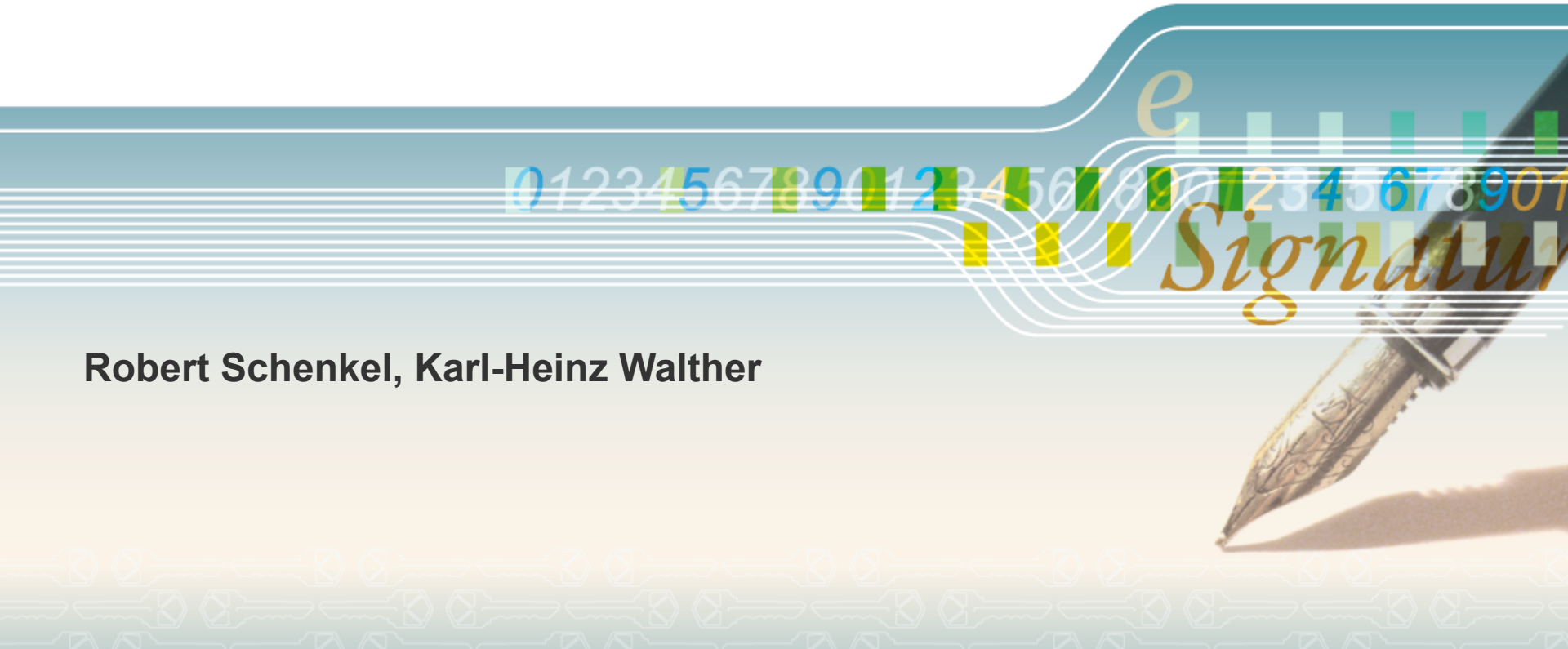
STAATSMINISTERIUM
DER JUSTIZ
UND FÜR EUROPA

Freistaat
SACHSEN

AK ITEG Workshop "Zugang für qualifiziert elektronisch signierte Dokumente"

06. März 2014



Robert Schenkel, Karl-Heinz Walther

Qualifizierte Elektronische Signatur - QES

Eigenschaften und Rahmenbedingungen

1. QES ist **gesetzlich** normiert
   - (Signaturgesetz, Signaturverordnung, BGB, EGovG, VwVfG…)
2. Technisch auf internationalen **Standards** basierend
3. **Bundesnetzagentur** sichert Aufbau und Überwachung einer sicheren und zuverlässigen Infrastruktur für qualifizierte elektronische Signaturen.
   - Anbieterakkreditierung (Trustcenter)
   - Produkt- und Herstellerinformationen
   - Algorithmenkatalog
   - Veröffentlichung Warnungen und Hinweise
4. **anerkannte** Prüf- und Bestätigungsstellen:
   - Bestätigung nach Signaturgesetz für geeignete Soft- und Hardwareprodukte (Lesegeräte, Signaturkarten – SSE, Signatursoftware – SAK)

