keyon

13. MAGGLINGER RECHTSINFORMATIKSEMINAR

19. März 2013

Entwicklung und Einsatz von Signaturserverdiensten

eberhard@keyon.ch

Über Keyon

- Experten im Bereich IT-Sicherheit und Software Engineering

keyon

Erstklassige Referenzen

keyon

Erstellen von elektronischen Signaturen

keyon

Lokale SuisseID

Der Benutzer signiert das Dokument lokal auf seinem PC unter Verwendung seiner lokalen SuisseID.

Mögliche Probleme sind:

- Installation der Smartcard – Abhängigkeit von Betriebssystem-Versionen
- Interaktion der unterschiedlichen Applikationen mit der Smartcard – unterschiedliches, für den Benutzer nicht transparentes Verhalten
- Die Organisation hat keine Kontrolle über die geleisteten Signaturen, die innerhalb oder ausserhalb des Unternehmens geleistet werden

keyon

Lokale SuisseID

- Der Mitarbeiter kann die Smartcard nach Hause nehmen und privat nutzen, obwohl die SuisseID einen Hinweis auf die Organisation enthalten kann. Für den Empfänger ist es nicht ersichtlich, ob die Signatur im privat oder im Namen der Organisation geleistet wurde.
- Automatische und sofortige «deaktivierung» des Signaturschlüssels, falls ein Mitarbeiter das Unternehmen verlässt (kein Zugriff mehr auf den Signaturschlüssel)

3.3.4 Dealing with Representatives

If the certificate owner happens to be a representative of a legal body or organisation according to article 5, paragraph 2 of VZertES [2], then the CSP **MUST** make sure that the legal entity specified in the appropriate attributes is capable of revoking the SuisseID certificates at any time.

eCH-0113: SuisseID specification

keyon

Zentraler Signaturserver

- Am 1. August 2011 traten die überarbeitete Verordnung zum Signaturgesetz (VZertES) sowie die technischen und administrativen Vorschriften (TAV ZertES) in Kraft, welche neben Smartcards neu auch zentrale Signaturdienste für die Erstellung von qualifizierten elektronischen Signaturen ermöglichen.
- In der EU werden aktuell analoge, sogenannte vertrauenswürdige Services standardisiert und auf Verordnungsstufe geregelt.

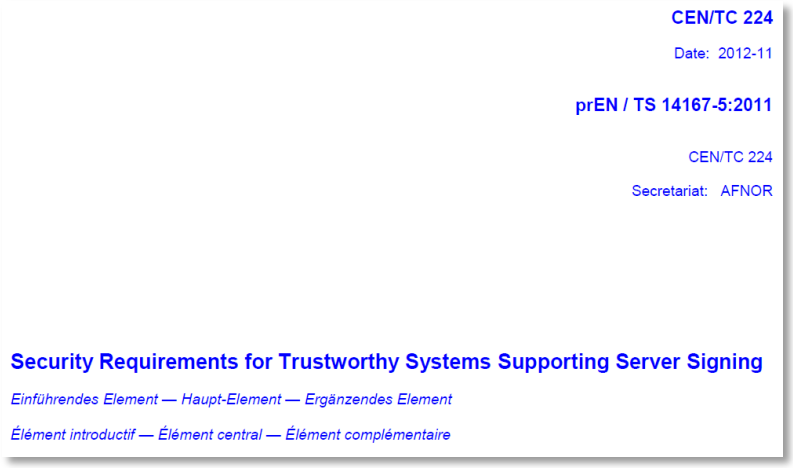
EUROPÄISCHE KOMMISSION

Brüssel, den XXX
COM(2012) 238/2

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt



CEN/TC 224

Date: 2012-11

prEN / TS 14167-5:2011

CEN/TC 224

Secretariat: AFNOR

Security Requirements for Trustworthy Systems Supporting Server Signing

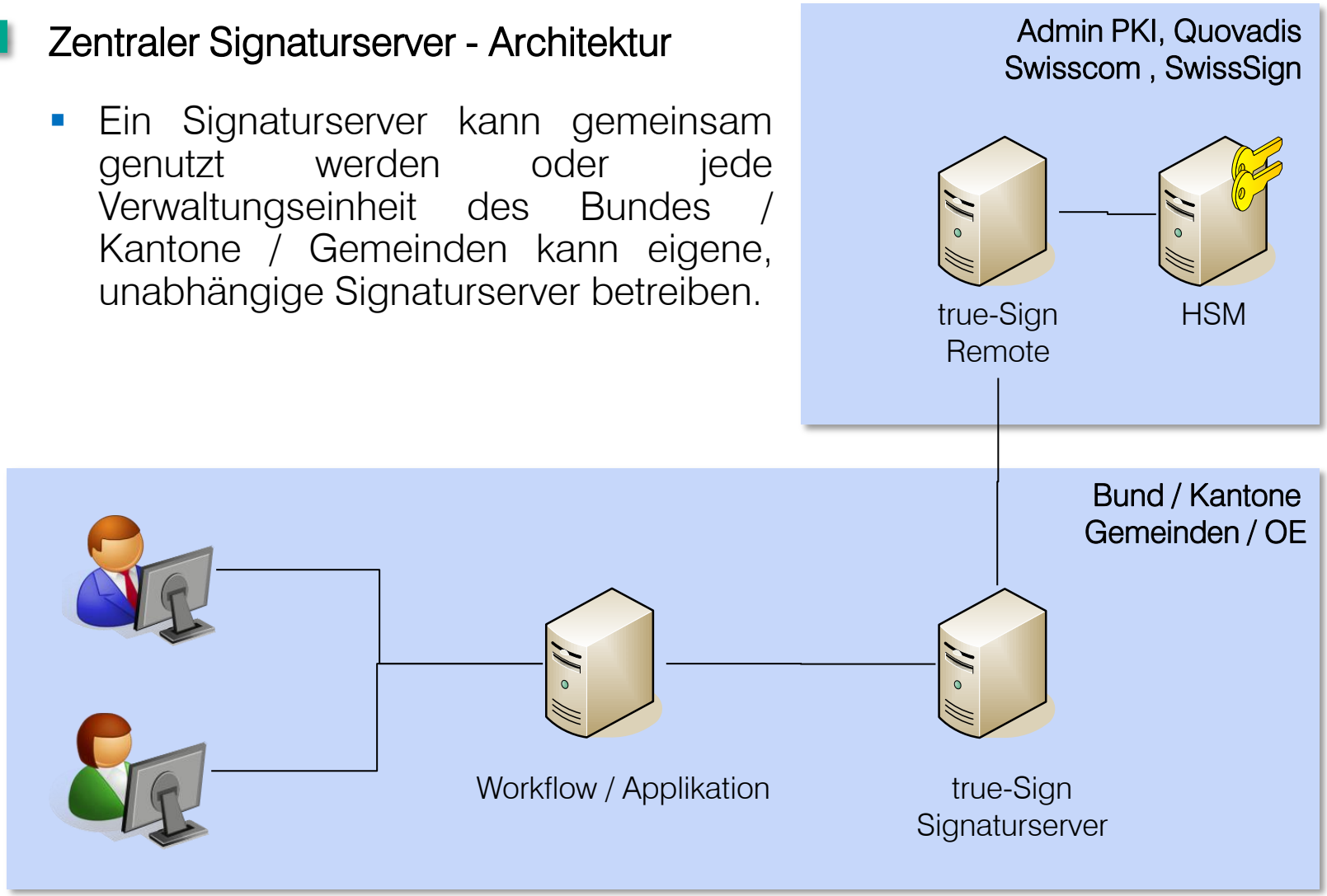
Einführendes Element — Haupt-Element — Ergänzendes Element

