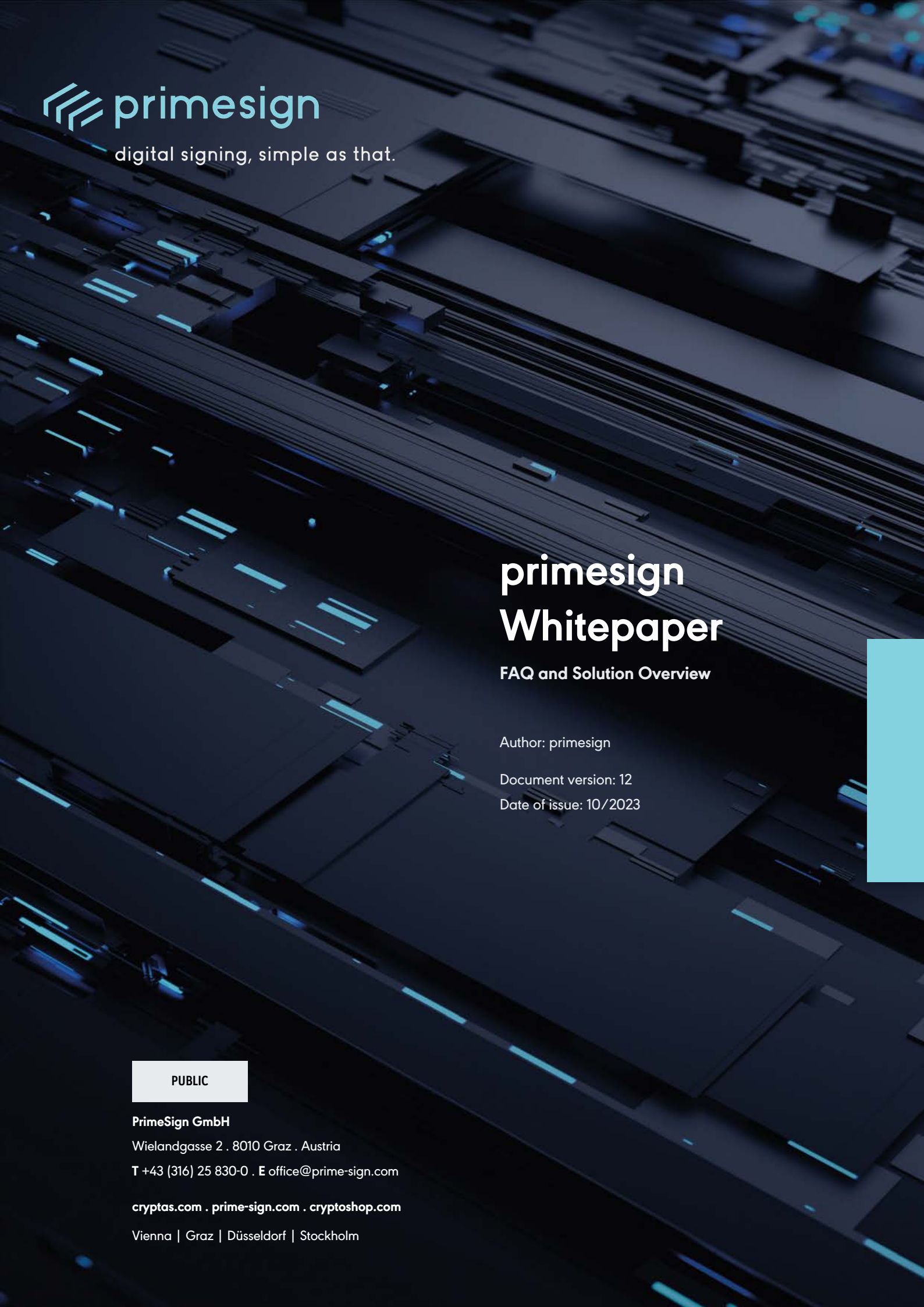

primesign

digital signing, simple as that.

primesign Whitepaper

FAQ and Solution Overview

Author: primesign

Document version: 12

Date of issue: 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

Vienna | Graz | Düsseldorf | Stockholm

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Document Information

Typographic conventions and changes regarding the document are provided below.

Typographic conventions

- Attention – please read carefully
- Further information and tips

```
Command
```

Revision history

All changes to this document are tracked in the following history.

Date	Name	Type of change	Version
20.05.2020	Rössler	Draft	1 (also 1.0D)
08.06.2020	Rössler	Draft	2
10.06.2020	Rössler	Draft	3
19.06.2020	Kreuzhuber	Review	4
25.06.2020	Rössler	Advanced	5
25.06.2020	Rössler	Advanced & remove Section 9 (PrInd)	6
26.06.2020	Rössler	Release version 1	7
30.06.2020	Rössler	Editorial changes	8
27.04.2021	Fruhmann	EN translation & update template	8
28.06.2021	Fruhmann	Editorial changes & update figures	9
22.06.2022	Fruhmann	Add primesign WRAPTOR & adapt to German version	10
04.07.2022	Fruhmann, Kreuzhuber, Rössler	Release & completion version 10	10
03.01.2023	Fruhmann	Update primesign MOBILE & add information about business certificates	11
25.10.2023	Kreuzhuber	Add Sign with German Identity Card & Qualified Timestamping	12

1. Management Summary

In addition to the existing product documentation of the primesign SIGNATURE SERVER, this document provides an application-oriented overview of typical solution scenarios and answers key questions. Although the document does not replace reading the detailed product documentation, it does provide practical guidance at an early stage, whether in the course of a purchase decision or already in preparation for implementation.

The document is structured as follows:

- Chapter 2 summarizes the most essential characteristics as well as the comprehensive feature set of our product. This introductory section complements other product documentation, such as the data sheet or manual.
- Chapter 3 answers and discusses a number of frequently asked questions. The questions are not purely technical but also relate to our entire solution system and various aspects of a signature process. Therefore the questions also cover aspects of electronic signatures in general and our trust center services in particular.
- Chapter 4 is devoted to the topic of how a company affiliation and/or roles and functions (powers of representation, etc.) can be represented in electronic signatures. The topic of qualified seal certificates ("company signatures") is also discussed.
- Chapter 5 examines the path taken by an electronic document in the course of a signature transaction (application of the signature) and based on the signature creation device used. For example, when using our remote signing service primesign MOBILE in conjunction with a primesign SIGNATURE SERVER on-premise setup, we can ensure that during a signature transaction, documents remain completely within the customer's IT infrastructure (also in combination with primesign WRAPTOR).
- Chapter 6 outlines two simplified but typical deployment architectures. One is an on-premise architecture; the other is the use of the primesign SIGNATURE SERVER as a Managed Service (SaaS).
- Chapter 7 provides an overview of the most important hardware and software requirements of a typical primesign SIGNATURE SERVER infrastructure.
- Chapter 8 describes some reference customer cases – further references are available upon request.
- Chapter 9 references a selection of documents for further reading.

2. The primesign SIGNATURE SERVER

The primesign SIGNATURE SERVER is the central signature infrastructure for electronic signatures in organizations or companies. Regardless of whether the primesign SIGNATURE SERVER is operated in the form of a (physical or virtual) appliance on-site (on-premise) or is used as a Managed Service (SaaS), the primesign SIGNATURE SERVER offers the right functionality for the entire range of electronic signature applications.

2.1. Typical use cases

The use cases for electronic signatures in organizations and companies are broad and complex. Almost everywhere where sign-offs or handwritten signatures on paper are required, the electronic signature with the primesign SIGNATURE SERVER is the suitable digital equivalent. Thus with the primesign SIGNATURE SERVER, digitization projects can be implemented consistently, comprehensively, and in a legally secure manner.

Exemplary use cases include:

- Sign any contract or document electronically
- Sign HR documents or employment contracts electronically
- Sign orders or confirmations electronically
- Termination of contracts
- Electronic signing of service instructions or forms
- Electronic SEALING of incoming/outgoing documents or invoices

2.2. No installation required

Users do not need to install the primesign SIGNATURE SERVER. The primesign SIGNATURE SERVER can be used as a web application with all common browsers and can thus be seamlessly integrated into web-based workflows (see Figure 1). No client software is required.

Therefore, rolling out the primesign SIGNATURE SERVER in organizations and companies is quite simple. Access rights (accounts) are assigned, and corresponding credentials (links to either the local on-premise or a SaaS instance) are distributed. In this way, every workstation can be easily retrofitted for electronic signatures.

