

# T-Systems Root Signing

## Leistungsbeschreibung

### 1 Allgemeines

Mit „T-Systems Root Signing“ bietet T-Systems eine Lösung für Institutionen und Unternehmen (im Folgenden: Kunde) an, die ihre eigenen Server- und Clientzertifikate anbieten und verwalten wollen.

Dabei wird der öffentliche Schlüssel des neuen Wurzelzertifikates des Kunden durch eine Zertifizierungsstelle (CA) der Deutschen Telekom (hier: „Deutsche Telekom Root CA 2“) signiert. Die CA des Kunden wird damit zur Sub-CA der Deutschen Telekom.

Das verwendete CA-Zertifikat der Deutschen Telekom ist bereits jetzt in den Root-Certificate-Stores der Browser Internet Explorer (und damit im gesamten Microsoft Windows Umfeld), Opera und Safari enthalten<sup>1</sup>.

Durch Verkettung der CA der Deutschen Telekom und der CA des Kunden wird erreicht, dass auch die vom Kunden ausgegebenen Zertifikate an ihre jeweiligen End-Teilnehmer von den oben genannten Plattformen als vertrauensvoll anerkannt werden – lästige und Verunsicherung streuende Warnhinweise entfallen.

Die Anforderungen an die Sicherheit der Sub-CAs in infrastruktureller, technischer und organisatorischer Hinsicht sind sehr anspruchsvoll und werden in diesem Dokument näher beschrieben.

### 2 Leistungen von T-Systems

Die Leistung von T-Systems setzt sich aus einmaligen und laufenden Bestandteilen zusammen.

(1) Einmalige Leistungen:

1. T-Systems stellt dem Kunden durch die "Deutsche Telekom Root CA 2" ein Zertifikat für den öffentlichen Schlüsselteil des neuen Wurzelzertifikats des Kunden mit einer einzelvertraglich festzulegenden Gültigkeit (maximal jedoch bis zum Jahr 2019) aus. Zu diesem Zweck stellt der Kunde einen PKCS#10 Zertifikats-Request zur Verfügung, der in Form eines Datenträgers durch autorisierte Mitarbeiter des Kunden im Rahmen eines noch abzustimmenden Prozesses am Standort von T-Systems an autorisierte Betriebskräfte des Trust Centers übergeben wird. Das Zertifikat wird nach der Generierung durch die "Deutsche Telekom Root CA 2" in Form eines Datenträgers mit einer PKCS#7 Datei an die autorisierten Mitarbeiter des Kunden unmittelbar übergeben. Die beschriebene Leistung gilt nur für ein Wurzelzertifikat des Kunden, das dem durch T-Systems vorgegebenen Sicherheitsniveau entspricht.

(2) Laufende Leistungen:

1. T-Systems führt jährliche Audits der CA-Umgebung des Kunden durch, um die Einhaltung der vereinbarten Policies zu überprüfen (Vor-Ort-Termine werden typischerweise nicht länger als einen Tag in Anspruch nehmen). Alle Prüfungsergebnisse werden dem Kunden mitgeteilt und vertraulich behandelt.
2. T-Systems stellt einen öffentlich zugänglichen Sperrservice für CA-Zertifikate in Form einer "Authority Revocation List (ARL)" zur Verfügung. Diese ARL wird alle sechs Monate oder unmittelbar im Falle der Sperrung einer CA erneuert und mittels einer redundanten LDAP Schnittstelle öffentlich zugänglich gemacht.
3. T-Systems informiert den Kunden umgehend, sobald der Verdacht einer Kompromittierung seiner CA-Umgebung besteht.

---

<sup>1</sup> Eine Integration in die Browserreihen von Mozilla wird angestrebt.