Élément introductif — Élément central — Élément complémentaire

keyon

Zentraler Signaturserver - Architektur

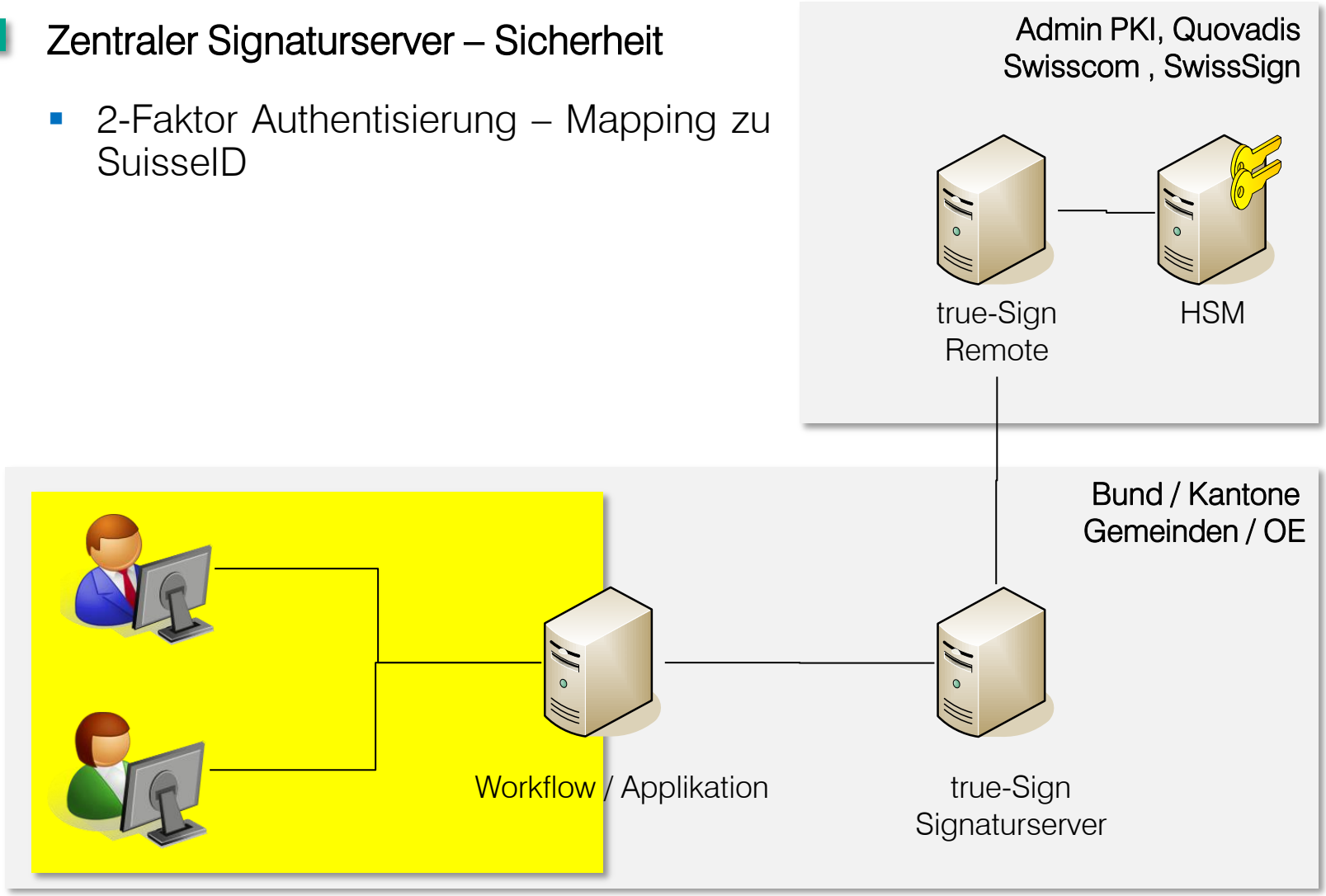
- Ein Signaturserver kann gemeinsam genutzt werden oder jede Verwaltungseinheit des Bundes / Kantone / Gemeinden kann eigene, unabhängige Signaturserver betreiben.



