Ein Mittelsmannangriff auf ein digitales Signiergerät

Bachelorarbeit
im Ein-Fach-Bachelorstudiengang Informatik
Christian-Albrechts-Universität zu Kiel
Alexander Koch 2011

1 Einleitung

Digitale Signaturen wurden insbesondere zu dem Zweck erdacht, den Handel zu vereinfachen und es zu ermöglichen, Verträge rechtsgültig auch über das Internet abschließen zu können.

Dazu hat die EU die *gemeinschaftlichen Rahmenbedingungen für elektronische Signaturen* in der Richtlinie 1999/93/EG festgehalten. Die Richtline wurde vom Mitgliedsland Deutschland im **Sig**natur**G**esetz umgesetzt.

In dieser Arbeit wird gezeigt, wie es einem Angreifer trotz Einsatz eines Produktes, welches die Anforderungen des Gesetzes erfüllt, möglich ist, Daten zu signieren. Ausgenutzt wird dabei eine nicht gesicherte USB-Verbindung zwischen einer *sicheren Signaturerstellungseinheit* und dem PC des unterzeichnenden Nutzers.

2 Gesetzesgrundlage

Die EU definiert die *gemeinschaftlichen Rahmenbedingungen für elektronische Signaturen* in der Richtlinie 1999/93/EG. Insbesondere festgelegt ist die gleichgestellte Rechtswirkung elektronischer Signaturen für ein unterzeichnetes elektronisches Dokument mit „handschriftlichen Unterschriften in Bezug auf Daten, die auf Papier vorliegen“ [1999/93/EG, Art. 5 Abs. 1].

Die EU-Richtlinie wurde von Deutschland durch das Signaturgesetz (SigG) umgesetzt. Der Gesetzgeber unterscheidet zwischen mehreren Güteklassen digitaler Signaturen. Der Begriff *digitale Signatur* kennzeichnet das Verknüpfen von zur Authentifizierung dienenden Daten mit zu signierenden Daten. Der Zusatz *fortgeschritten* beschreibt zusätzlich die Anforderungen, die zur Authentifizierung genutzen Daten so zu wählen, dass sie „ausschließlich dem Unterzeichner zugeordnet“ [1999/93/EG, Art. 2 Abs. 2] sind, eine Identifizierung des Unterzeichners ermöglichen, mit Mitteln erstellt werden, „die der Unterzeichner unter seiner alleinigen

Kontrolle halten kann“ [1999/93/EG, Art. 2 Abs. 2], und auf eine Art mit den Daten verknüpft werden, die ein Verändern der Daten erkennbar macht - um sicherzustellen, dass eine einmal getätigte Unterschrift für ein spezielles Dokument nicht auf ein anderes Dokument übertragen werden kann.

Die qualifizierte elektronische Signatur stellt schließlich die höchsten Ansprüche an ihre Umsetzung. Zusätzlich zu den Eigenschaften einer *fortgeschrittenen elektronischen Signatur* wird der Einsatz eines *qualifizierten Zertifikates* und einer *sicheren Signaturerstellungseinheit* gefordert. Das Zertifikat muss unter anderem den Anbieter, seine fortgeschrittene elektronische Signatur, sowie den Staat, in dem er niedergelassen ist, den Namen des Unterzeichners oder ein Pseudonym, die Gültigkeitsdauer und den Identitätscode des Zertifikats, sowie etwaige Beschränkungen enthalten.

Eine Signaturerstellungseinheit ist „eine konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird.“ [1999/93/EG, Art. 2 Abs. 5] *Sicher* ist diese, wenn die „für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten praktisch nur einmal auftreten können und [...] ihre Geheimhaltung hinreichend gewährleistet ist” [1999/93/EG, Anhang III]. Zudem wird verlangt, dass Signaturerstellungsdaten „mit hinreichender Sicherheit nicht abgeleitet werden können und die Signatur vor Fälschungen bei Verwendung der jeweils verfügbaren Technologie geschützt ist“ [1999/93/EG, Anhang III] sowie „die für die Erzeugung der Signatur verwendeten Signaturerstellungsdaten von dem rechtmäßigen Unterzeichner vor der Verwendung durch andere verlässlich geschützt werden können“ [1999/93/EG, Anhang III].

3 Digitale Signaturen in der Praxis

Die in der Richtlinie und dem SigG geforderten Eigenschaften an qualifizierte elektronische Signaturen werden von den Zertifizierungsdiensteanbietern[1] zumeist über Prozessorchipkarten realisiert, die das Zertifikat und - in einem geschützten Speicherbereich gegen Auslesen geschützt - den zugehörigen privaten Schlüssel beinhalten, auf dessen Grundlage die Signatur erstellt wird. Dies gewährleistet hinreichend die Geheimhaltung des privaten Schlüssels. Zum Signieren von Daten ist außerdem eine PIN erforderlich, die der Karte signalisiert, dass der Besitzer der Karte dem Inhaber der Karte entspricht.

[1]Eine Liste der Zertifizierungsdiensteanbieter in Deutschland wird unter http://www.bundesnetzagentur.de/ bereitgestellt

Nur wenige handelsübliche Computer allerdings besitzen die Fähigkeit, solche Chipkarten von Haus aus zu betreiben, so dass externe Chipkartenterminals erforderlich werden. Diese Terminals ermöglichen es auch, die PIN-Eingabe aus dem Rechnerkontext heraus zu ziehen, um ein Ausspähen der PIN durch auf dem PC installierte Schadsoftware zu verhindern. Um Hardwaremanipulationen am Gerät selbst auszuschließen, sind sie oft mit Sicherheitssiegeln versehen, die nach dem Öffnen des Gehäuses eine Manipulation erkennbar machen.

