STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

Fachtage Sächsisches E-Government Gesetz

Teil III - Fragen zur organisatorischen und technischen Umsetzung

Elektronische Kommunikation - E-Government Basiskomponente elektronische Signatur und Verschlüsselung

24.02.2016 | Robert Schenkel

Elektronische Kommunikation

- Verschlüsselte Kommunikation
  - E-Mail (SMGW)
  - De-Mail
  - OSCI (EGVP)
- Schriftformersetzende elektronische Verfahren
  - qualifizierte elektronische Signatur
  - De-Mail
  - Beweiswerterhaltung
  - neuer Personalausweis

Basiskomponente Elektronische Signatur und Verschlüsselung

STAATSBETRIEB SÄCHSISCHE INFORMATIK DIENSTE
Fachbereich 3.1 | E-Government- und Querschnittverfahren
Riesaer Str. 7 | 01129 Dresden

Tel.: +49 351 20545 280
Fax: +49 351 451 3264 9923
E-Mail: esv@sid.sachsen.de

Elektronische Kommunikation

- Sichere elektronische Kommunikation im Verwaltungsverfahren
- Dienste und Unterstützungsleistungen durch die Bak ESV

Verschlüsselte Kommunikation

- Anforderung nach SächsEGovG § 2Abs.1:
  - ..elektronische Kommunikation ermöglichen..
  - …Verschlüsselungsverfahren .. grundsätzlich anzuwenden

- Abgeleitete technische Anforderung für elektr. Nachrichten:
  - Sicherer Nachrichtentransport (**Transportverschlüsselung**) für ein- und ausgehende elektronische Nachrichten
  - In der Regel, d.h. wenn keine anderslautenden fachspezifischen Regelungen anzuwenden sind (Fachverfahren)

- Fachbezogene Anforderungen (durch zuständigen DSB / ITSB)
  - z.B. Inhaltsverschlüsselung für personenbeziehbare Daten

Elektronische Kommunikation: E-Mail

PKCS7 TLS

S/MIME Gateway

E-Mail

SMTP CA

PGP E2E

X509 SMGW

Trust

Verschlüsselte Kommunikation: E-Mail I

Über **Transportverschlüsselung** hinausgehend, weltweit standardisiert:

- E-Mail Signatur
  - Integritätssicherung, d.h. ist die Nachricht unverändert
  - Authentizität, d.h. wer ist der Urheber (Stichwort Class *Zertifikat)
  - Absender benötigt eigenes Zertifikat (Schlüssel)
- E-Mail Inhalts-Verschlüsselung
  - Vertraulichkeit, d.h. kein Dritter kann Inhalt zur Kenntnis nehmen
  - Absender benötigt öffentlichen Schlüssel des Empfängers
  - Absender benötigt i.d.R. eigenes Zertifikat (Schlüssel)
- Kombination Signatur und Verschlüsselung möglich und üblich

Verschlüsselte Kommunikation: E-Mail III

- **Handlungsoption 1: ohne Inhaltsverschlüsselung / -signatur**
  - „Minimalvariante“
  - Transportverschlüsselung aktivieren (Exchange ab 2007)
    - In der eigenen Infrastruktur
    - Durch den Provider bestätigen lassen, welche Maßnahmen in Bezug auf die Vertraulichkeit umgesetzt sind (vgl. Kapitel 4: Handlungsempfehlungen für Internet-Service-Provider, BSI und BSI TR-03108 Sicherer E-Mail-Transport)
    - *„…Die Übertragung der E-Mails zwischen den Provider-MTAs sollte verschlüsselt erfolgen. Dabei sollte insbesondere auch das Verfahren der Forward Secrecy genutzt werden…“*
  - Zuverlässig lässt sich die P2P-Transportverschlüsselung nur im Wirkungsbereich des KDN/SVN umsetzen.

Verschlüsselte Kommunikation: E-Mail IV

- **Handlungsoption 2: mit Inhaltsverschlüsselung / -signatur**:
  - *E-Mail muss über KDNII / SVN geroutet (transportiert) werden*
  - Sächsischen Verwaltungsnetzes (SVN /KDN II)
    - Transportverschlüsselung aktivieren (Exchange ab 2007)
  - Secure Mail Gateway (SMGW) der BakESV
    - Abschaltung / Ablösung ggf. existierender „passiver Nutzer SMGW“ (SMGW Messenger)
    - Inhaltsverschlüsselung aktivieren („aktiver Nutzer SMGW“) -> (Handreichung „Mandatierung Secure Mail Gateway)
  - SMGW Messenger Postfächer („passive Nutzer“) sind für die Zugangseröffnung „verschlüsselte Email“ für Verwaltungen in der Regel nicht geeignet

Verschlüsselte Kommunikation: E-Mail V

- **Handlungsoption 3: mit Inhaltsverschlüsselung / -signatur**
  - *E-Mail wird über Internet („provider“) geroutet*
  - Eigenbetrieb, z.B. Secure Mail Gateway Instanz (Zertificon Z1)
  - Landeslizenz Z1 nach Prüfung (Zertificon) nutzbar durch:
    - *allen Landesbehörden , Kommunalverwaltungen Sachsens*
    - *Forschungseinrichtungen der Länder, soweit sie mindestens zu 50% institutionell aus Landesmitteln gefördert werden.*
    - *Gerichten und sonstige Einrichtungen der Judikative der Länder*
  - Z1 Hardware/ VM‘s -> **Eigenbetrieb / Beschaffung**
  - Z1 Hardware Maintanance -> **Eigenbetrieb**
  - Z1 Software Support 5x9 -> **Eigenbetrieb**
  - Z1 Software Maintenance -> **Landeslizenz**
  - Kontakt Hersteller: https://www.zertificon.com/

Verschlüsselte Kommunikation: E-Mail VI

- Schlüssel (E-Mail Zertifikate):
  - Sachsen Global CA als TK der BakESV
  - Erhältlich für Funktionsadressen (Gruppenzertifikat)
  - aktuellste Handreichung c/o BakESV
    (Handreichung: „Beantragung: Sachsen Global CA E-Mail-Gruppenzertifikat“)

- Charakterisierung von prüfbaren E-Mail Zertifikaten (Marktbezeichnung)
  - *Class 1: E-Mail Adresse bestätigt*
  - *Class 2: E-Mail Adresse + Inhaber (nat./jur.) bestätigt*
  - *Class 3: E-Mail Adresse + Inhaber (nat./jur.) über Dokumente bestätigt*

