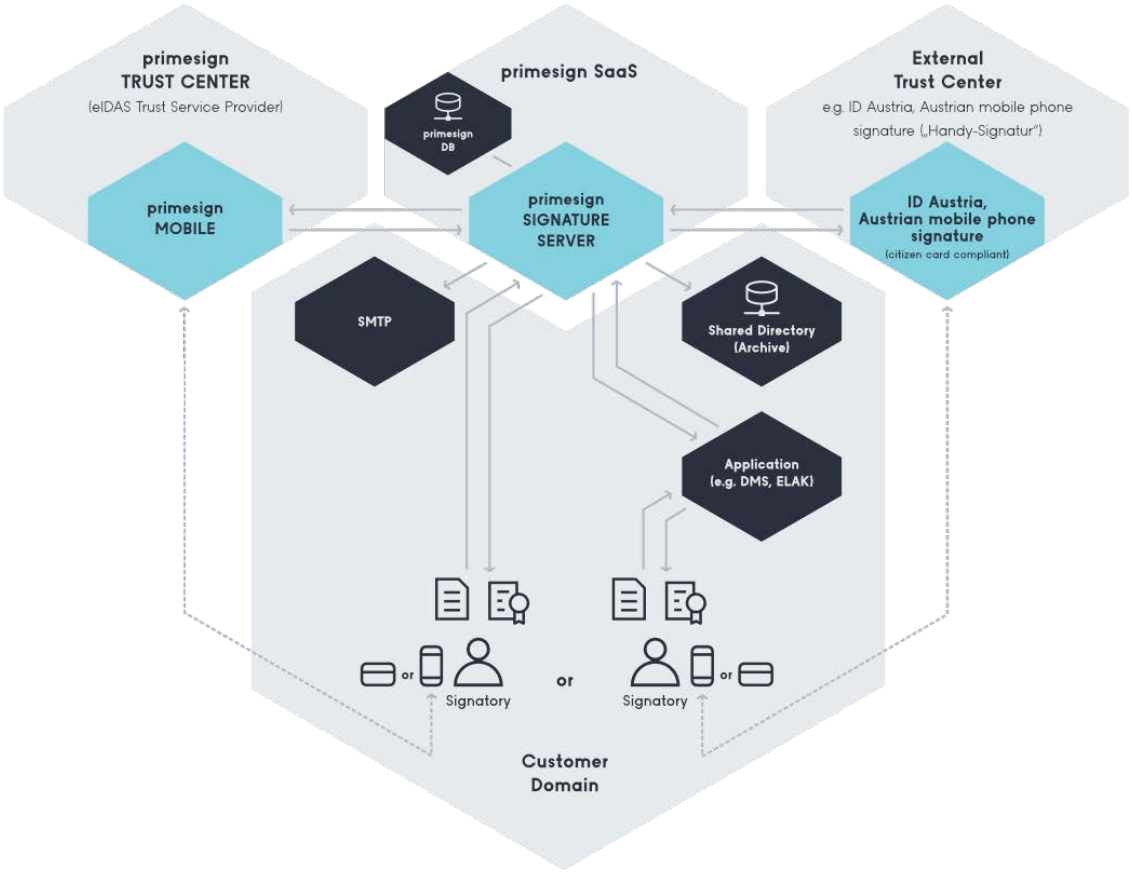

Abbildung 6: Vereinfachte, exemplarische Darstellung: Deployment-Variante SaaS

primesign SaaS (Private Cloud unseres SaaS-Betriebs)

Hauptelemente der SaaS-Infrastruktur:

- **primesign SIGNATURE SERVER:** Eine (oder mehrere) primesign SIGNATURE SERVER Appliances (Nodes), die einzeln oder optional in einem Fail-Over-Setup betrieben werden können.
- **primesign Datenbank (primesign DB):** Die primesign Datenbank bildet das Rückgrat unseres Services. Sie enthält alle relevanten Einstellungen unserer Lösung und verwaltet z.B. Unterschriftenläufe. Es wird eine breite Palette an verfügbaren Datenbanksystem unterstützt (siehe 7.2 und 7.3).