keyon

Zentraler Signaturserver – Sicherheit

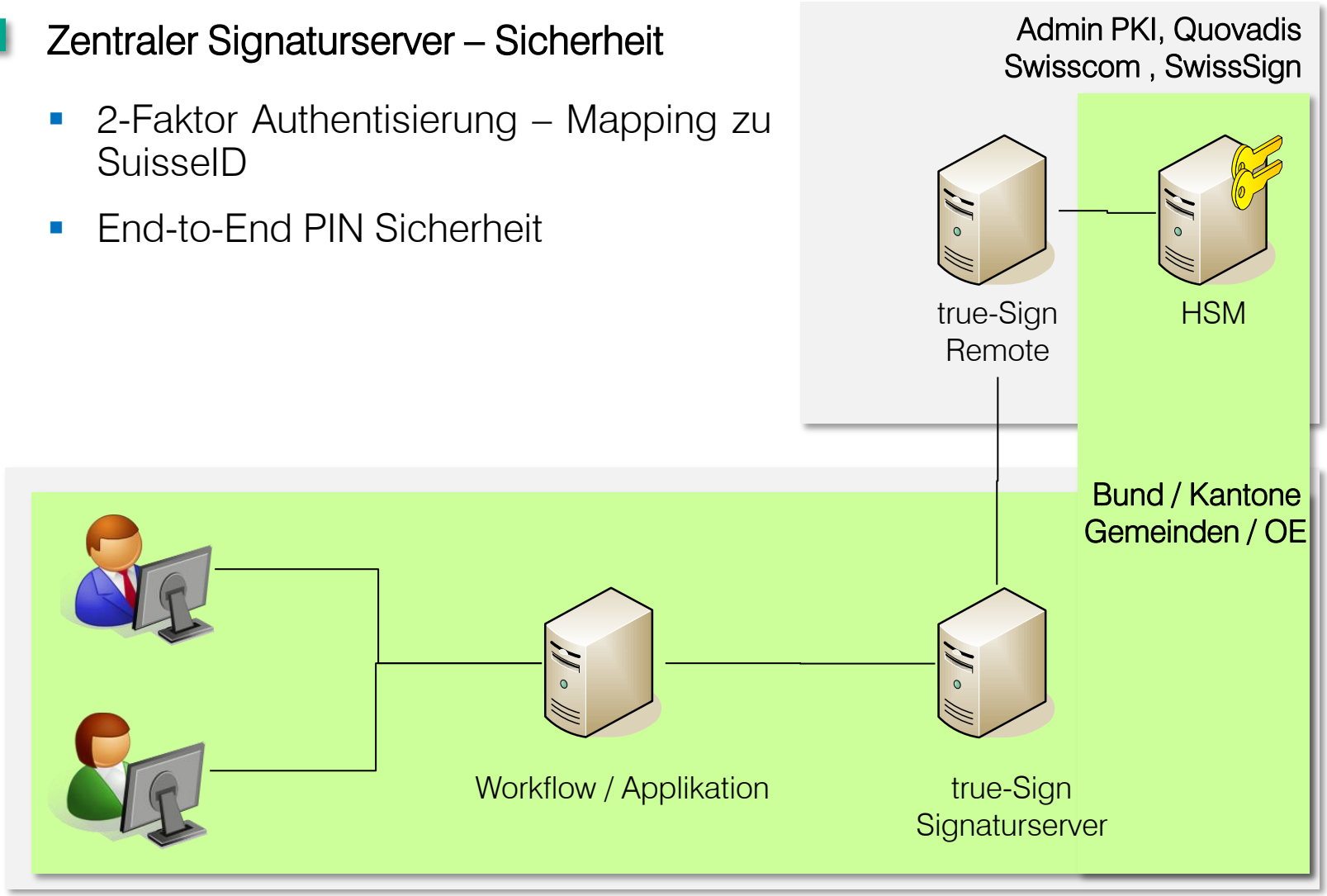
- 2-Faktor Authentisierung – Mapping zu SuisseID



keyon

Zentraler Signaturserver – Sicherheit

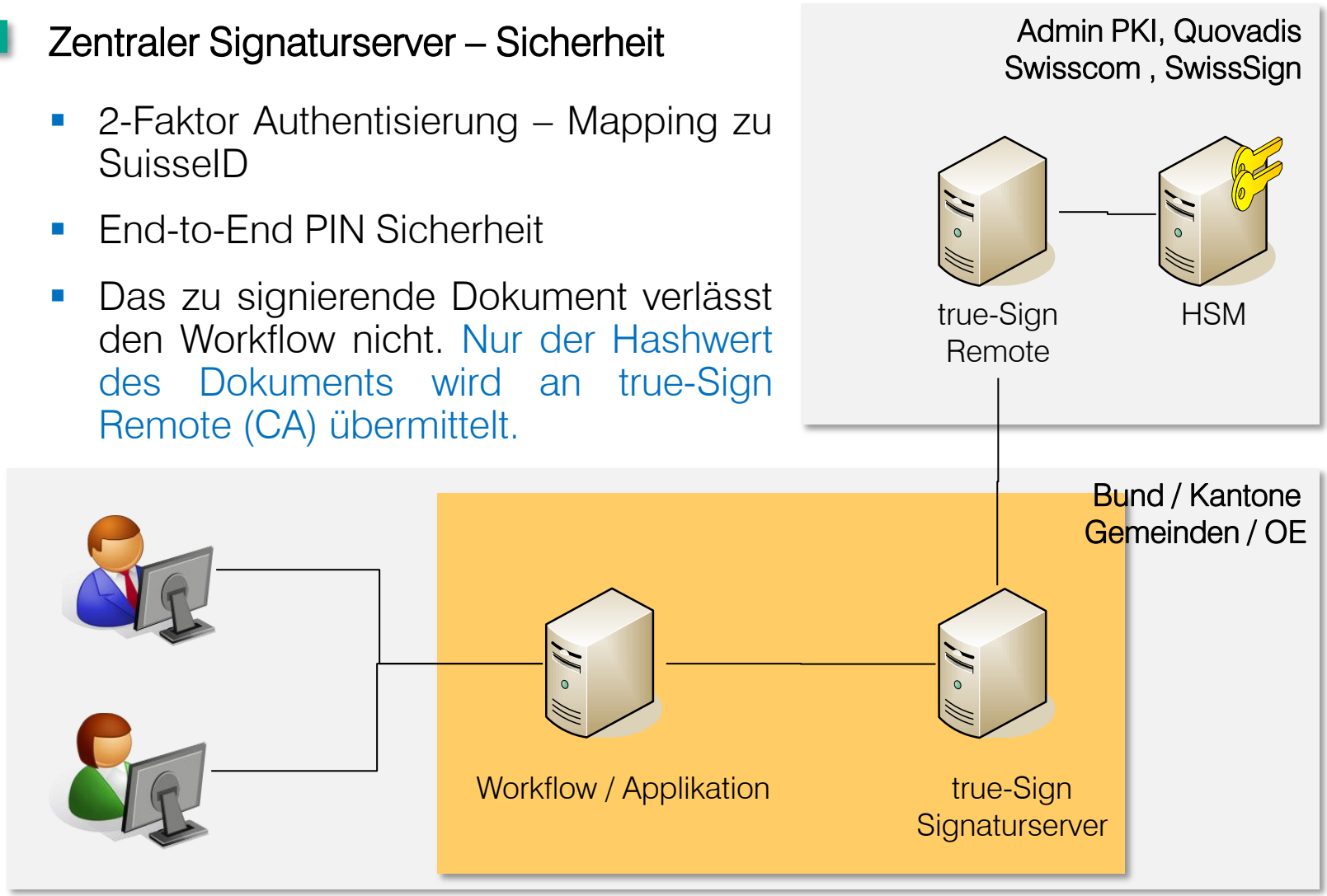
- 2-Faktor Authentisierung – Mapping zu SuisseID
- End-to-End PIN Sicherheit



