telekom
control

Telekom-Control

Österreichische Gesellschaft für
Telekommunikationsregulierung mbH

Informationen zur Anzeige nach § 6 Abs. 2 SigG

betreffend die Anzeige durch Zertifizierungsdiensteanbieter, die keine qualifizierten Zertifikate anbieten bzw. keine sicheren Signaturverfahren bereitstellen.

Allgemeines

Gemäß § 6 Abs. 2 SigG hat jeder Zertifizierungsdiensteanbieter die Aufnahme seiner Tätigkeit unverzüglich der Aufsichtsstelle (das ist die Telekom-Control-Kommission, Mariahilfer Straße 77–79, 1060 Wien) anzuzeigen. Er hat spätestens mit Aufnahme der Tätigkeit oder bei Änderung seiner Dienste ein Sicherheitskonzept sowie ein Zertifizierungskonzept für jeden von ihm angebotenen Signatur- und Zertifizierungsdienst samt den verwendeten technischen Komponenten und Verfahren vorzulegen.

Im vorliegenden Dokument wollen wir einen Überblick darüber geben, welche Informationen eine solche Anzeige enthalten sollte.

Neben allgemeinen Angaben zum Dienst sind bei der Anzeige vor allem das Sicherheits- und Zertifizierungskonzept von Bedeutung sowie ein Businessplan, der der Aufsichtsstelle eine Abschätzung der finanziellen Leistungsfähigkeit des Anbieters ermöglicht. Bei Anbietern, die keine qualifizierten Zertifikate anbieten, prüft die Aufsichtsstelle nur die Konsistenz der vorgelegten Konzepte und des Businessplans. Es gibt keine Mindestanforderungen an die Sicherheit oder die finanzielle Leistungsfähigkeit des Anbieters – wichtig ist nur, dass das angebotene Sicherheitsniveau im Konzept klar dargestellt ist und der Businessplan in sich stimmig ist, sodass für den angebotenen Dienst und die allfällig damit verbundene Haftung ausreichend Finanzmittel zur Verfügung stehen.

Das Sicherheits- und Zertifizierungskonzept dient der Information der Kommunikationspartner der Signatoren und ist daher öffentlich. Die Konzepte werden daher auch von der Aufsichtsstelle nicht vertraulich behandelt. Soweit Teile des Sicherheitskonzeptes ausnahmsweise vertraulich zu behandeln sind, sind sie als solche zu kennzeichnen. Der Businessplan wird als Betriebs- und Geschäftsgeheimnis des Betreibers von der Aufsichtsstelle vertraulich behandelt.

Allgemeine Angaben

Name des Zertifizierungsdiensteanbieters, Adressen (Tel., Fax, E-Mail, WWW), evtl. Firmenbuchnummer

Bezeichnung des Dienstes

> *Anmerkung: Gemäß § 6 Abs. 2 SigG ist „jeder" Signatur- und Zertifizierungsdienst anzuzeigen. Die Abgrenzung verschiedener Dienste desselben ZDA kann im Einzelfall schwierig sein. Einige Anhaltspunkte:*
>
> *Liegen sicherheitsrelevante Unterschiede vor – insbesondere hinsichtlich der Modalitäten der Identitätsprüfung –, so handelt es sich im Zweifel eher um verschiedene Dienste als um einen. Der Kommunikationspartner des Signators setzt sein Vertrauen in einen bestimmten Dienst. Bei verschiedenen Sicherheitsniveaus innerhalb desselben Dienstes muss er sich bei seiner Entscheidung am niedrigsten möglichen Sicherheitsniveau orientieren, weshalb diese Entscheidungen nicht sinnvoll sind.*
>
> *Die Vertrauensentscheidung des Kommunikationspartners des Signators (K) orientiert sich wahrscheinlich in den meisten Fällen an den vom ZDA verwendeten Schlüsseln. Wenn Ks Software mit einem neuen, unbekannten Schlüssel konfrontiert wird, wird K zur Entscheidung aufgefordert werden, diesen Schlüssel nicht, im Einzelfall oder dauerhaft zu akzeptieren. Bei einer Entscheidung, den Schlüssel dauerhaft zu akzeptieren, wird die Software bei künftigen Zertifikaten, die mit diesem Schlüssel erstellt wurden, K nicht mehr zur Entscheidung auffordern. Es ist daher empfehlenswert, Zertifikate verschiedener Dienste mit verschiedenen Schlüsseln zu signieren.*