Kundendomäne (Customer Domain)

- **UnterzeichnerIn (Signatory):** Es sind zwei beispielhafte UnterzeichnerInnen innerhalb der Domäne des Kunden dargestellt. Zum Signieren kann entweder unser Remote-Signing-Dienst primesign MOBILE, ID Austria oder die Handy-Signatur (A-Trust), der deutsche Online-Ausweis sowie eine Signaturkarte (z.B. Dienstkarte) genutzt werden.
- **SMTP-Server (optional):** SMTP wird zum Senden von E-Mails für Einladungen oder Erinnerungen (Unterschriftenläufe) verwendet. Um diese E-Mails von der Domäne des Kunden zu versenden, muss der Kunde Zugriff auf seinen SMTP-Server gewähren.
- **Geteiltes Verzeichnis für die Archivierung (optional): Shared Directory - Archive (optional):** Der primesign SIGNATURE SERVER unterstützt das automatische Schreiben signierter Dokumente auf einen externen Datenspeicher. Die Standardschnittstelle für diese automatische Exportfunktion ist ein freigegebener Ordner.
- **Application (optional):** Application steht für jede Art von verbundener Anwendung, wie z.B. der Elektronische Akt (ELAK), DMS, die unsere Webservice-Schnittstellen (oder andere Integrationsschnittstellen) zum Signieren von Dokumenten verwenden.

primesign Trust Service Provider

Wird primesign MOBILE oder primesign WRAPTOR zum Signieren von Dokumenten verwendet, wird die PrimeSign GmbH als Vertrauensdiensteanbieter (Trust Service Provider) an die kundenseitige Infrastruktur angebunden.

Hauptelement des primesign qualifizierten Remote-Signing-Service:

primesign MOBILE: Unser System verwendet ein Mobiltelefon, um UnterzeichnerInnen während des Signierens zu authentifizieren, und erstellt eIDAS-konforme PAdES-Signaturen. Bei Verwendung von primesign WRAPTOR erfolgt eine Identifizierung mittels ausgewählter eIDAS eIDs auf Basis derer ein primesign MOBILE Einmalzertifikat erstellt und zur Signatur genutzt wird.

Externes Trust Center z.B. Handy-Signatur des Bundes (A-Trust)

Werden Dokumente mit dem Remote-Signing-Dienst eines externen Trust Centers signiert, wird das externe Trust Center als Vertrauensdiensteanbieter (Trust Service Provider) an die kundenseitige Infrastruktur angebunden. In diesem Beispiel wird ID Austria bzw. die Handy-Signatur (A-Trust) exemplarisch als externes Signatur-Service herangezogen.

ID Austria bzw. Handy-Signatur: Serverseitige Infrastruktur der ID Austria / Handy-Signatur (derzeit von A-Trust betrieben).

Weitere Aspekte

Allgemeine Anmerkungen zur vereinfachten Abbildung:

- **End-to-End-Verschlüsselung über SSL / TLS oder IPSec:** Alle Verbindungen werden mit SSL / TLS oder IPSec verschlüsselt und authentifiziert.
- **Interne, externe und anonyme UnterzeichnerInnen**: Obwohl die Skizze nur interne UnterzeichnerInnen abbildet, unterstützt die vorgeschlagene Lösungsinfrastruktur auch externe BenutzerInnen, die sich außerhalb der Domäne des Kunden befinden sowie anonyme BenutzerInnen.
- **Unterstützte Signaturmittel:** Obwohl in der Skizze ausschließlich die Verwendung von Remote-Signing-Diensten (primesign MOBILE, ID Austria, Handy-Signatur) abgebildet wird, werden auch weitere Signaturmittel wie beispielsweise Smart Cards und andere Signatur-Token unterstützt.
- **Bei der Skizze handelt es sich um eine vereinfachte Darstellung der Lösungsinfrastruktur – nicht alle Verbindungen sind abgebildet:** Um die Skizze einfach und übersichtlich zu halten, sind einige bestehende Verbindungen nicht dargestellt. So werden z.B. Verbindungen zu externen Verifizierungsdiensten (OCSP, CRL, etc.) und andere Abhängigkeiten (optional: Active Directory) nicht abgebildet. Welche weiteren Verbindungen innerhalb einer Lösungsinfrastruktur vorkommen ist abhängig von den jeweiligen konkreten Anwendungsfällen und Integrationsszenarien.