Qualifizierte Elektronische Signatur - QES

Häufige Fragen

1. Wie funktioniert die elektronische Signatur?
   - Datei-Quersumme wird mittels eines persönlichen Schlüssels der signierenden Person verschlüsselt und Zertifikatsdaten angefügt
2. Wie erkennt man das Signaturniveau?
   - Anhand des Signaturzertifikates oder aus dem Prüfprotokoll
   - Kryptografisch unterscheiden sich fortgeschrittene und qualifizierte Signatur nicht
3. Wie verbreitet ist die qualifizierte elektronische Signatur?
   - Wenige Verfahren (z.B. E-Vergabe, elektr. Rechtsverkehr, EANV, … Rechnungen)
4. Was wird bei der Signaturprüfung geprüft?
   - Gültigkeit des Unterzeichnerzertifikates zum Signaturzeitpunkt -> Authentizität
   - Mathematische Prüfung (Hashwert) -> Integrität
   - Algorithmen (nach Algorithmenkatalog)

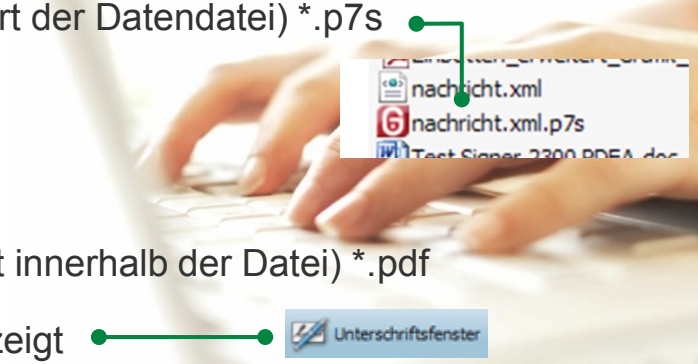
Qualifizierte Elektronische Signatur - QES

Häufige Fragen 2

5. Woran erkennt man ein signiertes Dokument?

- 3 grundsätzliche Formate Signatur: beigefügt, eingefügt, umhüllend

- Beigefügt (detached):
  - Separate Signaturdatei (signierter Hashwert der Datendatei) *.p7s
  - Typ der Datendatei kann beliebig sein



- Eingefügt (enveloped/ inline):
  - Verbreitet: PDF-Inline (Signierter Hashwert innerhalb der Datei) *.pdf
  - Hinweis auf Signatur wird im Viewer angezeigt

- Umhüllend (enveloped / container):
  - Signatur umfasste einen Datencontainer (Signierter Hashwert innerhalb des Containers) -> OSCI, DeMail

Qualifizierte Elektronische Signatur - qeS

Auswahl weiterführender Informationen zur qeS:

Bundesnetzagentur:

http://www.bundesnetzagentur.de/cln_1931/DE/Service-Funktionen/QualifizierteelektronischeSignatur/qualifizierteelektronischesignatur-node.html

BSI:

https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/BestaetigungnachdemSignaturgesetz/ListebestaetigterProdukte/listebestaetigterprodukte_node.html

Herstellerseite der Software für E-Government Basiskomponente ESV:

http://www.governikus.com/de/governikus_signer/6002745/

Beispiel für alternative Dienstleister:

https://www.signaturportal.de

Zugang für qeS

1. **Die Annahme signierter Dokumente**
   - i.d.R. dokumentenbasierte Signatur
   - Keine Anforderungen an den Zugangskanal!
   - Keine Anforderungen zur Nachrichtensignatur!
2. **Die (Eingangs-)Prüfung signierter Dokumente**
   - Technische Prüfung (Prüfdienst)
   - Inhaltliche Prüfung (Unterzeichner = Antragsteller?)
3. **Weiterverarbeitung elektronisch signierter Dokumente gleichberechtigt zu Papierdokumenten**
   - Einbindung in Verwaltungsprozesse

