Massenamtssignaturen

2 Lösungsansätze

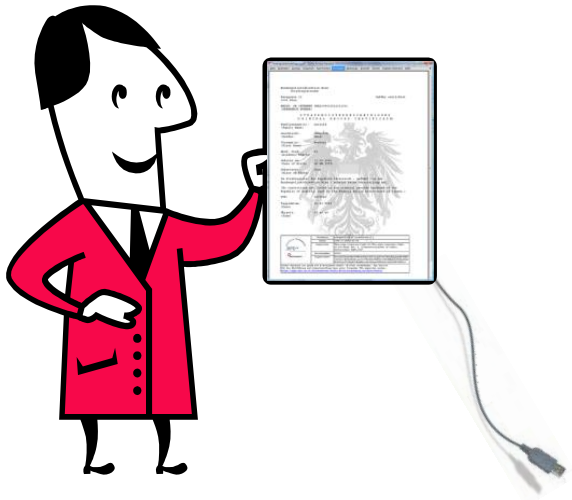
EGIZ E-Government Innovationszentrum

Thomas Rössler

Wien, 25. März

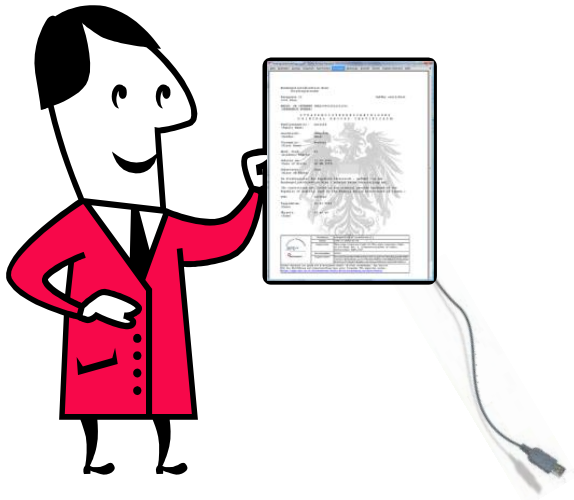
Inhalt

- Anforderungen
- Prinzipelle Lösungsansätze und Basismodule
  - PDF-AS Ansatz: MOA-AS
  - XML-DSig für Druckströme: MASS
- Zusammenfassung



Inhalt

- **Anforderungen**
- Prinzipelle Lösungsansätze und Basismodule
  - PDF-AS Ansatz: MOA-AS
  - XML-DSig für Druckströme: MASS
- Zusammenfassung



Anforderungen

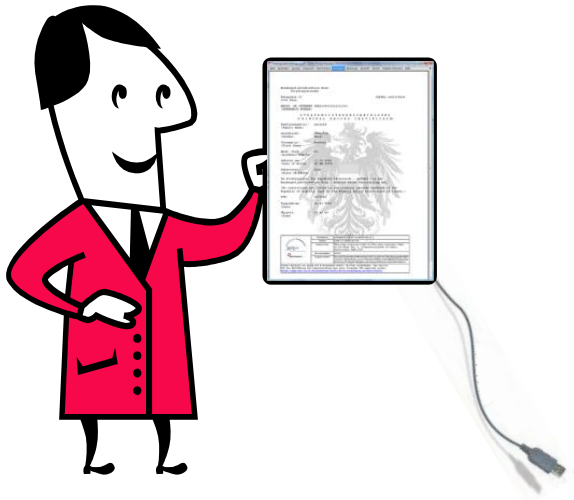
- Tools zur Integration in automatisierten Workflow-Systemen
- Tauglich für Massenverarbeitung
- Hohe Performance
- Integrierbar in Druckprozesse (auf Basis Druckstrom)

