GOVERNIKUS

# Trust Service Policy 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 die Trust Service Policy (im Folgenden kurz „Policy“ oder „TP“ 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
kontakt@governikus.de

Der TSP kann Teilaufgaben an Partner oder externe Anbieter auslagern.

Für die Einhaltung der Verfahren im Sinne dieses Dokuments bzw. etwaiger gesetzlicher oder zertifizierungstechnischer Anforderungen an den TSP, bleibt der TSP, vertreten durch die Geschäftsführung oder deren Beauftragte, verantwortlich.

### 1.1.2 Über dieses Dokument

Dieses Dokument definiert die Prozess- und Betriebsanforderungen, die für die Nutzung der von Governikus angebotenen Vertrauensdienste gelten, und legt die Richtlinien fest, die Governikus für die Bereitstellung von Diensten anwendet. Sie regelt das Zusammenwirken, Rechte und Pflichten der Teilnehmer der Vertrauensdienste.

Die gesamte TP ist verbindlich, soweit dies im Rahmen des zu Grunde liegenden deutschen bzw. europäischen Rechts zulässig ist. Sie enthält Aussagen über Pflichten, Gewährleistung und Haftung für die Teilnehmer. Soweit Garantien oder Zusicherungen betroffen sind, enthält die TP ausschließlich die für diesen Bereich ausdrücklich eingeräumten Garantien oder Zusicherungen.

Die Kenntnis der in dieser TP beschriebenen Anforderungen und Regeln sowie der rechtlichen Rahmenbedingungen erlaubt es Anwendern der Dienste, Vertrauen in die Komponenten und Teilnehmer aufzubauen und Entscheidungen zu treffen, inwieweit das durch die Vertrauensdienste gewährte Vertrauens- und Sicherheitsniveau für Anwendungen geeignet ist.

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

Detaillierte Festlegungen der technischen und operativen Umsetzung sind im Trust Service Practice Statement (im Folgenden „TSPS“ genannt) festgelegt.

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

### 1.1.3 Eigenschaften der Vertrauensdienste

Governikus bietet unter dieser TP diverse Dienste an, die die Anforderungen aus dieser TP in ihren speziellen Produkteigenschaften erfüllen. Die Dienste werden nach Möglichkeit barrierefrei angeboten.

Die Erfüllung der Anforderungen und Regelungen dieser TP wird in einem dazugehörigen Dokument, dem Trust Service Practice Statement (TSPS), beschrieben.

Vertrauensdienste, die mit dem Zusatz „qualifiziert“ genannt werden, sind qualifizierte Vertrauensdienste im Sinne der eIDAS-Verordnung. Derzeit umfasst diese TP keine qualifizierten Vertrauensdienste.

### 1.1.4 Kurzbeschreibung der Vertrauensdienste

Governikus bietet verschiedene Vertrauensdienste im Sinne der eIDAS-VO an:

- Validierungsdienste (ValidationServices)

  Validierungsdienste sind für die Bewertung der Korrektheit und Unversehrtheit elektronisch signierter, gesiegelter oder mit einem Zeitstempel versehener Unterlagen unabdingbar. Sie sorgen auch für Transparenz. Anwender können auf Anhieb feststellen, ob beispielsweise das verwendete Zertifikat für die Signaturerstellung oder für die Siegelerstellung zum Zeitpunkt der Signierung oder Siegelung gültig war. Validierungsdienste überprüfen also, ob die Anforderungen von eIDAS an eine (qualifizierte) elektronische Signatur oder ein Siegel erfüllt sind, um die Gültigkeit zu bestätigen oder zu widerlegen.

- Dienste zur Zustellung elektronischer Einschreiben (Electronic Registered Delivery Services, ERDS)

  Ein Dienst zur Zustellung elektronischer Einschreiben ist nach eIDAS ein elektronischer Dienst, der die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln ermöglicht und einen Nachweis der Handhabung der übermittelten Daten erbringt, darunter den Nachweis der Absendung und des Empfangs der Daten, und der die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung schützt.

Die Liste der angebotenen Vertrauensdienste kann in späteren Versionen dieser Policy erweitert werden.