keyon

Zentraler Signaturserver – Sicherheit

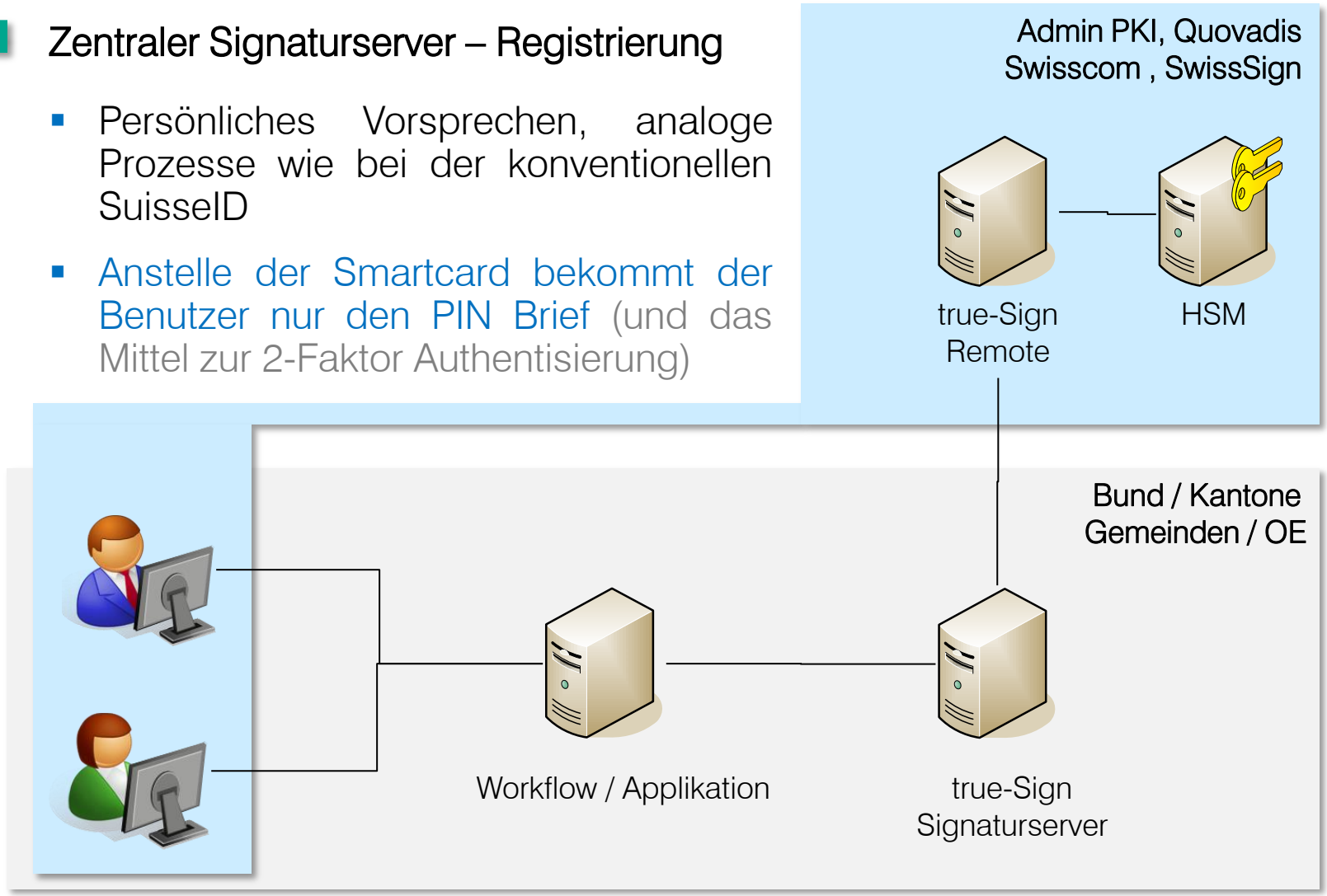
- 2-Faktor Authentisierung – Mapping zu SuisseID
- End-to-End PIN Sicherheit
- Das zu signierende Dokument verlässt den Workflow nicht. Nur der Hashwert des Dokuments wird an true-Sign Remote (CA) übermittelt.