PDF-AS Core und MOA-AS für PDF-basierte Amtssignaturen

MASS für Massenamtssignaturen

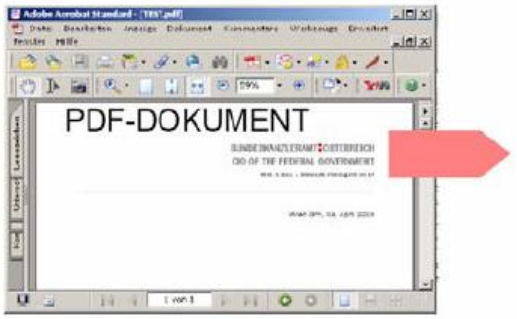
Inhalt

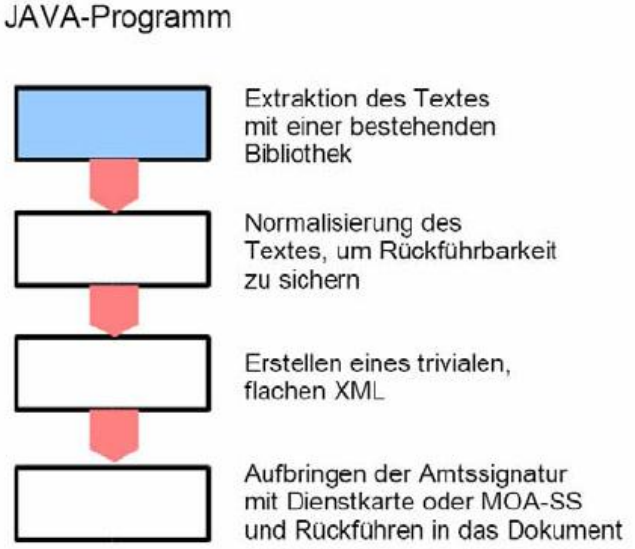
- Anforderungen
- **Prinzipelle Lösungsansätze und Basismodule**
  - **PDF-AS Ansatz: MOA-AS**
  - XML-DSig für Druckströme: MASS
- Zusammenfassung



PDF-AS Ansatz

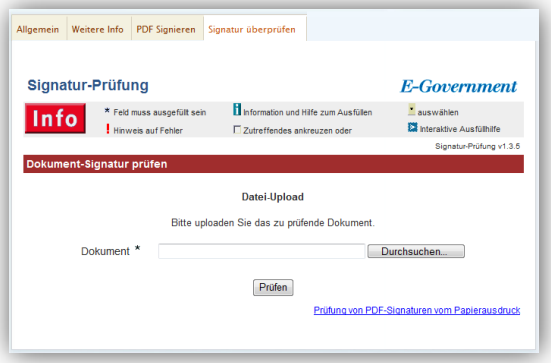
- PDF-AS basierte Amtssignatur:
  - nur für PDF-Dokumente
  - Signatur des binären Files oder nur des textuellen Inhalts
    - textuelle Signatur: Grundlage für Prüfung über Rekonstruktion