- Empfehlung: eigenes Zertifikat mindestens Class 2, besser Class 3

Verschlüsselte Kommunikation: E-Mail VII

- Informationsquellen (Sachsen, Stand Februar 2016)
  - Handlungsleitfäden SächsEgovG
    - SMI: http://www.egovernment.sachsen.de/E-Government-Gesetz.html (Download sowohl staatlich als auch kommunal)
    - SAKD: http://www.sakd.de/egovg_handlungsleitfaden.html
  - Handreichungen Bak ESV: Mandatierung Secure Mail Gateway V1.3
  - Support: esv@sid.sachsen.de
  - Geeignete Schlagwörter zur Internetrecherche „verschlüsselte E-Mail“:

    „S/MIME +Wiki“ / „PGP +Wiki“,

    „E-Mail +verschlüsseln“ / „E-Mail +Datenschutz“
- Whitepaper zur E-Mail Verschlüsselung:
  - https://www.sicher-im-netz.de/downloads/verschluesselung-e-mails
  - https://www.sicher-im-netz.de/downloads/sichere-e-mail-kommunikation
  - https://www.zertificon.com/services/whitepaper

Elektronische Kommunikation: De-Mail

Domäne

TLS

ITSP

De-Mail

Gateway

Portal

Konto

Zugangseröffnung

Verschlüsselte Kommunikation: De-Mail I

Transportverschlüsselung + Inhaltsverschlüsselung, nur für Deutschland:

- De-Mail Standard (P2P)
  - TLS zwischen den Akteuren (Sender/Provider/Empfänger)
  - Zusätzlich Transportsicherung (Providersignatur)
  - Qualifizierte Metadaten (Versandoptionen, Bestätigungen)

- De-Mail E2E (Ende zu Ende)
  - Vertraulichkeit, d.h. kein Dritter/Provider kann Inhalt zur Kenntnis nehmen
  - Schlüsselausgabe durch lokalen Browser
  - In i.d.R. Gateways nicht anwendbar, nur für Webzugriff (Browser erforderlich)

- De-Mails werden providerunabhängig zugestellt

Verschlüsselte Kommunikation: De-Mail II

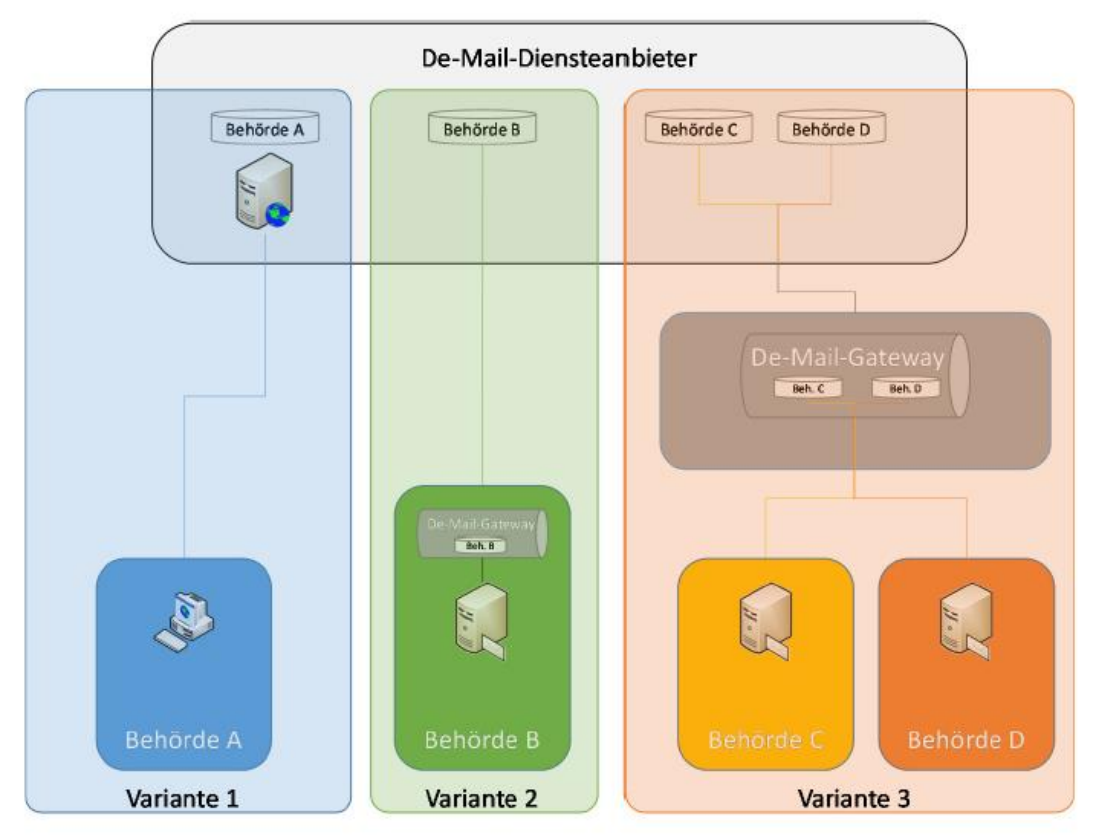
- **Handlungsoption 1:** unabhängig vom Netzanschluss :
  - Ausschließlich **Web Frontend** auf De-Mail Konto über Portal
    - Durch DMDA bereitgestellt
    - „Webmailer“
    - i.d.R. Bestandteil Kontovertrag

- **Handlungsoption 2:** unabhängig vom Netzanschluss :
  - *gesicherte Verbindung Behörde<>DMDA (TLS/PSK)*
  - **Eigenbetrieb** einer Gateway Lösung
    - Verschiedene Anbieter / DMDA am Markt
    - Ggf. Mehrkanallösung (OSCI, De-Mail, E-Mail) als elektronische Poststelle

Verschlüsselte Kommunikation: De-Mail III

- **Handlungsoption 3:** für **Teilnehmer SVN/KDN II** :
  - *E-Mail muss über KDNII / SVN geroutet (transportiert) werden*
  - **Zentrale Dienste** des Sächsischen Verwaltungsnetzes (SVN)
    - Transportverschlüsselung aktivieren (Exchange ab 2007)
  - De-Mail Gateway (Pilot) der Basiskomponente Elektronische Signatur und Verschlüsselung (**BakESV**)
    - De-Mail Konto beantragen (-> DMDA T-systems)
    - ITSP (SID) beauftragen (->DMDA T-Systems)
    - Behörde wir durch ITSP SID mandatiert (Handreichung „Nutzungsbedingungen für die Pilotierung De-Mail Gateway)
    - Behörden Admin übernimmt die behördeneigene Konfiguration
  - Webzugriff (DMDA) zusätzlich möglich