Angaben über bereits erfolgte oder mögliche spätere Änderungen des Sicherheits- und Zertifizierungskonzeptes

Anmerkung: Der Kommunikationspartner des Signators will das Sicherheits- und Zertifizierungskonzept nicht in jedem Einzelfall prüfen, sondern eine dauerhafte Vertrauensentscheidung fällen. Erhöht der ZDA das Sicherheitsniveau eines Dienstes zu einem bestimmten Zeitpunkt, so muss aus dem Konzept mit aller Deutlichkeit hervorgehen, dass Zertifikate, die vor dem Zeitpunkt der Änderung ausgestellt wurden, niedrigeren Sicherheitsanforderungen unterlagen. Bei einer Senkung des Sicherheitsniveaus würden die zuvor getroffenen Vertrauensentscheidungen gefährdet. Es wird daher empfohlen, spätere inhaltliche Änderungen im Sicherheits- und Zertifizierungskonzept explizit auszuschließen. Eine Änderung des Konzepts wird sinnvollerweise so vorgenommen, dass der Dienst eingestellt und unter neuem Namen ein anderer Dienst mit anderen Signaturerstellungsdaten aufgenommen wird.

Allgemeine Angaben zum Umfang der Haftung, die vom ZDA im Rahmen dieses Dienstes übernommen wird.

Anmerkung: ... soweit der ZDA darüber überhaupt disponieren kann

Absicherung dieser Haftung:

- Businessplan (siehe separate Excel-Tabelle)

  Anmerkung: Der Businessplan bezieht sich nur auf die Zertifizierungs- und Signaturdienste des Anbieters, nicht auf das Gesamtunternehmen. Wenn der Anbieter z. B. die Zertifikate gratis als Zugabe zu einem anderen Produkt anbietet, wird der Businessplan ausschließlich Aufwendungen, aber keine Erträge aufweisen.

- Angaben über eine evtl. abgeschlossene Haftpflichtversicherung

Checkliste zum Zertifizierungskonzept und zu signaturspezifischen Fragen des Sicherheitskonzeptes

Einleitung

Kernbestandteil der Anzeige nach § 6 Abs. 2 SigG ist das Sicherheits- und das Zertifizierungskonzept, das vom Anbieter für jeden von ihm angebotenen Signatur- und Zertifizierungsdienst samt den verwendeten technischen Komponenten und Verfahren vorzulegen ist.

Eine bestimmte Gliederung der Angaben ist vom SigG nicht vorgeschrieben. Die folgende Checkliste gibt ein mögliches Schema vor, nach dem die Anforderungen des SigG geprüft werden können. Die Checkliste orientiert sich dabei an den sicherheitsrelevanten Bestimmungen des SigG und des Entwurfs zur SigVO. Neben den signaturspezifischen Fragen soll das Sicherheitskonzept aber auch Fragen der allgemeinen IT-Sicherheit abdecken.

Die meisten Bestimmungen des SigG und der SigVO sind auf Anbieter qualifizierter Zertifikate oder sicherer Signaturverfahren zugeschnitten. Auf andere Anbieter werden die Fragen daher zum Teil nicht zutreffen. Das SigG verlangt von Zertifizierungsdiensteanbietern kein bestimmtes Sicherheitsniveau – solange die Zertifikate nicht als „qualifizierte Zertifikate“ und die Signaturverfahren nicht als „sichere“ Signaturverfahren im Sinne des SigG bezeichnet werden. Wichtig ist vor allem, dass das vom Anbieter für den konkreten Dienst

vorgesehene Sicherheitsniveau aus dem Sicherheits- und Zertifizierungskonzept klar und deutlich hervorgeht.

