STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

Fachtage Sächsisches E-Government Gesetz

Qualifizierte Elektronische Signatur

Umsetzungsoptionen über Basiskomponente ESV

16. Februar 2016 | Robert Schenkel

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

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, De-Mail

Zugang für QES

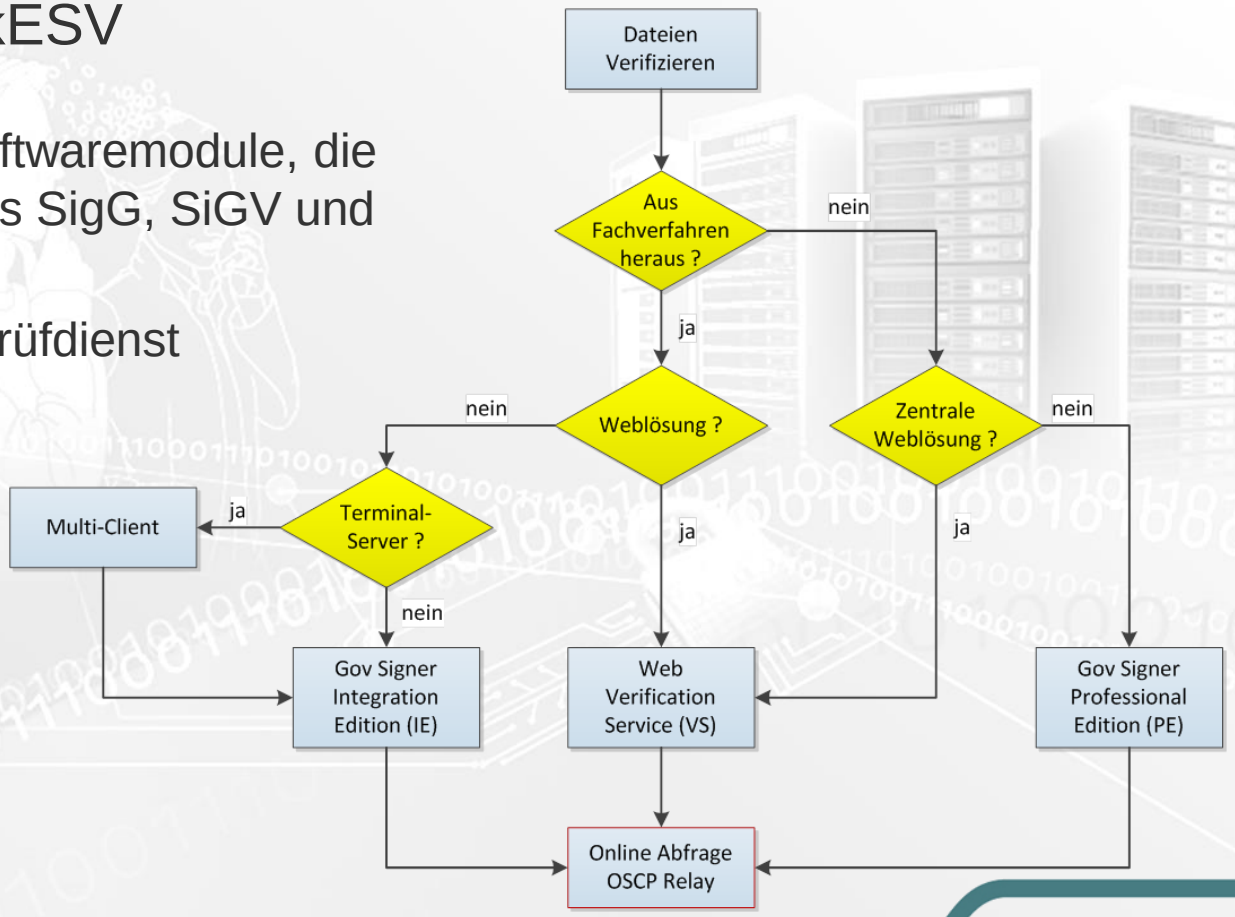
Zugangskanal

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

Technische Umsetzungsmöglichkeiten QES

Verifikation über BakESV

- Online- und offline Softwaremodule, die die Anforderungen des SigG, SiGV und eIDAS-VO erfüllen.
- Zentraler Zertifikats Prüfdienst (OCSP/CRL Relay)
- Prüfung EU-weit