7. Anforderungen des primesign SIGNATURE SERVERs

Die nachfolgenden Abschnitte liefern einen groben Überblick über die wesentlichsten Anforderungen an ein primesign SIGNATURE SERVER Setup. Weiterführende Details finden Sie in Dokumentationen der jeweiligen Komponenten. Diese Dokumentationen sind im Zweifel auch normativ. Die folgenden Abschnitte dienen der ersten Orientierung.

7.1. Zertifikatsanforderungen (Signaturmittel)

Unser Produkt unterscheidet sich zu ähnlichen Signaturlösungen am Markt durch seine Offenheit für die Nutzung verschiedenster Signaturmittel und Zertifikate. Insbesondere im Bereich der persönlichen Signatur können neben dem primesign eigenen Signaturzertifikat – primesign MOBILE Zertifikat (optional auch in Kombination mit primesign WRAPTOR, siehe 3.18), auch Signaturmittel und Zertifikate anderer Vertrauensdiensteanbieter standardmäßig verwendet werden. Dazu gehören z.B. ID Austria oder die Handy-Signatur, verschiedene Dienstkarten, oder andere Signaturmittel, wie z.B. Signaturmittel auf Basis von Hardware Security Modulen (HSMs).

Zudem sind wir nicht nur Software- und hochspezialisierter Produkthersteller, sondern auch Trust-Center-Betreiber (eIDAS-Vertrauensdiensteanbieter). Dadurch können wir optimierte, durchgängige End-to-End-Lösungen anbieten, von der Ausstellung eines (qualifizierten) Zertifikates bis zu dessen Nutzung mit dem primesign SIGNATURE SERVER, oder in angeschlossenen Anwendungen wie dem Elektronischen Akt oder einem DMS.

Wir bieten eine standardmäßige Unterstützung für folgende Signaturmittel und Zertifikate:

- primesign MOBILE (Vertrauensdiensteanbieter PrimeSign GmbH) – unser qualifizierter Remote-Signing-Dienst, siehe 3.19
- primesign WRAPTOR (qualifizierte Signatur mit primesign MOBILE Einmalzertifikat auf Basis vorhandener eIDAS eIDs, z.B. deutscher Online-Ausweis, ID Austria oder Handy-Signatur siehe 3.18)
- ID Austria oder Handy-Signatur (österreichische E-Government – Bürgerkarteninitiative; Vertrauensdiensteanbieter A-Trust)
- Signaturkarten, die über die standardisierte Middleware-Schnittstelle Security Layer (v.1.2) zur Signatur ansprechbar sind (Middleware ist vom Kartenherausgeber bereitzustellen).
- Softwareschlüssel und Zertifikate verschiedenster Vertrauensdiensteanbieter

Signaturmittel und Signaturdienste weiterer Vertauensdiensteanbieter können auf Wunsch integriert werden.

7.2. Hardwareanforderungen

7.2.1. primesign SIGNATURE SERVER (relevant bei On-Premise-Betrieb)

Im Allgemeinen wird der primesign SIGNATURE SERVER als virtuelle Appliance angeboten und ausgeliefert. Die minimalen Systemanforderungen der Appliance sind im Handbuch bzw. Setup-Guide zusammengefasst [4].