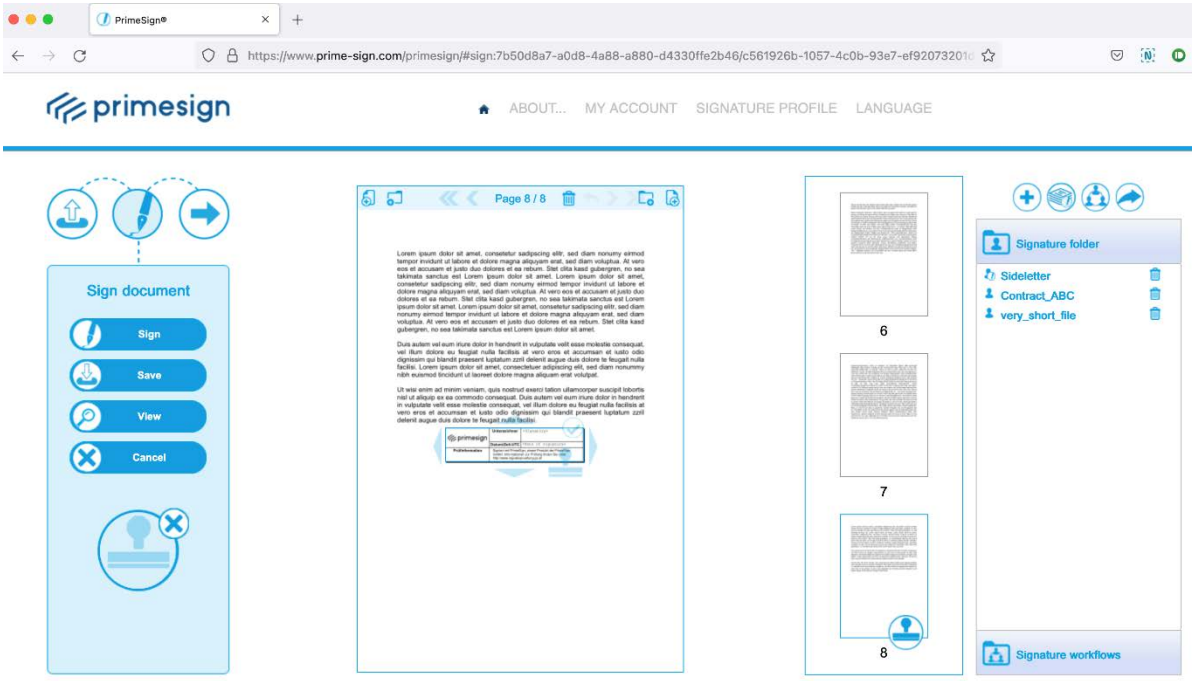

Figure 1: primesign SIGNATURE SERVER Web UI

2.3. Supported signature creation devices

The primesign SIGNATURE SERVER supports a wide variety of signature creation devices (signing certificates) from different providers. It also has standard integrations with the most established ones. On request, further signature creation devices (signing certificates) for which we do not offer integration as a standard can also be connected to the primesign SIGNATURE SERVER (see section 3.1). These include, e.g., signature cards from other providers.

Our recommendation: Sign with qualified certificates (primesign MOBILE certificates) issued by our own eIDAS-compliant trust center - primesign TRUST CENTER. Or use selected eIDAS eIDs to create a qualified signature with a primesign MOBILE one-time certificate – immediate signing; prior registration with primesign is not required.

2.4. Visual signature signet

Make a statement with your electronic signature! With primesign, you can create your personal visual signature signet. A visual signet can resemble, for instance, your personal handwritten signature (see Figure 2) or a corporation's official seal.

Adding a visual signature signet to documents gives recipients of your electronically signed documents the familiar representation of a "conventional" signature or company seal. Recipients can immediately see the signature verification information. This reinforces the acceptance of electronically signed documents.

Nevertheless, with the primesign SIGNATURE SERVER, you can also create invisible signatures. In this case, no visual signature signet is added to the document. The signature is only visible in the document properties, but maintains the same legal validity and security as a visible signature.

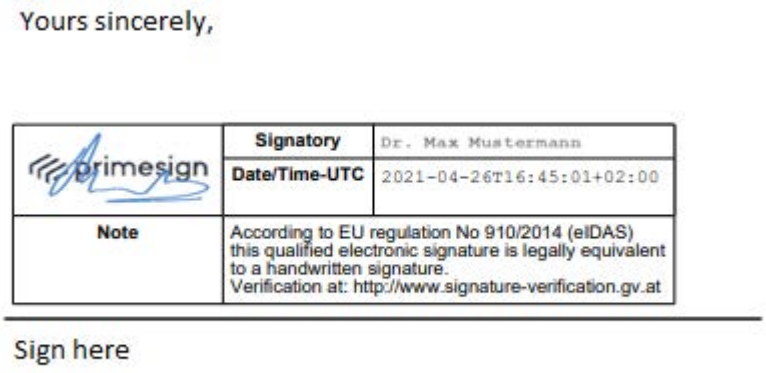

Figure 2: Example of a personal visual signature signet

2.5. The signature infrastructure

The primesign SIGNATURE SERVER was designed as a comprehensive system and is therefore suitable for a wide range of use cases. It can act as a core component of a comprehensive signature infrastructure (see Figure 3).

Figure 3: primesign SIGNATURE SERVER for many use cases

INTERNAL USE CASES

Internal use cases are the most obvious use cases of our signature solution. In this context, our system is used for handling personal signatures at the workplace or in the company, e.g., for internal signing flows, circular resolutions, the submission of documents to be signed, or the immediate signing of individual documents.

EXTERNAL USE CASES

In this context, the primesign SIGNATURE SERVER acts as a hub for submitting purchase orders, commissions, or for processing contracts with customers or partners, etc. With the primesign SIGNATURE SERVER, you can share signing flows with external parties such as your customers or business partners. Alternatively, the primesign SIGNATURE SERVER can also be made accessible externally so that electronically signed documents can be received in a legally secure manner.

MASS PROCEDURES

The primesign SIGNATURE SERVER can also be used as a central signature server that efficiently and automatically signs large volumes of documents electronically (usually connected to other mass systems via an integration interface). Examples include electronic invoices, contract documents, letters to customers, notices, offers, official signatures, or the application of electronic seals.

SIGNING FLOWS

The primesign SIGNATURE SERVER handles signing flows automatically with both internal and external users. This way electronic signing flows can be carried out easily and efficiently with various participants at different levels.

Example 1: On level 1, two employees sign; then a department head is automatically invited for countersigning.

Example 2: The legal department signs off on the accuracy of the contract in advance – this is also possible by initialing. Then the document is automatically submitted to the two directors, who sign simultaneously.

Example 3: First, an assistant opens and initiates the entire signing flow and initially invites signer 1 to sign; then signers 2 and 3 are requested to sign simultaneously, etc.

Signing flows via the primesign SIGNATURE SERVER allow for any number of combinations and levels of participants (see Figure 4).

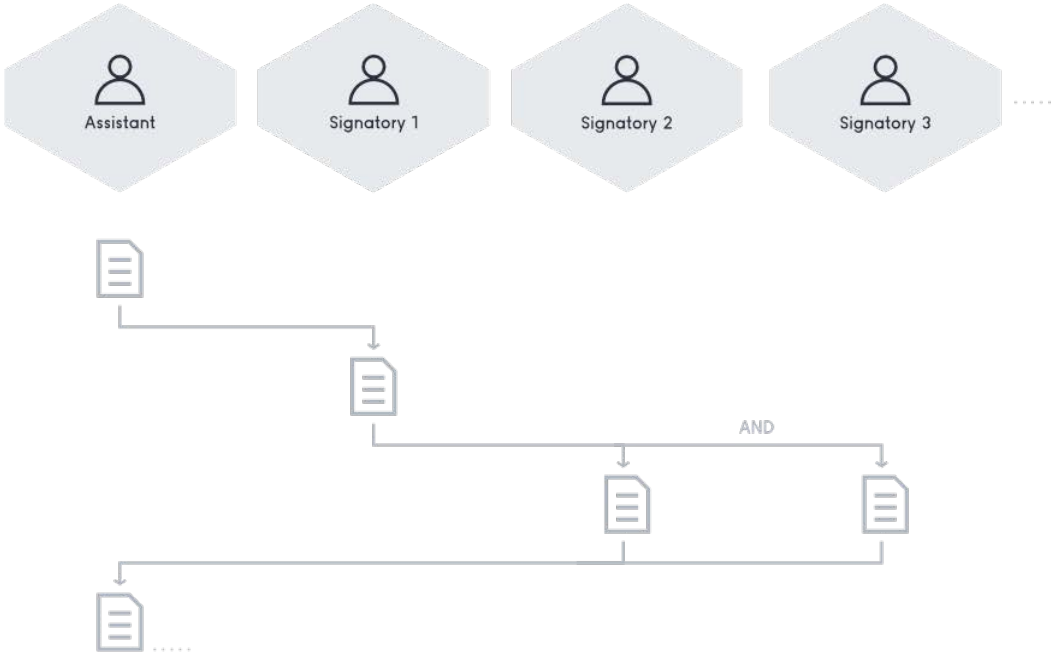

Figure 4: Signing flows at different levels (example)

2.6. Key features of the primesign SIGNATURE SERVER

The primesign SIGNATURE SERVER differs from similar solutions on the market in that it can be used with a wide variety of electronic signature creation devices (signing certificates). Particularly in the area of personal signatures, in addition to primesign's own signing certificates (primesign MOBILE certificates), the primesign SIGNATURE SERVER can also be used with signing certificates from other providers as a standard. These include, for example, ID Austria, the Austrian mobile phone signature, employee cards, e-cards, or other signature creation devices or HSMs. In addition, selected eIDAS eIDs, such as German Identity Card, ID Austria or the Austrian mobile phone signature, can also be used via primesign WRAPTOR for immediate signing with primesign one-time certificates. Prior registration with primesign is not required.

