GOVERNIKUS

Trust Service Practice Statement der Governikus GmbH & Co. KG

Arno Fiedler
Prof. Dr. Christoph Thiel

Version V.1.0

Inhalt

1 Einleitung

1.1 Einführung und Überblick

Dieses Dokument beschreibt das Trust Service Practice Statement (im Folgenden kurz „TSPS“ genannt) für die von der Governikus GmbH & Co. KG betriebenen Vertrauensdienste

- Validierungsdienste und
- Dienste zur Zustellung elektronischer Einschreiben (kurz Zustellungsdienste).

1.1.1 Vertrauensdiensteanbieter

Der Vertrauensdiensteanbieter (Trust Service Provider, im Folgenden TSP genannt) ist – auch im juristischen Sinne – die

Governikus GmbH & Co. KG (kurz: Governikus)
Hochschulring 4
28359 Bremen

1.1.2 Über dieses Dokument

Dieses Dokument definiert die detaillierten Festlegungen der technischen und operativen Umsetzung der Vertrauensdienste. Generelle Prozess- und Betriebsanforderungen sind in der Trust Service Policy (im Folgenden kurz „Policy“ oder „TP“ genannt) festgelegt.

Die Struktur dieses Dokumentes folgt weitgehend dem Internet-Standard RFC 3647 “Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework”.

Aus Gründen der Übersichtlichkeit werden die für Anforderungen und Regelungen, die nur einen spezifischen Vertrauensdienst betreffen, in einem entsprechenden Anhang A bzw. B dargestellt.

1.1.3 Eigenschaften der Vertrauensdienste

Siehe TP.

1.2 Name und Kennzeichnung des Dokuments

Dokumentname:	Trust Service Practice Statement der Governikus GmbH & Co. KG
Kennzeichnung (OID):	Dieses Dokument erhält die Governikus Policy-OID
	1.3.6.1.4.1.28939.8.8.2.1
Version:	1.0

1.3 Nutzung der Vertrauensdienste

Dieses TSPS wird durch die Governikus GmbH & Co. KG gepflegt und aktualisiert. Der Beauftragte der Geschäftsführung übernimmt die Abnahme des Dokuments.

Dieses TSPS wird jährlich überprüft und aktualisiert. Eine Änderung wird durch eine neue Versionsnummer dieses Dokumentes kenntlich gemacht.

Kontaktdaten:

Governikus GmbH & Co. KG
Hochschulring 4
28359 Bremen

Tel: +49 421 204 95 – 0
Fax: +49 421 204 95 – 11
E-Mail: kontakt@governikus.de

1.3.1 Genehmigung und Freigabe dieses Trust Service Practice Statements

Mit der Abnahme durch den IT-Direktor erhält das Dokument den Status "gültig", der zugleich das Datum des Inkrafttretens angibt.

Vor der Abnahme können die betroffenen interessierten Parteien innerhalb von 14 Arbeitstagen nach Bekanntgabe Kommentare zur vorgeschlagenen Fassung des TSPS einreichen. Nach Ablauf dieser Frist kann die Leitung der Governikus das TSPS genehmigen, wenn keine wesentlichen Vorbehalte gegen den wesentlichen Inhalt der vorgeschlagenen Fassung bestehen.

Alle an dem Dokument vorgenommenen Änderungen im Vergleich zur vorherigen Fassung werden in der Historie des Dokuments festgehalten.

Das genehmigte TSPS wird als pdf-Dokument veröffentlicht und Mitarbeitern und den Teilnehmern und Akteuren der Vertrauensdienste unverzüglich mitgeteilt.

2 Veröffentlichungen und Verzeichnisse

2.1 Verzeichnisse

Siehe Trust Service Policy.

2.2 Veröffentlichung von Informationen

Alle öffentlichen Informationen werden unter folgender Adresse auf dieser Webseite veröffentlicht

https://www.governikus.de/trust

2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Alle relevanten öffentlichen Dokumente werden mindestens jährlich überprüft und aktualisiert veröffentlicht. Eigene Verzeichnisdienste werden nicht betrieben. Die Aktualität der jeweiligen Verzeichnisdienste der TSP bei der Prüfung von Zertifikaten liegt in deren Verantwortung.

2.4 Zugriffskontrollen auf Verzeichnisse

Die veröffentlichten Dokumente und Zertifikate können unentgeltlich 24x7 auf der in Abschnitt 2.2 genannten Webseite der Governikus abgerufen werden. Es gibt keine Zugriffsbeschränkungen für lesenden Zugriff. Änderungen der Verzeichnis- und Webinhalte werden ausschließlich vom TSP vorgenommen.

Weitere, nicht öffentliche Dokumente, können bei begründetem Interesse auf Nachfrage in den relevanten Teilen ausgegeben werden.

2.5 Zugang und Nutzung von Diensten

Siehe Trust Service Policy.