Optional kann der primesign SIGNATURE SERVER aber auch als physische Appliance ausgeliefert werden, z.B. wenn keine Infrastruktur (Hypervisor) für den Betrieb unserer virtuellen Appliance verfügbar oder gewünscht ist.

7.2.2. Signaturmittel

⚠ Die nachfolgenden Ausführungen zu den Hardwareanforderungen seitens Signaturmittel sind rein informativ, da diese vom jeweiligen Herausgeber (Trust Center) festgelegt werden müssen.

Unter der Voraussetzung, dass die zu signierenden Dokumente die IT-Infrastruktur des Kunden nicht verlassen dürfen, kann die Verwendung von Fernsignaturmitteln die Kombination mit einem entsprechenden On-Premise-Setup und in diesem Zusammenhang auch die Anschaffung von zusätzlichen Hardwarekomponenten erfordern. Dies ist jedoch optional und wird letztendlich vom gewählten Signaturmittel und dem entsprechenden Vertauensdiensteanbieter bedingt.

Bei der Verwendung der ID Austria oder Handy-Signatur (A-Trust) z.B. ist die Installation der A-Trust Signatur-Box erforderlich um sicherzustellen, dass zu signierende Dokumente die IT-Infrastruktur von Kunden nicht verlassen. Wird primesign MOBILE (auch in Zusammenhang mit primesign WRAPTOR) in Kombination mit einem entsprechenden On-Premise-Setup verwendet, ist keine zusätzliche Hardware erforderlich. Zu signierende Dokumente verbleiben immer vollständig in der IT-Infrastruktur von Kunden.

Beim Einsatz von Signaturkarten sind – ebenfalls gem. den Angaben des jeweiligen Herausgebers – Kartenleser zur Nutzung der Signaturkarten am Arbeitsplatz als Hardware erforderlich.

7.3. Softwareanforderungen

7.3.1. primesign SIGNATURE SERVER (relevant bei On-Premise-Betrieb)

Über die reinen Betriebsanforderungen der virtuellen Appliance hinaus, benötigt der primesign SIGNATURE SERVER primär nur eine Datenbank (externe Datenbank empfohlen) angebunden.

Die jeweils unterstützten Datenbanken sind im Handbuch bzw. Setup-Guide zusammengefasst [4].

Weitere Eckdaten bzw. Softwareanforderungen, je nach Konfiguration und Use-Cases (Auszug aus der Dokumentation des primesign SIGNATURE SERVER):

- Wenn die signierten PDF-Dokumente Long-Term-Validation (LTV) unterstützen sollen, so ist der Zugriff auf die Widerrufs-Status-Services des verwendeten Signaturzertifikates notwendig. Typischerweise sind dies die Ports 443, 80 und 389.
- Wenn Single-Sign-On (SSO) verwendet wird, so wird dies über einen Microsoft IIS realisiert. Hierfür ist die Installation eines Microsoft IIS WebServers sowie der Zugriff auf das Active Directory (LDAP-Endpunkt) erforderlich.
- Wenn die Adressbuchfunktionalitäten genutzt werden, so ist der Zugriff auf das Active Directory (LDAP-Endpunkt) erforderlich.
- Wenn Unterschriftenläufe genutzt werden (d.h. BenutzerInnen laden andere BenutzerInnen zum Signieren eines Dokumentes ein), so ist die Anbindung eines SMTP-Servers erforderlich.
- Wenn die Directory-Scanner-Funktionalität verwendet wird, so müssen die anzubindenden Verzeichnisse zugreifbar und entsprechende Lese-Schreib-Rechte gegeben sein.

Darüber hinaus skizziert das Dokument „primesign SIGNATURE SERVER – Solution Overview" [2] weiterführende Deployment-Varianten, etwa für den Fall einer SSO-Realisierung über eine IIS-Integration.