Technische Umsetzungsmöglichkeiten QES

Verifikation über BakESV

- 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

Technische Umsetzungsmöglichkeiten QES

Verifikation über BakESV

- 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

Technische Umsetzungsmöglichkeiten QES

Leistungen Bak ESV (Signaturerstellung & -prüfung

- Signatursoftware für Benutzer und Verfahrensintegration
  - Signer Professional Edition, Signer Integration Edition, Websigner
- Betrieb zentraler Zertifikats-Prüfdienst
  - Governikus OCSP/CRL Relay
- Betrieb Prüfdienst für signierte Daten
  - Governikus Web Verificaton Service (Webservice & GUI)
- Bereitstellung EGVP
  - EGVP Backend Sachsen, EGVP Enterprise
- Indirekte Nutzung über Bak Formularservice

Governikus Signer Professional (PE)

Governikus Signer

Integritätsprüfung lokal; Validierung über 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

Registrierung: http://www.sid.sachsen.de/signatur.htm

Governikus Signer Integration (IE)

Governikus Signer

Integritätsprüfung lokal; Validierung über E-Government Plattform

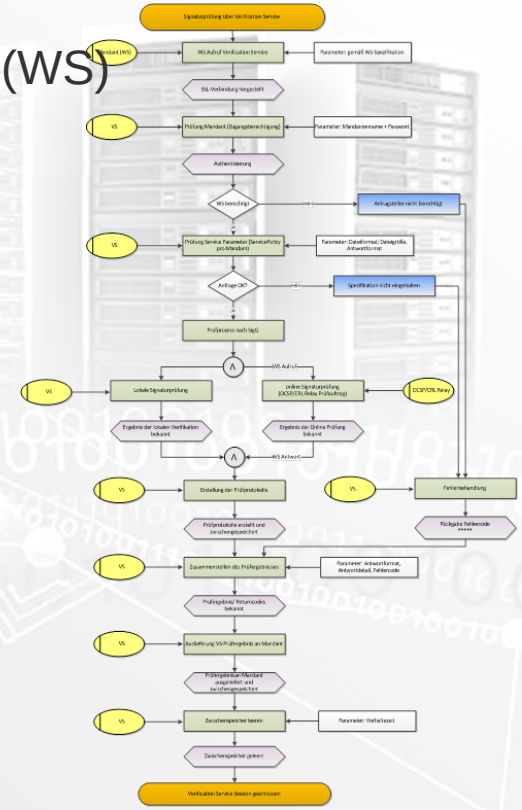
- Einbindung in Fachverfahren („Click-Minimierung“)
- Zentrale Vorgaben zu lokalen Funktionsumfang (Default: wie PE)
- Eigene JRE – keine Java-Pflege erforderlich
- Funktionsumfang wie (PE)
- Einsatz: eingebunden z.B. in VIS.Sax (Installationsoption)
- Kompatibilität: Windows, openSUSE, Terminalserver
- Mehr Information über esv@sid.sachsen.de
- Download für registrierte Nutzer:
  https://circa.sachsen.de/Members/irc/egov/pb_bak_esv/library?l=/auslieferung_governikus&vm=detailed&sb=Title

Governikus Web Verification Service (WS)

Governikus Signer

Integritätsprüfung in - und Validierung über - 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)



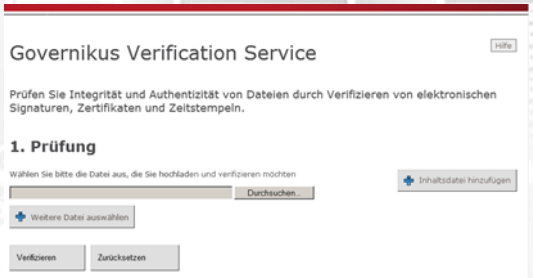
- Einsatzgebiet: Anbindung von Fachverfahren, DMS
- Beispiel: SLT (EDAS), BakESV (SMGW)
- Parallelbetrieb Test- und Produktivsystem

- Voraussetzung: SSL Verbindung zu E-Government Plattform

Governikus Web Verification Service (GUI)

Integritätsprüfung in - und Validierung über - 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