Möchte ein Benutzer eine Datei signieren, benötigt er noch eine Anwendungssoftware, die die Kommunikation mit dem Chipkartenterminal bzw. der Chipkarte selbst übernimmt und es so ermöglicht, die eigentliche Signatur zu erstellen. Dazu wird ein Hashwert der zu signierenden Daten erstellt, an die Signaturkarte gesendet, und auf dieser mit dem von außen nicht zugänglichen privaten Schlüssel verschlüsselt.

4 Analyse eines konkreten Produktes

Für diese Arbeit wurde ein Standardprodukt des akkreditierten Zertifizierungsdiensteanbieters Deutsche Post Com GmbH ausgewählt. Das Produkt besteht aus einem Set verschiedener Komponenten: Es beinhaltet eine Prozessorchipkarte des Typs Infineon SLE66CX680PE mit dem Betriebssystem StarCOS 3.2, die nach dem Signaturgesetz zertifiziert wurde und zur Erstellung von qualifizierten elektronischen Signaturen geeignet ist. Im Set enthalten ist ein Cherry SmartTerminal ST-2000U mit integrierter Tastatur zur PIN-Eingabe sowie eine aus zwei Optionen frei wählbare Anwendungssoftware (hier: intarsys SignLive! CC). Zum Signieren von elektronischen Dokumenten wird zusätzlich zu den im Set enthaltenen Komponenten ein PC benötigt. Zur Inbetriebnahme ist es erforderlich, das Chipkartenterminal mit einer freien USB-Schnittstelle des PCs zu verbinden, einen Treiber und die Anwendungssoftware zu installieren. Ein User wählt dann in der Software die gewünschten Operationen aus. Die Anwendung greift über den installieren Gerätetreiber per USB auf das Chipkartenterminal zu und kommuniziert auf diese Weise mit der Chipkarte.

Bei der Durchführung eines Signaturvorgangs entsteht eine PKCS#7-Signaturdatei, deren Aufbau von [RFC5652] festgelegt ist.

Die Analyse eines Signaturvorgangs lässt folgende Eigenschaften erkennen:

- Das Chipkartenterminal gibt sich als Circuit Card Interface Device aus, und folgt den in [CCID] festgelegten Kommunikationsprotokollen.

- Die Chipkarte unterstützt die von [ISO7816] festgelegten Kommandos.
- Die in der erzeugten Signaturdatei enthaltenen Zertifikate werden im Klartext von der Chipkarte an den PC übertragen.
- Die PIN-Eingabe erfolgt vor dem Übermitteln des zu signierenden Message-Digest.
- Bei PIN-Eingabe wird nach jedem Tastendruck an den PC übermittelt, dass eine (aber nicht welche) Taste gedrückt wurde.
- Der MessageDigest der zu signierenden Datei wird genau wie der auf der Karte berechnete SignatureValue im Klartext übertragen.

5 Angriff

Aufgrund der ungesicherten USB-Verbindung ist es möglich, übertragene Daten abzugreifen und zu manipulieren. Im Rahmen der Arbeit wurde gezeigt, dass es möglich ist, ein Gerät transparent in die USB-Verbindung einzuschleifen, das für den Angreifer verschiedene Aufgaben übernimmt:

- Das Gerät verhält sich so lange transparent, wie der Angreifer keine Daten signieren möchte.
- Überträgt der Angreifer per Funk Daten zum eingeschliffenen Gerät, wartet dieses auf den nächsten Signaturvorgang.
- Das Gerät schreibt die im Klartext übertragenen Zertifikate mit und verhält sich weiterhin transparent.
- Das Gerät wartet auf die PIN-Eingabe und meldet bei erfolgreicher Eingabe einen Fehler an den Anwender-PC, der den User dazu bewegen soll, die PIN erneut einzugeben.
- Das Gerät übernimmt die weitere zum Signieren erforderliche Kommunikation mit der Chipkarte. Insbesondere ist es möglich, einen eigenen messageDigest an die Karte zu übertragen, um ein eigenes Dokument zu signieren.
- Das Gerät ermöglicht ein Abrufen der erzeugten Signatur per Funk.

6 Fazit

Vom Gesetzgeber wird die Sicherung der privaten Schlüssel zur Erzeugung des signatureValue auf sicheren Signaturerstellungseinheiten gefordert, um Missbrauch zu verhindern. Jedoch wird nicht gefordert, dass die Verbindung zwischen einer sicheren Signaturerstellungseinheit und dem Anwender-PC abgesichert wird. Dadurch ist es möglich, unter Verwendung spezieller Geräte qualifizierte elektronische Signaturen zu fälschen.

Die hier analysierte und angegriffene Lösung ist nur eine von vielen. Bei anderen Implementierungen, wie dem elektronischen Personalausweis, wurde die ausgenutzte Schwachstelle der ungesicherten Verbindung bereits behoben. Eine Absicherung ist jedoch noch nicht vom Gesetz gefordert, so dass unklar ist, ob und wann Umsetzungen mit abgesicherten Komponentenverbindungen solche mit ungesicherten Verbindungen verdrängen.

Literatur

[1999/93/EG] Europäisches Parlament, Europäischer Rat. Gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Dezember 1999.

[RFC5652] Internet Engineering Task Force. RFC 5652 - Cryptographic Message Syntax (CMS), September 2009.

[ISO7816] ISO/IEC. 7816 - Identification cards — Integrated circuit cards, Januar 2005.

[CCID] USB Device Working Group. Specification for Integrated Circuit(s) Cards Interface Devices, April 2005.