3 Identifizierung und Authentifizierung

Die Identifizierung und Authentifizierung von Kunden und Anwendern für die Vertrauensdienste

- Validierungsdienste und
- Zustellungsdienste

erfolgt gemäß dienst- und kundenspezifischen Anforderungen sowie den Anforderungen der entsprechenden Standards (z.B. eIDAS-VO, EN 319 401, EN 319 521 oder den relevanten Technischen Richtlinien des BSI).

Konkretisierungen zu Identifizierung und Authentifizierung der Teilnehmer und Akteure eines Vertrauensdienstes werden, falls gegeben, in den Anhängen A bzw. B dieses TSPS aufgeführt.

4 Betriebsanforderungen

Konkretisierungen zu Betriebsanforderungen eines Vertrauensdienstes werden, sofern diese über die einschlägigen Anforderungen aus EN 319 401 hinausgehen, in den Anhängen A bzw. B dieses TSPS aufgeführt.

Die Anforderungen an die Beendigung des Vertrauensdienstes sind im Beendigungskonzept aka Termination Plan beschrieben.

5 Nicht-technische Sicherheitsmaßnahmen

Konkretisierungen zu nicht-technischen Sicherheitsmaßnahmen eines Vertrauensdienstes werden, falls gegeben, in den Anhängen A bzw. B dieses TSPS in den jeweiligen Abschnitten Nicht-technische Sicherheitsmaßnahmen aufgeführt.

5.1 Infrastrukturelle Sicherheitsmaßnahmen (Physical Controls)

Governikus hat ein ISMS eingeführt, welches die Sicherheitsanforderungen der Dienste, Prozesse und Verfahren überwacht, welche von diesem TSPS abgedeckt werden.

Diese Sicherheitsmechanismen sind dem Grad der Bedrohung im Umfeld der angebotenen Vertrauensdienste angemessen.

5.1.1 Standort und Aufbau

Die Server von Governikus befinden sich in sicheren Rechenzentren und werden (auf der Ebene des Betriebssystems) von Mitarbeitern des Rechenzentrums verwaltet und betrieben.

Die Sicherheit der Rechenzentren wird durch eine entsprechende Zertifizierung nachgewiesen, deren Existenz und Gültigkeit Governikus regelmäßig im Rahmen eines im Rahmen eines Compliance-Audits überprüft.

Mehrere Ebenen physischer Sicherheitskontrollen beschränken den Zugang zu den sensiblen Hardware- und Software-Systemen, die für die Durchführung von Operationen verwendet werden. Die verwendeten Systeme sind so konfiguriert, dass nur autorisierte Mitarbeiter darauf zugreifen können.

Die Umgebung ist physisch geschützt und dient der Verhinderung und Erkennung von unzulässiger Nutzung, den Zugriff auf oder die Offenlegung von sensiblen Informationen.

5.1.2 Physischer Zugang

Governikus stellt sicher, dass die relevanten Systeme mit physischen Sicherheitsmechanismen geschützt werden, insbesondere, dass kein unbefugter Zugriff auf die Hardware erfolgen kann und jederzeit manuell oder elektronisch unbefugtes Eindringen überwacht wird. Weiterhin wird ein Zugangsprotokoll geführt und regelmäßig überprüft.

Der physische Zugang zu den Rechenzentren, einschließlich Datenbankservern, Routing- und Switching-Komponenten sowie Firewalls ist ausreichend eingeschränkt.

Alle IT-Komponenten (Server, Datenbanken), die für die Implementierung von Governikus Diensten erforderlich sind, befinden sich an besonders gesicherten Standorten. Nur Administratoren haben Zugang zu den Räumlichkeiten nach dem Vier-Augen-Prinzip, dabei wird jeder Zutritt revisionssicher protokolliert.

Besucher können die Räumlichkeiten von Governikus nicht ohne Unterstützung von autorisierten Mitarbeitern betreten. In allen relevanten Sicherheitsbereichen müssen die Besucher von ununterbrochen von autorisierten Mitarbeitern begleitet werden.

5.1.3 Stromversorgung und Klimatisierung

Das Rechenzentrum verfügt über branchenübliche Stromversorgungs- und Klimatisierungssysteme, um eine geeignete Betriebsumgebung zu schaffen. Weiterhin sind die Rechenzentren mit einer unterbrechungsfreien Stromversorgung ausgestattet, um ein reibungsloses Herunterfahren der Systeme oder die Wiederherstellung zu ermöglichen.

5.1.4 Wassergefährdung

In den Rechenzentren wurden angemessene Vorkehrungen getroffen, um die Auswirkungen von Wassereinwirkung zu minimieren.

5.1.5 Brandverhütung und -schutz

Die Rechenzentren verfügen über branchenübliche Brandverhütungs- und –Schutzmechanismen.

5.1.6 Lagerung von Medien

Empfindliche physische Datenträger werden in einem Tresor aufbewahrt, um sie vor zufälligen Schäden (wie Wasser, Feuer, elektromagnetische Felder usw.) zu schützen. Medien, die Prüfungsdaten, Archivdaten oder Sicherungsinformationen enthalten, werden dupliziert und sicher aufbewahrt.

Papierbasierte Informationen werden über einen Dienstleister sicher vernichtet.