keyon

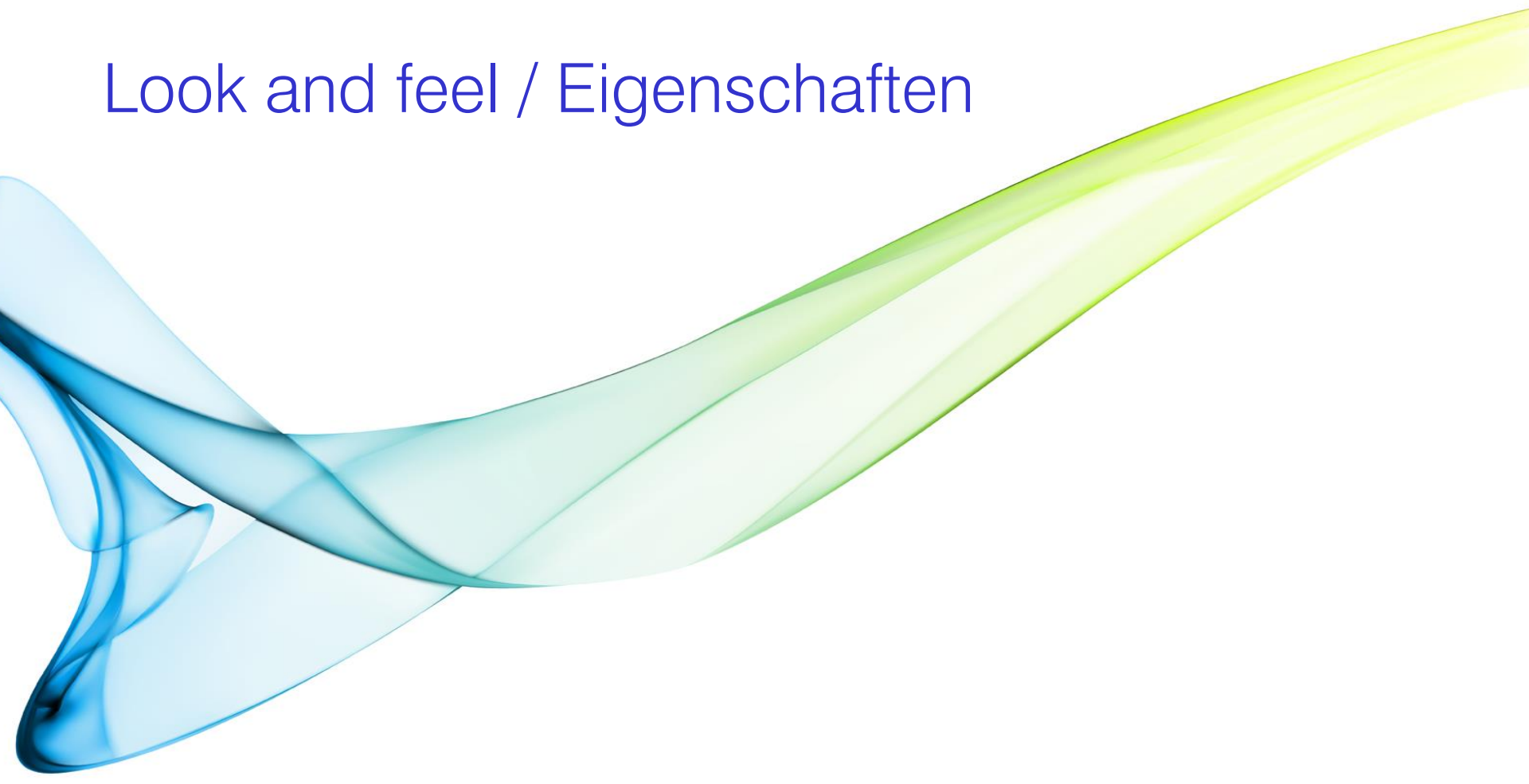
Zentraler Signaturserver – Registrierung

- Persönliches Vorsprechen, analoge Prozesse wie bei der konventionellen SuisseID
- Anstelle der Smartcard bekommt der Benutzer nur den PIN Brief (und das Mittel zur 2-Faktor Authentisierung)



keyon

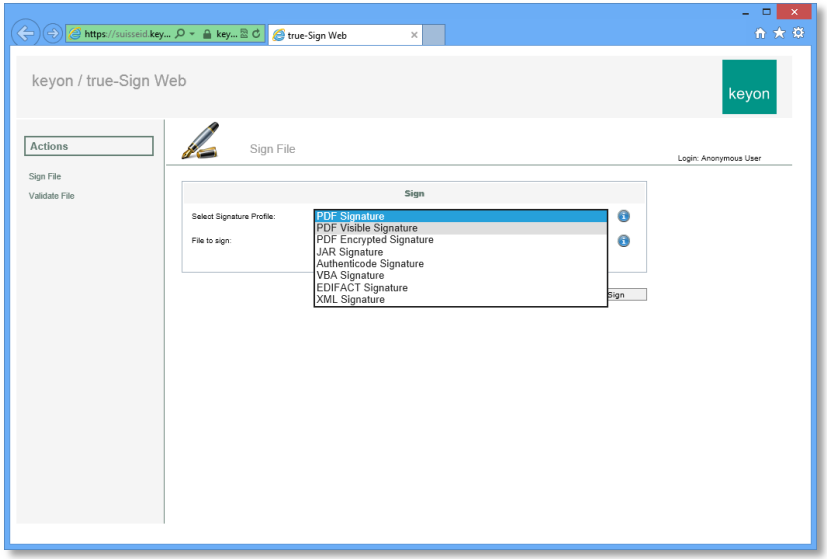
Look and feel / Eigenschaften

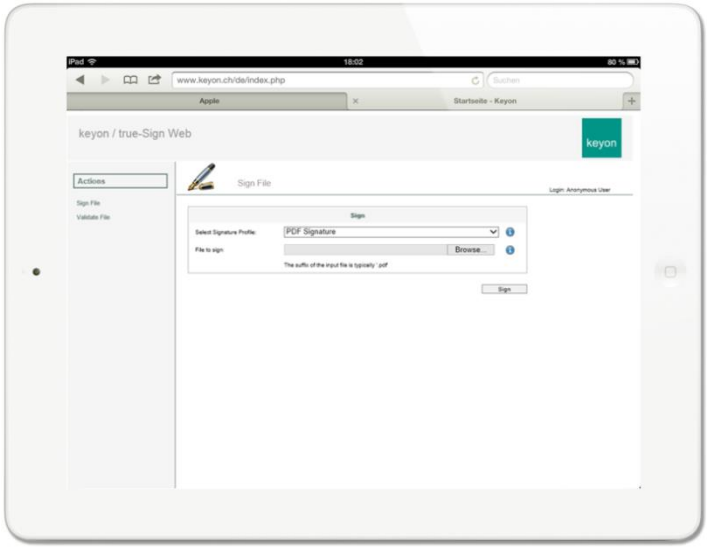


Look and feel / Eigenschaften

Signaturvorgang aus Sicht des Benutzers

- Browserbasiert innerhalb von Workflows





keyon

Signaturvorgang aus Sicht des Benutzers – Mobile Anwendung

- In dedizierten Applikationen über Webservices
- Auf mobilen Geräten ohne Smartcard / USB Anschluss