Verschlüsselte Kommunikation: De-Mail IV



Quelle: De-Mail Leitfaden (BMI 2015)

Verschlüsselte Kommunikation: De-Mail V

Entscheidungskriterium	De-Mail mit Gateway	De-Mail per Web Frontend
Nutzung aller De-Mail-Funktionen	+	+
schnelle Verfügbarkeit	-	+
geringe Anschaffungskosten	-	+
nutzbar ohne Integrationsaufwand	-	+
automatisierter Versand (Anbindung an Fachverfahren)	+	-
Einbindung vieler Prozesse	+	-
Einbindung in bestehende E-Mail-Infrastruktur	+	-
geeignet für größere Fallzahlen	+	-
geeignet für viele Nutzer in der Institution	+	-

Option3

ITSP / Bak ESV

Quelle: Grundlagen für den Einsatz von De-Mail in der öffentlichen Verwaltung (BMI 2012)

Verschlüsselte Kommunikation: De-Mail VI

- Informationsquellen (Sachsen, Stand Februar 2016)
  - Dokumentation zur Pilotierung (Handreichung „De-Mail im Freistaat Sachsen“)
  - Handreichungen Basiskomponente ESV über esv@sid.sachsen.de in der jeweils aktuellsten Version anfragen

- Zentrale Informationsseite zu De-Mail (BMI):
  - http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/De-Mail-integrieren/de-mail_integrieren_node.html

- Handreichungen des BMI:
  - http://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/De-Mail/2012_06_21_cc_de_mail_grundlagen_v1_0_download.pdf
  - http://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/De-Mail/**De-Mail_Leitfaden.pdf**

Elektronische Kommunikation: EGVP

OSCI

ERV

E2E

EGVP

JAVA

SAFE

Intermediär

Empfangsbestätigung

Verschlüsselte Kommunikation: EGVP I

Transportverschlüsselung + Inhaltsverschlüsselung, nur für Deutschland:

- OSCI Standard (**O**nline **S**ervices **C**omputer **I**nterface)
  - OSCI Transport (A) + OSCI Inhalt (B)
  - i.d.R. Asynchrone OSCI Kommunikation (Intermediär)
  - Ende zu Ende Verschlüsselung („doppelter Umschlag“)
  - Kommunikationsstandard mit höchsten Schutzanforderungen

- EGVP (**E**lektronisches **G**erichts und **V**erwaltungs**p**ostfach)
  - OSCI Kommunikationsszenario bundesweit
  - Rollenbasiertes Konzept (Bürger, Behörde) -> SAFE
  - Client, Verzeichnisdienst, Intermediär
  - Durch die Justiz (**ERV**) initiiert und eingesetzt, Öffnung für die allg. Verwaltung

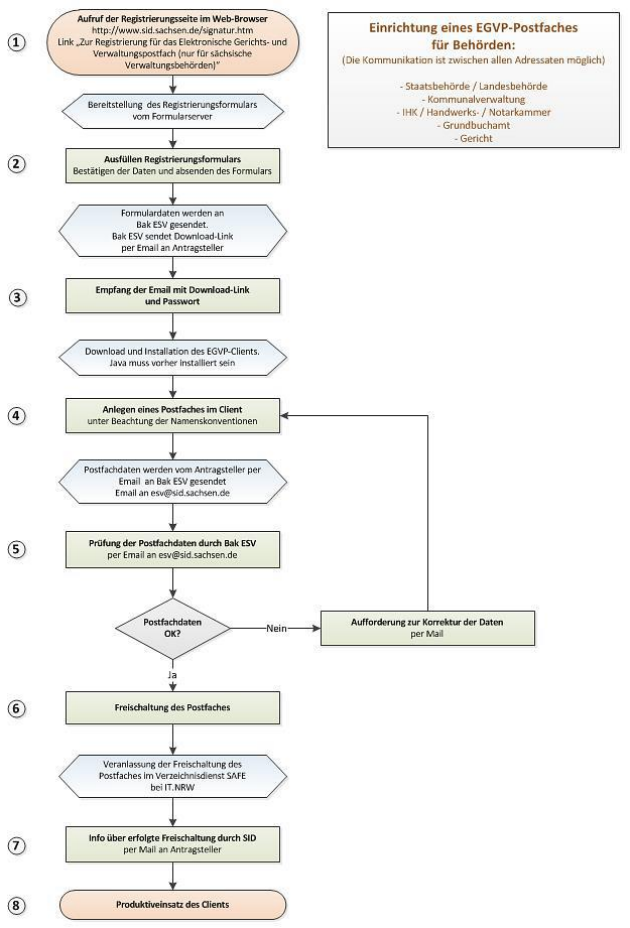
Verschlüsselte Kommunikation: EGVP II

- **Handlungsoption 1:** EGVP Clientsoftware
  - **Eigenbetrieb** einer Gateway Lösung
    - Verschiedene Anbieter am Markt
    - in Kombination mit anderen verschlüsselten Kanälen (Email, De-Mail)
    - OSCI-Intermediärspostfach über Bak ESV
    - Verzeichnisdienst SAFE Erstregistratur über Bak ESV
- **Handlungsoption 2:** EGVP Clientsoftware :
  - **Eigenbetrieb** EGVP Enterprise
    - Softwarebereitstellung über Bak ESV
    - 1st Level Support über Bak ESV
    - OSCI-Intermediärspostfach über Bak ESV
    - Verzeichnisdienst SAFE Erstregistratur über Bak ESV

Verschlüsselte Kommunikation: EGVP IV

- **Handlungsoption 3:** EGVP Clientsoftware :
  - **Eigenbetrieb** EGVP Backend
    - Softwarebereitstellung über BakESV
    - 1st Level Support über BakESV
    - OSCI-Intermediärspostfach über BakESV
    - Verzeichnisdienst SAFE Erstregistratur über BakESV

Verschlüsselte Kommunikation: EGVP V



- Benötigte Zertifikate werden in der lokalen Installation (Backend) erstellt oder alternative Zertifikate eingespielt
- Hinweis: Behörden sollten NICHT die Bürgerrolle nutzen (Bürgerclient)

