

Leitstelle E-Government Sachsen

Basiskomponente

Elektronische Signatur und Verschlüsselung

**Mandatierung Secure Mail Gateway**

Version 1.3



# **Nutzung Secure Mail Gateway (SMGW) im Freistaat Sachsen über die E-Government Basiskomponente Elektronische Signatur und Verschlüsselung**

Der Freistaat Sachsen stellt für die sichere Übertragung von Nachrichten über das Internet Dienste im Rahmen der E-Government Basiskomponenten (BAK ESV) zur Verfügung.

Dieses Schreiben ist Grundlage zur Mandatierung für das Secure Mail Gateway.

Zur Produktivsetzung müssen folgende Schritte durchlaufen werden:

1. Registrierung auf den Seiten der BAK ESV <http://www.sid.sachsen.de/signatur.htm>
2. Initialisierung eines Projektes innerhalb des SID und Zusendung der Registrierungs- und Projektunterlagen durch SID
3. Umsetzung der technischen und organisatorischen Maßnahmen (siehe Checkliste) durch Mandanten
4. Prüfung der technischen Voraussetzungen durch BAK ESV
5. Freigabe als Mandant
6. Aktive Anbindung des Mandanten an das Secure Mail Gateway durch das Betriebsteam des SMGW

Rahmenbedingungen lt. Punkt 1:

Die zentralen Kosten der Mandatierung (Betrieb SMGW Server, einmalige Setupkosten für das Einrichten des Postfachs, Support SMGW) werden durch die Basiskomponente Elektronische Signatur und Verschlüsselung des Freistaates Sachsen abgedeckt.

Die mandantenbezogenen Zertifizierungskosten (gegebenenfalls anfallende Kosten für Signatur- und Verschlüsselungszertifikat des Mandanten) werden durch den Mandanten getragen.

Beratung und Unterstützungsleistungen können über die Basiskomponente abgerufen werden.

Supportanfragen werden von dem Mandanten direkt an die Basiskomponente ([esv@sid.sachsen.de](mailto:esv@sid.sachsen.de)) oder den User Help Desk der E-Government Plattform gestellt.

Die Basiskomponente informiert den Mandanten 3 Arbeitstage vor Beginn der Arbeiten über Wartungsfenster und deren Auswirkungen, wenn mit Systemausfällen zu rechnen ist oder die Wartungsdauer voraussichtlich 240 min. übersteigt.

Das SMGW ist für eine Verfügbarkeit von 98,5% ausgelegt. Störungen außerhalb des beherrschbaren Leistungsbereiches werden nicht angerechnet. Die maximale kontinuierliche Unterbrechungszeit des Dienstes pro Woche beträgt 240 min.

#### Kontaktdaten Mandant:

Herr/Frau Mustermann  
Postanschrift

Tel: +49  
Fax +49  
Email: mustermann@xyz.de

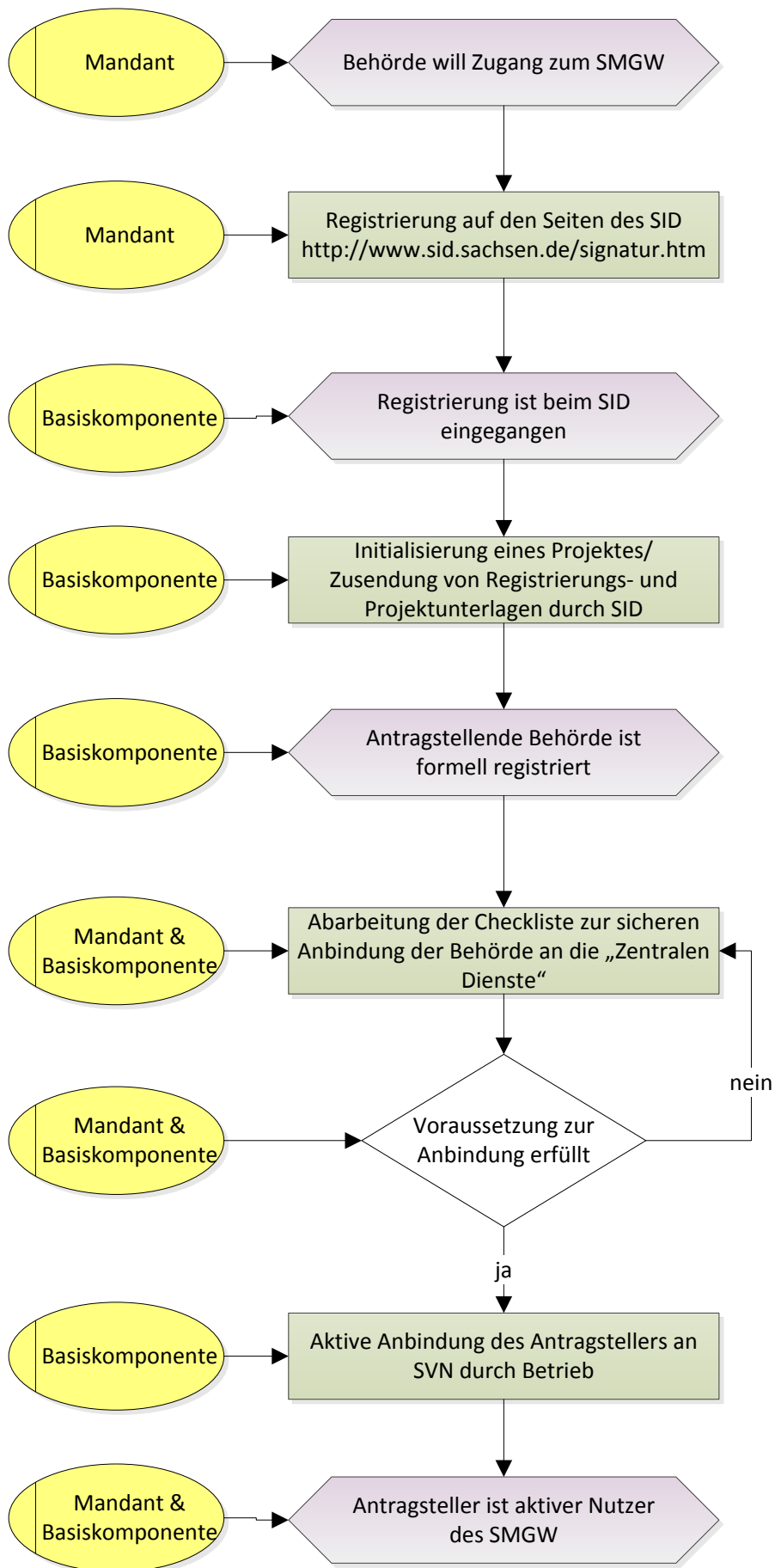
#### Kontaktdaten User Help Desk:

Tel.: 0800 2255 742 1500

#### Kontaktdaten Basiskomponente Bak ESV:

Staatsbetrieb Sächsische Informatik Dienste  
Fachbereich 3.1 | E-Government- und Querschnittverfahren  
Riesaer Str. 7  
01129 Dresden

Tel.: +49 351 20545 280  
Fax: +49 3578 33 55 47 32  
Email: esv@sid.sachsen.de



## Checkliste Mandanten-Anschluss an SVN SecureMail Gateway

- ☐ Prüfung Voraussetzungen
  - ☐ Absicherung Mailtransport innerhalb SVN/KDN (IPSEC oder StartTLS)
  - ☐ Anti Spoofing gewährleistet
- ☐ Auswahl des Trustcenters für Organisationszertifikat
- ☐ Beschaffung des Organisationszertifikats
- ☐ Auswahl des Trustcenters für SSL-Serverzertifikat
- ☐ Beschaffung des SSL-Serverzertifikats
- ☐ Prüfung ob Abweichungen von den Standard-Regeln (Eingänge, Ausgänge) erforderlich sind
  - Wenn ja: ☐ Definition der Policy-Abweichungen (Betriebskonzept Teil 2 Tabellen 2,3 und 4)
- ☐ Entscheidung ob alle Teilnehmer der Domäne über das SMGW geleitet werden sollen
  - Wenn nein: ☐ Auflistung der E-Mailadressen, (ggf. Angabe ob persönliches Zertifikat vorhanden ist und zwingend auf dem SMGW zu installieren ist) (Tabellen 5, 6)
- ☐ Löschung aller passiven Postfächer der eigenen Maildomäne (ggf. Abfrage beim SID)
- ☐ Entscheidung ob spezielle interne oder externe Gruppen mit besonderer Policy verarbeitet werden müssen
  - Wenn ja: ☐ Definition der Policy-Abweichungen (gem. *Tabellen 3 und 4*)
    - ☐ Auflistung Gruppenname, Mitglieder, Beschreibung, Policy-Name (*Tabellen 7, 8*)
- ☐ Entscheidung ob spezielle interne oder externe Einzeladressen mit besonderer Policy behandelt werden müssen
  - Wenn ja: ☐ Definition der Policy-Abweichungen (gem. Tabellen 3 und 4)
    - ☐ Auflistung Gruppenname, Mitglieder, Beschreibung, Policy-Name (*Tabellen 7, 8*)
- ☐ Klärung ob Hinterlegung von WebSafe-Nutzer-Passworten bei den Administratoren gewollt und von den eigenen Sicherheitsanforderungen erlaubt wird
- ☐ Prüfung ob Domänen spezifische Texte der Messenger-Antworttexte erforderlich sind
  - Wenn ja: ☐ Bearbeitung der *Tabelle 10*
- ☐ Festlegung der Ansprechpartner für SMGW-Administratoren auf Seiten der eigenen Domäne
  - ☐ Erstellung der *Tabelle 11*
- ☐ Abstimmung der SMGW bezogenen Support Aufgaben mit dem eigenen (oder beauftragten) UHD
- ☐ Erstellung der Informationsmittel für interne Mailanwender
- ☐ Veröffentlichung des eigenen Organisationszertifikat /PGP-Domain-Keys