Zugang für qeS

Spannungsfeld

Technik

- Zugangskanäle
- Hard-/ Softwareausstattung
- Szenarien (allgemein vs. verfahrensspezifisch)
- Aufbewahrung der signierten Dokumente
- Netzanbindung (Prüfung=Online Service)

Organisation

- qeS „gleichberechtigt“ zu Papier
- „Veraktung“ elektronischer Dokumente
- Umgang mit nicht erfolgreichen Signaturprüfungen (ungültig, unbestimmt)
- Email Signatur, Veröffentlichung des Zuganges (Webseiten etc.)
- Virtuelle *Poststelle*
- Vergleich Dokument-Inhalt und Unterzeichner (-> Verfahren)

Zugang für qeS

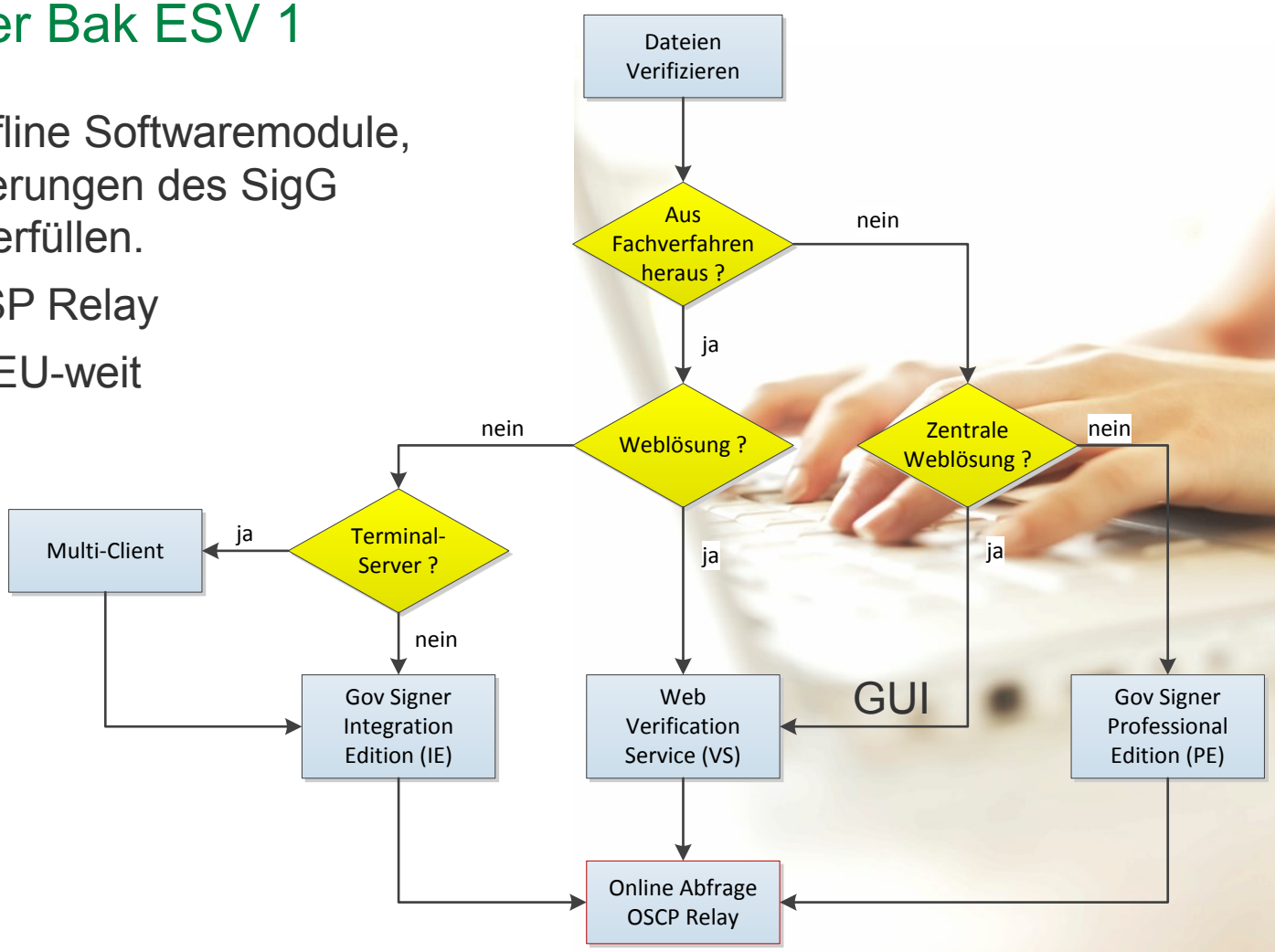
Zugangskanaloptionen

Kanalspezifik	E-Mail (SMTP)	Filetransfer (FTP, WS, HTTP,…DVD)	OSCI (EGVP,…)	SMGW (SMTP)	Formular
Eingangsprüfung automatisch?	✗	✗	✓	✓	✓
Nachprüfung direkt möglich?	✗	✗	✓	✗	✓
Einreicher	∞	N .. ∞	Ca. 40.000	∞	∞

Technische Umsetzungsmöglichkeiten

Verifikation über Bak ESV 1

- Online- und offline Softwaremodule, die die Anforderungen des SigG und des SigV erfüllen.
- Zentrales OCSP Relay
- Prüfung auch EU-weit



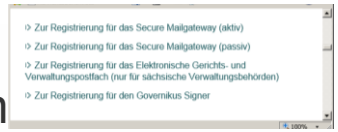
Technische Umsetzungsmöglichkeiten

Verifikation über Bak ESV 2

- Gemeinsame Eigenschaften der Verifikationsmodule:
  - ✓ math. Prüfung (Integritätsprüfung)
  - ✓ Online-Prüfung (Validierung)
  - ✓ Format PKCS#7/CAdES
  - ✓ Format PDF Inline /PAdES
  - ✓ Format XML / XADES
  - ✓ Format OSCI
  - ✓ Format De-Mail