Verschlüsselte Kommunikation: EGVP VI

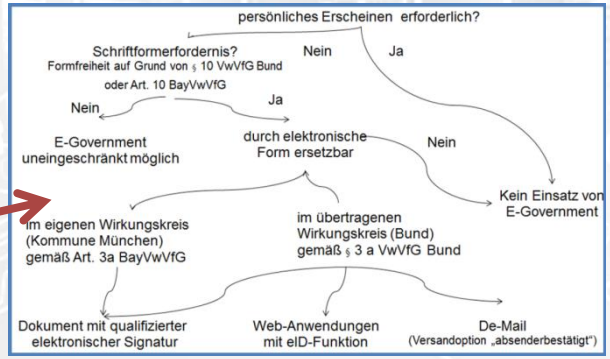
- Softwarebereitstellung:
  - EGVP Enterprise (Option 2): esv@sid.sachsen.de
  - EGVP Backend (Option 3): http://www.sid.sachsen.de/signatur.htm
    -> Formular „*Zur Registrierung für das Elektronische Gerichts- und Verwaltungspostfach (nur für sächsische Verwaltungsbehörden*)“
- 1st Level Support: esv@sid.sachsen.de
- OSCI-Intermediärspostfach: automatisch, mit Registrierung in SAFE
- Verzeichnisdienst (Ersteintrag): durch Bak ESV, Handreichungen:
  - Kurzanleitung **Registrierung und Freischaltung** Elektronisches Gerichts- und Verwaltungspostfach (EGVP)
  - **Namenskonvention** für die Einrichtung eines EGVP-Postfachs für sächsische Behörden (Adressbucheinträge, Zertifikat und Postfachbezeichnungen)

Elektronischer Schriftformersatz

- Vollständig elektronische Abwicklung von Verwaltungsprozessen
- Dienste und Unterstützungsleistungen durch Bak ESV

Schriftformersetzende elektronische Verfahren

- Schriftformerfordernis:
  - normalerweise **eigenhändig** unterschrieben
  - **ausschließlich** für solche Schriftformerfordernisse von Bedeutung, die in einer Rechtsvorschrift (Gesetz oder Verordnung) angeordnet sind.
  - Einzelne fachgesetzliche Regelungen schließen die „elektronische Schriftform“ aus (z.B. Arbeitsrecht/Kündigung)
- Elektr. Schriftformersatz:
  - QES / De-Mail / nPA
- Ist die Schriftform immer „angeordnet“?



Quelle: Leitfaden Online-Ausweisfunktion in Behörden, BMI

- **BSI TR-03107 Teil 2**: Schriftformersatz mit elektronischem Identitätsnachweis
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html

Schriftformersetzende elektronische Verfahren

PKCS7 SigG

SAK SiGV

QES

TR-ESOR Verifikation

Trustcenter

Signaturkarte Kartenleser

Schriftformersetzende elektronische Verfahren: QES I

- Grundlage: SigG, SigV, EU-VO 910/2014 (eIDAS)
  - hier: Fokus SigG, SigV
- QES: fortgeschrittene elektronische Signatur auf Basis eines qualifizierten Zertifikates (SigG) unter Verwendung einer Sicheren Signaturerstellungseinheit (Signaturkarte, HSM)
- QES: für natürliche Personen, ggf. zzgl. Attribute
- Lebenszyklus der QES-Signatur:
  - Erstellen
  - Prüfen
  - Bewahren