Besides, we are a software producer and trust center operator and can thus offer optimized end-to-end solutions, from the issuing of a certificate to its use with the primesign SIGNATURE SERVER – or in connected applications.

Furthermore, the unique product features and the overall ease in applying these features set the primesign SIGNATURE SERVER apart from other signature solutions. These features include, e.g., batch signature capability, free positioning of the visual signature signet (incl. selection of several different signets), initialing (initials visible on each page), basic PDF editing functions, and the ability to use selected eIDAS eIDs for immediate signing without prior registration with primesign.

The following list presents a small selection of the most prominent features of the primesign SIGNATURE SERVER:

- Client-free signing of PDF documents (web interfaces)
- Can be optimally used in conjunction with our primesign certificates (primesign MOBILE certificates) and trust center services
- Supports various electronic signature creation devices such as signature cards or remote signing services (such as primesign MOBILE, German Identity Card or ID Austria/the Austrian mobile phone signature)
- Creation of qualified personal signatures or qualified seals
- Guaranteed long-term verifiability (PAdES and LTV-compliant)
- Implementation of signing flows, also with multiple parties (internal/external)
- Creation and use of templates for signing flows
- Minimal UI for optimal integration in applications (SOAP integration interface)
- primesign WRAPTOR: Use selected eIDAS eIDs to create a qualified signature with a primesign MOBILE one-time certificate – immediate signing; prior registration with primesign is not required
- Unified Trust: Highest legal significance and uniform signatures, always sign with primesign certificates, regardless of which signature creation device is used; one legal framework, one responsible trust partner and maximum legal significance – primesign WRAPTOR makes it possible.
- Batch signature capability (e.g., with primesign MOBILE or primesign WRAPTOR): Sign a batch of PDF documents at once; thanks to the primesign WRAPTOR, also with eIDAS identities or existing third-party signing certificates
- On-premise or as a Managed Service (SaaS); when using our remote signing service primesign MOBILE in conjunction with a primesign SIGNATURE SERVER on-premise setup, we can guarantee that during a signature transaction, documents remain completely within the customer's IT infrastructure (also in combination with primesign WRAPTOR)
- Visible signatures (manual or automatic placement of the visual signature signet)
- Placement of visual signature signets using placeholders that can already be set during document creation
- Editing tools for PDF documents and conversion of selected Office documents to PDF (PDF/A optional)

For more information about the primesign SIGNATURE SERVER see the Data Sheet or Product Manual, or the following sections of this document.

3. Frequently Asked Questions

3.1. Which levels of trust can be achieved for electronic signatures?

The primesign SIGNATURE SERVER can be used to create a wide variety of electronic signatures with different levels of trust. These include qualified signatures and seals, which signify the highest level of trust and legal significance.

The level of trust of an electronic signature is defined by the level of trust of the underlying signing certificate. If the signature creation device used is based on a qualified electronic certificate (e.g., primesign MOBILE certificate), the primesign SIGNATURE SERVER can use this signature creation device to apply qualified electronic signatures to documents.

The primesign SIGNATURE SERVER supports a wide variety of signature creation devices (signing certificates) from different providers and also has standard integrations with the most established ones. This sets the primesign SIGNATURE SERVER apart from other signature solutions. On request, further signature creation devices, e.g., signature cards from other providers for which we do not offer integration as a standard, can also be connected to the primesign SIGNATURE SERVER.

The following signature creation devices are supported by default:

- **primesign MOBILE** (primesign qualified remote signing service)
- If our remote signing service primesign MOBILE is used in conjunction with a primesign SIGNATURE SERVER on-premise setup, we can guarantee that during a signature transaction, documents remain completely within the customer's IT infrastructure.
- **primesign WRAPTOR** (qualified signature with a primesign MOBILE one-time certificate based on selected eIDAS eIDs, e.g. German Identity Card, ID Austria/Austrian mobile phone signature, see 3.18)
    - If primesign WRAPTOR is used in conjunction with a primesign SIGNATURE SERVER on-premise setup, documents also remain completely in the customer's IT infrastructure during a signature transaction (see **primesign MOBILE**).
- **ID Austria/Austrian mobile phone signature (A-Trust)**
    - Can be used with or without the A-Trust Signature-Box: By using the A-Trust Signature-Box, it is guaranteed that during the a signature transaction, the documents remain in the customer's IT infrastructure. The use of the A-Trust Signature-Box is subject to a fee.

- **Signature cards, which can be accessed for signing via a local middleware software that is compatible with the primesign SIGNATURE SERVER.** A compatible middleware is a software

for using the signature card installed locally on the end-user device - such as the desktop. The software must provide the security layer protocol as a signature interface (Security Layer version 1.2 [1]). Examples of compatible middleware clients: A-Trust asign client, it-Solution trustdesk, MOCCA middleware, etc. The middleware is usually provided by the card provider. Today, this covers almost all commonly used citizen and employee cards of the Austrian administration, such as:

- Employee cards of the Austrian public administration (issued by or prepared for certificates of A-Trust).
- A-Trust signature cards

In addition, primesign can also connect a wide variety of server-side signature creation devices, such as those required for applying official signatures or (qualified) seals. Server-side signatures include, e.g., software certificates/keys or signature keys stored in an HSM. Server-side signatures are primarily based on an HSM (list of supported HSMs upon request) and software certificates.

3.2. Which document formats are signed?

The primesign SIGNATURE SERVER only signs PDF documents based on the international signature standard PAdES. Compliance with this standard ensures long-term and product-independent verifiability of PDF documents created and signed with the primesign SIGNATURE SERVER. The signed PDF documents are verifiable with common standard PDF tools.

Although the primesign SIGNATURE SERVER only generates PDF signatures, a wide variety of Office documents can be forwarded to the server or opened for signing. They are converted by the primesign SIGNATURE SERVER to a PDF document using an integrated PDF converter.

[1] see https://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/Index.html and typical middleware products: https://www.buergerkarte.at/downloads-karte.html

3.3. How long can I verify an electronic signature?

If the signature is LTV-compliant, long-term verification information is embedded in the signed document. This enables a complete verification of the signature even after years and without external dependencies. Signatures created with primesign certificates in particular, such as primesign MOBILE signatures or primesign WRAPTOR signatures, meet all requirements in this respect and, in conjunction with the primesign SIGNATURE SERVER, guarantee long-term verifiability of electronic signatures.

primesign relies on proven standards. primesign signatures meet the requirements of level "LT" according to ETSI TS 103 172 V2.2.2.[2]

3.4. How do I verify an electronic signature?

Our solution – the primesign SIGNATURE SERVER – offers an optional signature verification function. We use the same verification software that is used by the Austrian supervisory authority for trust services and electronic signatures – the Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR). This verification software is also used by the public verification service (www.signaturpruefung.gv.at).

With the optional verification function of the primesign SIGNATURE SERVER, users can verify all signatures (even signatures from different sources) in a document. This function can be accessed in the primesign SIGNATURE SERVER's user interface.

Alternatively, the DSS framework provided by the EU Commission[3] can also be connected for signature verification.

3.5. Qualified Electronic Timestamping

Electronic signatures created with primesign always contain the signing time. This time is determined by the local server time of the primesign SIGNATURE SERVER used and, in the case of signatures with primesign MOBILE and primesign WRAPTOR, is also checked against the primesign TRUST CENTER by means of a plausibility check.

Depending on the use case, there may be additional formal requirements for documenting the signing time of a document. These requirements can be met with primesign by using qualified timestamping according to eIDAS.

A so-called timestamp links an electronic document to the exact official time and thus guarantees the existence of a document at a certain point in time. This is sometimes necessary, especially in

[2] https://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf
[3] https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/doc/dss-documentation.html

applications where submission dates are documented, e.g. in tender and procurement procedures. In combination with LTV (see 3.3), the maximum evidential value of an electronically signed document is reached – even after many years. Furthermore, some signature verification services require timestamps to label signatures as fully valid even after the certificate has expired (this advantage is particularly relevant in combination with one-time signing).

primesign SIGNATURE SERVER can be configured to add a qualified timestamp during signing. No additional user action required.

By default, primesign SIGNATURE SERVER does not add a timestamp. However, timestamping can be activated on request and requires prior commercial clarification.

3.6. Electronic signatures at the workspace

The primesign SIGNATURE SERVER has a web-based user interface which, in addition to signing documents, also features a variety of additional functions (e.g., signing flows, PDF editor functions).

To apply a personal electronic signature to a document, users simply access the primesign SIGNATURE SERVER user interface via a web browser and select the PDF document to be signed from the file system (or use drag & drop).

In a next step, users can immediately sign the selected document using all functions of the primesign SIGNATURE SERVER. They can even initiate signing flows with colleagues or external parties (such as partners, customers, citizens, etc.).

Again, depending on the configuration, various signature creation devices are available for signing (e.g., primesign MOBILE, selected eIDAS eIDs such as German Identity Card, ID Austria/the Austrian mobile phone signature, employee card).

At the end of the signature process, the signed PDF document can be saved to the workstation.