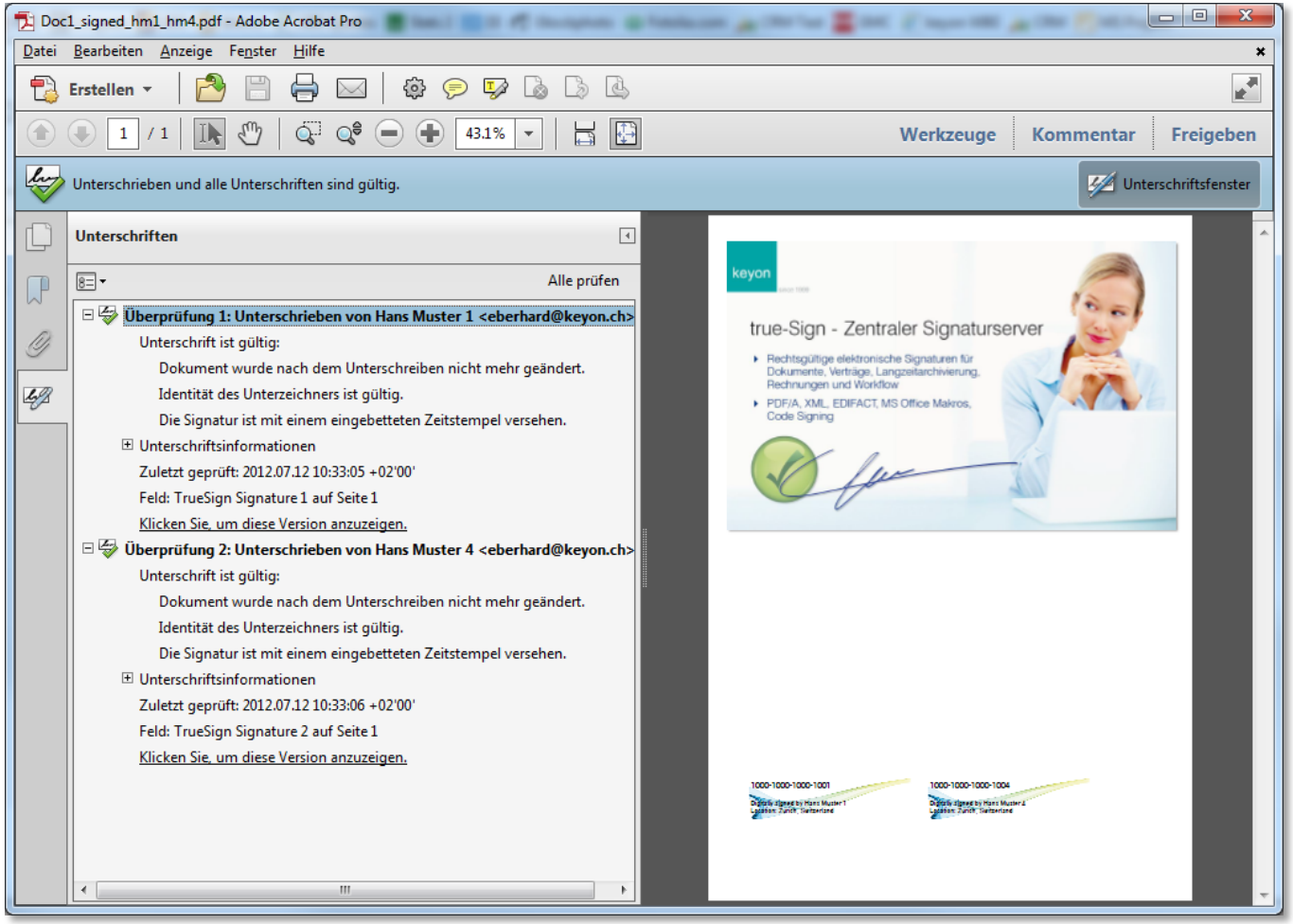
keyon

Signaturvorgang aus Sicht des Servers

- Die zu signierenden Daten verlassen den Workflow nicht.
- Nutzung bestehender Authentisierungsmerkmalen (Smartcard der Admin PKI, Smartcard der VRSG, OTP, SMS, SAML, etc.)
- Aktuelle Statusprüfung des Signaturzertifikats vor dem Signieren
- Einfache Einbindung von Zeitstempeln
- Konvertieren / Validieren von Dokumentenformaten (beispielsweise von PDF nach PDF/A oder von MS Word nach PDF/A)
- Kontrollierte Verwendung von Signaturschlüsseln innerhalb eines definierten Kontexts (Geltungsbereich nach ZertES, Art. 7 Abs. 2 Bst. b ZertES)
- Protokollieren der Signatur- und Prüfaktivitäten
- Validieren von signierten Dokumenten, erstellen eines definierten Prüfberichts

Look and feel / Eigenschaften

Einfaches Erstellen von Kollektivunterschriften



keyon

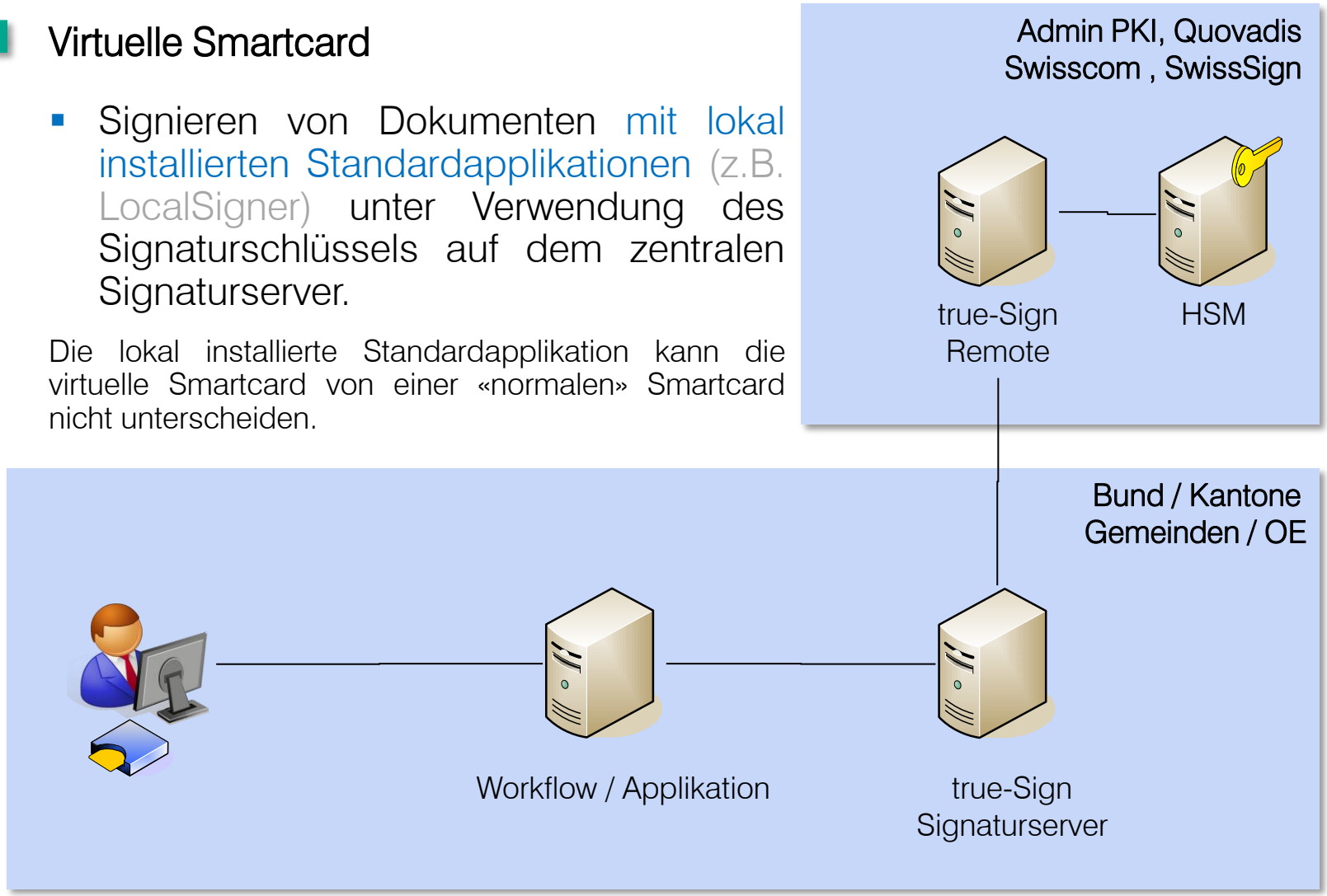
Alternative Einsatzgebiete eines zentralen Signaturserver