PDF-AS Ansatz

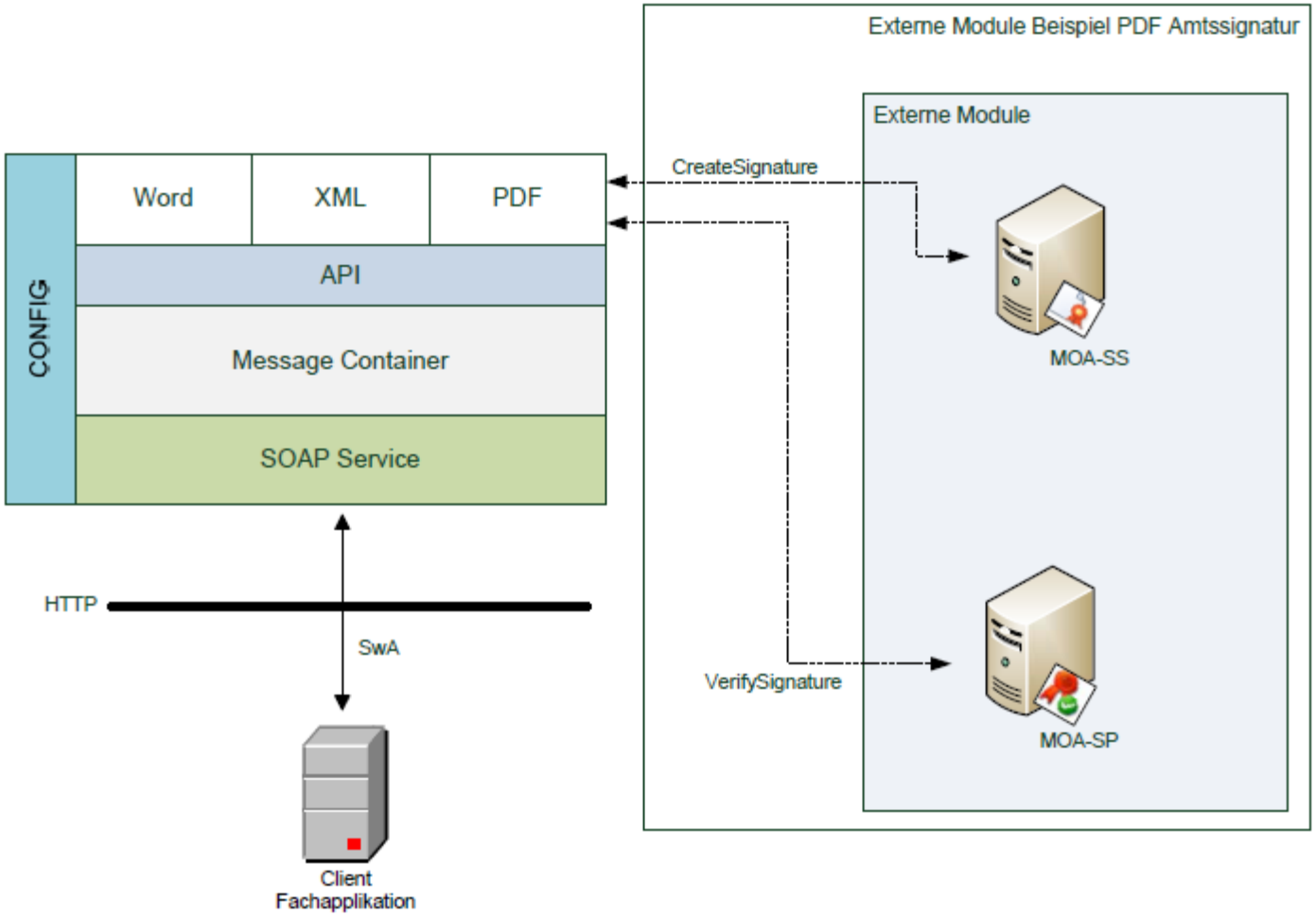
- Prüfung bei vorhandener Datei: trivial durch lokale Anwendung oder mittels einer Web-Applikation:



- Prüfung vom Ausdruck: Eingabe des textuellen Inhalts

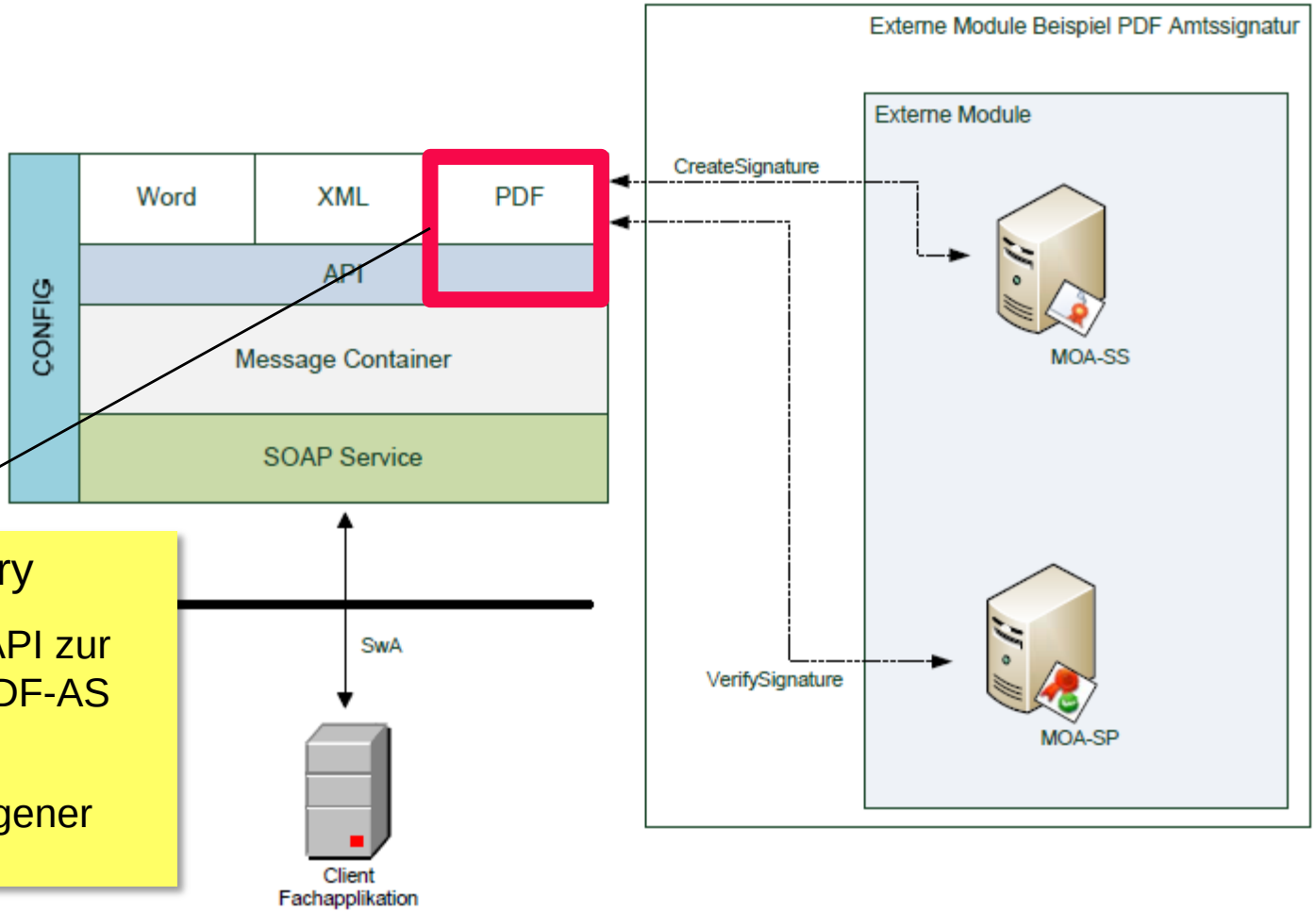
Modul: MOA-AS

- MOA-AS



Modul: MOA-AS

- MOA-AS



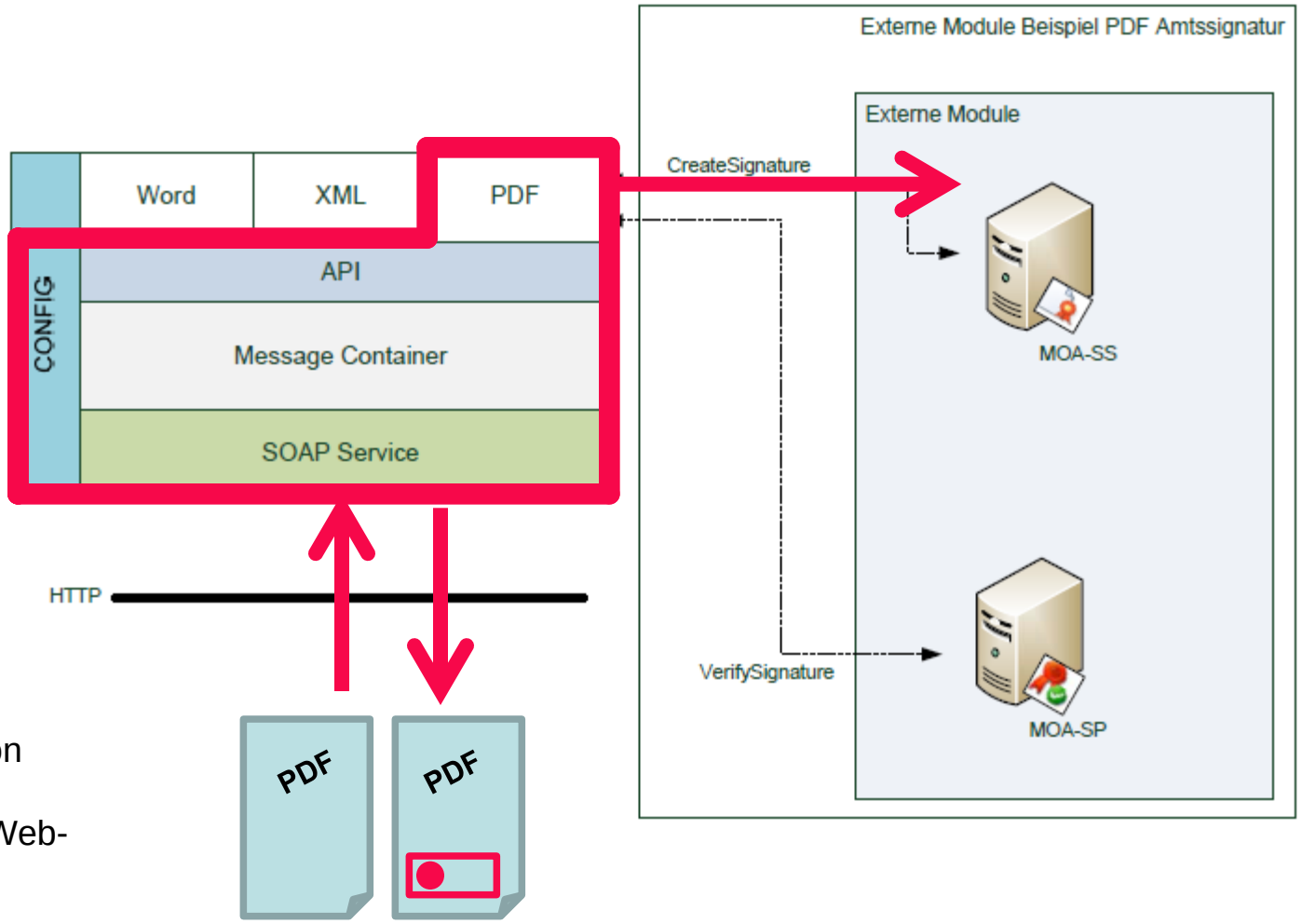
PDF-AS Core Library

Java-Modul mit API zur Erstellung von PDF-AS Signaturen.

Zur Erstellung eigener Anwendungen

Modul: MOA-AS

- MOA-AS



Analog zu MOA-SS dient MOA-AS zur Signatur von Einzeldokumenten (PDF-Dokumenten) über eine Web-Service Schnittstelle

MOA-AS

- PDF-AS Tools für den Desktop (z.B. dienstkartenbasiert)
  - PDF-Over (Desktop-Tool)
  - Word2PDFAS (Word Plugin)