### 3 Mitwirkung und Pflichten des Kunden

- (1) Der Kunde verpflichtet sich, seine CA-Policy (damit sind gemeint: Certification Practice Statement und Certificate Policy) an T-Systems zu übergeben, damit T-Systems die Vereinbarkeit der Policy mit der eigenen Policy überprüfen kann.
- (2) Der Kunde darf Zertifikate nur im Rahmen seiner definierten Tätigkeit ausstellen.
- (3) Die CP/CPS des Kunden beschreibt, das zusätzlich zur Identitätsprüfung von Individuen und Organisationen, angemessene Maßnahmen ergriffen werden, um sicher zu stellen, dass der Antragsteller die im Zertifikat referenzierte Domäne bzw. E-Mail-Adresse besitzt und/oder kontrolliert.
- (4) Die Root-CA des Kunden und alle Sub-CAs werden während der gesamten Gültigkeitsdauer des ausgestellten Zertifikats in den zu definierenden Räumlichkeiten und der Umgebung des Kunden gemäß der Policy des Kunden betrieben. Um ein einheitliches Sicherheitsniveau zu gewährleisten, die jährlichen Audits der CA-Umgebung zu erleichtern und um den Anforderungen der regelmäßigen Verlängerung der Webtrust Zertifizierung zu genügen, darf von dieser Maßgabe nur im Ausnahmefall abgewichen werden. Etwaige Änderungen bedürfen in jedem Fall einer Abstimmung mit T-Systems. Eine erneute Prüfung durch T-Systems ist dann obligatorisch. Die Kosten dafür sind durch den Kunden zu tragen.
- (5) Der Kunde gewährleistet die Sicherheit seiner CA-Umgebung während der gesamten Gültigkeitsdauer des ausgestellten Zertifikats.
- (6) Der zu signierende CA-Schlüssel des Kunden wird in einem Hardware Security Modul (HSM) erzeugt und gespeichert. Die Schlüsselpaare der davon abgeleiteten Sub-CAs werden in HSM erzeugt und gespeichert, davor erzeugte Schlüsselpaare befanden sich zu keinem Zeitpunkt auf einem an das Internet angeschlossene Endgerät und werden in HSM gespeichert.
- (7) Der Kunde gewährleistet, dass der Datenträger, der im Rahmen von Nummer 2 Abs. 1 Ziffer 1 zur Verfügung gestellt wird, inhaltlich und technisch einwandfrei ist und verpflichtet sich, diesen vor Übergabe an T-Systems dahingehend zu untersuchen.
- (8) Der Kunde muss erklären, dass das Schlüsselpaar der relevanten Root-CA des Kunden unter seiner alleinigen Kontrolle stand und steht.
- (9) Der Kunden informiert T-Systems über geplante sicherheitsrelevante Änderungen der CA-Umgebung und Services, um T-Systems eine Prüfung der Übereinstimmung mit der CA-Policy des Telekom Trust Centers zu ermöglichen. Im Falle von Abweichungen wird der Kunde die geplanten Maßnahmen nicht ohne Zustimmung durchführen.
- (10) Der Kunden verpflichtet sich, einen Maßnahmenkatalog aufzustellen, in dem aufgezeigt wird, wie eine Kompromittierung der CA bei dem Kunden verhindert werden soll. Änderungen der Maßnahmen, z.B. um diese dem Stand der Technik anzupassen, werden vom Kunden rechtzeitig bekannt gegeben und mit T-Systems abgestimmt. Die Mindestanforderungen werden in (11) dargelegt.
- (11) Die Mindestanforderungen an die vom Kunden zu treffenden Maßnahmen werden im Folgenden dargestellt:
  1. Berechtigungskonzept (Physical and Environmental Security and System Access Management)
    - a. In einem Berechtigungs- und Rollenkonzept müssen Rollen und deren jeweiligen Berechtigungen definiert sein. Ferner müssen die Personen, welche die Rollen ausüben, dargelegt werden.
    - b. Es muss zu jeder Zeit sichergestellt sein, dass nur berechtigte Mitarbeiter Zugriff auf schützenswerte Dokumente und kritische Systeme haben.
    - c. Der Zugriff auf kritische Systeme im Kernbereich des Trust Centers darf nur im 4-Augen-Prinzip erfolgen.
    - d. Sollte der Zutritt eines geschützten Bereichs von Dritten nötig sein (z.B. bei Wartungsarbeiten), so darf dieser nur im Beisein von berechtigtem Personal erfolgen.
    - e. Die Produktion von Smart cards sowie der Druck und Versand von PIN-Briefen darf nur von zuverlässigen und qualifizierten Registrierungsstellenmitarbeitern erfolgen.