5.1.7 Abfallentsorgung

Die wesentlichen sensiblen Dokumente und Materialien kommen nur in elektronischer Form vor. Medien, die zur Sammlung oder Übertragung sensibler Informationen verwendet werden, werden vor der Entsorgung sicher gelöscht.

5.1.8 Offsite-Backup

Governikus führt regelmäßige Routine-Backups von kritischen Systemdaten, Audit-Log-Daten und anderen sensiblen Informationen durch.

5.2 Organisatorische Sicherheitsmaßnahmen

Das Management der Vertrauensdienste ernennt unter Berücksichtigung notwendiger Rollentrennungen die sicherheitsrelevanten Rollen und ordnet diese geeigneten Mitarbeitern zu. Falls für eine Rolle notwendig, wird ein Vier-Augenprinzip vorgesehen. Bei der Belegung der Rollen wird eine entsprechende Funktionstrennung sowie eine notwendige Mindestanzahl berücksichtigt. Details dazu sind im Rollenkonzept beschrieben.

5.3 Personelle Sicherheitsmaßnahmen

Governikus stellt ausschließlich zuverlässiges, qualifiziertes Personal ein. Vor Aufnahme der Tätigkeit im sicherheitskritischen Bereich wird die Fachkunde geprüft und erforderlichenfalls eine entsprechende Schulung durchgeführt.

5.4 Sicherheitsüberprüfung

Seitens des Bereiches Personalwesen von Governikus wird sichergestellt, dass bei Rollen, welche eine spezifische Sicherheitsüberprüfung erfordern, diese Überprüfungen vor Aufnahme der Tätigkeit des Mitarbeiters erfolgreich absolviert wurden.

5.5 Archivierung von Unterlagen

Alle gesetzlich geforderten Unterlagen werden elektronisch archiviert. Dabei werden die Empfehlungen des BSI zur Langzeitarchivierung TR-ESOR umgesetzt. Im Falle einer Betriebseinstellung greift das entsprechende Konzept, auch „Termination Plan“ genannt.

5.6 Schlüsselwechsel

Nicht anwendbar.

5.7 Kompromittierung und Wiederherstellung

Für die Vertrauensdienste gibt es ein Sicherheitsvorfallmanagement, dass die in Abschnitt 7.9 der ETSI EN 319 401 festgelegten Anforderungen erfüllt:

a) Governikus überwacht alle Aktivitäten im Zusammenhang mit dem Zugang zu und der Nutzung von Informationssystemen und Dienstanfragen;

b) Bei den Überwachungsmaßnahmen wird die Sensibilität der erfassten Informationen berücksichtigt und analysiert;

c) Abnormale Systemaktivitäten, die auf eine potenzielle Sicherheitsverletzung

hinweisen, einschließlich des Eindringens in das System und das Netz werden erkannt und als Alarme gemeldet;

d) Governikus überwacht die folgenden Ereignisse:
   i. das Starten und Beenden der Protokollierungsfunktionen; und
   ii. Verfügbarkeit und Nutzung der benötigten Dienste.

e) Governikus handelt zeitnah und koordiniert, um schnell auf Vorfälle zu reagieren und die Auswirkungen von Sicherheitsverstößen zu begrenzen;

f) Governikus ernennt vertrauenswürdige Rollen, die Warnungen über potenziell kritische Sicherheitsvorfälle nachgehen und sicherstellen, dass relevante Vorfälle gemäß den festgelegten internen Verfahren gemeldet werden;

g) Governikus hat Verfahren eingerichtet, um die jeweils zuständigen Behörden gemäß den geltenden Rechtsvorschriften über eine relevante Sicherheitsverletzung oder jeden Integritätsverlust, der erhebliche Auswirkungen auf den Vertrauensdienst und die personenbezogenen Daten hat, zu benachrichtigen.

h) Wenn die Verletzung der Sicherheit oder der Verlust der Integrität wahrscheinlich eine natürliche oder juristische Person, für die der Vertrauensdienst erbracht wurde, beeinträchtigt, benachrichtigt Governikus die betreffende natürliche oder juristische Person unverzüglich von der Verletzung der Sicherheit oder dem Verlust der Integrität;

i) Die Systeme von Governikus werden regelmäßig überwacht, um Anhaltspunkte für böswillige Aktivitäten zu ermitteln, indem automatische Mechanismen zur Verarbeitung der Prüfprotokolle eingesetzt werden, und das Personal wird bei möglichen kritischen Sicherheitsereignissen alarmiert;

j) Für jede Schwachstelle, unter Berücksichtigung ihrer möglichen Auswirkungen,
   i. erstellt Governikus einen Plan zur Abschwächung der Schwachstelle und setzt diesen um; oder
   ii. dokumentiert Governikus die Entscheidung, dass die Schwachstelle nicht behoben werden muss, z. B. wenn die Kosten für die potenziellen Auswirkungen die Kosten für die Behebung nicht rechtfertigen.

k) Verfahren zur Meldung von Vorfällen und zur Reaktion darauf werden so angewandt, dass der Schaden durch Sicherheitsvorfälle und Störungen möglichst gering gehalten wird.