  - OO2PDFAS (OpenOffice Plugin)
  - PDF-Signer (Adobe Acrobat Plugin)

bedingen eine lokale Bürgerkartenumgebung und Signaturkarte, zum Beispiel MOCCA-Lokal

http://www.buergerkarte.at/de/pdf-signieren/downloads.html

- MOA-AS:

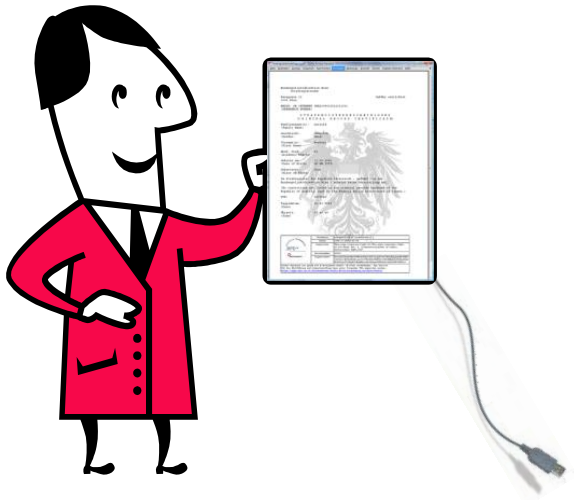
  http://demo.egiz.gv.at/plain/projekte/signatur_im_e_government/moa_amtssignatur_moa_as

- PDF-AS Kernbibliothek:

  http://egovlabs.gv.at/projects/pdf-as/

Inhalt

- Anforderungen
- **Prinzipelle Lösungsansätze und Basismodule**
  - PDF-AS Ansatz: MOA-AS
  - **XML-DSig für Druckströme: MASS**
- Zusammenfassung