Bei der Formulierung einer Anzeige nach § 6 Abs. 2 SigG – insbesondere bei der Abfassung eines Sicherheits- und Zertifizierungskonzepts – sollten die Interessen der Adressaten dieser Texte maßgeblich sein:

- Hauptadressaten sind die Kommunikationspartner der Signatoren. Der Empfänger einer signierten Nachricht muss anhand des Sicherheits- und Zertifizierungskonzepts eine Entscheidung treffen können, ob er dem Zertifikat vertraut. Wie prüft der ZDA die Identität des Signators? Inwieweit sind die vom ZDA eingesetzten technischen Verfahren sicher (falsche Zertifikate, falsche oder unaktuelle Verzeichnisdienste etc.)? Inwieweit übernimmt der ZDA auch Verantwortung für die vom Signator eingesetzten technischen Komponenten und Verfahren? Wie sind allfällige Haftungsansprüche abgesichert. – Zu bedenken ist insbesondere auch, dass der Kommunikationspartner des Signators das Sicherheits- und Zertifizierungskonzept nicht bei jedem einzelnen Geschäftsfall prüfen will. Vielmehr soll das Konzept für ihn geeignet sein, eine dauerhafte Entscheidung zu treffen, ob er Zertifikaten aus diesem Dienst vertraut.

- Die Signatoren selbst sind von allfälligen Mängeln beim ZDA oft nur mittelbar betroffen. Wird einem Dritten ein falsches Zertifikat ausgestellt, dann betrifft das den ehrlichen Signator, der ein echtes Zertifikat besitzt, nur indirekt: Die Glaubwürdigkeit des ZDA und damit der Wert des eigenen Zertifikates sinkt. Für den Signator kann aber z. B. ein rascher und zuverlässiger Widerruf des eigenen Zertifikates auch unmittelbar bedeutsam sein.

- Die Aufsichtsstelle hat die Interessen der Signatoren und ihrer Kommunikationspartner im Rechts- und Geschäftsverkehr zu wahren.

Technische Verfahren

Überblick über die – im folgenden zum Teil noch näher angesprochenen – Verfahren und Standards:

Datenformat des Zertifikats (z. B. X.509v3)

Verwendetes Hashverfahren (z. B. RIPEMD-160, SHA-1)

Verwendetes Verfahren zur Signaturerstellung (z. B. RSA), Schlüssellänge in Bit

Signaturprüfdaten (öffentlicher Schlüssel, evtl. Fingerprint des Schlüssels oder eines bestehenden, z. B. selbst signierten Zertifikates)

Formate bzw. Protokolle für Verzeichnis- und Widerrufsdienste

Zertifizierungskonzept

Datenformat des Zertifikats (z. B. X.509v3)

Angaben zu den Datenfeldern im Zertifikat. Welche der folgenden Felder sind vorhanden? Gibt es Besonderheiten bei der Codierung?

- Name des ZDA, Staat seiner Niederlassung

- Name des Signators / Pseudonym (Welcher Zeichensatz kommt für den Namen des Signators in Frage, wie geht der ZDA mit Namen anderer Schriftsysteme um, wie sind Pseudonyme gekennzeichnet?)
- Angaben über eine Vertretungsmacht oder andere rechtlich relevante Eigenschaften des Signators
- Beginn und Ende der Gültigkeit des Zertifikats (Gültigkeitszeitraum)
- eindeutige Kennung des Zertifikats
- gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats
- gegebenenfalls eine Beschränkung des Transaktionswertes, auf den das Zertifikat ausgestellt ist
- andere Angaben?

Wie werden die Angaben im Zertifikat überprüft? Für die Richtigkeit welcher Angaben haftet der ZDA in welchem Ausmaß (vgl. § 23 SigG)?

Überprüfung der Identität des Signators:

- Beschreibung des Verfahrens zur Identitätsprüfung
- Wenn Zertifikate auch an andere als an natürliche Personen ausgestellt werden (z. B. Serverzertifikate):
  - An wen werden die Zertifikate ausgestellt (z. B. juristische Personen, Behörden)?
  - Was kann als Name des Signators im Zertifikat eingetragen werden?
  - Wie wird die Zuordnung des Zertifikates zum Signator geprüft (Vertretungsmacht, Besitz der Signaturerstellungsdaten)?
- Wird die Identitätsprüfung vom ZDA selbst oder von Registrierungsstellen vorgenommen?
  - Evtl. Angaben darüber, welche Registrierungsstellen es gibt bzw. wie die Registrierungsstellen ausgewählt werden.
  - Anforderungen an das Personal der Registrierungsstellen

Überprüfung anderer Eigenschaften des Signators:

- Implizite Eigenschaften: Ist der Kreis der Personen, an die Zertifikate ausgestellt werden, beschränkt?
- Beschreibung des Verfahrens, mit dem die anderen Eigenschaften überprüft werden

Sicherheitskonzept

Signaturerstellungsdaten

Die folgenden Fragen beziehen sich auf die Signaturerstellungsdaten des ZDA. Wenn z. B. für die Zertifizierung, Widerrufslisten und einen Zeitstempeldienst unterschiedliche Signaturerstellungsdaten verwendet werden, ist dieser Abschnitt evtl. mehrfach anzuwenden.