Für die Vertrauensdienste gibt es eine Business Continuity-Planung, die die folgenden Elemente enthält:

a) Die Bedingungen für die Aktivierung des Plans,

b) Verfahren für Notfälle;

c) Ausweichverfahren;

d) Verfahren zur Wiederaufnahme des Betriebs;

e) Anforderungen an die Sensibilisierung und Ausbildung;

f) Regelmäßige Tests von Notfallplänen:

g) Die Anforderung, kritische kryptografische Materialien (d. h. sichere kryptografische Geräte und Aktivierungsmaterialien) an einem anderen Ort zu lagern;

h) Definitionen für „akzeptabler Systemausfall“ und eine „akzeptable Wiederherstellungszeit“;

i) Festlegungen für die Häufigkeit von Sicherungskopien von wichtigen Geschäftsinformationen und Software;

j) Verfahren zur weitestgehenden Sicherung ihrer Einrichtung in der Zeit nach einer Katastrophe und vor der Wiederherstellung einer sicheren Umgebung entweder am ursprünglichen oder an einem entfernten Standort.

6 Technische Sicherheitsmaßnahmen

Die technischen Sicherheitsmaßnahmen für die Vertrauensdienste

- Validierungsdienste und
- Zustellungsdienste

erfolgen gemäß dienst- und kundenspezifischen Anforderungen sowie den Anforderungen der entsprechenden Standards (z.B. eIDAS, EN 319 401, EN 319 521 oder Technische Richtlinien des BSI).

Konkretisierungen zu den technischen Sicherheitsmaßnahmen eines Vertrauensdienstes werden, falls gegeben, in den Anhängen A bzw. B dieses TSPS aufgeführt.

7 Profile von Zertifikaten, Sperrlisten und OCSP

Nicht anwendbar.

8 Auditierung und andere Prüfungen

Siehe Trust Service Policy.

9 Sonstige geschäftliche und rechtliche Regelungen

Siehe Trust Service Policy.

Anhang A: Validierungsdienst

Anwendungs- und Geltungsbereich des Trust Service Practice Statements

Bei dem Validierungsdienst handelt es um einen nichtqualifizierten, normalisierten Signaturzertifikatsvalidierungsdienst. Signaturprüfungen sind nicht Bestandteil des Dienstes. Der Dienst stellt die Funktion der Validierung von Signaturzertifikaten alleinig für Clients zur Verfügung, welche von Governikus entwickelt wurden. Diese Clients können die Signaturzertifikatsvalidierung an den angebotenen Dienst auslagern und die Ergebnisse für ihre eigenen fachlichen Zwecke verwenden. Einer dieser Zwecke kann es sein, die eingeholten Ergebnisse im Zusammenhang mit der Prüfung einer elektronischen Signatur zu verwenden.

Es gilt daher zu beachten, dass die Anforderungen an einen Signaturvalidierungsdienst nach ETSI TS 119 441 sowie ETSI TS 119 442 nur eingeschränkt auf den hier betrachteten Signaturzertifikatsvalidierungsdienst anwendbar sind. Es sei allerdings angemerkt, dass die durch den Signaturzertifikatsvalidierungsdienst bereitgestellten Informationen dazu geeignet sind, den Teil der Signaturzertifikatsvalidierung innerhalb einer Signaturvalidierung zu erfüllen, sodass letztere den Anforderungen aus ETSI EN 319 102-1, ETSI EN 319 102-2 und ETSI TS 119 172-4 genügen kann. Eine solche Signaturvalidierung würde dann aber außerhalb des Anwendungsbereichs des betrachteten Dienstes erfolgen.

Service Design des Validierungsdienstes

Die Nutzung des Signaturzertifikatsvalidierungsdienstes im Kontext einer Signaturvalidierung veranschaulicht Schaubild 1.