  - ✓ Attributzertifikat
  - ✓ Zertifikate
  - ✓ bos-Prüfprotokoll HTML
  - ✓ bos-Prüfprotokoll PDF

Mandatierung

Leistungen Bak ESV



- Links zur **Registrierung**: http://www.sid.sachsen.de/signatur.htm
- Links zum **Download**: http://circa.sachsen.de/Public/irc/egov/Home/main

- Zugang CIRCA Server (Projektbereich BakESV):
  - Liste mit bis zu 3 Personen pro Ressort an BakESV
  - Mitteilung der Personen **bis 20.03.2014** an Projektleitung der BakESV

- Leistungen der Bak ESV, Teilkomponenten Signatur und OSCI:
  - Signatursoftware für Benutzer und Verfahrensintegration (Signer PR & IE)
  - Betrieb zentraler Online-Prüfdienst (Governikus OCSP/CRL Relay)
  - Betrieb Prüfdienst für signierte Daten (Governikus WebVerifier)
  - Bereitstellung EGVP (EGVP Backend Sachsen, EGVP Enterprise)
  - Support, Pflege und Weiterentwicklung für die angebotenen Funktionen

Governikus Signer Professional (PE)

Integritätsprüfung lokal; Validierung über Dienste der E-Government Plattform

- Desktopsoftware: Lokale Installation – für Verifikation keine Signaturhardware erforderlich
- Eigene JRE – keine Java-Pflege erforderlich
- Installationsoptionen: mit oder ohne online-Updatefunktion
- Einsatz: z.B. im Rahmen EU-DLR in ca. 360 Behörden
- Verteilung als MSI Paket
- Funktionen: Signieren, Verifizieren
  Verschlüsseln, Entschlüsseln
- Kompatibilität: Windows, Linux,
  Windows-Terminalserver