Angaben zur Erzeugung der Signaturerstellungsdaten

- Angaben zur Zufallsqualität (technischer Zufall – eigene Hardwareeinrichtung, signatorbezogener Zufall – z. B. Mausbewegungen, Pseudozufallszahlen, ...)? Wird der Zufall auf seine statistische Zufallsqualität geprüft?

- Werden die Signaturerstellungsdaten außerhalb jener Komponente erzeugt, in der sie gespeichert werden?

Angaben zur Speicherung der Signaturerstellungsdaten (z. B. in einer dezidierten Hardware, die sie niemals verlassen, auf einem auslesbaren Datenträger, auf der Festplatte). Gibt es ein Backup der Signaturerstellungsdaten?

Angaben zum Zugriffsschutz auf die Signaturerstellungsdaten (z. B. Verschlüsselung der Signaturerstellungsdaten, Autorisierungscodes, Verteilung der Signaturerstellungsdaten oder der Autorisierungscodes auf mehrere Personen, ...)

- Erfolgt die Zertifizierung online oder offline?

Angaben zur Lebensdauer der Signaturerstellungsdaten.

Zertifizierungsvorgang

Erfolgt die Erstellung und Anzeige des Zertifikates
– in einer dezidiert dafür eingesetzten und abgeschlossenen Hardwareeinheit
– auf einem dezidiert für Zertifizierungszwecke gewidmeten Rechner
– auf einem Rechner, der auch der Verwaltung der Signatoren dient
– auf einem Rechner, der auch für andere Aufgaben eingesetzt wird?

Erfolgt die Hashgenerierung über das vorbereitete Zertifikat
– in einer dezidiert dafür eingesetzten und abgeschlossenen Hardwareeinheit
– auf einem dezidiert für Zertifizierungszwecke gewidmeten Rechner
– auf einem Rechner, der auch der Verwaltung der Signatoren dient
– auf einem Rechner, der auch für andere Aufgaben eingesetzt wird?

Erfolgt die Anwendung der Signaturerstellungsdaten auf den Hashwert
– in einer dezidiert dafür eingesetzten und abgeschlossenen Hardwareeinheit
– auf einem dezidiert für Zertifizierungszwecke gewidmeten Rechner
– auf einem Rechner, der auch der Verwaltung der Signatoren dient
– auf einem Rechner, der auch für andere Aufgaben eingesetzt wird?

Welcher Personenkreis kann einen Zertifizierungsvorgang vornehmen? Gibt es ein Vieraugenprinzip? Ist dieses technisch abgesichert?

Verzeichnis- und Widerrufsdienste

Verzeichnisdienste

Wird ein Verzeichnisdienst angeboten? Ist dieser 24 Stunden / 7 Tage in der Woche zugänglich? Angaben, wie Ausfallssicherheit gewährleistet ist, evtl. Angaben über Mindestverfügbarkeiten, für die der ZDA haftet.

Protokolle, über die auf den Verzeichnisdienst zugegriffen werden kann (z. B. LDAP, HTTP). Adresse (URL, X.400) des Verzeichnisdiensts. Wird eine Spezialsoftware benötigt? Ist diese vom ZDA (kostenfrei?) erhältlich?

Ist der Kreis der zugriffsberechtigten Personen eingeschränkt?

Ist der Abruf entgeltfrei?

Hat der Signator eine Möglichkeit, den Zugriff auf sein Zertifikat einzuschränken?

Widerrufsdienste

Wird ein Widerrufsdienst angeboten?

Welche Möglichkeiten bestehen, einen Widerruf einzuleiten?
– Ist ein selbst signierter Antrag auf Widerruf möglich?
– Welche Möglichkeiten bestehen bei Verlust der Signaturerstellungsdaten (z. B. telefonischer Widerruf mittels Angabe einer Transaktionsnummer)?
– Widerruf durch einen Vertreter oder Rechtsnachfolger (z. B. im Todesfall)?