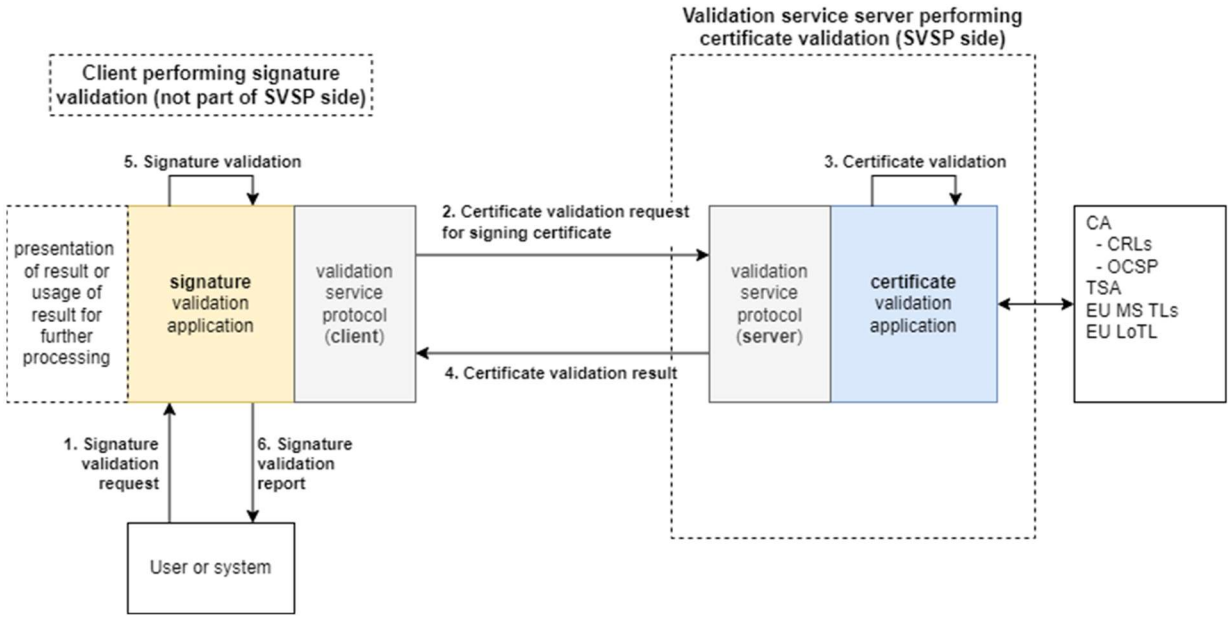

Schaubild 1: Anwendungsbereich des Dienstes im Kontext einer Signaturvalidierung

Der Signaturzertifikatsvalidierungsdienst führt lediglich eine Zertifikatsvalidierung von mit einer Anfrage übergebenen Signaturzertifikaten durch. Anfragende Clients lagern z.B. die

Validierung eines Signaturzertifikats (einschließlich z.B. der Qualitätsbestimmung des Signaturzertifikats, Zertifikatspfadvalidierung und Überprüfung der Sperrinformationen der beteiligten Zertifikate) an den Signaturzertifikatsvalidierungsdienst aus. Der Ablauf einer solchen durch einen Client ausgeführten Validierung ist beispielhaft in Schaubild 1 skizziert und folgt den folgenden Schritten:

1. Ein System oder ein Benutzer (je nach Client) veranlasst den Client, eine Signaturvalidierung durchzuführen.
2. Der Client extrahiert das Signaturzertifikat aus der Signatur und sendet eine Zertifikatsvalidierungsanfrage (potenziell samt einer proprietären Validierungsrichtlinie) über ein proprietäres Protokoll an den Signaturzertifikatsvalidierungsdienst.
3. Der Signaturzertifikatsvalidierungsdienst führt die Zertifikatsvalidierung durch, die unter anderem folgendes umfasst:
    - Qualitätsbestimmung (ist das Zertifikat EU-qualifiziert)
    - Typbestimmung (ist das Zertifikat eines für elektronische Signaturen oder Siegel oder Website-Authentisierung)
    - Validierung der Zertifikatskette (z. B. schreibt die Richtlinie das Gültigkeitsmodell und die weitere Verwendung und Interpretation der während der Validierung des Zertifikatspfads erhaltenen Sperrinformationen vor)
4. Das Ergebnis der Zertifikatsvalidierung wird in Form eines maschinenlesbaren, proprietären Validierungsberichts zurückgegeben. Dieser enthält detaillierte Informationen über die Zertifikatspfadvalidierung und alle beteiligten Antworten der Vertrauensdiensteanbieter.
5. Der Client führt die Signaturvalidierung durch, die unter anderem folgendes umfassen kann:
    - Berechnung und Vergleich des Digest- und des Signaturwertes (einschließlich der Überprüfung der verwendeten kryptografischen Primitive auf ihre Eignung)
    - Die Verwendung des Ergebnisses der Signaturzertifikatsvalidierung, um festzustellen, ob das Signaturzertifikat zum relevanten Zeitpunkt gültig war (der relevante Zeitpunkt hängt von der Richtlinie ab, die der Client für die Signaturvalidierung anwendet).

Teilnehmer und Akteure der Validierungsdienste

Siehe Trust Service Policy.

Betriebsanforderungen

Validierungsprozess

Der Validierungsprozess des Signaturzertifikatsvalidierungsdienstes entspricht den Anforderungen aus der ETSI EN 319 102-1, welche an die Validierung von Signaturzertifikaten im Kontext einer Validierung von elektronischen Signaturen gestellt werden.

Der Validierungsprozess gibt an den anfragenden Client einen maschinenlesbaren, proprietären Validierungsbericht zurück. Dieser enthält pro geprüftem Signaturzertifikat eine Statusanzeige für dessen Validierung. Die im Bericht aufgeführten Statusanzeigen sind

konform zu den Anforderungen aus der ETSI EN 319 102-1, welche sich auf die Signaturzertifikatsvalidierung beziehen.

Sofern für Signaturzertifikatsvalidierung anwendbar, ist gemäß dem in ETSI EN 319 102-1 spezifizierten Algorithmus der Status der Signaturvalidierung entweder TOTAL-PASSED, TOTAL-FAILED oder INDETERMINATE.