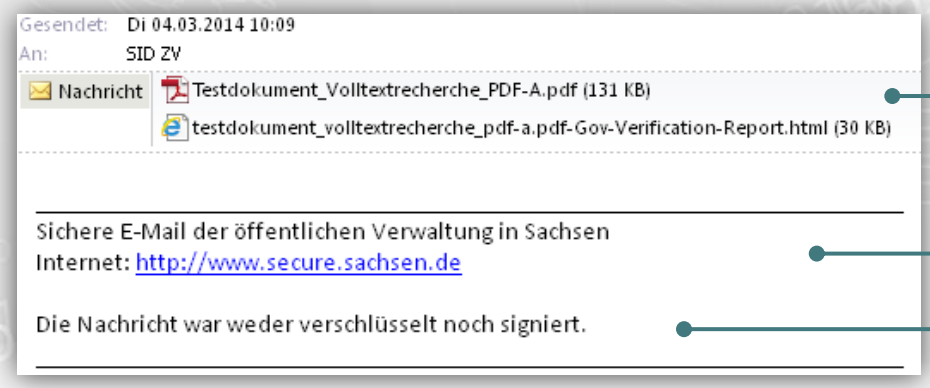
- Einsatzgebiet: gelegentlicher, manueller Prüfbedarf (als Fallback Szenario geeignet)
- Beispiel: BakESV
- Parallelbetrieb Test- und Produktivsystem

- Pro Mandant (Organisation) ein Passwort

Verification Service via Secure Mail Gateway (SMGW)

Integritätsprüfung in - und Validierung über - E-Government Plattform

- Anbindung an das SMGW als „aktiver Nutzer“
  http://www.sid.sachsen.de/signatur.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

Anwendungen in Sachsen

Elektronischer Rechtsverkehr

EU- Dienstleistungsrichtlinie

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

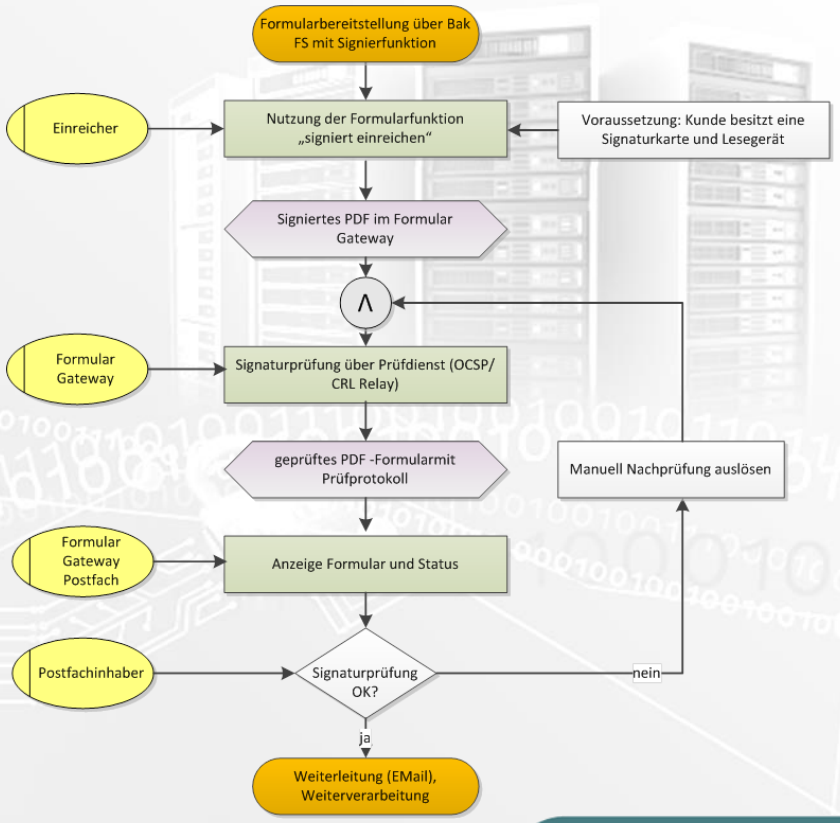
Weiterführende Informationsquellen:

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



Weiterführende Informationsquellen:

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

Zusammenfassung I

- 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)
- 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 II

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

Erfahren Sie mehr…

Sie finden uns unter:
www.sid.sachsen.de

Fachbereich 3.1 | E-Government- und Querschnittverfahren

Riesaer Straße 7

01129 Dresden

Telefon 0351 20545 280

E-Mail esv@sid.sachsen.de