Schriftformersetzende elektronische Verfahren: QES II

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

Schriftformersetzende elektronische Verfahren: QES III

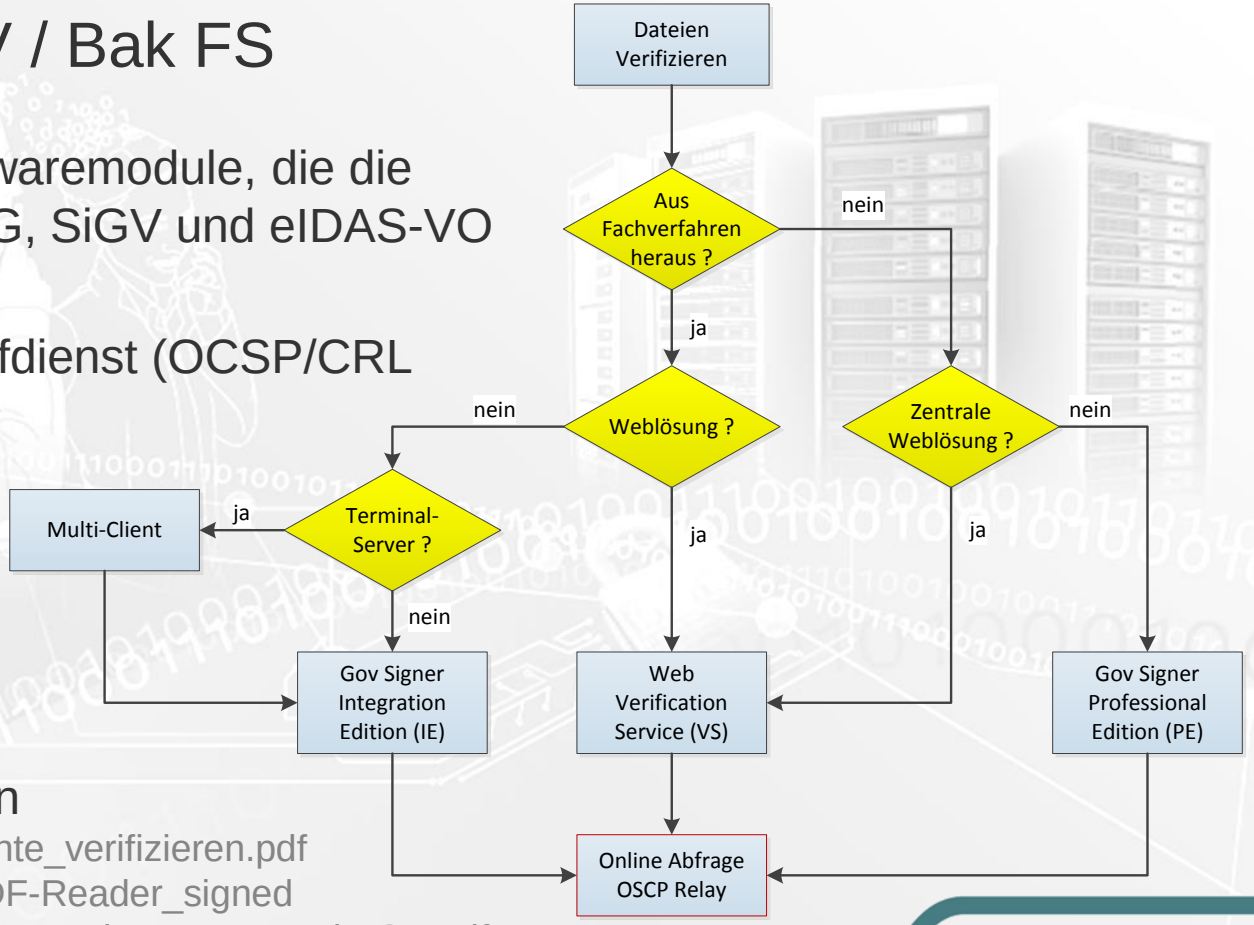
Zugangskanal

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**	∞	∞

Schriftformersetzende elektronische Verfahren: QES IV

Leistungen Bak ESV / Bak FS

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



- Details: Handreichungen
  - Leitfaden_signierte_Dokumente_verifizieren.pdf
  - Ungueltige-Signaturen-im-PDF-Reader_signed
  - 20160216_ Zugang für signierte Dokumente – BakESV.pdf

Schriftformersetzende elektronische Verfahren: QES V

Auswahl weiterführender Informationen zur QES:

- Bundesnetzagentur:
  http://www.bundesnetzagentur.de/cln_1431/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:
  https://www.governikus.com/de/governikus_signer/6002745/
- Beispiel Zugangseröffnung QES: http://www.smf.sachsen.de/eSignatur.html
- Beispiel für alternative Dienstleister: https://www.signaturportal.de

Schriftformersetzende elektronische Verfahren

qES (im Auftrag)

Authentisierungsniveau

ITSP **De-Mail (absenderbestätigt)**

Gateway Portal

Konto

Zugangseröffnung

Schriftformersetzende elektronische Verfahren: De-Mail I

De-Mail

- De-Mail in bestimmten Konfigurationen anwendbar (Versandoptionen)
- Optionen stehen jedem De-Mail Anwender zur Verfügung (Ausnahme: Abholbestätigung -> „Zustellung“)
- Schriftformersatz durch De-Mail:
  - Authentisierungsniveau „hoch“ erforderlich (Absender)
  - Absenderbestätigung durch DMDA „Absenderbestätigt“
- Bestätigungsnachrichten des DMDA tragen **QES**
- LF BMI:„..aufgrund von Veraktungs- und Langzeitspeicherungsanforderungen die Behörde für die beweiswerterhaltende Speicherung der Bestätigungsnachrichten Sorge tragen muss….“

Schriftformersetzende elektronische Verfahren: De-Mail II

De-Mail

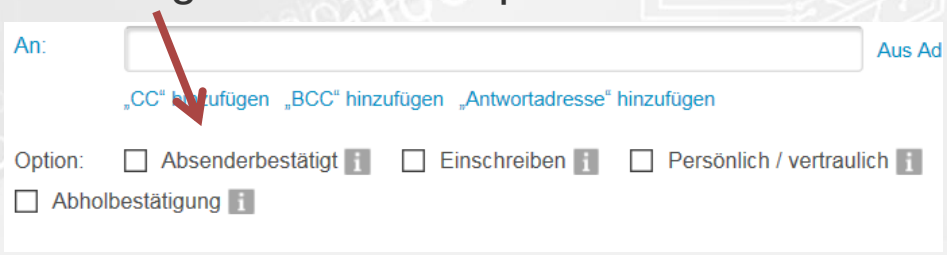
- Pilotierung -> **Ausgang** schriftformersetzend:

  Gateway ITSP:

  - User-Admin vergibt Rechte für den Teilnehmer in der Organisation
  - Versandoptionen, z.B. „Absenderbestätigt“ wird durch Teilnehmer fallbezogen aktiviert (Plugin, Steuerbefehl)

  Webfrontend DMDA:

  - Anmeldung mit Authentisierungsniveau „hoch“
  - Aktivierung der Versandoption aus Webfrontend



Schriftformersetzende elektronische Verfahren: De-Mail III

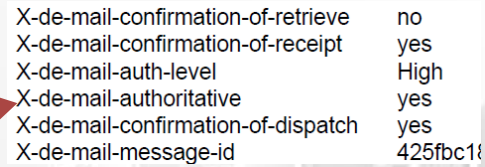
- Pilotierung -> **Eingang** schriftformersetzend:

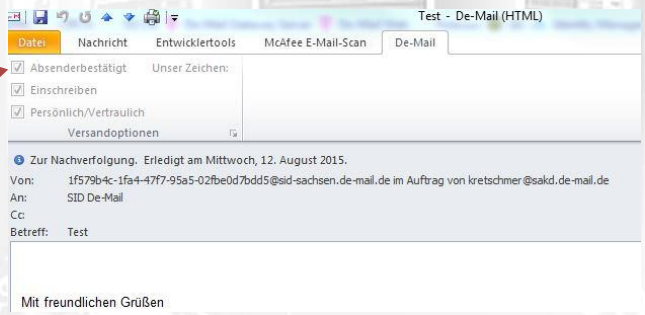
  Gateway ITSP

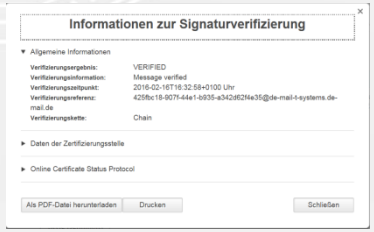
  - Im X-Header (Absenderbestätigt -> X-de-mail-authoritative=yes)
  - Lokales Plugin zur Visualisierung verwenden
  - vgl. BSI – TR 01201 Teil 3.4

  Webfrontend DMDA:

  - Visualisierung im Postfach → „hoch + absenderbestätigt“
  - Signatur überprüfen →







Schriftformersetzende elektronische Verfahren: De-Mail IV

- Informationsquellen (Sachsen, Stand Februar 2016)
  - Dokumentation zur Pilotierung (Handreichung „De-Mail im Freistaat Sachsen“)
  - Handreichungen Basiskomponente ESV über esv@sid.sachsen.de in der jeweils aktuellsten Version anfragen