Ein anfragender Client hat die Möglichkeit, einer Validierungsanfrage eine Prüfrichtlinie mitzugeben. Hierfür ist ein proprietäres Richtlinienschema vorgesehen. Dem Client stehen vordefinierte Richtlinien zur Verfügung. Ferner kann dieser aus der vordefinierten Menge an Vorgabenparametern eine individuell zusammengestellte Richtlinie übergeben. Übergibt der Client keine Prüfrichtlinie, so wählt der Signaturzertifikatsvalidierungsdienst in Abhängigkeit des Sitzes des ausstellenden Vertrauensdiensteanbieters, des Dienstetyps, dem Ausstellungsdatum sowie der Niveauangaben (qualifiziert oder nichtqualifiziert) eine passende Prüfrichtlinie aus. Die Detaillierte Prüfrichtlinie wird mit dem zurückgegebenen Validierungsbericht transparent ausgegeben. Diese Informationen kann der anfragende Client in einen ETSI TS 119 102-2 konformen Prüfbericht übernehmen.

Der Validierungsprozess stellt sicher, dass die verwendete Signaturvalidierungspolicy mit den Nutzungsbedingungen der bei der Validierung involvierten und abgefragten Vertrauensdiensteanbieter übereinstimmt.

Bei gleichbleibendem Input im Sinne der ETSI EN 319 102-1 Abschnitt 5.1.3 Note 5, liefert der Signaturzertifikatsvalidierungsdienst stets den gleichen Output.

Interfaces

Der Kommunikationskanal zwischen dem Anwender und dem Signaturzertifikatsvalidierungsdienst ist gesichert und verschlüsselt, d.h. Governikus gewährleistet die Authentizität, Integrität sowie auch die Vertraulichkeit der übertragenen Daten.

Validierungsbericht

Der Validierungsprozess gibt an den anfragenden Client einen maschinenlesbaren, proprietären Validierungsbericht zurück. Dieser enthält pro geprüftem Signaturzertifikat eine Statusanzeige für dessen Validierung. Die im Bericht aufgeführten Statusanzeigen sind konform zu den Anforderungen aus der ETSI EN 319 102-1, welche sich auf die Signaturzertifikatsvalidierung beziehen.

Dass die Antwort auf die Signaturzertifikatsvalidierung die OID der Validierungspolicy beinhaltet, wird zu Ende 2025 umgesetzt.

Der von dem Signaturzertifikatsvalidierungsdienst bereitgestellte Validierungsbericht kann durch die anfragende Clientanwendung in einen Bericht übersetzt werden, der den Anforderungen aus ETSI TS 119 102-2 entspricht.

Der proprietäre Signaturzertifikatsvalidierungsbericht zeigt einen der drei in ETSI EN 319 102-1 definierten Status an, d. h. TOTAL-PASSED, TOTAL-FAILED oder INDETERMINATE. Ebenso enthält dieser Teilindikationen gemäß ETSI EN 319 102-1.

Der Signaturzertifikatsvalidierungsbericht berichtet über jede der verarbeiteten Validierungsbedingungen (vorgegeben durch die proprietäre Prüfrichtlinie), einschließlich aller Validierungsbedingungen, die von der Implementierung implizit angewendet wurden.

Die Identität des Diensteanbieters (Governikus) kann aus dem Signaturzertifikatsvalidierungsbericht ausgelesen werden.

Der Validierungsbericht wird mit einer elektronischen Signatur versehen. Das Zertifikat, auf dem die Signatur basiert, stammt aus der Governikus internen PKI.

Bedingungen und Konditionen des Validierungsdienstes

Die vom Signaturzertifikatsvalidierungsdienst durchgeführte Validierung von Signaturzertifikaten entspricht den Anforderungen der ETSI EN 319 102-1 soweit diese auf die Signaturzertifikatsvalidierung anwendbar sind. Die neueste Version der EN 319 102-1, zu der die Konformität gewährleistet ist, ist die Version 1.2.1.

Kryptographische Vorgaben

Um sicherzustellen, dass der Prozess der Signaturzertifikatsvalidierung stets korrekte Ergebnisse liefert, verwendet die zugrunde liegende Implementierung stets aktuelle Implementierungen von getesteten und weit verbreiteten kryptografischen Bibliotheken.

Die Gültigkeit bzw. Verwendbarkeit von kryptographischen Algorithmen basiert stets auf der aktuellen Version des Papiers „SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms“, siehe https://www.sogis.eu/uk/supporting_doc_en.html. Zum Zeitpunkt der Erstellung dieses Dokuments ist die aktuelle und unterstützte Version die Nummer 1.3. Der Inhalt dieses Papiers ist in einen maschinenlesbaren Katalog übersetzt, der Gültigkeitszeiträume von kryptographischen Primitiven und Signaturschemata enthält, die im Zusammenhang mit der Signatur- und Zertifikatsvalidierung verwendet werden. Diese Gültigkeitszeiträume werden automatisiert verwendet, um alle Signaturen zu validieren, die im Zusammenhang mit der Signaturzertifikatsvalidierung auftreten (z.B. Signaturen auf: Zertifikaten, CRLs, OCSP-Antworten, Zeitstempeln).