## 1.2 Name und Kennzeichnung des Dokuments

| | |
|---|---|
| Dokumentenname: | Trust Service Policy der Governikus GmbH & Co. KG |
| Kennzeichnung (OID): | Dieses Dokument erhält die Governikus Policy-OID |
| | 1.3.6.1.4.1.28939.8.8.1.1 |
| Version | 1.0 |

## 1.3 Teilnehmer und Akteure der Vertrauensdienste

Teilnehmer und Akteure der Vertrauensdienste

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

sind jeweils der

- entsprechende Vertrauensdienst selbst (ggf. unterteilt in verschiedene Komponenten) sowie
- Kunden (die den Vertrauensdienst beauftragen),
- Anwender des jeweiligen Dienstes und
- Vertrauende Dritte (Relying Parties).

Konkretisierungen der Teilnehmer und Akteure eines Vertrauensdienstes werden, falls gegeben, in den Anhängen A bzw. B dieser TP in den jeweiligen Abschnitten Teilnehmer und Akteure aufgeführt.

## 1.4 Nutzung der Vertrauensdienste

### 1.4.1 Geeignete Nutzung

Vertrauensdienste, die dieser TP unterliegen, können im Allgemeinen für alle gemäß der eIDAS-VO vorgesehenen Zwecke verwendet werden. Kunden und Anwender sind dafür verantwortlich, die Vertrauensdienste so zu verwenden, dass die Verwendung den anwendbaren gesetzlichen Bestimmungen entspricht.

Weitere Regelungen sind in dem zu dieser TP gehörenden TSPS beschrieben.

### 1.4.2 Grenzen der Nutzung

Die Verwendung von Vertrauensdienste für Dienste und Systeme, die bei Störungen oder Ausfällen zu großen materiellen oder immateriellen Schäden führen sowie Schäden an Leib und Leben verursachen können, ist nicht gestattet.

Hiervon abweichende Regelungen können im Einzelnen mit dem Vertrauensdiensteanbieter schriftlich vereinbart werden.

## 1.5 Administration der TP

### 1.5.1 Zuständigkeit für das Dokument

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

Diese TP 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

### 1.5.2 Genehmigung und Freigabe dieser TP

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 der TP einreichen. Nach Ablauf dieser Frist kann die Leitung der Governikus die TP 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.

Die genehmigte Richtlinie wird als PDF-Dokument veröffentlicht und Mitarbeitern und den Teilnehmern und Akteuren der Vertrauensdienste unverzüglich mitgeteilt.

# 2 Veröffentlichungen und Verzeichnisse

## 2.1 Verzeichnisse

Nicht anwendbar, da keine eigenen Verzeichnisdienste bereitgestellt werden.

## 2.2 Veröffentlichung von Informationen

Alle öffentlichen Informationen werden unter folgender Adresse auf der Webseite veröffentlicht

https://www.governikus.de/trust

Im Rahmen der Vertrauensdienste

- Validierungsdienste und
- Zustellungsdienste

werden die Zertifikate der Vertrauensdienste zur Kommunikationsabsicherung mit Kunden und Anwendern (TLS-Zertifikate) und zur Validierung der von Vertrauensdiensten ausgestellten Siegel (für Validierungsberichte und Evidenzen) veröffentlicht.

Veröffentlicht werden zudem

- Trust Service Practice Statement (TSPS)
- Allgemeine Geschäftsbedingungen von Governikus
- Policy Disclosure Statement

Nicht (allgemein) veröffentlicht werden aufgrund ihrer Sensibilität, aus sicherheitstechnischen Erwägungen und mit dem Status als Geschäftsgeheimnis u.a. folgende Dokumente

- Sicherheitskonzept
- Kryptokonzept
- Beendigungskonzept (Termination Plan)

## 2.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

Diese Regelungen sind im zum TP gehörenden TSPS beschrieben.

## 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

Die Vertrauensdienste der Governikus werden öffentlich angeboten und sind nach dem Zustandekommen der Kundenbeziehung mittelbar für jedermann zugänglich. Hierbei erfolgt der Zugriff auf die Dienste ausschließlich über von Governikus entwickelte Software, welche in Abgrenzung zu nicht-Governikus Software alleinig dazu in der Lage ist, die Dienste erfolgreich anzusprechen. Sie können grundsätzlich von allen genutzt werden, die den Allgemeinen Geschäftsbedingungen, der Verpflichtungserklärung, der TP und dem dazugehörigen Trust Service Practice Statement (TSPS) der Governikus zugestimmt haben (zusammengefasst: Terms & Conditions). Governikus ist bestrebt ihre Dienste barrierearm anzubieten.