- Zentrale Informationsseite zu De-Mail (BMI):
  - http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/De-Mail-integrieren/de-mail_integrieren_node.html

- Handreichungen des BMI:
  - http://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/De-Mail/2012_06_21_cc_de_mail_grundlagen_v1_0_download.pdf
  - http://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/De-Mail/**De-Mail_Leitfaden.pdf**

Schriftformersetzende elektronische Verfahren

ArchiSafe

Beweiswert

BSI

TR-03125

kryptografisch

S1

Beweiswert

Timestamp

Evidence Record

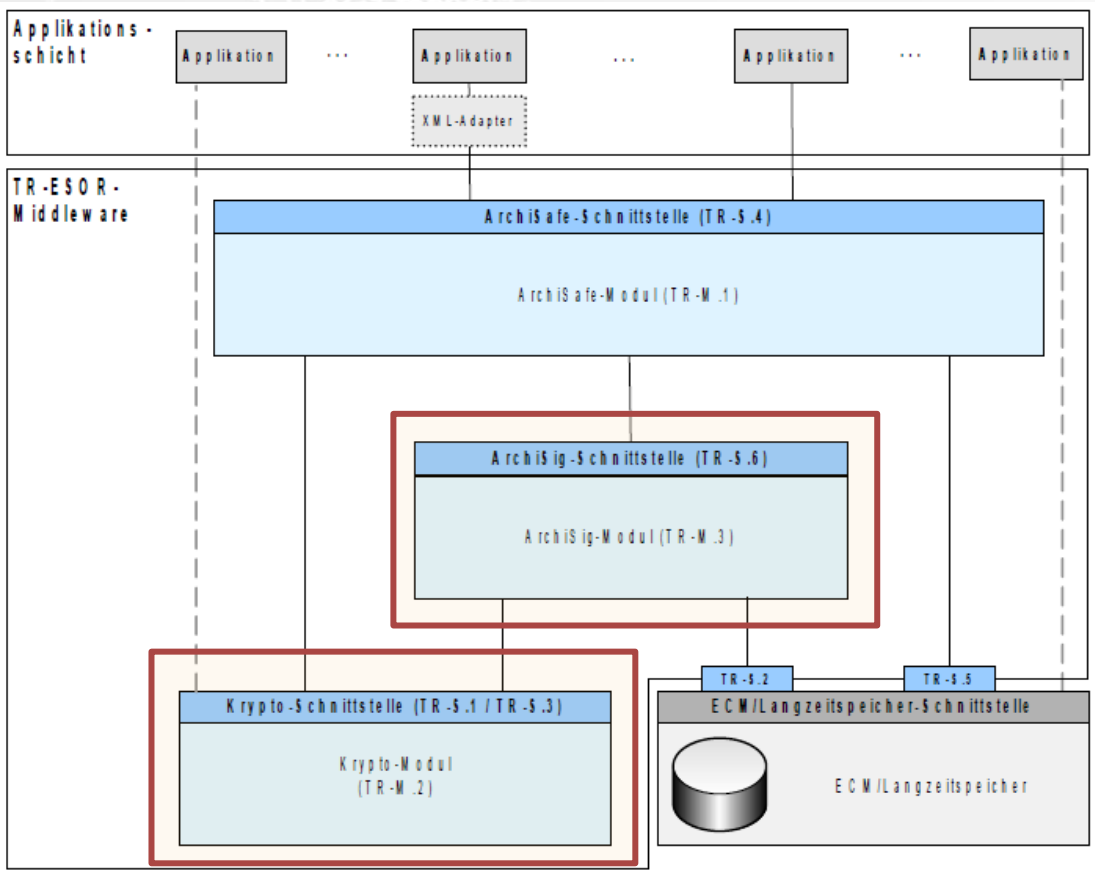
ArchiSIG

Schriftformersetzende elektronische Verfahren: TR-ESOR

- Beweiswert=kryptografische Sicherung, aber: Algorithmen werden schwach
- TR-ESOR: langfristige und rechtssichere Aufbewahrung
  (kryptografisch behandelter
  elektronischer Dokumente („Übersignatur“)
- Bak ESV: Kryptomodul , ArchiSigmodul, Verification Server (TR-ESOR-M.2, TR-ESOR-M.3)
- Bak ESV -> Zentrale Pflege der Krypto- und Vertrauensdienste
- Z.Zt. nicht abgedeckt durch Bak: TR-ESOR-Middleware (S4), ArchiSafe-Modul, ECM/Langzeitspeicher(S2,S5)
- Achtung: TR-ESOR und Aktenkontext! (Metadaten)

Schriftformersetzende elektronische Verfahren: TR-ESOR

Referenzarchitektur TR-ESOR



Quelle: TR-ESOR 1.2, BSI

Bak ESV

Kryptomodul

S1+S3+S6 Schnittstelle:
Signaturerstellung (optional)
Signaturprüfung
Qual. Zeitstempel (DRV)
Ver- und Entschlüsselung

Schriftformersetzende elektronische Verfahren: TR-ESOR

- Informationsquellen
  - Unterstützung und Mandatierung durch Basiskomponente ESV über esv@sid.sachsen.de
- Herstellerinformation der durch BakESV eingesetzen Module:
  - https://www.governikus.com/de/governikus_lza/5952804/
- Standards zur Beweiswerterhaltung (BSI):
  - https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html
- Informationen des BMI (Kapitel 4):
  - http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/egovg_minikommentar.pdf?__blob=publicationFile

Schriftformersetzende elektronische Verfahren

eID BerCA

BSI TR-03130

Port 24727 PAOS

nPA

AusweisAPP PIN

Temporäres Bürgerkonto

Datenschutz

Schriftformersetzende elektronische Verfahren: nPA I

- neuer Personalausweis = eID-Funktion & optional QES
- hier: eID-Funktion als Schriftformersatz