Seitens des primesign SIGNATURE SERVERs gibt es keine zusätzlichen Anforderungen an den Client. Das User-Interface des primesign SIGNATURE SERVERs ist rein webbasiert und kann mit allen gängigen Web-Browsern genutzt werden, ohne Java-Installation oder sonstiger aktiver Komponenten. Ansonsten gibt es seitens unseres Produktes keine weiteren Softwareanforderungen an den Client-Arbeitsplatz.

7.3.2. Signaturmittel

⚠ Die nachfolgenden Ausführungen zu den Softwareanforderungen seitens Signaturmittel sind rein informativ. Anforderungen seitens Signaturmittel müssen vom jeweiligen Herausgeber (Trust Center) dargelegt werden.

Bei Fernsignaturdiensten, wie primesign MOBILE (auch in Kombination mit primesign WRAPTOR) oder der Handy-Signatur des Bundes (A-Trust), ist bspw. ein Mobiltelefon bzw. Smartphone erforderlich. Bei A-Trust ist auf Smartphones eine zusätzliche App erforderlich, um eine Signatur auszulösen. Bei primesign MOBILE genügt jedes SMS-fähige Mobiltelefon (keine App erforderlich), um qualifizierte Remote-Signaturen auszulösen. Bei Nutzung des deutschen Online-Ausweises siehe 3.17.

Kommen Signaturkarten zum Einsatz (Dienstkarten etc.), so muss/wird der Herausgeber der Signaturkarten auch eine entsprechende Client-Software zur Verfügung stellen (Middleware), mit der die Signaturkarte angesprochen werden kann (siehe 3.1).

7.3.3. SOAP-Integrationsschnittstellen

Der primesign SIGNATURE SERVER bietet eine Reihe von Integrationsschnittstellen. Wir empfehlen die Verwendung unserer SOAP PrimeSignWorkflowService Schnittstelle für die Anbindung der elektronischen Signatur z.B. in ein Dokumentenmanagementsystem.

Zudem verfügt der primesign SIGNATURE SERVER über eine synchrone SOAP-Signaturschnittstelle, um automatisierte Signaturen performant ausführen zu können (zum Beispiel für serverseitige Signaturerstellungsprozesse bzw. Massenverfahren, oder das automatisierte Aufbringen von qualifizierten Siegeln). Auch kann über einen synchronen Schnittstellenbefehl die PDF-Konvertierungsfunktion – auf Wunsch auch PDF/A-konform – eigenständig genutzt werden (PrimeConvert).

Das Dokument primesign SIGNATURE SERVER – Integration Documentation [3] bietet eine ausführliche Dokumentation der Standard-Integrationsschnittstellen des primesign SIGNATURE SERVERs.

8. Referenzen

8.1. Bundeskanzleramt Österreich

primesign wird für die persönliche digitale Signatur (PDS) im Elektronischen Akt (ELAK im Bund, sprich Fabasoft eGov-Suite) genutzt und wurde direkt in dieses System integriert. So können ELAK-NutzerInnen direkt im webbasierten Workflow des ELAK mit primesign elektronisch unterschreiben. Dazu wird das zu unterfertigende PDF-Dokument an den vom BKA betriebenen primesign SIGNATURE SERVER übergeben, wo dann eine individuelle Signatur platziert und durchgeführt werden kann.

Zudem wird primesign auch zur Einbringung von PDF-basierten Förderformularen genutzt. Eine eigene primesign-Instanz nimmt hierbei PDF-Formulare von BürgerInnen entgegen und veranlasst die Bürgerin oder den Bürger das PDF vor der Übermittlung zu unterschreiben (mit der Handy-Signatur oder der Bürgerkarte).