3.7. Integration of electronic signatures in external applications

Documents to be signed are transferred from an application via the SOAP interface, either as a single document or as a batch of documents.

According to the SOAP interface, users can sign a single document - or a batch of documents - with their corresponding signature creation device. If several signature creation devices are available for signing (e.g., primesign MOBILE, selected eIDAS eIDs such as German Identity Card, ID Austria/the Austrian mobile phone signature, employee card), users can select their signature creation device before triggering the signature. If desired, the entire user interface of the primesign SIGNATURE

SERVER can be made available. This allows a document to be read or the appropriate signature signet to be selected and placed in the correct position in a document.

Successfully signed documents, or a corresponding error message, are transmitted back to the external application via our SOAP interface.

The integration of primesign at ELAK-im-Bund is listed as a reference. The description of the SOAP interface is also referenced at the end of the document.

3.8. Repeated or multiple signing of documents

With the primesign SIGNATURE SERVER, documents can be signed multiple times. This also applies to documents that have already been signed in advance. Such documents can be signed once again (e.g., countersigning).

With the primesign SIGNATURE SERVER, a document can therefore be signed as often as desired. This can be done regardless of whether (multiple) signatures have already been applied with primesign, or whether the document already contains other signatures from other sources or external parties. External signatures previously applied to a document must, however, comply with the PAdES signature standard and must not lock or encrypt the PDF document.

For multiple signing, a previously signed document is reloaded in the primesign SIGNATURE SERVER's user interface (or transferred to the primesign SIGNATURE SERVER via SOAP interface).

Before re-signing, existing signatures of a document can be verified with the signature verification function of the primesign SIGNATURE SERVER. This way, the correctness of all previously applied signatures, regardless of their sources, can be ensured in advance. The rest of the signing process is identical to applying a single signature.

3.9. Batch signature – triggering multiple signatures at once

The primesign SIGNATURE SERVER supports batch signature processing. This means that multiple signatures to be applied to a batch of documents only need to be triggered once. However, the signature creation device used (signature card and middleware or the corresponding remote signature) must support batch signature processing. primesign MOBILE as well as primesign WRAPTOR support batch signature processing by default. By using primesign WRAPOR, it is thus possible to use selected eIDAS identities such as, e.g., German Identity Card, ID Austria/the Austrian mobile phone signature for batch signing. When triggering a batch signature with primesign MOBILE or primesign WRAPTOR, up to 30 documents can be signed at once.

Batch signature processing is also supported by the A-Trust boxes and the signature cards mentioned in 3.1 (with the corresponding a.sign client or MOCCA middleware components).

A batch signature can be triggered via the user interface of the primesign SIGNATURE SERVER using the signature folder function. All documents submitted or added by the user that are yet to be signed can be signed by the user in a batch – i.e., all signatures can be triggered at once (for example via PIN entry or mobile TAN service). The documents can then be processed further in the batch – as a ZIP file – or individually.

The transfer of documents to be signed from another application takes place via the SOAP interface. Documents are either transferred individually or as a batch. According to the SOAP interface, a single document – or the batch – can then be signed directly with the corresponding signature creation device. If several signature creation devices are available for signing, users can select their desired signature creation device before triggering the signatures. The successfully signed documents, or a corresponding error message, are transmitted back to the application via our SOAP interface.

3.10. Two-factor authentication

Today, only two-factor authentication processes are used for qualified signatures. Typically, the signature creation device used already requires two-factor authentication, such as a signature card or a mobile phone signature (e.g., ID Austria/Austrian mobile phone signature). Two-factor authentication is given either through possession of the signature card + knowledge of the PIN; or knowledge of the password + possession of the mobile phone, i.e., SMS/App, etc.

A qualified signature creation device approved for such signatures and usable with the primesign SIGNATURE SERVER always ensures two-factor authentication.

3.11. Integration interfaces

The document "primesign SIGNATURE SERVER – Integration Documentation" [3] provides a detailed description of the primesign SIGNATURE SERVER's standard integration interface.

3.12. primesign SIGNATURE SERVER – multi-client capability

It is possible to connect multiple organizations (clients) to one server or to achieve client separation through virtual instances. In the case of the former approach (multiple organizations on one server), it is recommended to administrate users via an external Active Directory and connect it to primesign. Note that the clients must be organized under an Active Directory domain.

In contrast, clients that are to be strictly separated are each mapped through their own virtual instances of the primesign SIGNATURE SERVER. This achieves complete separation based on

independent key material for encrypting the documents and data processed on the servers in each case.

How a client is mapped is ultimately determined by the customer's requirements.

3.13. How to understand the term "user licenses"?

The term "user licenses" does not refer to clients or data centers. "User licenses" refers to the number of so-called named users (i.e., signing persons with their own user account and signature profile) per server instance. Named users can use the full features of the primesign SIGNATURE SERVER. This includes the signature folder function as well as the possibility to start a signing flow or to use templates for signing flows. In addition, an unlimited number of personal signature profiles can be created for named users.

3.14. How to quickly get a signing certificate?

If a signing certificate is not yet available, the primesign TRUST CENTER offers a simple and immediately feasible way to have a qualified primesign MOBILE certificate issued online via remote identification such as video boarding or eID (e.g., German Identity Card, ID Austria/Austrian mobile phone signature). The issuance of a primesign MOBILE certificate takes only a few minutes and can be started around the clock from the comfort of your home or office. Identification by video is available daily from 7 am to 10 pm CET.

3.15. Which video identification services does primesign offer?

As a trust service provider, PrimeSign GmbH has connected several video legitimation services of established providers for the issuance of qualified signing certificates. PrimeSign GmbH also has the corresponding authorization to use these services for legitimation and to offer them accordingly.

Among others, the video authentication services of Kapsch, of the Oesterreichische Staatsdruckerei (Austrian State Printing House), or of WebID Solutions GmbH are offered (alphabetical order).

Connection with other eIDAS-compliant video identification service providers is possible upon request.

> As an alternative to video identification, selected eIDAS eIDs can also be used for identification and thus for the issuance of a primesign MOBILE signing certificate (see 3.16).

3.16. Which eIDAS eIDs are supported by primesign?

The following eIDAS eIDs are supported by primesign for signing with primesign WRAPTOR (see 3.18) or as an alternative to video identification when issuing a primesign MOBILE certificate via our primesign OnBoarding system:

- ID Austria
- Austrian mobile phone signature
- German Identity Card
- More eIDs will follow

3.17. What do I need to use the German Identity Card?

To use the German Identity Card, the following requirements must be met:

- ID card with the activated eID function. The following ID cards can be used: ID card, eID card for EU/EEA citizens, electronic residence permit
- AusweisApp (or comparable applications)
- Set PIN. You have set a self-selected, six-digit PIN.
- Card reader or smartphone (with NFC) for reading the ID card

3.18. What is primesign WRAPTOR?

As a new service of our trust center, primesign WRAPTOR enables the quick and easy creation of qualified electronic signatures based on selected eIDAS eIDs. Technically, users are identified via their eID. Then, a primesign MOBILE one-time certificate is issued "on-the-fly" and used immediately and only for this one signature. In practice, users simply select to authorize a signature via an existing eID in the primesign SIGNATURE SERVERs user interface. Thus, with primesign WRAPTOR, existing eIDs can be used for immediate signing with primesign one-time certificates. Prior registration with primesign is not required. primesign WRAPTOR is supported by the primesign SIGNATURE SERVER by default.

There are numerous advantages for customers:

- **No registration with primesign required:** Signatures are created based on already existing eIDAS eIDs. Ideal for occasional use.
- **Signing with eIDAS eIDs:** Ideal for multinational companies that want to give their employees and customers the ability to sign quickly and easily with a qualified signature. eIDAS eIDs supported by primesign WRAPTOR are constantly being expanded.
- **Batch signature processing:** With primesign WRAPTOR, it is possible to use selected eIDAS eIDs or existing third-party signing certificates for batch signing.
- **Confidentiality**: When using primesign WRAPTOR in conjunction with a primesign SIGNATURE SERVER on-premise setup, during a signature transaction (application of the signature), documents completely remain in the customer's IT infrastructure.
- **Unified Trust & Unified Liability:** Always sign with primesign certificates, regardless of which signature creation device is used; one legal framework, one responsible trust partner – primesign TRUST CENTER
- **Unified Trust & long-term verifiability:** Regardless of the eID used, primesign WRAPTOR creates long-term verifiable and legally binding qualified signatures with a primesign MOBILE one-time certificate. primesign guarantees that signatures will still be verifiable in 30+ years.

The primesign OnBoarding system also supports primesign WRAPTOR. Customers benefit from the ability to use selected eIDAS eIDS as an alternative to video boarding for identification as part of the issuance process of a primesign MOBILE signing certificate. Customers can thus have a primesign MOBILE signing certificate (persistent signing certificate, valid up to 5 years, see 3.20) issued around the clock and within minutes.

3.19. What is primesign MOBILE?

primesign MOBILE is the qualified remote signing service from primesign. With primesign MOBILE, qualified signing is straightforward. You can conveniently trigger signatures with your mobile phone

without having to install an additional app. The basis for qualified signing with primesign MOBILE is a so-called qualified signing certificate (primesign MOBILE certificate). A distinction is made here between one-time and persistent signing certificates (see 3.20). primesign MOBILE is supported by the primesign SIGNATURE SERVER by default.