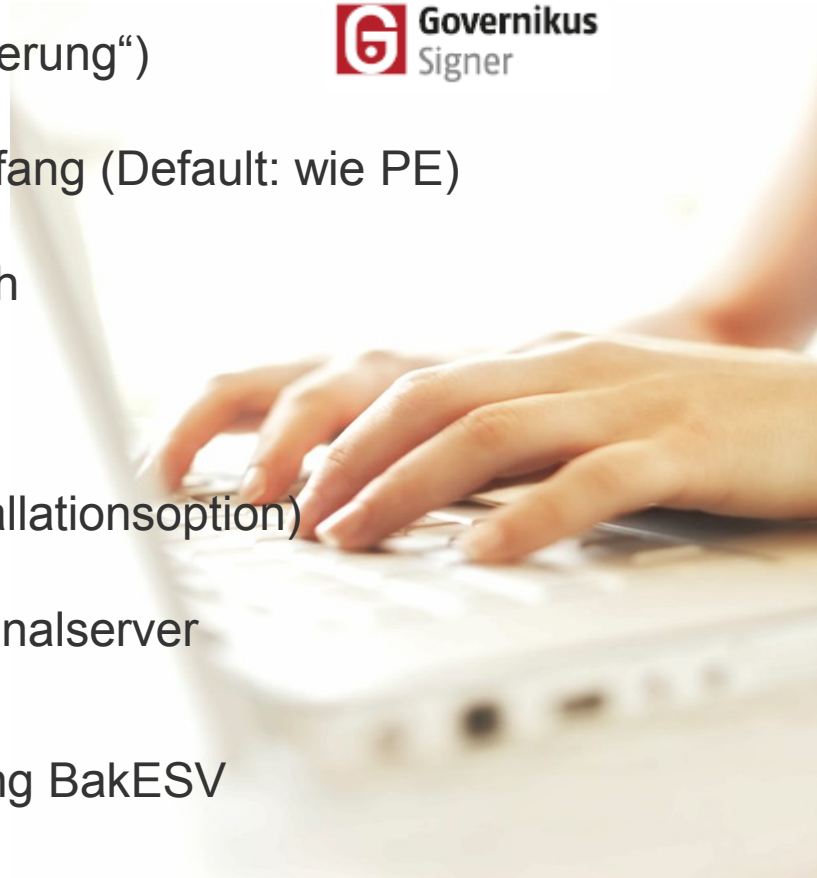
- Information/Registrierung: http://www.egovernment.sachsen.de/818.htm

Governikus Signer Integration Edition (IE)

Integritätsprüfung lokal; Validierung über Dienste der E-Government Plattform

Governikus Signer

- Einbindung in Fachverfahren („Click-Minimierung“)
- Zentrale Vorgaben zu lokalen Funktionsumfang (Default: wie PE)
- Eigene JRE – keine Java-Pflege erforderlich
- Funktionsumfang wie (PE)
- Einsatz: eingebunden z.B. in VIS.Sax (Installationsoption)
- Kompatibilität: Windows, openSUSE, Terminalserver



- Mehr Information über Kontakt zur Betreuung BakESV
- Download:
  https://circa.sachsen.de/Members/irc/egov/pb_bak_esv/library?l=/auslieferung_governikus&vm=detailed&sb=Title

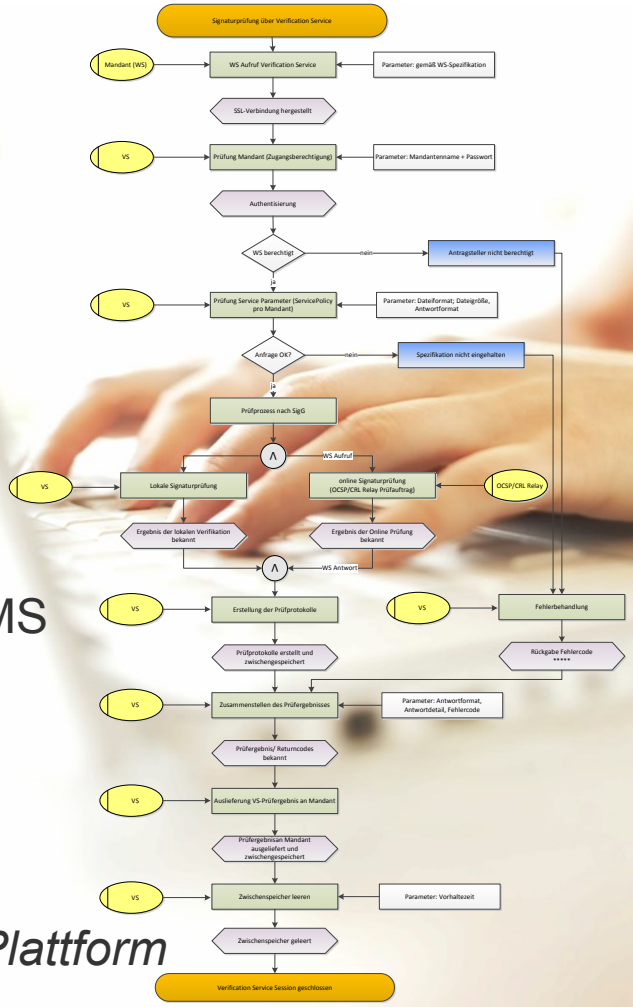
Governikus Web Verification Service (VS-Webservice)

