Abgeordnetenhaus BERLIN

Drucksache 19 / 14 238
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

der Abgeordneten Franziska Brychcy und Tobias Schulze (LINKE)

vom 08. Dezember 2022 (Eingang beim Abgeordnetenhaus am 09. Dezember 2022)

zum Thema:

Sichere Übermittlung von Certificate Authority (CA)-Zertifikaten der Public-Key-Infrastruktur (PKI) der Berliner Verwaltung

und **Antwort** vom 20. Dezember 2022 (Eingang beim Abgeordnetenhaus am 23. Dez. 2022)

Senatsverwaltung für Inneres, Digitalisierung und Sport
Stab Landes-InfSiBe / V IKT-Sic Ju

Frau Abgeordnete Franziska Brychcy (LINKE) und Herrn Abgeordneten Tobias Schulze (LINKE)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/14238
vom 08.12.2022
über Sichere Übermittlung von Certificate Authority (CA)-Zertifikaten der Public-Key-Infrastruktur (PKI) der Berliner Verwaltung

---

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Vorbemerkung:
Zertifikate bestehen aus drei Teilen: Inhaltsdaten, dem öffentlichen Schlüssel des Zertifikatsinhabenden sowie einer kryptografischen, digitalen Signatur. Die Signatur wird bei Endzertifikaten durch die übergeordnete Zertifizierungsstelle (CA) und bei der Wurzelzertifizierungsstelle (Root-CA) durch sich selbst an ein Zertifikat angebracht. Die Signatur hat zwei Aufgaben: Den/die InhaberIn ausweisen sowie zu gewährleisten, dass die Inhaltsdaten nicht verändert wurden. Die Inhaltsdaten und die Signatur werden durch einen Prüfenden, z.B. den Webbrowser beim Aufruf einer Webseite, durch kryptografische Mechanismen geprüft. Gibt es hier Diskrepanzen, wird das Zertifikat als ungültig eingestuft.

Zertifikate sind per Design digital signiert und dadurch vor Manipulation geschützt. Es ist daher aus Sicht des Manipulationsschutzes nicht notwendig, die Zertifikatsdateien verschlüsselt zu transportieren. Der relevante RFC (Request for Comments) warnt ausdrücklich davor, den Zertifikatsabruf über HTTPS bereitzustellen, da bei der Zertifikatsprüfung zirkuläre Abhängigkeiten entstehen können (https://www.rfc-editor.org/rfc/rfc5280).

Die privaten Schlüssel der durch das ITDZ Berlin betriebenen CAs werden durch Hardware Security Module (HSM) gesichert und sind dort nicht herauslösbar.
Die Webserver, auf denen die CA-Zertifikate angeboten werden, werden in den Rechenzentren des ITDZ Berlin betrieben und sind vor unbefugtem Zugriff geschützt.
Eine Manipulation des HTTP-Datenstroms würde auffallen, denn:

- Manipuliert ein Angreifender den HTTP-Datenstrom zum Aufrufenden der Webseite und zeigt falsche Informationen über die Zertifikate an, fällt dies bei der Prüfung der Angaben auf der Webseite mit den in den Zertifikaten hinterlegten Informationen auf.
- Manipuliert ein Angreifender zusätzlich im HTTP-Datenstrom die Angaben in den Zertifikaten selbst, passt die Signatur im Zertifikat nicht mehr zu den Inhaltsdaten und das Zertifikat wird als ungültig erkannt.

Für einen erfolgreichen Angriff müsste ein Angreifender zusätzlich einem Anwendenden ein durch den Angreifenden selbst ausgestelltes Zertifikat zukommen lassen. Die Übermittlung müsste zudem den Eindruck erwecken, von der ITDZ Berlin PKI zu kommen. Zertifikate werden an Endnutzende von wenigen bekannten E-Mail-Adressen des ITDZ Berlin per SMIME-signierter E-Mail versendet.

Das Zertifikatsvertrauen in Browsern und Betriebssystemen von öffentlichen Zertifizierungsstellen wird hergestellt, indem die Browser- und Betriebssystemhersteller entscheiden, welche CA-Zertifikate als vertrauenswürdig eingestuft werden. Diese Entscheidung obliegt also im Regelfall nicht dem Endnutzenden. Es erscheint unwahrscheinlich, dass ein normaler Endnutzender die Echtheit der mehreren hundert im Betriebssystem als vertrauenswürdig eingestuften CA-Zertifikate überprüft. Auch hier ließe sich dann die Frage der Authentizität der von diesen CAs ausgestellten Zertifikate stellen.

Die aktuell durch das ITDZ Berlin betriebene PKI-Infrastruktur ist nicht für die Zertifikatsvergabe an BürgerInnen konzipiert und wird so auch nicht betrieben, eben weil Endnutzende der Root-CA des ITDZ Berlin nicht automatisch vertrauen können. Aktuell gibt es viele Behörden, die eigene PKI-Lösungen betreiben. Die PKI des ITDZ Berlin ist nicht verpflichtend für die Berliner Behörden. Die Umstellung auf einen IKT-Basisdienst PKI entsprechend den Vorgaben des EGovG Berlin wird im Rahmen eines laufenden Projektes PKI bis Ende 2024 erfolgen. Die Laufzeit des Projektes wird maßgeblich durch den Aufbau der erforderlichen Betriebsstrukturen und Zertifizierungsfristen bedingt.

1. Wie sollen Bürger*innen die Certificate Authority (CA)-Zertifikate der Public-Key-Infrastruktur (PKI) der Berliner Verwaltung sicher erhalten, um z. B. S/MIME-signierte E-Mails zu prüfen oder sicherzustellen, dass sie für das korrekte Zertifikat verschlüsseln?