8.2. Bundesrechenzentrum

Das österreichische Bundesrechenzentrum nutzt einen lokalen primesign SIGNATURE SERVER für persönliche elektronische Signaturen durch MitarbeiterInnen des Unternehmens. Es wurde auch eine SSO-Anbindung (Domain) realisiert. MitarbeiterInnen werden so nahtlos authentifiziert und bekommen (gruppenspezifische) Signaturprofile freigeschalten. Einerseits signieren die MitarbeiterInnen des BRZ die Dokumente direkt in der primesign Weboberfläche (mit Dienstkarte, Handy-Signatur), zum anderen nutzt aber auch das BRZ eine der BKA-ähnlichen Integration in deren Fabasoft eGov-Suite, um auch darin (individuelle) elektronische Unterschriften direkt vornehmen zu können.

8.3. Landtag Steiermark und Steiermärkische Landesregierung

Das Land Steiermark betreibt eine zentrale primeisgn Infrastruktur zur Abwicklung aller klassischen Signatur- und Amtssignaturprozesse. Bezogen auf die Transaktionszahlen nutzen der Landtag Steiermark und die Steiermärkische Landesregierung die primesign Infrastruktur vor allem dazu, um alle ausgehenden, amtlichen Dokumente des Landes automatisiert mit einer Amtssignatur zu versehen. Die zentrale Amtssignatur – realisiert mit der primesign Infrastruktur des Landes – ist ein wesentliches Element fast aller elektronischen Prozesse. Alle ausgehenden Dokumente werden mit primesign amtssigniert.

Zudem wurde das Workflow-System des steiermärkischen Landtages mit der zentralen primesign Infrastruktur verbunden, sodass die Abgebordneten und MitarbeiterInnen des Landtages ihre

persönlichen elektronischen Signaturen mit primesign aufbringen können. Hierbei wurde die persönliche elektronische Signatur mit primesign in das Workflow-System des Landtages integriert.

8.4. Weitere Referenzen

Weitere Referenzen sind auf Anfrage und in Abstimmung mit unseren Kunden erhältlich.

9. Weiterführende Dokumente und Beilagen

In diesem Abschnitt referenzieren wir einige weiterführende Dokumente:

[1] CRYPTAS / PrimeSign GmbH: **Produktdatenblatt primesign SIGNATURE SERVER**, in der jeweils gültigen Version. In Deutscher und Englischer Sprache.

[2] CRYPTAS / PrimeSign GmbH: **primesign SIGNATURE SERVER – Standard Solution Overview**, in der jeweils gültigen Version. Kurzüberblick über die wesentlichsten Hauptfunktionen und technischen Merkmale unseres Produktes. Das Dokument zeigt auch Screenshot-Sequenzen typischer, einfacher Use-Cases, einschließlich der Verwendung unterschiedlicher Signaturmittel, wie der A-Trust Handy-Signatur oder primesign MOBILE. In Englischer Sprache.

[3] CRYPTAS / PrimeSign GmbH: **primesign SIGNATURE SERVER – Integration Documentation**, in der jeweils gültigen Version. API-Dokumentation zur typischen Anbindung des primesign SIGNATURE SERVERs an externe Anwendungen (wie z.B. den ELAK).

[4] CRYPTAS / PrimeSign GmbH: **primesign SIGNATURE SERVER Appliance Documentation**, in der jeweils gültigen Version. Handbuch und Setup-Guide für die Errichtung und den Betrieb eines primesign SIGNATURE SERVERs (als virtuelle/physische Appliance).

[5] CRYPTAS / PrimeSign GmbH: **Häufig gestellte Fragen – primesign MOBILE** in der jeweils gültigen Version. Sammlung häufig gestellter Fragen und Antworten rund um primesign MOBILE (inklusive primesign MOBILE für Adobe Acrobat Sign). In Deutscher und in Englischer Sprache.

[6] CRYPTAS / PrimeSign GmbH: **primesign MOBILE – Getting Started Guide for Integrators (CSC API)** in der jeweils gültigen Version. Sammlung technischer und organisatorischer Informationen zur Integration der primesign Signatur via CSC API. In Englischer Sprache.