keyon

Virtuelle Smartcard

- Signieren von Dokumenten mit lokal installierten Standardapplikationen (z.B. LocalSigner) unter Verwendung des Signaturschlüssels auf dem zentralen Signaturserver.

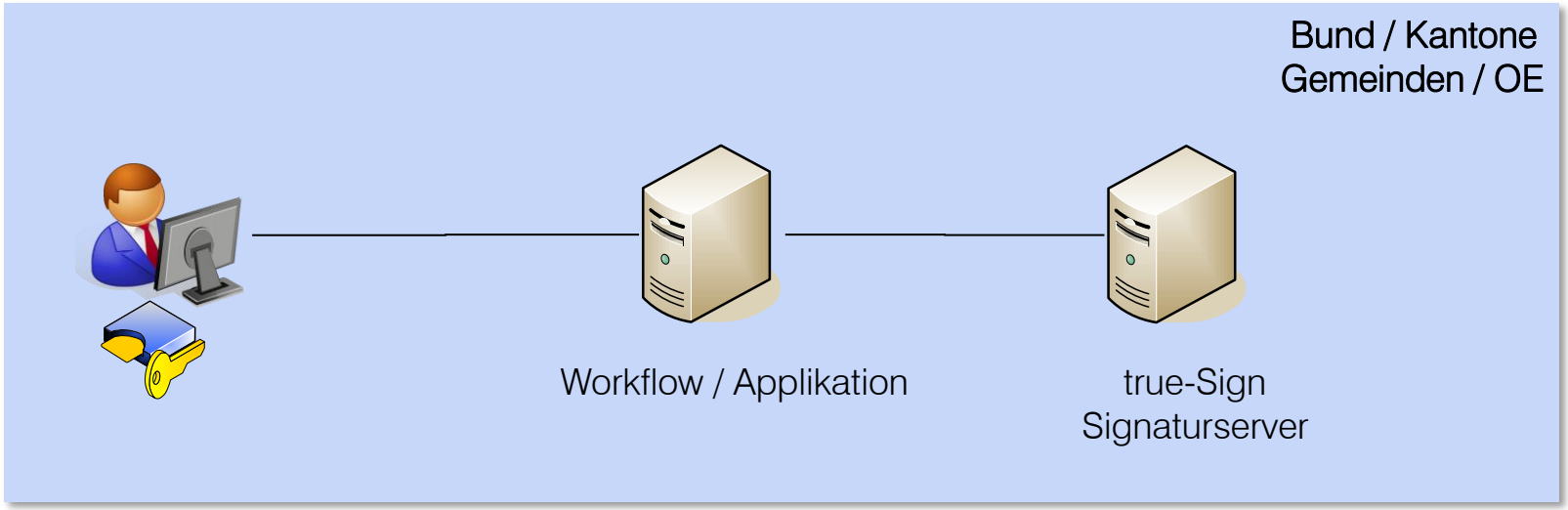
Die lokal installierte Standardapplikation kann die virtuelle Smartcard von einer «normalen» Smartcard nicht unterscheiden.



keyon

Server Signatur mit lokaler Smartcard

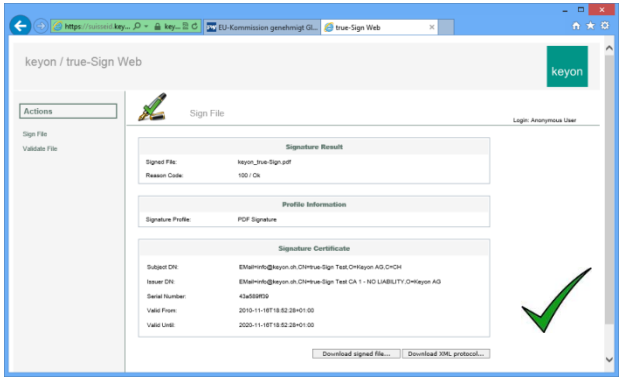
- Signieren von Dokumenten innerhalb eines Servergestützten Workflows unter Verwendung des Signaturschlüssels auf der lokalen Smartcard.