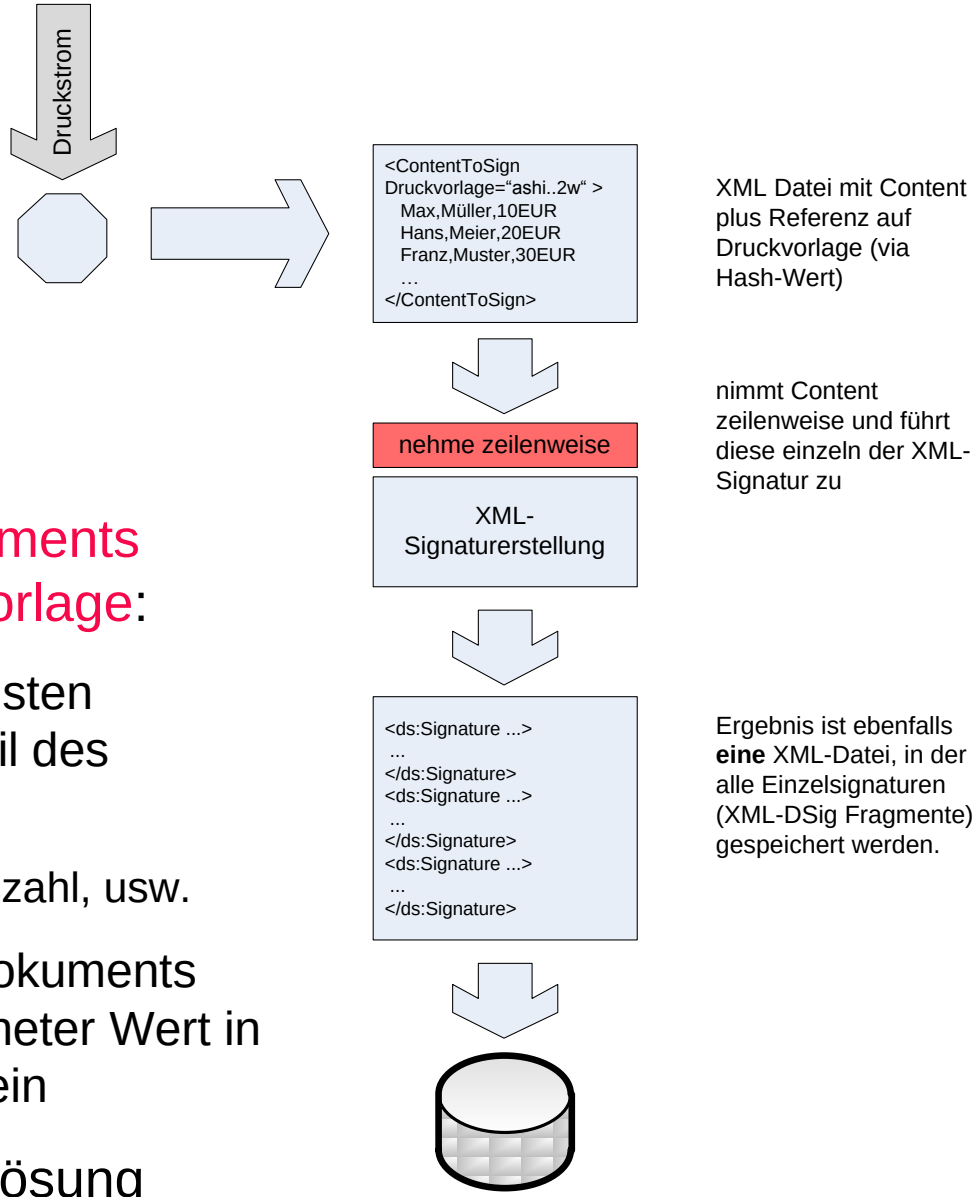


MASS – Anforderungen

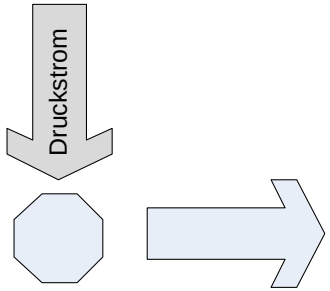
- Erstellung von Amtssignaturen
- Performance an erster Stelle
  - Große Anzahl an Signaturen in relativ kurzer Zeit
- Unterschiedliche Eingangsdaten
  - bspw. auf Basis von Druck-stromdaten einer Druckstraße
- Unterstützung unterschiedlicher Signaturformate und –typen
  - XML/CMS Signaturen, fortgeschrittene elektronische Signatur