2. Bauliche Maßnahmen
  - a. Baulich getrennter und abgeschlossener Bereich (Trust Center-Bereich).
  - b. Das Gebäude oder der Gebäudeteil, in welchem die CA des Kunden untergebracht ist, muss permanent gegen unbefugten Zutritt gesichert sein.
  - c. Verstärkung von Wänden und Türen.
3. Einbruchmeldeanlage und Zugangsregelung
  - a. Zutrittskontrolle zum Trust Center mit Umsetzung/Unterstützung der in 1a) definierten Rollen.
  - b. Einbruchmeldeanlage mindestens bestehend aus
    - i. Türsensoren
    - ii. Fenstersensoren
    - iii. Bewegungsmeldern
  - c. Meldungen laufen bei einem Sicherheitsdienst auf, der innerhalb einer definierten Reaktionszeit eine Vorortüberprüfung durchführt (der Zutritt zum Kernbereich des Trustcenters erfolgt dabei nur unter Wahrung des 4-Augen Prinzips).
4. Brandmeldeanlage
  - a. Brandmeldeanlage mit automatischer Alarmierung des Sicherheitsdienstes.
5. Videoüberwachung
  - a. Von kritischen Bereichen (des Kernbereichs des Trust Centers).
  - b. Optional Eingangsbereichen.
6. Siegel-Etiketten
  - a. Durch die Verwendung und Verwaltung von Siegel-etiketten muss die Unversehrtheit von Hardwarekomponenten jederzeit nachweisbar sein.
7. Safes
  - a. Schützenswerte Dokumente, Datenträger, Hardware, Software o.ä. müssen in Safes gelagert werden.
8. HSMs (Key Life Cycle Management Controls)
  - a. Schlüssel der Root-CA des Kunden  
Der Schlüssel der Root-CA ist in einer Root-Key-Zeremonie zu erstellen und auf einem HSM zu speichern. Sicherungskopien der Schlüssel müssen in Safes und/oder bei Notaren hinterlegt werden. Ein Zugriff auf die Schlüssel darf nur im 4-Augen-Prinzip möglich sein.
  - b. Schlüssel der Sub-CAs des Kunden  
Die Schlüssel der Sub-CAs müssen ebenfalls auf HSMs gespeichert werden.
9. Infrastruktur – Netzwerk (System Access Management)
  - a. Ein hohes Sicherheitsniveau der Netzwerkinfrastruktur muss in einem Konzept dargelegt und entsprechend umgesetzt sein.

## 4 Kompromittierung der CA des Kunden

(1) Für T-Systems ist es von besonderer Wichtigkeit, dass eine Kompromittierung der CA vermieden wird. Eine Kompromittierung liegt nach Ansicht von T-Systems vor, wenn unter Verwendung des gültigen geheimen Schlüssels der CA des Kunden durch unbefugte Dritte ein Zertifikat ausgestellt wurde oder wenn unbefugte Dritte über notwendigen Daten zur Kompromittierung der CA des Kunden verfügen.

(2) Im Fall eines Verdachts der Kompromittierung oder im Fall der tatsächlichen Kompromittierung sollen der Kunde und T-Systems zur Aufklärung beizutragen. Hierbei soll insbesondere auch die Einbindung eines unabhängigen und fachkundigen Dritten (zum Beispiel "TÜV IT") beitragen.

(3) Der Kunden muss T-Systems umgehend informieren, sobald der Verdacht einer Kompromittierung oder eine Kompromittierung der CA des Kunden besteht.

(4) Für den Fall eines Verdachts der Kompromittierung oder einer Kompromittierung der CA des Kunden entscheidet T-Systems, ob das CA-Zertifikat des Kunden in die Authority Revocation List der "Deutsche Telekom Root CA 2" eingetragen und die Sperrung anderweitig veröffentlicht wird.

## 5 Abstimmung und Zusammenarbeit

(1) Die Parteien prüfen gegenseitig ihre CA Policies und stimmen diese ab. Änderungen dieser CA Policies müssen von T-Systems bzw. vom Kunden rechtzeitig bekannt gegeben und abgestimmt werden. T-Systems ist zu der Abstimmung nur verpflichtet, sofern diese Änderungen Auswirkungen auf die CA Policies des Kunden haben. Die Pflicht zur Bekanntgabe bleibt hiervon unberührt.

(2) Stellt sich im Verlauf der von T-Systems angestrebten Webtrust-Zertifizierung heraus, dass dies zu erhöhten Anforderungen an die Betriebsumgebung des Kunden führt, strebt T-Systems eine enge und vertrauensvolle Zusammenarbeit über deren Implementierung an. Sollte der Kunde diesen erhöhten Anforderungen nicht entsprechen, und T-Systems deswegen die Webtrust-Zertifizierung nicht erreichen, ist T-Systems zur außerordentlichen Kündigung berechtigt. Der Kunde ist seinerseits zur außerordentlichen Kündigung berechtigt, wenn der zur Erreichung der Anforderungen notwendige Aufwand unverhältnismäßig ist

## 6 Vertraulichkeit

T-Systems und der Kunde werden alle gegenseitig erlangten und als vertraulich gekennzeichneten Informationen vertraulich behandeln. Dies bezieht sich auch auf Informationen, die bereits im Rahmen der Diskussion über eine Zusammenarbeit weitergegeben worden sind.