3.20. primesign MOBILE certificates – which types are available?

The qualified remote signing service primesign MOBILE offers one-time signing certificates as well as persistent signing certificates with a lifetime of currently up to 5 years. Our own eIDAS-compliant trust center is authorized to issue qualified primesign MOBILE certificates.

The qualified one-time signing certificate is issued "on-the-fly", has a validity of a few minutes, and is only valid for one signature transaction. It is generally preferred for online contract conclusions (enabled by our integration interfaces and an immediately preceding video legitimation or identification via eID). A primesign MOBILE one-time certificate is also issued when signing with primesign WRAPTOR (see 3.18).

The persistent signing certificate has a validity of up to 5 years. It is therefore well suitable for use cases and users who sign on a recurring basis, such as employees or business customers. You can have a persistent signing certificate issued online in just a few minutes using our OnBoarding service (see 3.14).

Both certificate types offer the same functional and legal characteristics, are secure, and deploy the highest level of legal significance. Here, too, the customer requirements and the use case are the decisive factors in selecting the appropriate type.

3.21. primesign for Adobe Acrobat Sign

primesign MOBILE is the remote signing service from primesign that can also be used for qualified electronic signatures in Adobe Acrobat Sign. primesign MOBILE can be used directly with Adobe Acrobat Sign to quickly and easily trigger document signatures. For more information about primesign MOBILE for Adobe Acrobat Sign, visit our website: www.prime-sign.com/adobe. primesign MOBILE for Adobe Acrobat Sign can also be purchased directly from our online store.

"Sign with eID" (primesign WRAPTOR) can also be used with Adobe Acrobat Sign. Users can use their existing eIDAS eID (e.g. German Identity Card, ID Austria or Austrian mobile phone signature) to create a qualified signature with a primesign MOBILE one-time certificate – immediate signing; prior registration with primesign is not required.

3.22. primesign in the Fabasoft eGov Suite

primesign is integrated as a standard signature provider in the Fabasoft eGov Suite. The Fabasoft eGov Suite uses the primesign web application to apply personal electronic signatures to documents seamlessly and without media discontinuity.

"Sign with eID" (primesign WRAPTOR) can also be used with Fabasoft eGov Suite. Users can use their existing eIDAS eID (e.g. German Identity Card, ID Austria or Austrian mobile phone signature) to create a qualified signature with a primesign MOBILE one-time certificate – immediate signing; prior registration with primesign is not required.

3.23. CSC support

primesign is a member of the Cloud Signature Consortium[4]. The Cloud Signature Consortium is an international association of experts from academia and the industrial sector to create a new standard for cloud-based digital signatures (CSC standard). Our remote signing service primesign MOBILE is CSC-compliant and can thus be easily integrated with a variety of signature applications via CSC API. Thus, both signing with primesign MOBILE signing accounts and "Sign with eID" (primesign WRAPTOR) can easily be integrated into CSC-compliant signature applications.

See [6] for more information on integrating the CSC-API.

[4] https://cloudsignatureconsortium.org/

4. Representation of Company Affiliation, Roles and Functions in Electronic Signatures

For a legally binding electronic signature – i.e., an electronic signature legally equivalent to a handwritten signature – a natural person needs a qualified signing certificate. This certificate is bound to the natural person. All authorizations and powers of representation that a person already possesses and which have already been established legally can also be exercised in the electronic environment. Proof can be provided by conventional means.

There are several ways to represent company affiliation, roles, and functions in electronic signatures. For example, they can be embedded in the certificate AND displayed in the visual signature signet or they can be displayed "only" in the visual signature signet and not be embedded in the certificate.

EMBEDDED IN THE CERTIFICATE AND DISPLAYED IN THE SIGNATURE SIGNET

All data embedded in a qualified signing certificate must be strictly verified by the certification authority issuing the certificate – this is a so-called trust service provider, such as PrimeSign GmbH, which is supervised by the state and operates in accordance with EU law. In the simplest case, a certificate embeds personal data verified via recognized (official) IDs or comparable documents. Personal data embedded in primesign signature certificates is either checked against the ID via video identification or taken from the eID used for registration (e.g., ID Austria/Austrian mobile phone signature).

In the context of primesign business certificates, additional attributes such as the affiliation to an organization, functions, and roles within this organization (e.g., such as the function of the managing director, the authorized signatory) or email addresses can also be embedded in the certificate upon appropriate proof (i.e., an excerpt from the company register). All recipients of a document signed with such a certificate can see this additional information by verifying the signature. The recipient of a signed document can also trust the correctness of the information from a legal point of view. primesign transfers the obligations to provide, verify or ensure the correctness of these attributes to the respective organizations. For the issuance of business certificates, organizations must therefore enter into a contractual relationship with primesign.

The following points are agreed upon in this contractual relationship:

- The organization is the owner of the domain *.sampleorganization.at, and the allocation of email addresses to employees is under its sole control
- Holders of organizational email addresses (e.g., john.doe@sampleorganization.at) are allowed to carry the organization affiliation in the certificate (the official organization name stated in the company register must be entered as attribute "O" in the field "applicant").
- If a role is brought within the organization, the following applies: The organization must provide primesign with a data set linking the person's email address to the role and provide primesign with the necessary evidence (e.g., john.doe@sampleorganization.at contains the role managing director).
- According to the Terms and Conditions for the Use of Qualified Certificates of PrimeSign Gmbh, an obligation to revoke a certificate comes into effect if certified data in the qualified certificate change. This also applies to attributes such as organization affiliation, role, and email address. If an authorization expires, the organization must initiate a certificate revocation immediately.

  Even if the obligations to provide, verify or ensure the correctness of attributes are transferred to the respective organizations, the corresponding source for such authorizations, such as the company register in the case of managing directors, remains legally normative, as in the conventional case.

As an advantage over the world of paper, the personal data embedded in an electronic signing certificate allow at any time to track beyond doubt who made a declaration – even by mistake – and confirmed it with their signature. The function or role embedded in the signing certificate can also be displayed in the visual signature signet. In this way it is immediately visible to recipients when opening a document.

ONLY DISPLAYED IN THE SIGNATURE SIGNET

With the primesign SIGNATURE SERVER, a function or role can be displayed "only" in the visual signature signet, but not embedded in the certificate. This corresponds to the conventional handling, in which the signatory himself – e.g., an authorized signatory by adding "p.p.a. " – expresses their power of representation. Displaying functions and roles in the visual signet of electronic signatures but not embedding it in the certificate, for example, is highly suitable for powers of representation which are established in the internal relationship of a company, i.e., by rules of procedure and an organizational chart, but which do not necessarily find their way into the company register (e.g., purchaser, salesperson) or are subject to a certain dynamic.

The representation of the company affiliation in an electronic signature is similar to the representation of a function or role. In the case of the company affiliation ideally, the name of the legal entity for which the natural person works is embedded as a verified and documented attribute in its personal qualified signing certificate. In this way, the person would have all relevant characteristics recognizable as a verified attribute in its personal signing certificate (for example, name + role of managing director + company + FB number). As described previously, the company affiliation can, however, also be displayed only in the visual signature signet and not embedded in the certificate.

In addition, there is also the "electronic signature of a company": the so-called electronic seal. An electronic qualified seal is legally accepted throughout the EU, is based on the eIDAS Regulation, and is technically similar to the qualified electronic signature for natural persons. Legally, the seal corresponds to the "digital stamp", i.e., it serves as proof of origin (the document originates from the company identified in the seal certificate) and proof of integrity (the document has not been subsequently altered). The only significant legal difference from the qualified signature of a natural person is that a seal does not represent a declaration of intent. As with the signature on paper, a declaration of intent always requires the acting person(s) and thus the electronic signature(s) of the person(s) authorized.

It is also possible to combine a seal certificate of a company and a qualified signing certificate of the acting person and apply them together. However, if the qualified signing certificate of the acting person already contains the company reference as verified information (attributes), an additional seal would not be necessary per se. The company seal, on the other hand, can also be used on its own, for example, to sign invoices, outgoing documents, or general terms and conditions in mass processes.

For registration with some official EU-wide applications, such as the European Product Registry for Energy Labelling (EPREL database), there is the need for companies to have an electronic seal for electronic verification. With our solution – the primesign MOBILE SEAL – you can have your company quickly and easily registered in the EPREL database. The primesign MOBILE seal is available as an annual package. The annual package includes:

- The issuance of a qualified primesign MOBILE SEAL certificate (in the name of your company)
- A primesign PREMIUM account for our online signing service (www.prime-sign.com)
- An unlimited number of seal transactions per year (fair use principle)

Note: In the course of the application, you will also receive a personal primesign MOBILE signing certificate (qualified signing certificate according to eIDAS). In addition to the seal certificate, the signing certificate can be used for personal electronic signatures (certificate and transactions are included in the price).

The issuance of the primesign MOBILE SEAL certificate takes place online and requires video identification by a person authorized to represent the organization. In addition, further proof, such as, e.g., an excerpt from the company register, must be submitted. For further information about our offer and the issuing process visit our website: www.cryptas.com/trust-center. The primesign MOBILE SEAL can also be purchased directly in our online store.