Als Richtlinie zur Erstellung weitgehend barrierefreier Internetinhalte dienen in erster Linie die Web Content Accessibility Guidelines (WCAG) des W3C.

## 3 Identifizierung und Authentifizierung

Details zur Umsetzung dieser Anforderungen werden im TSPS in den Anhängen A und B dargestellt.

## 4 Betriebsanforderungen

Die Betriebsanforderungen für die Vertrauensdienste

- Validierungsdienste und
- Zustellungsdienste

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

Konkretisierungen zu Betriebsanforderungen eines Vertrauensdienstes werden, falls gegeben, in den Anhängen A bzw. B des TSPS aufgeführt.

## 5 Nicht-technische Sicherheitsmaßnahmen

Die Nicht-technischen Sicherheitsmaßnahmen für die Vertrauensdienste

- Validierungsdienste und
- Zustellungsdienste

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

Die Gewährleistung geeigneter infrastruktureller, organisatorischer und personeller Sicherheitsmaßnahmen ist eine Voraussetzung für den sicheren Betrieb der Vertrauensdienste. Diese Sicherheitsmaßnahmen sind im TSPS in ihren wesentlichen Grundzügen beschrieben. Detaillierte Informationen hierzu sowie zum Informations- und IT-Sicherheits-Managementprozess sind in einem Sicherheitskonzept festgeschrieben. Darüber hinaus wird regelmäßig eine Risikoanalyse mit Risikobewertung durchgeführt und dokumentiert. Diese werden nicht veröffentlicht, können aber im Rahmen der Konformitätsprüfung eingesehen werden.

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

### 5.1 Infrastrukturelle Sicherheitsmaßnahmen (Physical Controls)

Die infrastrukturellen Sicherheitsmaßnahmen sind für die Vertrauensdienste im TSPS Kapitel 5 beschrieben.

### 5.2 Organisatorische Sicherheitsmaßnahmen

Die Maßnahmen sind im TSPS beschrieben.

### 5.3 Personelle Sicherheitsmaßnahmen

Die Maßnahmen sind im TSPS beschrieben.

### 5.4 Sicherheitsüberwachung

Die Maßnahmen sind im TSPS beschrieben.

### 5.5 Archivierung

Die Maßnahmen zur Archivierung sind im TSPS beschrieben.

### 5.6 Schlüsselwechsel

Nicht anwendbar, da keine Zertifikatserstellung erfolgt.

### 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, die Details dazu sind im TSPS aufgeführt.

## 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-VO, EN 319 401, EN 319 521 oder Technische Richtlinien des BSI).

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

# 7 Profile von Zertifikaten, Sperrlisten und OCSP

Nicht anwendbar.

# 8 Auditierung und andere Prüfungen

Das Governikus Informationssicherheits-Managementsystem (ISMS) ist ein Rahmenwerk für die systematische Steuerung von Informationssicherheitsrisiken. Dieses wird vom TÜV Rheinland gemäß ISO/IEC 27001:2013 auditiert. Der Geltungsbereich umfasst insbesondere den Betrieb der selbstentwickelten und vertriebenen Software. Das Zertifikat ist unter folgender URL abrufbar:

https://www.certipedia.com/companies/590648/system_certificates?locale=de

Für das Jahr 2024 ist geplant, auch die Zustelldienste und die Validierungsdienste in den Geltungsbereich aufzunehmen.

# 9 Sonstige geschäftliche und rechtliche Regelungen

## 9.1 Gebühren

Die Gebühren für die Nutzung sind der Preisliste der Governikus zu entnehmen.

## 9.2 Finanzielle Verantwortung

Die finanzielle Verantwortung trägt die Geschäftsführung der Governikus.

## 9.3 Vertraulichkeit von Geschäftsdaten

Die Vertraulichkeit wird durch geeignete technische und organisatorische Maßnahmen sichergestellt.

## 9.4 Datenschutz und Personendaten

Die für die Dienste verwendeten personenbezogenen Zertifikate werden ausschließlich für die notwendige Nutzungsdauer gespeichert. Die aktuellen Ansprechpartner für den Datenschutz werden in dem Policy Disclosure Statement benannt.

## 9.5 Gewerblicher Schutz- und Urheberrechte

Regelungen hierzu finden sich in den individuellen Kundenverträgen. In der Regel basieren diese auf den Allgemeinen Geschäftsbedingungen von Governikus, wie etwa den Allgemeinen Servicebedingungen, Besonderen Vertragsbedingungen oder Nutzungsbedingungen. Davon abweichend können insbesondere bei über Ausschreibungen beschaffte Leistungen auch spezielle Bedingungswerke der Auftraggeber zum Tragen kommen.