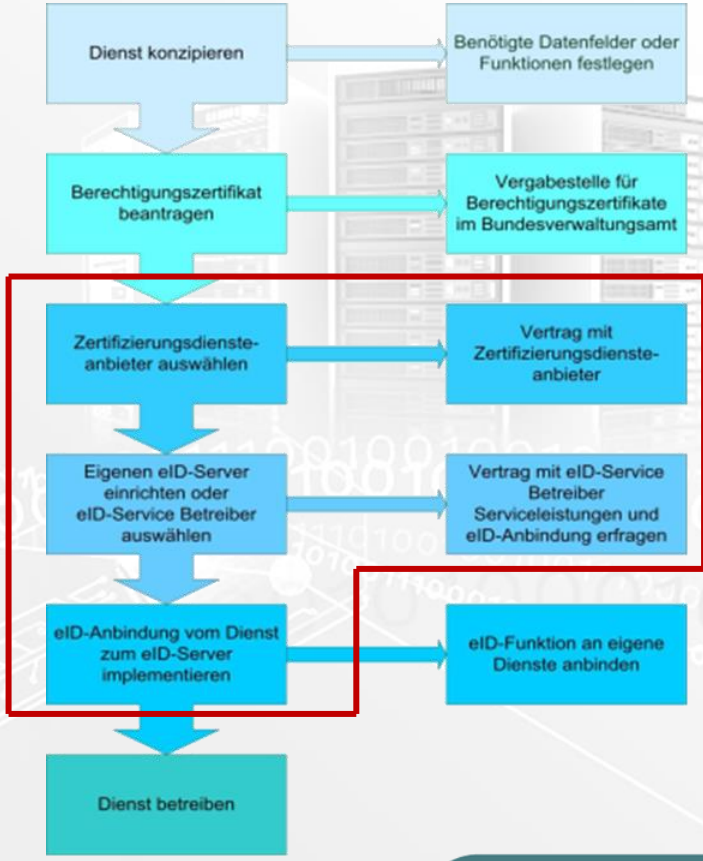
	Online-Ausweisfunktion	Unterschriftsfunktion
Logik	„Das bin ich“	„Das habe ich unterschrieben“
Zweck	Sicherer Identitätsnachweis	Rechtsverbindliche Unterschrift
Anbieter	Staat	Zertifizierungs-diensteanbieter
Aktivierung	Personalausweisbehörde	Zertifizierungs-diensteanbieter
Anzeige	Identität des Diensteanbieters und angeforderte Daten	Zu unterzeichnendes Dokument
Zugriffsschutz	eID-PIN	Signatur-PIN

- eID-Funktion muss aktiv freigeschaltet werden (Inhaber)
- Optionale QES ist kostenpflichtig -> wie Signaturkarte

Quelle: Der Personalausweis Anwenderhandbuch für Wirtschaft und Verwaltung, BMI

Schriftformersetzende elektronische Verfahren: nPA II

- Empfohlenes Vorgehen →
- Verschiedene Anbindungsvarianten
- Bak ESV unterstützt, entsprechend der avisierten Anbindungsvariante (markierter Bereich ->)



Quelle: Der Personalausweis Anwenderhandbuch für Wirtschaft und Verwaltung, BMI

Schriftformersetzende elektronische Verfahren: nPA III

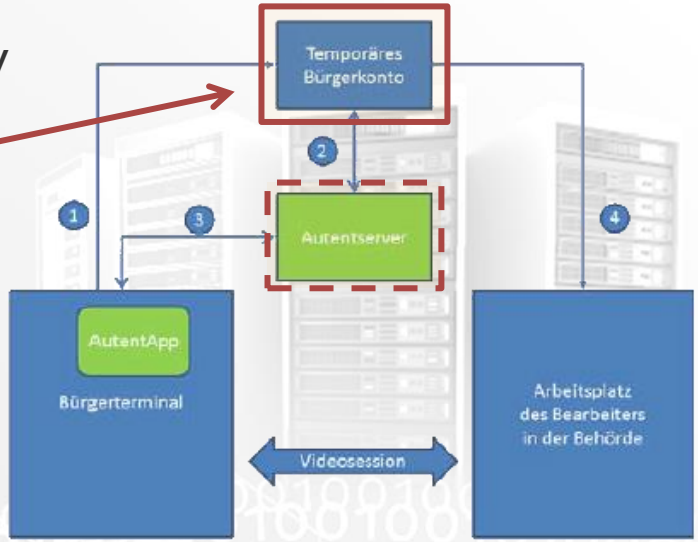
- Handlungsoptionen:
  1. FV + Eigenes BerZert. + eID Service Anbieter (vgl. personalausweisportal.de)
  2. FV + Eigenes BerZert. + eID-Service BakESV
  3. FV + Sachsen BerZert. + eID-Connect BakESV + eID Service BakESV
  4. Formularservice BakFS + Einreichoption „nPA“ + FV
- eID mit eigenem Berechtigungszertifikat (1 und 2):
  - Berechtigungszertifikat von BVA -> Prüfung Rechtmäßigkeit ~ 250
  - Techn. Berechtigungszertifikat -> durch Trustcenter ~ 800 - 2500/a
  - Setup auf eID-Service -> durch DL ~ 1000
  - Changes (z.B. SSL) -> ~ 250
  - Betrieb eID Service: ext. DL (?? Euro) oder BakESV (Opt.2)

Schriftformersetzende elektronische Verfahren: nPA IV

Einbindungsvarianten eID-Services über Bak ESV

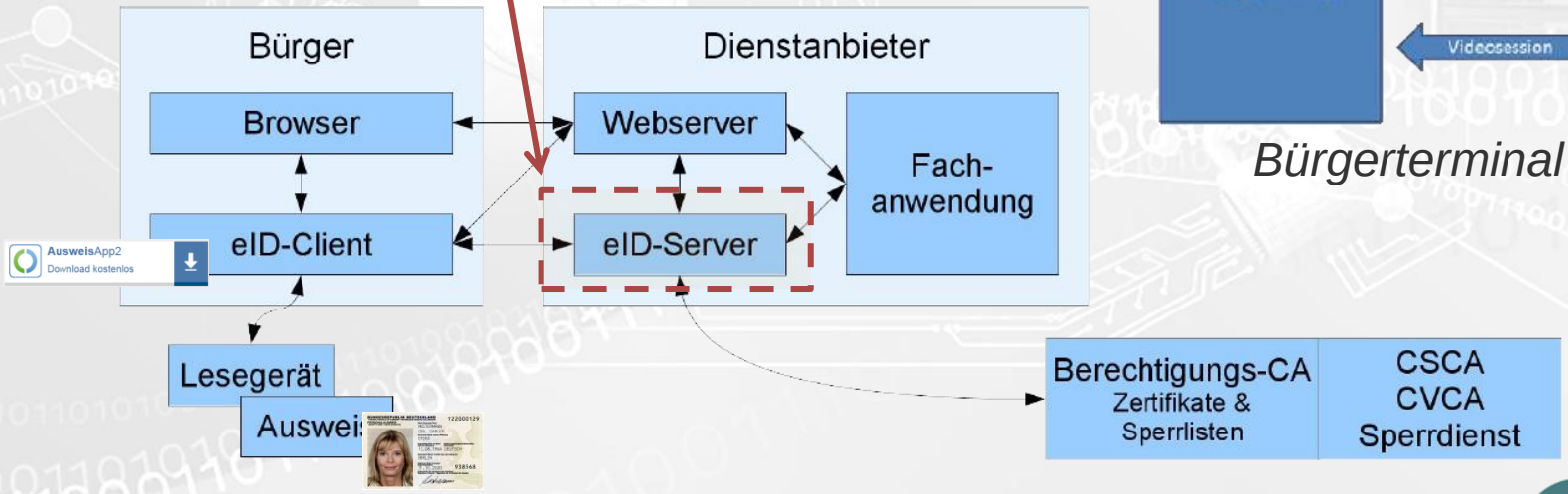
Bak ESV
eID Service (ext.)