5. Document Security and Signature Transactions

A frequently recurring question relates to the whereabouts of a document to be signed during a signature transaction (application of the signature), when the document is not supposed to leave the customer's IT infrastructure. How can it be ensured that sensitive documents remain in the customer's IT infrastructure throughout the entire signature process (document upload, application of the signature, document archiving)?

To ensure that a document does not leave the customer's IT infrastructure, the primesign SIGNATURE SERVER must be operated on-site (on-premise) in any case. Additionally, the signature creation device used also plays a decisive role and must be chosen accordingly.

If the primesign SIGNATURE SERVER is operated on-premise, a document remains in the customer's IT infrastructure at least until the signature is actually triggered. The server can be operated either as a virtual appliance or optionally as a hardware appliance.

After the signature has been triggered, the signature creation device (certificate) used is decisive for whether or not a document still remains in the customer's IT infrastructure.

> Our portfolio includes both the on-premise installation of the primesign SIGNATURE SERVER and the provision of a virtual server as part of our operating infrastructure (SaaS as part of our private cloud). If the primesign SIGNATURE SERVER is operated as SaaS, documents to be signed inevitably leave the customer's IT infrastructure, regardless of which signature creation device is used.

The combination of both, an on-premise operation of the primesign SIGNATURE SERVER and an appropriate signature creation device can then ensure that documents remain in the customer's IT infrastructure during the entire signature process (document upload, application of the signature or rather signature transaction, document archiving).

If, for example, a signature card is used, it is always guaranteed that a document remains in the infrastructure of the primesign SIGNATURE SERVER and at the signatory's workstation. Further infrastructure or components are not required. In explicit terms: The signature is created via the primesign SIGNATURE SERVER operated on-premise and via the signatory's signature card connected locally to the PC workstation – the document does not leave these areas.

Document also remain completely within the customer's IT infrastructure during the entire signature process if a primesign SIGNATURE SERVER on-premise setup is used in conjunction with our remote signing service primesign MOBILE or primesign WRAPTOR (see 3.19 and 3.18). Documents to be signed are not transmitted to primesign. primesign only receives the so-called hash value (fingerprint) of the documents to be signed. The document content cannot be derived from this.

When signing with ID Austria or the Austrian mobile phone signature (unless used in combination with primesign WRAPTOR), special precautions must be taken to ensure that documents do not leave the customer's IT infrastructure. So that the entire document does not have to be transmitted to A-Trust, A-Trust offers an additional hardware component (Signature-Box) that prepares the document to be signed locally. In this way, it is guaranteed that during the entire signature process (including the application of the signature), the document remains in the customer's IT infrastructure. The primesign SIGNATURE SERVER can be connected out of the box to the A-Trust Signature-Box and uses it as "gateway" to A-Trust.

The following table shows the relationship between the respective deployment approach and the signature creation device used and its effect on the whereabouts of documents to be signed during a signature transaction (application of the signature).

Table 1: Document security depending on the respective deployment architecture and signature creation device

Documents to be signed remain in the customer's IT infrastructure			
		Deployment Architecture primesign SIGNATURE SERVER	
		on-premise	*SaaS (Private Cloud of CRYPTAS)*
Signature creation device including any additional requirements	***Server-side signature creation*** *With a SW key/certificate or with a signature key/certificate stored in an HSM directly connected to or configured on the primesign SIGNATURE SERVER*	**Yes**	No
	Signature card *for example employee card, citizen card. Independent of the trust service provider.*	**Yes**	No
	ID Austria/Austrian mobile phone signature (A-Trust) without local components and not used in conjunction with primesign WRAPTOR	No	No
	ID Austria/Austrian mobile phone signature (A-Trust) with local component A-Trust Signature-Box on-premise	**Yes**	No
	primesign MOBILE	**Yes**	No
	primesign WRAPTOR	**Yes**	No

6. Exemplary Deployment Architectures

This section describes and outlines two typical deployment architectures: a simple on-premise setup and its equivalent as a Managed Service (SaaS).

> The schematic representations of the deployment architectures are simplified and focus on the most essential core elements. Further aspects, such as redundancies, single sign-on (domain authentication), LDAP connections, failover, and backup, etc., are not shown for reasons of simplification.

6.1. On-premise

The exemplary architecture shown in Figure 5 intends to provide an overview of the individual components of an on-premise setup and shows the dependencies between the main system elements.

The figure exemplarily shows the connection of remote signing services, such as primesign MOBILE or the ID Austria/Austrian mobile phone signature (A-Trust). When using primesign MOBILE in conjunction with a primesign SIGNATURE SERVER on-premise setup, we can ensure that, during a signature process, documents always remain completely within the customers' IT infrastructure (also in combination with primesign WRAPTOR). When using ID Austria/the Austrian mobile phone signature (unless used in combination with primesign WRAPTOR), an additional hardware component (Signature-Box) is required if documents to be signed must not leave the customer's IT infrastructure (not shown in Figure 5, see chapter 5).

If electronic signatures are created with signature cards or employee cards, all connections to remote signing services or their operators cease to exist, and the figure can be reduced to the elements of the "customer domain".

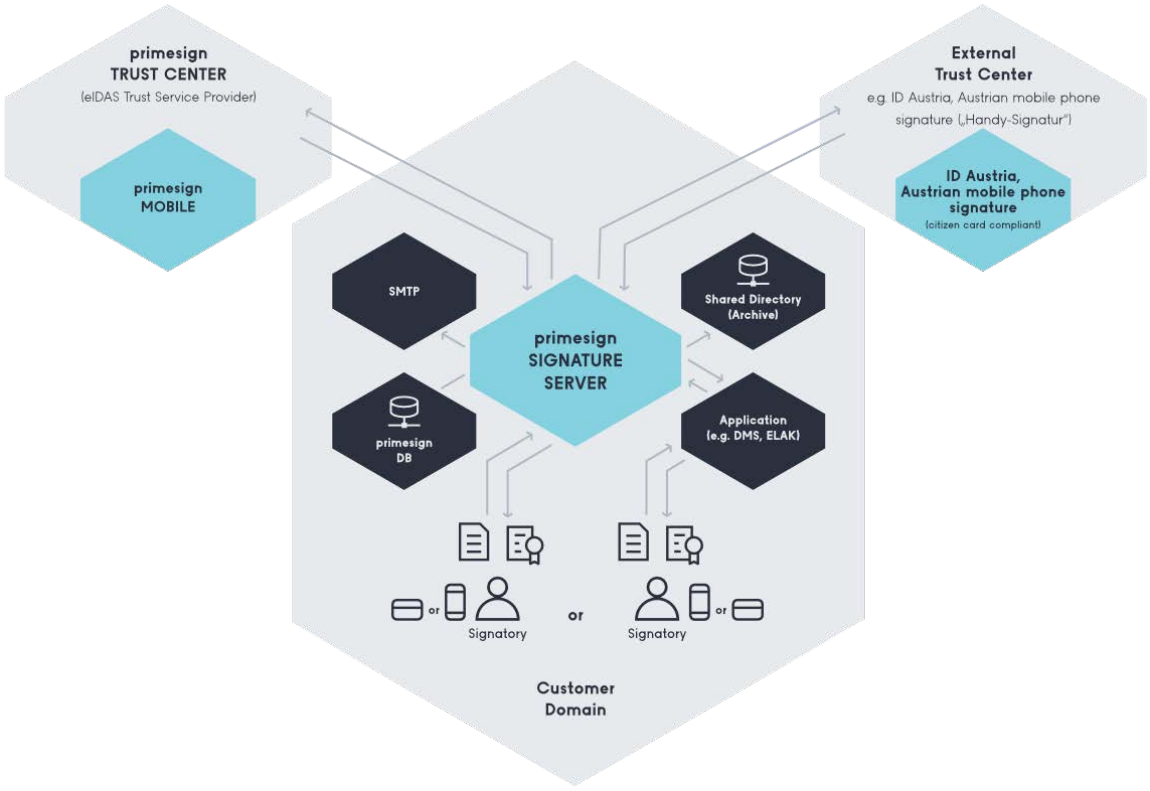

Figure 5: Simplified, illustrative deployment architecture on-premise

Customer Domain

Main elements of the on-premise signature infrastructure at customer-side:

- **primesign SIGNATURE SERVER:** One (or more) primesign SIGNATURE SERVER appliances (nodes) operating individually or optionally in a fail-over setup.
- **primesign database (primesign DB):** The primesign database is the backbone of our service. It contains all the relevant settings for our solution and manages, e.g., signing flows. A wide range of available database systems is supported (see 7.2 and 7.3).
- **Signatory:** Two exemplary signatories within the customer's domain are shown. For signing, either our remote signing service primesign MOBILE (also in combination with primesign WRAPTOR), ID Austria/the Austrian mobile phone signature (A-Trust), the German Identity Card or a signature card can be used.
- **SMTP server (optional):** SMTP is used to send emails for invitations or reminders (signing flows). To send those emails from the customer's domain, the customer must grant access to their SMTP server.