Die MASS Idee

- Signaturerstellung über gesamtes Dokument ineffizient
- Signaturerstellung über variable Teile des Einzeldokuments plus Referenz auf die Druckvorlage:
  - Variable Teile machen in meisten Fällen nur einen geringen Teil des Gesamtdokuments aus
    - Namen, Adresse, Geschäftszahl, usw.
  - Unveränderliche Teile des Dokuments fließen als bereits vorberechneter Wert in die Signaturberechnung mit ein
- Garantiert eine performante Lösung

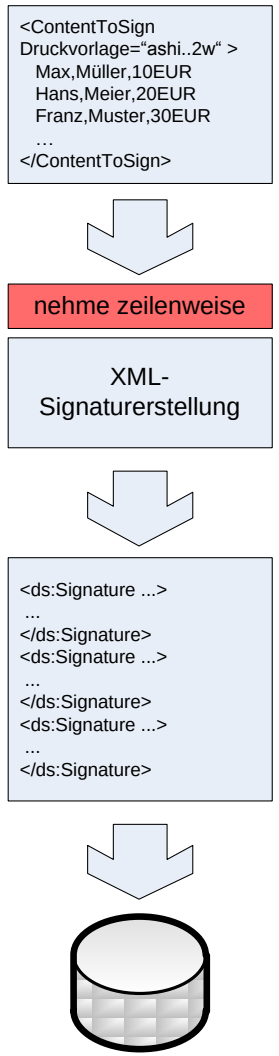


Die MASS Idee



- Prüfbarkeit:
  - Prüfung der Amtssignatur nur über den Weg der Verifizierung
  - die Signaturen werden nach Erstellung beim Signator (Behörde) archiviert
  - Im Prüfungsfall verschiedene Szenarien denkbar, jedoch sind diese Szenarien überwiegend manuell. Zum Beispiel:
    - die archivierte Signatur wird elektronisch verifiziert – damit ist Authentizität der variablen Daten sichergestellt; über die mit der Signatur verknüpfte Druckvorlage ist auch die Authentizität des restlichen Druckbilds prüfbar.

      → **Gesamtes Dokument verifiziert**



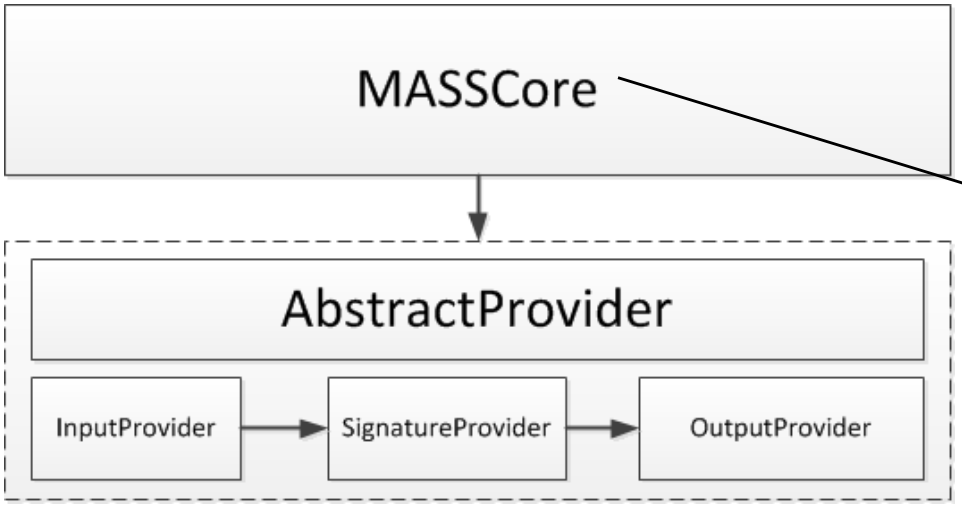
XML Datei mit Content plus Referenz auf Druckvorlage (via Hash-Wert)

nimmt Content zeilenweise und führt diese einzeln der XML-Signatur zu

Ergebnis ist ebenfalls **eine** XML-Datei, in der alle Einzelsignaturen (XML-DSig Fragmente) gespeichert werden.