Integritätsprüfung in - und Validierung - über Dienste der E-Government Plattform

- Mandantenfähiger Prüfdienst mit Webservice-schnittstelle (WS)
- Über WS wird die zu prüfende Datei übergeben
- Rückgabe: Prüfergebnis + Protokoll
- Anbindung: SSL im Intranet
- Mandant: Absicherung über Passwort (-hash)

- Einsatzgebiet: Anbindung von Fachverfahren, DMS
- Beispiel: SLT (EDAS), BakESV (SMGW)
- Parallelbetrieb Test- und Produktivsystem

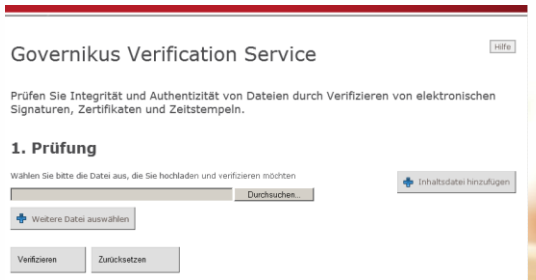
Voraussetzung: SSL Verbindung zu *E-Government Plattform*



Governikus Web Verification Service (VS-GUI)

Integritätsprüfung in - und Validierung über - Dienste der E-Government Plattform

- Grundsätzliche Funktion (VS-GUI) wie über WS-Schnittstelle
- die zu prüfende Datei(-en) werden über GUI übergeben
- Rückgabe: Protokoll
- Anbindung: SSL im Intranet
- Einsatzgebiet: gelegentlicher, manueller Prüfbedarf (als Fallback Szenario geeignet)
- Beispiel: BakESV
- Parallelbetrieb Test- und Produktivsystem



- Testbeispiel: https://esigtest.egov.sachsen.de/VerificationService/Welcome.action

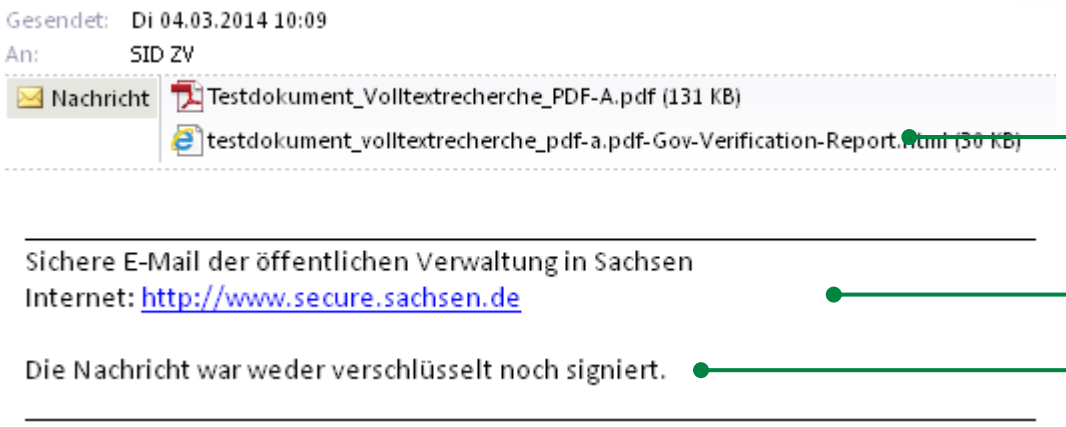
Verification Service via Secure Mail Gateway (SMGW)