- **Shared Directory - Archive (optional):** The primesign SIGNATURE SERVER supports automatic writing of signed documents to an external data storage. The default interface for this automatic export function is a shared folder.
- **Application (optional):** "Application" stands for any kind of connected application, such as the electronic file (ELAK), DMS, etc., that uses our web service interfaces (or other integration interfaces) to sign documents.

primesign Trust Service Provider

In case the qualified remote signing service primesign MOBILE is used to sign documents (also in combination with primesign WRAPTOR), the primesign TRUST CENTER is connected to the customer's infrastructure as a trust service provider.

primesign MOBILE: This is the core system of our own qualified remote signing service. It uses a mobile phone to authenticate the signatory during a signature process and creates eIDAS-compliant PAdES signatures. If our remote signing service is used in conjunction with a primesign SIGNATURE SERVER on-premise setup, it is ensured that documents are not transferred in their entirety to the trust center (also in combination with primesign WRAPTOR). When using primesign WRAPTOR, selected eIDAS eIDs are used for identification based on which a primesign MOBILE one-time certificate is created and used for signing.

External trust center (e.g., ID Austria/Austrian mobile phone signature (A-Trust))

In case the remote signing service of an external trust center is used to sign documents, an external trust center is connected to the customer's infrastructure as a trust service provider. We use ID Austria/the Austrian mobile phone signature (A-Trust) as an example of an external signing service.

ID Austria or Austrian mobile phone signature: This part shows the server-side infrastructure of ID Austria/the Austrian mobile phone signature (currently operated by A-Trust).

Other aspects

Some general comments on the simplified figure:

- **End-to-end encryption via SSL/TLS or IPSec:** All connections are encrypted and authenticated using SSL/TLS or IPSec.
- **Internal, external, and anonymous signatories**: Although the figure shows only internal signatories, the proposed solution infrastructure also supports external users located outside the client's domain, as well as anonymous users.

- **Supported signature creation devices:** Although the figure only shows the use of remote signing services (primesign MOBILE, ID Austria, Austrian mobile phone signature), smart cards and other signature tokens are also supported.
- **The figure is simplified – not all connections are shown:** To keep this figure simple, some existing connections are not shown. For example, connections to external verification services (OCSP, CRL, etc.) and other dependencies (optional: Active Directory) have been omitted. Which further connections occur depends on the specific use cases and integration scenarios.

6.2. SaaS

Figure 6 outlines the setup of the primesign SIGNATURE SERVER infrastructure as a Managed Service (SaaS). It shows a simplified example of the corresponding architecture and the individual components.

In a SaaS setup, the documents to be signed are always transferred to the managed service. Thus it is not possible to keep the content of a document within the customer's IT infrastructure.

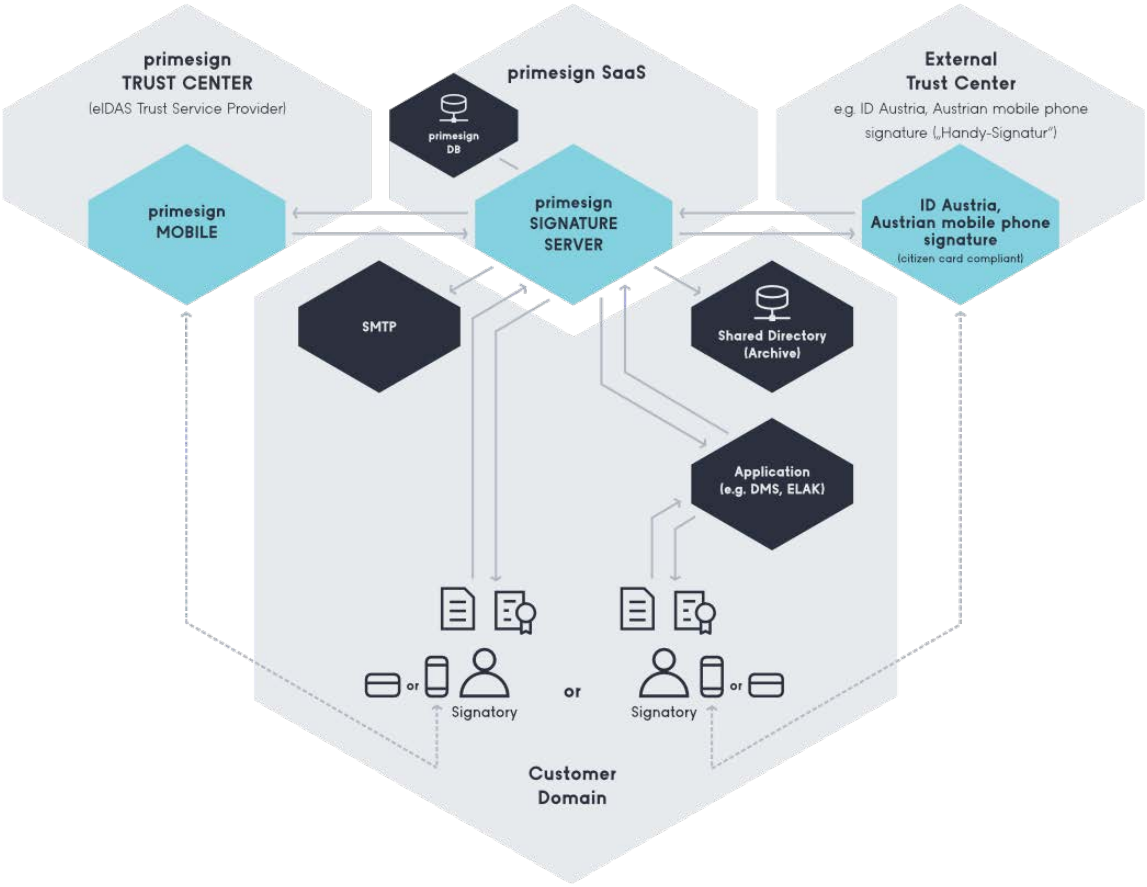

Figure 6: Simplified, illustrative deployment architecture SaaS

primesign SaaS (private cloud of our SaaS operation)

Main elements of the SaaS infrastructure:

- **primesign SIGNATURE SERVER:** One (or more) primesign SIGNATURE SERVER appliances (nodes) operating individually or in a fail-over setup.
- **primesign database (primesign DB):** The primesign database is the backbone of our service. It contains all the relevant settings for our solution and manages, e.g., signing flows. A wide range of available database systems is supported (see 7.2 and 7.3).

Customer Domain

- **Signatory:** Two exemplary signatories within the customer's domain are shown. For signing, either our remote signing service primesign MOBILE (also in combination with primesign WRAPTOR), ID Austria/the Austrian mobile phone signature (A-Trust), the German Identity Card or a signature card can be used.
- **SMTP server (optional):** SMTP is used to send emails for invitations or reminders (signing flows). To send those emails from the customer's domain, the customer must grant access to their SMTP server.
- **Shared Directory - Archive (optional):** The primesign SIGNATURE SERVER supports automatic writing of signed documents to an external data storage. The default interface for this automatic export function is a shared folder.
- **Application (optional):** "Application" stands for any kind of connected application, such as the electronic file (ELAK), DMS, that uses our web service interfaces (or other integration interfaces) to sign documents.

primesign Trust Service Provider

In case the qualified remote signing service primesign MOBILE is used to sign documents (also in connection with primesign WRAPTOR), the primesign TRUST CENTER is connected to the customer's infrastructure as a trust service provider.

primesign MOBILE: This is the core system of our own qualified remote signing service. It uses a mobile phone to authenticate the signatory during a signature process and creates eIDAS-compliant PAdES

signatures. When using primesign WRAPTOR, selected eIDAS eIDS are used for identification based on which a primesign MOBILE one-time certificate is created and used for signing.

External trust center (e.g., Austrian mobile phone signature/ID Austria (A-Trust))

In case the remote signing service of an external trust center is used to sign documents, an external trust center is connected to the customer's infrastructure as a trust service provider. We use ID Austria/the Austrian mobile phone signature (A-Trust) as an example of an external signing service.

ID Austria/Austrian mobile phone signature: This part shows the server-side infrastructure of ID Austria/the Austrian mobile phone signature (currently operated by A-Trust).

Other aspects

Some general comments on the simplified figure:

- **End-to-end encryption via SSL/TLS or IPSec:** All connections are encrypted and authenticated using SSL/TLS or IPSec.
- **Internal, external, and anonymous signatories**: Although the figure shows only internal signatories, the proposed solution infrastructure also supports external users located outside the client's domain, as well as anonymous users.
- **Supported signature creation devices:** Although the figure only shows the use of remote signing services (primesign MOBILE, ID Austria, Austrian mobile phone signature), smart cards and other signature tokens are also supported.
- **The figure is simplified – not all connections are shown:** To keep this figure simple, some existing connections are not shown. For example, connections to external verification services (OCSP, CRL, etc.) and other dependencies (optional: Active Directory) have been omitted. Which further connections occur depends on the specific use cases and integration scenarios.

7. primesign SIGNATURE SERVER Requirements

This chapter provides a rough overview of the most essential requirements of our primesign SIGNATURE SERVER solution. Details can be found in the documentation for the respective components (this documentation is also normative in case of uncertainty). The following sections serve for initial orientation.