Massen-Amtssignatur – Konzept

- Modulare Architektur für maximale Flexibilität
- Providerbasiertes Modell garantiert modulare Gestaltung aller am Signaturprozess beteiligten Komponenten
  - InputProvider: liefert Eingangsdaten für Signaturberechnung
  - SignatureProvider: erstellt Signatur
  - OutputProvider: schreibt/legt erstellte Signaturen ab



Prozessablauf von zentralem Modul **MASSCore** gesteuert

einlesen von Daten, Signaturerstellung, schreiben der Signaturen

Massen-Amtssignatur – Beispiel

- Generisches Framework im MASS-OpenSource-Projekt implementiert
  - auf Basis Java 6
- Musterimplementierung für Stadt Wien:
  - Eingangsdaten werden zeilenweise aus Textdatei gelesen
  - Signaturerstellung erzeugt XML enveloping Signaturen
  - Erstellte Signaturen werden in eine Datei geschrieben
    - Pro Signatur eine Datei
    - Dateiname basierend auf Geschäftszahl (enthalten in Eingangsdaten)
  - Erfahrungswerte (Wien): „*... Bedenken bezüglich der Laufzeit scheinen hinfällig …*“
    7000 Strafverfügungen in 27 Minuten
    bei Test auf Notebook

Produktives System performanter!

Massen-Amtssignatur – Woher?

- Zur Verfügung gestellt auf Open Source Plattform des Digitalen Österreichs:

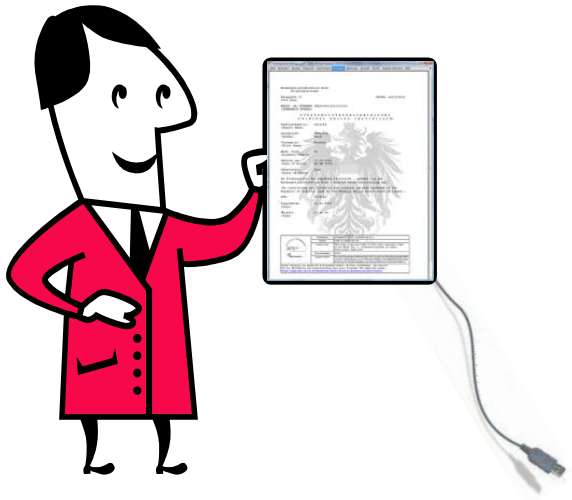
  http://egovlabs.gv.at/projects/mass/

- Aufgrund des gewählten Software-Konzepts kann diese Anwendung für beliebige andere Massenverfahren verwendet werden, zum Beispiel:
  - Serienbriefe aus Office Anwendungen

  → es müssen Input-/OutputProvider implementiert werden

Inhalt

- Anforderungen
- Prinzipelle Lösungsansätze und Basismodule
  - PDF-AS Ansatz: MOA-AS
  - XML-DSig für Druckströme: MASS
- Zusammenfassung



Zusammenfassung

- 2 Verfahren:
  - PDF-AS basiert: nur für PDF Dokumente
  - XML-DSig basiert: für beliebige Daten (auch Druckstrom)
- 2 Werkzeuge:
  - PDF-AS: als Java-Bibliothek für eigene Anwendungen oder in Form von MOA-AS als serverseitiges Tool zur Signatur von Einzeldokumenten via Web-Service Schnittstelle
  - MASS: ein flexibles Modul, dass zur Erstellung von Amtssignaturen auf Basis von – bspw. – Druckstromdaten geeignet ist (hoch performant)
- Konsequenz: der Prüfprozess ist vom Lösungsweg abhängig

Danke für Ihre Aufmerksamkeit

EGIZ E-Government Innovationszentrum

Dr. Thomas Rössler
thomas.roessler@egiz.gv.at

Wien, 25. März