Zu welchen (Geschäfts-)Zeiten können die jeweiligen Widerrufsmöglichkeiten vorgenommen werden? Wie lange ist jeweils die maximale Dauer bis zur Veröffentlichung des Widerrufs?

Welcher Personenkreis kann einen Widerrufsvorgang vornehmen? Gibt es ein Vieraugenprinzip? Ist dieses technisch abgesichert?

Formate des Widerrufsdienstes (Widerrufslisten), Protokolle, über die darauf zugegriffen werden kann (z. B. LDAP, HTTP). Adresse (URL, X.400) des Widerrufsdiensts. Wird eine Spezialsoftware benötigt? Ist diese vom ZDA (kostenfrei?) erhältlich?

Wenn Certificate Revocation Lists eingesetzt werden: In welchen Zeitabständen werden diese maximal aktualisiert. Erfolgt eine Aktualisierung im Anlassfall?

Zeitstempeldienste

Werden Zeitstempeldienste angeboten? Werden Zeitstempeldienste für eigene Zwecke (Zertifikatserzeugung oder Widerrufsdienst) eingesetzt?

Auf welchen Zeitgeber greift der Zeitstempeldienst zurück (z. B. Funksignal DCF 77)?

Maßnahmen gegen einen Ausfall oder eine Kompromittierung der Verbindung zum Zeitgeber: Nachlaufgenauigkeit der Systemuhr? Plausibilitätsprüfung durch einen zweiten Zeitgeber?

Insgesamt gewährleistete Ganggenauigkeit des Zeitstempeldienstes

Angaben zur allgemeinen IT-Sicherheit

Durch welche Maßnahmen ist der Schutz vor unbefugtem Zutritt gewährleistet?
– zu den jeweils eingesetzten Signaturerstellungsdaten
– zu den für die Zertifizierung eingesetzten technischen Komponenten
– zu den für den Verzeichnisdienst eingesetzten technischen Komponenten
– zu den für den Widerrufsdienst eingesetzten technischen Komponenten

Durch welche Maßnahmen ist der Schutz vor unbefugtem Zugriff gewährleistet?
– unbefugte Zugriffe von außen, z. B. über das Internet
– unbefugte Zugriffe von innen, z. B. durch Mitarbeiter

Wenn die Identitätsprüfung über Registrierungsstellen durchgeführt wird: Wie wird der Datenverkehr zwischen den Registrierungsstellen und der Zertifizierungsstelle gesichert?

Schutz vor Elementarereignissen (Feuer, Wasser, Stromausfall, ...)

Schutz vor Datenverlust (z. B. Angaben zur Backupstrategie)

Technische Komponenten beim Signator

Anmerkung: Die Sicherheit der Komponenten beim Signator ist in erster Linie für diesen selbst wichtig. Aber auch der Kommunikationspartner des Signators (K) ist daran interessiert. Stellt der ZDA im Rahmen eines bestimmten Dienstes Zertifikate nur an Personen aus, die eine bestimmte sichere Technologie – z. B. eine Chipkarte –einsetzen, dann kann K darauf vertrauen, dass auch diese sichere Technologie verwendet wurde.

Gerade im Bereich der nicht qualifizierten Zertifikate wird es für den ZDA aber oft unerheblich sein, welche Komponenten der Signator einsetzt. Der ZDA stellt daher z. B. auch für Schlüssel, die auf schlechter Zufallsqualität beruhen, Zertifikate aus, da er über die Schlüsselgenerierung keine oder keine verlässlichen Informationen hat. Ein ZDA, der z. B. Zertifikate für Netscape oder Internet Explorer ausstellt, weiß zwar aufgrund des HTTP-Verbindungsaufbaus, mit welchem Browser der Signator arbeitet. Er kann aber nicht nachprüfen: ob es sich nicht um einen anderen Browser handelt, der sich als Netscape ausgibt; ob der Signator ein bestimmtes Kryptographiemodul verwendet; ob das RSA-Verfahren in diesem sorgfältig implementiert wurde etc. Der ZDA will wahrscheinlich dafür auch keine Verantwortung übernehmen.