Das SOG-IS-Papier wird alle zwei bis drei Jahre aktualisiert, und der zuständige Mitarbeiter der Governikus prüft spätestens alle drei Monate, ob eine aktualisierte Version vorliegt. Sobald ein aktualisiertes SOG-IS-Papier vorliegt, wird die Übersetzung in die maschinenverarbeitbare Form und deren Qualitätssicherung so schnell wie möglich durchgeführt, damit die Signaturzertifikatsvalidierung den aktuellen Empfehlungen folgt. Dieses wird durch die aktive Mitarbeit der Governikus im Gremium ETSI ESI unterstützt, welches die SOG-IS Anforderungen im „Algopaper“ abbilden.

Bereitstellung von Prüfinformationen

Die Anforderungen an das automatisierte Dokumentieren, welche Prüfung mit welcher zugrundeliegenden Produktversion durchgeführt wurde, ist bereits technisch umgesetzt, muss allerdings noch bis Ende 2025 in eine gemeinsame Datenhaltung überführt werden.

Personenbezogene Daten werden ausschließlich in Form von Signaturzertifikaten verarbeitet.

Signaturvalidierungsprotokoll und -Bericht

Das vom Signaturzertifikatsvalidierungsdienst genutzte Protokoll ist nicht zu dem in der ETSI TS 119 442 vorgegebenen Protokoll konform. Allerdings ist dieses aufgrund des Umstandes, dass es sich ausschließlich um die Validierung von Signaturzertifikaten und nicht generell um die Validierung signierter Objekte handelt, eine zulässige Abweichung.

Der Kommunikationskanal zwischen dem Signaturzertifikatsvalidierungsdienst und einer proprietären Governikus Anwendung, welche diesen konsumiert, ist durch TLS 1.2 abgesichert.

Anhang B: Zustelldienste

Teilnehmer und Akteure der Zustelldienste

Teilnehmer des Zustelldienstes elektronischer Rechtsverkehr (ERV) sind

a) bebPo aas/ eBO aaS,
b) Kunden (Subscriber) von bebPo aas/ eBO aaS sind juristische Personen,
c) Anwender sind Mitarbeitende der juristischen Personen, die einen E-Mail-Client bedienen. Diese agieren als Absender oder Empfänger von zuzustellenden Inhalten,
d) Vertrauende Dritte können Evidenzen anfordern, hierzu muss vorab die Berechtigung und die Zustimmung der Beteiligten geklärt werden.

Identifizierung und Authentifizierung

Identifizierung

Der Zustelldienst der Governikus verifiziert die Identität des Absenders und des Empfängers durch einen Dritten gemäß der Vorgaben der Justiz über eingerichtete Prüfstellen.

beBPo: Der Zustelldienst der Governikus verifiziert die Identität des Absenders und des Empfängers durch einen Dritten gemäß der Vorgaben der Justiz über eingerichtete Prüfstellen.

eBO: Der Zustelldienst der Governikus verifiziert die Identität des Absenders und des Empfängers durch einen Dritten gemäß den Vorgaben der Justiz über die Kommunikation mittels Notaren.

Identifizierung des Empfängers und Übergabe des Nutzinhalts

Alle Empfänger werden durch einen Dritten gemäß ERVV (Elektronischer-Rechtsverkehr-Verordnung) identifiziert und dürfen nur dann als Empfänger fungieren, wenn sie im SAFE (Verzeichnisdienst des ERV) hinterlegt sind.

Je nach Rolle des verwendeten Postfachs (beBPo, eBo), wird die Identifizierung durch eine eingesetzte Prüfstelle oder einen Notar durchgeführt.

Authentifizierung von Absender und Empfänger und Übergabe des Nutzinhalts.

Der Zustelldienst der Governikus authentifiziert den Absender, bevor dieser den Nutzinhalt übermittelt, und er authentifiziert den Empfänger, bevor der Nutzinhalt an diesen übergeben wird.

Eingehende Nachrichten: Der Absender (Teilnehmer im ERV) wird durch eine Prüfung der VHN-Signatur (Vertrauenswürdiger Herkunftsnachweis) identifiziert. Diese Signatur wurde bei Erstellung der Nachricht mit einem Zertifikat der Bundesnotarkammer (BNotK) erzeugt. Das Zertifikat ist entweder für den Absender ausgestellt worden, oder wird per Fernsignatur verwendet.
Bei der E-Mail-Weiterleitung wird der Empfänger über das E-Mail-Postfach und die IP-Adresse des Empfänger-Mailservers authentifiziert. Die Anbindung des Empfänger-Mailservers erfolgt durch einen VPN-Tunnel.

Bei der Weiterleitung per XTA (XÖV Transport Adapter - Protokoll zur Nachrichtenübertragung via https), wird der Empfänger über das Serverzertifikat authentifiziert. Auch in diesem Fall erfolgt die Anbindung durch einen VPN-Tunnel.