Bak ESV
eID Connect



Bürgerterminal Sachsen

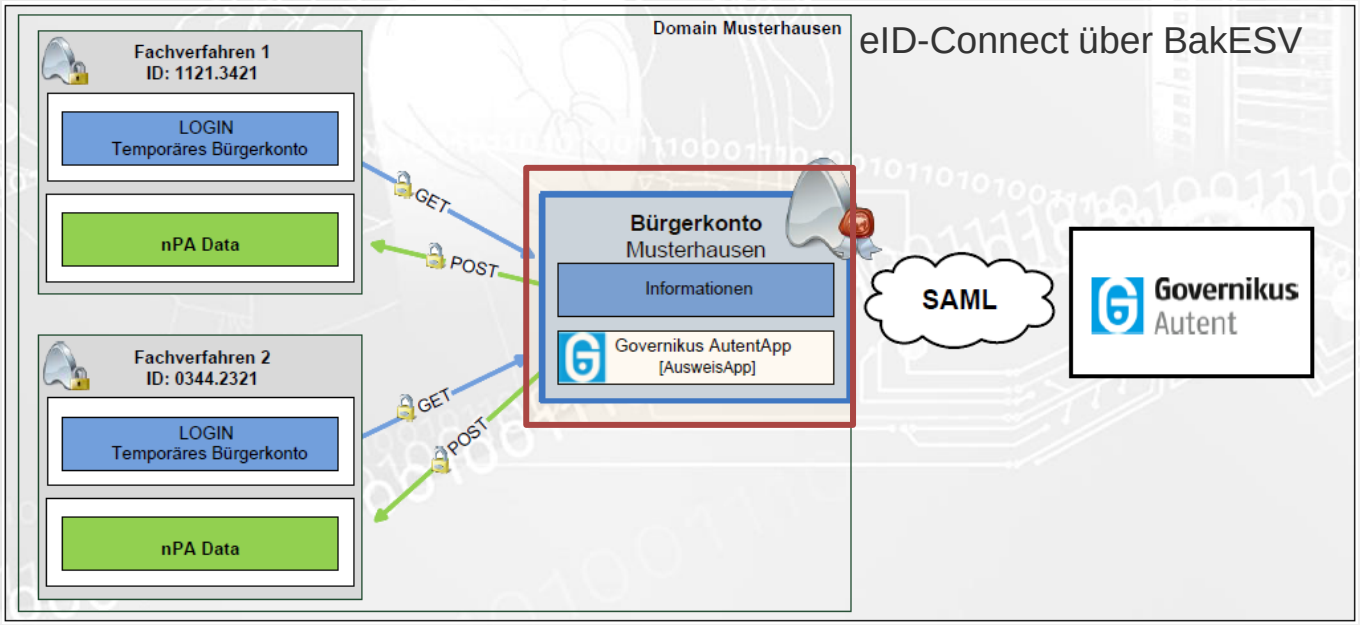
eID-Dienst Sachsen



Quellen: personalausweisportal.de, BMI; BSI-TR-03127, BSI

Schriftformersetzende elektronische Verfahren: nPA V

- eID-Connect unter Nutzung eines Landes-Berechtigungszertifikates
  - nPA Daten + Transaktionsprotokoll (Revisionssicherheit)
  - FV muss Erforderlichkeit der Daten nachweisen (zust. DSB)



Quellen: Governikus KG

Schriftformersetzende elektronische Verfahren: nPA VI

- Mandatierung, Testsystem und Anfragen: esv@sid.sachsen.de
- VITAKO Informationen:
  - Leitfäden Berechtigungszertifikat und Prozesse: http://www.vitako.de/Publikationen/Seiten/Leitfaeden.aspx
- Zentrale Informationsseite zum nPA (BMI):
  - http://www.personalausweisportal.de/DE/Home/home_node.html
- Handreichungen des BMI (Auswahl):
  - http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Weitere-Informationen/Leitfaden_Online_Ausweisfunktion_in_Beh%C3%B6rden.html
  - http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Steuerungsprojekte/eID/Erfahrungsberichte_Buergerkonten.pdf?__blob=publicationFile&v=2
  - http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Ergebnisdokumente/Berlin-Nutzung-eID-Basisdienstes--Leitfaden.html

Diskussion

- Support zur Bak ESV: esv@sid.sachsen.de

Quellen / Bildnachweis

De-Mail Logo:
Von IT-Stab des Bundesministerium des Innern im Auftrag der Beauftragten der Bundesregierung für Informationstechnik - De-Mail Informationen, Logo, https://de.wikipedia.org/w/index.php?curid=5798701

nPA Logo:
Von Bundesministerium des Innern, http://www.personalausweisportal.de/DE/Home/home_node.html

Governikus Signer Logo:
Von Governikus KG, http://www.governikus.com

Governikus LZA Logo:
Von Governikus KG, https://www.governikus.com

EGVP Logo:
Von ‚Die Website des Elektronischen Gerichts- und Verwaltungspostfachs', www.egvp.de

Zertificon Logo:
Von Zertificon Solutions GmbH , https://www.zertificon.com/

Logo der OSCI-Leitstelle
Von Informationstechnikzentrum Bund - 2016 https://www.itzbund.de/

Erfahren Sie mehr…

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

Riesaer Straße 7

01129 Dresden

Telefon 0351 20545 0

Telefax 0351 20545 109