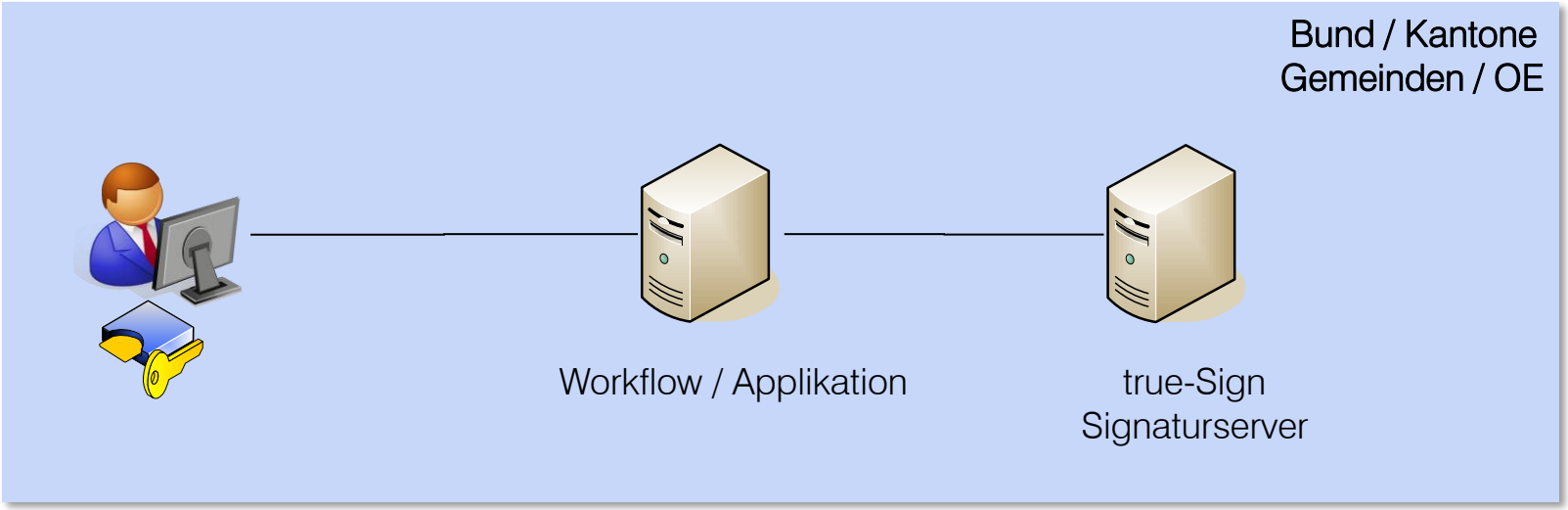


Alternative Einsatzgebiete

Validieren von Dokumenten

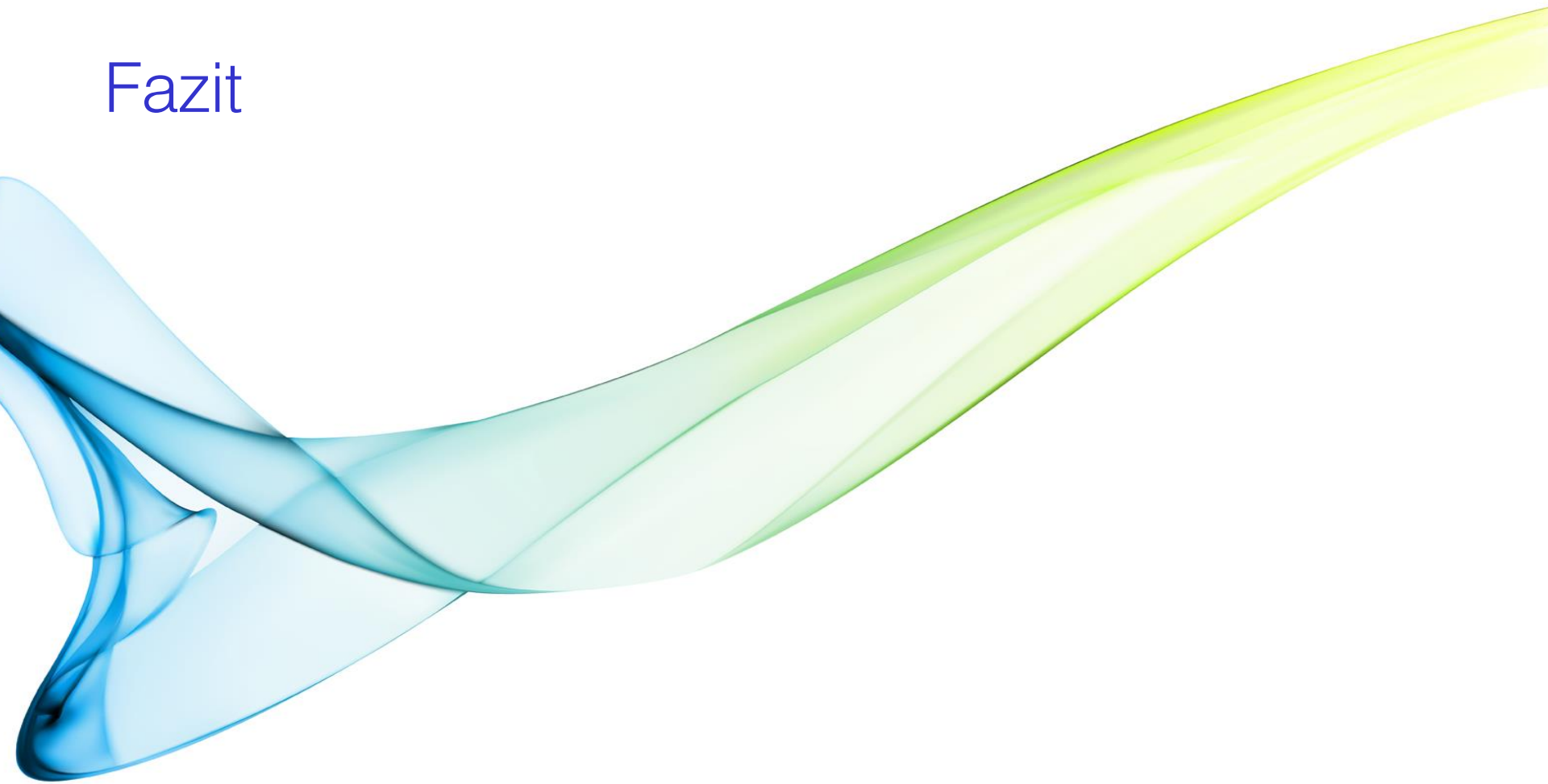
- Validieren von Dokumenten unter Einbezug von aktuellen Zertifikats-Statusinformationen und allenfalls weiteren, organisationsbezogenen Informationen der Unterzeichner.





keyon

Fazit



keyon

Fazit

- Zentrale Signaturserver gewinnen an Bedeutung
  - Gesetzgebung
  - Einfaches und kontrolliertes Erstellen von elektronischen Signaturen
- Prozesse und Technologie sind sicher, verfügbar und erprobt
- Hohe Benutzerakzeptanz

Vielen Dank für Ihre Aufmerksamkeit

keyon

Bei Fragen stehe ich Ihnen gerne zur Verfügung.