7.1. Certificate requirements (signature creation devices)

Our product differs from similar signature solutions on the market in that it is open to the use of a wide variety of signature creation devices and certificates for electronic signatures.

Particularly in the area of personal signatures, the unique selling point of the primesign SIGNATURE SERVER is that in addition to primesign's own signing certificates (primesign MOBILE certificates, also in combination with primesign WRAPTOR, see 3.18), signing certificates from other providers can also be used as a standard. These include, for example, ID Austria or the Austrian mobile phone signature, employee cards, e-cards, or other signature creation devices or HSMs.

Besides, we are also a software producer and a trust center operator (eIDAS trust service provider) and can thus offer optimized end-to-end solutions, from the issuing of a (qualified) certificate to its use with the primesign SIGNATURE SERVER – or in connected applications such as the electronic file or a DMS.

Specifically, we offer standard support for the following signature creation devices and signing certificates:

- primesign MOBILE (PrimeSign GmbH) – our qualified remote signing service, see 3.19
- primesign WRAPTOR (qualified signature with a primesign MOBILE one-time certificate based on selected eIDAS eIDs, e.g. German Identity Card, ID Austria/Austrian mobile phone signature, see 3.18)
- ID Austria or Austrian mobile phone signature (A-Trust)
- Any signature card that can be addressed for signatures via the standardized middleware interface Security Layer (v.1.2).
    - Middleware is to be provided by the card provider
- Software keys and certificates from various trust service providers

Additional signature creation devices and signing services from other trust service providers can be integrated upon request.

7.2. Hardware requirements

7.2.1. primesign SIGNATURE SERVER (relevant for on-premise operation)

In general, we offer and deliver the primesign SIGNATURE SERVER as a virtual appliance. The minimum system requirements of the appliance are summarized in the manual or setup guide [4].

Optionally, the primesign SIGNATURE SERVER can also be delivered as a physical appliance, for example, if no infrastructure (hypervisor) for the operation of our virtual appliance is available or desired.

7.2.2. Signature creation devices

The following explanations of hardware requirements for signature creation devices are purely informative since these must be specified by the respective issuer (trust center).

Provided that the documents to be signed must not leave the customer's IT infrastructure, the use of a remote signing service may require the combination with a corresponding on-premise setup and in some cases the acquisition of additional hardware components. However, this is optional, depends on the remote signing service chosen and the corresponding trust service provider.

When using ID Austria or the Austrian mobile phone signature (A-Trust), for example, the installation of an additional hardware component, the A-Trust Signature-Box, is required to ensure that documents remain in the customer's IT infrastructure even during a signature transaction (application of the signature). If primesign MOBILE (also in combination with primesign WRAPTOR) is used in conjunction with a corresponding primesign SIGNATURE SERVER on-premise setup, no additional hardware is required. Documents to be signed always remain completely within the customer's IT infrastructure.

When signature cards are used, card readers for using the signature cards at the workstation are required as hardware – this also following the specifications of the respective provider.

7.3. Software requirements

7.3.1. primesign SIGNATURE SERVER (relevant for on-premise operation)

Beyond the operational requirements of the virtual appliance, the primesign SIGNATURE SERVER only requires a database connected (external database recommended).

The respective databases supported are summarized in the manual or setup guide [4].

Further key data or requirements, depending on configuration and use cases are listed below (excerpt from primesign SIGNATURE SERVER documentation):

- If the signed PDF documents are to support Long Term Validation (LTV), access to the revocation status services of the signing certificate used is required. Typically, these are ports 443, 80, and 389.
- If Single Sign-On (SSO) is used, this is implemented via a Microsoft IIS. Access to the Active Directory (LDAP endpoint) is required.
- If the address book functionalities are used, then access to the Active Directory (LDAP endpoint) is required.
- If signing flows are carried out (i.e., users invite other users to sign a document), the connection of an SMTP server is necessary.
- If the directory scanner functionality is used, the directories to be connected must be accessible and the corresponding read/write permissions must be granted.

The document primesign SIGNATURE SERVER – Solution Overview [2] also outlines further deployment options, such as in the case of SSO realization via an IIS integration.

On the part of the primesign SIGNATURE SERVER, there are no additional requirements for the client. The user interface of the primesign SIGNATURE SERVER is purely web-based and can be used with all common web browsers, without Java installation or other active components. Besides the presence of a web browser, our product does not impose any software requirements on the client workstation.

7.3.2. Signature creation devices

The following explanations of the requirements for signature creation devices are purely informative. Requirements for signature creation devices must be specified by the respective issuer (trust center).

Remote signing services, such as primesign MOBILE (also in combination with primesign WRAPTOR) or the Austrian mobile phone signature (A-Trust), require a mobile phone or smartphone, for example. With A-Trust, on smartphones, an additional app is required to trigger a signature. With primesign MOBILE, any SMS-enabled mobile phone (no app required) is sufficient to trigger qualified remote signatures. See 3.17 for using the German Identity Card.

If signature cards are used (employee cards, etc.), the issuer of the signature cards must/will also provide appropriate client software (middleware) with witch the signature card can be addressed (see 3.1.)

7.3.3. SOAP interfaces

The primesign SIGNATURE SERVER offers a number of integration interfaces. The appendix references a short description of our current workflow interface (SOAP) [3], which we primarily recommend.

In addition, the primesign SIGNATURE SERVER has a synchronous SOAP signature interface to enable automated signatures to be executed with high performance (for example, for server-side signature creation processes or mass procedures, or the automated application of qualified seals).

Furthermore, the PDF conversion function – PDF/A-compliant if desired - can also be used independently via a synchronous interface command (PrimeConvert).

8. References

8.1. Austrian Federal Chancellery

primesign is used for the personal digital signature (PDS) in the electronic file (ELAK in the federal government, i.e., Fabasoft eGov-Suite) and was directly integrated into the system. This allows ELAK users to sign electronically with primesign directly in the web-based workflow of the ELAK. For this purpose, the PDF document to be signed is transferred to the primesign SIGNATURE SERVER operated by the BKA, where an individual signature can then be placed and triggered.

In addition, primesign is also used to submit PDF-based funding applications. A dedicated primesign instance accepts PDF forms from citizens and prompts citizens to sign the PDF before submission (using the Austrian mobile phone signature or a citizen card).

8.2. Austrian Federal Computing Center

The Austrian Federal Computing Center (or BRZ) uses a local primesign SIGNATURE SERVER for personal electronic signatures by employees of the company. An SSO connection (domain) was also integrated. Each employee is therefore seamlessly authenticated and has (group-specific) signature profiles activated. On the one hand, the BRZ employees sign the documents directly in the primesign web interface (with their employee card or the Austrian mobile phone signature). On the other hand, the BRZ also uses an integration similar to that of the BKA in their Fabasoft eGov Suite to implement (individual) electronic signatures directly.

8.3. The Styrian Parliament and the Styrian Government

The province of Styria operates a central primesign infrastructure for handling all classic signature and official signature processes. In terms of transaction numbers, the Styrian Parliament and the Styrian Government use the primesign infrastructure mainly to automatically apply official signatures to all outgoing official documents of the province. The official signature – implemented using the province's primesign infrastructure – is the main element of almost all electronic processes. All outgoing documents are officially signed using primesign.

In addition, the workflow system of the Styrian Parliament was connected to the central primesign infrastructure so that members and staff of the Parliament can apply their personal electronic signatures using primesign. I.e., the personal electronic signature with primesign was integrated into the workflow system of the Styrian Parliament.

8.4. Further references

Further references are available upon request and in coordination with our customers.

9. Additional Documents and Supplements

This section includes reference to additional documents:

[1] CRYPTAS / PrimeSign GmbH: **Product Data Sheet primesign SIGNATURE SERVER** as amended. Available in English and German language.

[2] CRYPTAS / PrimeSign GmbH: **primesign SIGNATURE SERVER – Standard Solution Overview**, as amended. Brief overview of the main functions and technical features of our product. The document also shows screenshot sequences of typical, simple use cases, including the use of different signature creation devices, such as the Austrian mobile phone signature (A-Trust) or primesign MOBILE. In English language.

[3] CRYPTAS / PrimeSign GmbH: **primesign SIGNATURE SERVER – Integration Documentation**, in the respective valid version. API documentation for the typical connection of the primesign SIGNATURE SERVER to external applications (such as the ELAK).

[4] CRYPTAS / PrimeSign GmbH: **primesign SIGNATURE SERVER Appliance Documentation**, as amended. Manual and setup guide for setting up and operating a primesign SIGNATURE SERVER (as a virtual/physical appliance).

[5] CRYPTAS / PrimeSign GmbH: **Frequently asked questions – primesign MOBILE,** in the respective valid version. Collection of frequently asked questions and answers about primesign MOBILE (including primesign MOBILE for Adobe Acrobat Sign). In German and in English language.

[6] CRYPTAS / PrimeSign GmbH: **primesign MOBILE – Getting Started Guide for Integrators (CSC API),** in the respective valid version. Collection of technical and organizational information about integrating the primesign signature via CSC API. In English language.