Zu 1.:
Es wird auf die einleitenden technischen Hintergrundinformationen in der Vorbemerkung verwiesen.

2. Weshalb ist die Webseite http://pki.verwalt-berlin.de Stand heute (08.12.2022) nur per unverschlüsseltem HTTP und nicht per Transport-Layer-Security (TLS)-verschlüsselter Verbindung zu erreichen?

Zu 2.:
Die Erreichbarkeit der Webseite per HTTP war eine frühere Designentscheidung, basierend auf den einleitenden technischen Hintergrundinformationen in der Vorbemerkung.

3. Wie soll ohne TLS sichergestellt werden, dass die unter http://pki.verwalt-berlin.de herunterladbaren Zertifikate nicht kompromittiert wurden?

Zu 3.:
Eine Kompromittierung der heruntergeladenen Zertifikate ist aufgrund der Ausführungen in der Vorbemerkung ausgeschlossen.

4. Wann soll dieser Missstand beseitigt werden?

Zu 4.:
Der Abruf der auf der Webseite zugänglichen Informationen ist im Zuge einer Neukonzeptionierung und Erweiterung der ITDZ Berlin PKI vor kurzem von HTTP auf HTTPS umgestellt worden. Der Missstand wird daher als behoben angesehen.

5. Haben die Mitarbeiter*innen bei der PKI der Berliner Verwaltung entsprechende Fachkenntnisse über Kryptographie? Falls ja, weshalb ist eine so zentrale Seite nicht kryptografisch abgesichert?

Zu 5.:
Die Mitarbeitenden erfahren regelmäßige Schulungen und externe Beratung. Bezüglich der kryptografischen Absicherung der Webseite wird auf die Vorbemerkung verwiesen.

6. Wie schätzt der Senat das Risiko ein, das durch Import eines nicht authentifiziert heruntergeladenen CA-Zertifikats entstehen kann?

Zu 6.:
Das Risiko wird aufgrund der Ausführungen in der Vorbemerkung als nicht existent betrachtet.

7. Wie viele Berliner Behörden setzen über eine nicht kryptografisch abgesicherte Verbindung heruntergeladene Zertifikate ein?

Zu 7.:
Zertifikate der ITDZ Berlin PKI werden bei 93 Behörden eingesetzt. Die Endzertifikate werden über geeignete Wege, z.B. signierte E-Mails, an die Nutzenden übertragen.

8. Wie möchte der Senat sicherstellen, dass dadurch kein Schaden entstanden ist oder entstehen könnte?

Zu 8.:
Siehe Antworten zu den Fragen 4 und 6.

9. Weshalb ist die Berliner Verwaltungs-PKI nicht durch eine global akzeptierte Certificate Authority (CA) cross-signiert, so dass die von ihr ausgestellten Zertifikate automatisch vertrauenswürdig sind und Bürger*innen und Behörden nicht gezwungen sind, die Sicherheit ihrer Systeme durch den händischen Import eines CA-Zertifikats potentiell zu kompromittieren?

Zu 9.:
Die durch das ITDZ Berlin betriebene PKI ist nur für den verwaltungsinternen Einsatz vorgesehen. Aus diesem Grund wurde eine Entscheidung insbesondere aus Kostengründen, außerordentlich hohem Betriebsaufwand und basierend auf den obigen Ausführungen gegen ein Cross-Signing getroffen. Der Betrieb von nur intern verwendeten PKI-Infrastrukturen ohne ein Cross-Signing ist branchenüblich. Siehe auch PKI-Beispiel der Europäischen Zentralbank (http://www.pki.ecb.europa.eu/pki/default.htm).
Der Bedarf an öffentlich anerkannten Zertifikaten wurde im Rahmen der Beauftragung des Projektes PKI in einer Wirtschaftlichkeitsuntersuchung mit dem Ergebnis untersucht, dass für diese Anforderungen der Kauf von Zertifikaten von qualifizierten externen Anbietern deutlich wirtschaftlicher ist als der Eigenbetrieb einer global akzeptierten CA.

10. Welche Kosten entstehen Berliner Behörden durch die so ausgestellten Zertifikate (bitte nach unterschiedlichen Zertifikatstypen unterscheiden) und wie bewertet der Senat die Kosten insbesondere im Hinblick auf die eklatanten Sicherheitsmängel der ausgegebenen Zertifikate, bzw. der zu diesen gehörenden Vertrauenskette?

Zu 10.:
Die Zertifikate der ITDZ Berlin PKI haben derzeit einen einheitlichen monatlichen Preis und werden nicht nach Verwendungszweck unterschieden. Der monatliche Preis beträgt 7,90 €. Für ca. 33.000 Zertifikate werden Kosten erhoben. Die Betriebsbereiche des ITDZ Berlin erkennen aus der derzeitigen Faktenlage, die sich aus der Vorbemerkung ergibt, keine Sicherheitsmängel der ausgestellten Zertifikate.

11 Sind Erstattungen durch das IT Dienstleistungszentrum Berlin (ITDZ) an die Stellen geplant, die für diese Zertifikate Mittel aufwenden mussten? Falls nein, weshalb nicht?

Zu 11.:
Da kein erkennbares Risiko besteht, ist nicht von Erstattungen auszugehen.

Berlin, den 20. Dezember 2022

In Vertretung

Dr. Ralf Kleindiek
Senatsverwaltung für Inneres, Digitalisierung und Sport