Ausgehende Nachrichten: Der Absender (Kunde) wird über das absendende E-Mail-Postfach, sowie die IP-Adresse des Kunden-Mailservers authentifiziert. Beim Nachrichteneingang per XTA, wird der Absender über das Clientzertifikat authentifiziert. Auch in diesem Fall erfolgt die Anbindung durch einen VPN-Tunnel.
Der Empfänger wird durch sein zugehöriges Postfachzertifikat authentifiziert. Die ausgehende Nachricht wird mit seinem öffentlichen Schlüssel verschlüsselt, dieser wird anhand der SAFE-ID aus dem SAFE-Verzeichnisdienst abgerufen.

Betriebsanforderungen

Verfügbarkeit:
Die verarbeitenden Systeme sind redundant ausgelegt.

Integrität:
Die signierten Hashwerte der Anhänge im vhn.xml stellen die Integrität der Nutzerinhalte sicher.

Vertraulichkeit:
Zwischen dem GMM und den Systemen der Absender bzw. des Empfängers liegen die Nachrichten ausschließlich verschlüsselt für den Empfänger vor. Zwischen GMM und Kunden (Mailserver/XTA-Webservice) liegt eine Transportverschlüsselung per SMTPS/HTTPS und VPN-Tunnel vor. Die Vertraulichkeit der Absender-/Empfängeridentität wird durch eine durchgängige Transportverschlüsselung sichergestellt.

Austausch mit dem Absender/Empfänger:
Die signierten Hashwerte der Anhänge im vhn.xml stellen die Integrität der Nutzerinhalte sicher. Die signierte vhn.xml wird dem Empfänger übermittelt. Beim Outbound-Versand wird die vhn.xml durch den GMM generiert und signiert.

Verteilte Systemkomponenten:
Auch in den verteilten Systemen (Clustering) verhält sich das System wie vorgenannt beschrieben. Nach der Erstellung der signierten vhn.xml wird diese bei der Nachricht immer mitgeführt.

Speicherung:
Die Nutzerinhalte befinden sich nur für die notwendige Dauer der Verarbeitung auf den Systemen von Governikus.

Entspricht der Dateiname eines zu versendeten Anhangs nicht den Vorgaben, so wird der Dateiname durch das ERDS geändert. Die Änderung wird ebenfalls im Laufzettel gegenüber dem Outbound-Absender kommuniziert.

Zeitbezug

Der Zustelldienst der Governikus protokolliert die verschiedenen Aktionen (Senden und Empfangen) mit einer genauen Zeitangabe im elektronischen Poststellenbuch und im Laufzettel.

Ereignisse und Evidenz (Nachweise)

Der Nachweis über den Versand wird über den Laufzettel in der Weiterleitungsbestätigung gegenüber. dem Outbound-Absender zur Verfügung gestellt. Dieses wird über das signierte vhn.xml gegenüber dem Empfänger einer Nachricht bereitgestellt.

Der Anwender wird über das E-Mail-Postfach und die IP-Adresse des Empfänger-Mailservers authentifiziert. Diese Anwenderauthentifizierung wird in den Log-Dateien des ERDS-Mailservers archiviert.

Archivierung der Identifikationsdaten

Die Archivierung der Anwender-Identifikationsdaten obliegt den BeBPo-Prüfstellen (für BeBPo) oder dem SAFE-Registrierungssystem (für eBO).

Die Archivierung der Anwender-Identifikationsdaten für beA (besondere elektronische Anwaltspostfächer) obliegt der Bundesrechtsanwaltskammer (BRAK).

Die Archivierung der Anwender-Identifikationsdaten für beN (besondere elektronische Notarpostfächer) obliegt der Bundesnotarkammer (BNotK).

Die Archivierung der Anwender-Identifikationsdaten für beSt (besondere elektronische Steuerberaterpostfächer) obliegt der Bundessteuerberaterkammer (BStBK).

Nachweise mittels Laufzettel

Der Zustelldienst fragt die SAFE-ID des Empfängers im zugehörigen SAFE ab. Dies wird in Form von GMM-Logs archiviert. Es obliegt den jeweiligen SAFE-System des Empfängers, dass dort nur überprüfte Identitäten hinterlegt sind. Dies wird über den Laufzettel dokumentiert und archiviert. Auch die Dokumenten- und Signaturprüfung ist im Laufzettel dokumentiert.

Weiterhin enthält der Laufzettel Informationen darüber, wann die E-Mail an den ausgehenden Mailserver übergeben wurde. In den ERDS-Mail-Server-Logs ist ersichtlich, wann die Nachricht an den Empfänger-Mail-Server übermittelt wurde. Dabei haben ausschließlich dafür qualifizierte Administratoren Zugriff auf die Protokolle/Logdateien der ERDS-Systemkomponenten.

Die genannten Protokolle & Logdateien werden nur teilweise archiviert. E-Mail-Logs werden seit Inbetriebnahme des Dienstes 18 Monate archiviert, sonstige 30 Tage.