Ist die Ausstellung von Zertifikaten an den Einsatz einer bestimmten Hardware oder Software gebunden, die vom ZDA bereitgestellt oder empfohlen wird, oder kann der Signator von ihm selbst in beliebiger Weise generierte Signaturerstellungsdaten zertifizieren lassen, solange er nur ein geeignetes Format (z. B. PKCS#10) verwendet?

Wenn vom Signator selbst in beliebiger Weise generierte Signaturerstellungsdaten zertifiziert werden: In welcher technischen Form stellt der Signator seinen Antrag (z. B. PKCS #10 oder Bezeichnung und Versionsnummer der unterstützten Browser)? Ist die Verwendung eines bestimmten Signaturverfahrens (z. B. RSA) oder einer bestimmten Schlüssellänge Bedingung für die Ausstellung des Zertifikates?

Wenn eine bestimmte Hardware oder Software Bedingung für die Ausstellung eines Zertifikates ist:

- Erzeugung der Signaturerstellungsdaten:

  - Werden die Signaturerstellungsdaten durch den ZDA erzeugt und dem Signator übergeben? Ist in diesem Fall sichergestellt, dass keine Kopie der Signaturerstellungsdaten beim ZDA verbleibt? Oder bewahrt der ZDA ein Backup der Signaturerstellungsdaten auf?

  - Erfolgt die Erzeugung der Signaturerstellungsdaten in einer vom ZDA dem Signator bereitgestellten Hardware (z. B. Chipkarte)?

  - Angaben zur Zufallsqualität (technischer Zufall – eigene Hardwareeinrichtung, signatorbezogener Zufall – z. B. Mausbewegungen, Pseudozufallszahlen, ...)? Wird der Zufall auf seine statistische Zufallsqualität geprüft?

- Speicherung der Signaturerstellungsdaten: In einer eigenen Hardware, die sie niemals verlassen? Auf einem auslesbaren Datenträger (Diskette oder Speicherkarte)? Auf der Festplatte im PC des Signators?

- Wie erfolgt die Auslösung des Signaturvorgangs (z. B. PIN-Eingabe)? Kann der Benutzer die Autorisierungscodes frei wählen oder verändern? Gibt es Eingabeerleichterungen für die Autorisierungscodes oder sind diese ausgeschlossen?

- Erfolgt die Generierung des Hashwertes in einer vom ZDA bereitgestellten Hardware oder Software?

- Erfolgt die Anwendung der Signaturerstellungsdaten auf den Hashwert in einer vom ZDA bereitgestellten Hardware oder Software?

- Ist vorgesehen, dass die Signaturschlüssel auch für Verschlüsselung oder Authentifizierung verwendet werden können? Oder werden dem Signator separate Verschlüsselungs- und/oder Authentifizierungsschlüssel zur Verfügung gestellt?

- Sind die signierbaren Datenformate beschränkt – auf welche Formate? Sind dynamische Veränderungen oder Unsichtbarkeiten in diesen Datenformaten ausgeschlossen? Stellt der ZDA Hardware oder Software bei, die sichere Datenformate generiert, Datenformate auf dynamische Veränderungen oder Unsichtbarkeiten prüft oder die gesicherte Anzeige der zu signierenden ermöglicht? Kommuniziert diese Hardware oder Software in gesicherter Form mit der Signaturerstellungseinheit?

Evaluierungen

Verpflichtet sich der ZDA im Sicherheitskonzept dazu, selbst technische Komponenten oder Verfahren einzusetzen, die evaluiert sind? Um welche Komponenten handelt es sich? Nach welchen Kriterien wurde evaluiert?

Sind die vom ZDA allenfalls dem Signator zur Verfügung gestellten Komponenten oder Verfahren evaluiert? Nach welchen Kriterien?

Adressen

Ihre Ansprechpartner bei der Telekom-Control GmbH in Fragen der elektronischen Signatur:

- Dieter Kronegger (für rechtliche und organisatorische Fragen), 01/58058-407, dieter.kronegger@tkc.at
- Gernot Fuchs (für technische Fragen), 01/58058-306, gernot.fuchs@tkc.at

- Martin Pahs (für wirtschaftliche Fragen, insbesondere zum Businessplan), 01/58058–503, martin.pahs@tkc.at

Telekom-Control GmbH, Mariahilfer Straße 77–79, 1060 Wien