Integritätsprüfung in - und Validierung über - Dienste der E-Government Plattform

- Anbindung an das SMGW als „aktiver Nutzer“
  http://www.egovernment.sachsen.de/819.htm (Registrierung)

- Zugangsvoraussetzungen (Auswahl):
  - IPSEC Anbindung oder Exchange ab Version 2007 erforderlich
  - Konfiguration als berechtigter Empfänger (z.B. vps@sid.sachsen.de)

- Eingehende E-Mail wird ergänzt durch (Prüfprotokoll + Footer)



Optional:
Email Signatur und Verschlüsselung ein- /ausgehend

Elektronisches Gerichts- und Verwaltungspostfach (EGVP)

Integritätsprüfung lokal; Validierung über Dienste der E-Government Plattform

- Automatische Signaturprüfung mit Nachprüfmöglichkeit
- Rechtssichere OSCI Kommunikation
- Interne Weiterleitung per E-Mail möglich
- Fachverfahrensanbindung über Filesystem oder implementierte Schnittstelle (z.B. DMS Systeme)
- Kein Mehrbenutzerzugriff auf ein geöffnetes Postfach
- Rollentrennung (Verwaltung <> Bürger/Unternehmen)
- Support für Verwaltung über BakESV; für Bürger über www.egvp.de

Anwendungen in Sachsen

Elektronischer Rechtsverkehr

EU- Dienstleistungsrichtlinie

http://www.egvp.de/behoerden/Behoerden_Sachsen_1.pdf

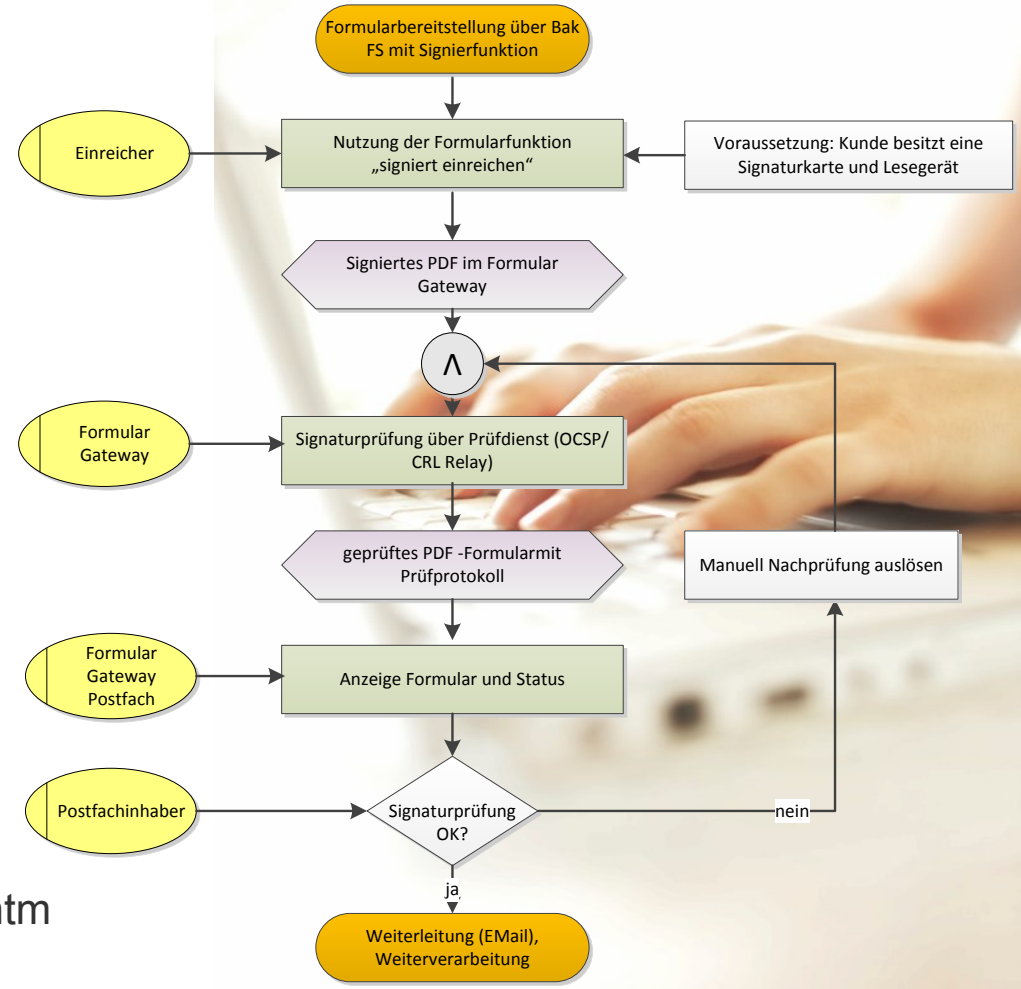
Weiterführende Informationsquellen:

- http://www.egvp.de (**nicht** für **Softwaredownload** Behörde, ausschließlich für die Rolle Bürger!)
- http://www.egovernment.sachsen.de/819.htm (**Registrierung und Download für Behörden**)
- http://www.governikus.com/de/egvp/6002734/ (Herstellerseite EGVP)

Verification Service via Formulargateway (Bak FS)

Integritätsprüfung in - und Validierung über - Dienste der E-Government Plattform

- Formular mit qeS
- Zugang für formularbasierte Verfahren



- Kontakt: egov-fs@sid.sachsen.de
- www.sid.sachsen.de/formularservice.htm

Zusammenfassung

Signiertes Dokument empfangen – Was nun?

1. Kryptografische Sicherung (Schutz vor Schwächung von Algorithmen):
   - BSI Richtlinie zur beweiwerterhaltenden Speicherung (BSI TR- 03125)
     https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html
   - Manuelle Übersignatur (erfordert Signaturarbeitsplatz)
2. Mindestanforderungen für elektronisch signierte Rechnungen (Beispiel):
   - 10 Jahre Aufbewahrungsfrist mit Gewährleistung von:
   - Echtheit der Herkunft, die Unversehrtheit des Inhalts, Lesbarkeit der Rechnung

- Bei Eingang nach SigG prüfen!
- Prüfprotokoll zusammen mit den signierten Daten geschützt ablegen
- Falls Ausdruck: immer zusammen mit Prüfprotokoll
- Technische Prüfung ersetzt nicht Inhaltsprüfung!
- Formatkonvertierung = Verlust der Signatur / Rechtswirkung

Zusammenfassung

Stichpunkte für die Umsetzung

- Automatische Eingangsprüfung ?
- manuelle Nachprüfmöglichkeit ?
- Zentrale (Funktions-)Adresse pro Behörde „Poststelle“ ?
- manuelle Weiterverteilung durch „Poststelle“?
- Anbindung an / Erweiterung von Fachverfahren?
  Beispiel: Formulare, VIS.SAX
- Formatstandards festlegen,
  Beispiel: http://www.egvp.de/bearbeitung/sachsen/formatstandards/index.php

Kontaktadressen

Basiskomponente Elektronische Signatur und Verschlüsselung

Projektleitung BaK ESV

SÄCHSISCHES STAATSMINISTERIUM
DER JUSTIZ UND FÜR EUROPA

Referat V3 I Projektsteuerung

Hospitalstraße 7 I 01097 Dresden

Tel.: +49 (0)351 564 1961

Karl-Heinz.Walther@smj.justiz.sachsen.de I
www.justiz.sachsen.de

Betreuung Bak ESV

STAATSBETRIEB SÄCHSISCHE
INFORMATIK DIENSTE

Fachbereich 3.1 | E-Government- und
Querschnittverfahren

Riesaer Str. 7 | 01129 Dresden

Tel.: +49 351 20545 280

esv@sid.sachsen.de | www.sid.sachsen.de

Vielen Dank für Ihr Interesse…