### 9.6 Gewährleistungsansprüche und Garantien

Wie zu Ziffer 9.5.

### 9.7 Haftungsausschlüsse

Wie zu Ziffer 9.5.

### 9.8 Haftungsbeschränkung

Wie zu Ziffer 9.5.

### 9.9 Schadensersatz

Wie zu Ziffer 9.5.

### 9.10 Laufzeit und Kündigung

Wie zu Ziffer 9.5.

### 9.11 Kommunikation

Wie zu Ziffer 9.5.

### 9.12 Nachträge/Änderungsanträge

Wie zu Ziffer 9.5.

### 9.13 Bestimmungen zur Schlichtung und Konfliktlösung

Wie zu Ziffer 9.5.

### 9.14 Gerichtsstand

Wie zu Ziffer 9.5.

### 9.15 Einhaltung geltenden Rechts

Wie zu Ziffer 9.5.

### 9.16 Sonstige Bestimmungen

Entfällt.

# Anhang A: Validierungsdienst

## Anwendungs- und Geltungsbereich der Policy

Bei dem Validierungsdienst handelt es um einen nichtqualifizierten, normalisierten Signaturzertifikats-validierungsdienst. 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 Signaturzertifikats-validierungsdienst 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.

Weitere Details der Umsetzung sind dem Anhang A des TSPS zu entnehmen.

## Teilnehmer und Akteure der Validierungsdienste

Teilnehmer eines Validierungsdienstes sind

- der Validierungsdienst selbst,
- Kunden (Subscriber) des Validierungsdienstes: natürliche oder juristische Personen, die nach einer Beauftragung des Validierungsdiensts elektronische Signaturzertifikate einreichen.
- Anwender: Anwender sind Anwendungen oder natürliche Personen, die mit dem Validierungsdienst interagieren.
- Vertrauende Dritte (Relying Parties): Dritte, die, ohne Kunde oder Anwender zu sein, auf die Validierungsberichte zuzugreifen und ihnen zu vertrauen können.

## 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.

Weitere Details der Prüfung sind dem Anhang A des TSPS zu entnehmen.

### Interfaces

Weitere Details der Prüfung sind dem Anhang A des TSPS zu entnehmen.

### Signaturvalidierungsbericht

Weitere Details der Prüfung sind dem Anhang A des TSPS zu entnehmen.

### Vertragsbedingungen

Weitere Details zu den Vertragsbedingungen sind den Allgemeinen Vertragsbedingungen und dem Policy Disclosure Statement PDS zu entnehmen.

# Anhang B: Zustelldienste

## Anwendungs- und Geltungsbereich der Policy

Ein Dienst zur Zustellung elektronischer Einschreiben ist nach eIDAS ein elektronischer Dienst, der die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln ermöglicht und einen Nachweis der Handhabung der übermittelten Daten erbringt, darunter den Nachweis der Absendung und des Empfangs der Daten, und der die übertragenen Daten vor Verlust, Diebstahl, Beschädigung oder unbefugter Veränderung schützt.

Bei dem hier beschriebenen Zustelldienst handelt es um einen nichtqualifizierten, normalisierten Dienst im Bereich des elektronischen Rechtsverkehrs. In der Ausprägung beBPo werden die Vorgaben der Justiz umgesetzt. In der Ausprägung eBO werden die Vorgaben der Justiz über die Kommunikation mittels Notare umgesetzt.

## Teilnehmer und Akteure der Zustelldienste

Teilnehmer des Zustelldienstes elektronischer Rechtsverkehr (ERV) sind

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

## Identifizierung und Authentifizierung

Der Zustelldienst der Governikus verifiziert die Identität des Absenders und des Empfängers durch einen Dritten gemäß den Vorgaben der Justiz über eingerichtete Prüfstellen. Nähere Angaben dazu sind dem Annex B des TSPS zu entnehmen.

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.

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

Nähere Angaben dazu sind dem Annex B des TSPS zu entnehmen.

## Betriebsanforderungen

Nähere Angaben dazu sind dem Annex B des TSPS zu entnehmen.

## Ereignisse und Evidenz (Nachweise)

Nähere Angaben dazu sind dem Annex B des TSPS zu entnehmen.