Der Weg zur eigenen GnuPG Smartcard

Martin Beier
Development Engineer RFID-Applications
Linxens Germany GmbH
Email: martin.beier@tif-it.org

Volker Zeihs
PKI-Abteilung
Allianz Technology SE
Email: volker.zeihs@tif-it.org

***Zusammenfassung*—2016 begannen die Autoren an einer Smartcard-Lösung für sich und die Mitglieder ihres Hackerspaces zu arbeiten. Das Ziel der Smartcard-Lösung ist die Verschlüsselung auf PCs und Smartphones sicherer, einfacher und für jedermann bezahlbar zu gestalten. Als größtes Problem hat sich dabei die Beschaffung der benötigten Smartcards herausgestellt. Alle anderen Probleme und zu Weilen lustige oder interessante Ereignisse auf dem Weg zur eigenen Smartcard werden in dieser Arbeit beleuchtet.**

Das Ziel dieser Arbeit ist es, dem Leser eine Hilfestellung für ihren eigenen Weg zur GnuPG kompatieblen Smartcard zu geben und einen Ausblick auf die von uns angestrebten Lösung für bis jetzt noch ungelöste Probleme zu zeigen.

Diese Arbeit hat keinen wissenschaftichen Anspruch und soll lediglich unseren Weg zur eigenen GnuPG-Smartcard aufzeigen.

I. Was ist das Problem?

2016 diskutierten wir in unserem Hackerspace über den Zusatand der täglichen Kommunikation untereinander. Dabei stellten wir fest, dass ein erheblicher Teil dieser Kommunikation unverschlüsselt ist.

In der weiteren Diskusion stellten wir fest, dass ein Großteil unserer Kommunikation über E-Mails und verschiedene Instant Messenger abläuft. Obwohl die meisten von uns GnuPG auf ihren PCs verwenden, findet dies kaum Anwendung auf dem Smartphone. Die Gründe hierfür liegen zum einem in Sicherheitsbedenken: Ist mein privater Schlüssel auf dem Smartphone sicher? Die Verwendung einer guten Passphrase kann bei Geräten mit eingeschränkter Tastatur zum Problem werden. Die Einrichtung der Verschlüsselung auf dem Smartphone und das Schlüssel-Management zwischen verschiedenen Geräten (z. B. Smartphone, Tablet und PC) wurde ebenso als Problem gesehen.

Es stellt also ein Problem dar, seine Schlüssel über mehrere Geräte zu synchronisieren und gleichzeitig vor unberechtigtem Zugang zu schützen. Um mehr unserer täglichen Kommunikation zu verschlüsseln, müssen wir Verschlüsselung auf dem Smartphone einfach benutzbar und sicher machen.

II. Related Work

- AppletPlayground von Martin Paljak https://github.com/martinpaljak/AppletPlayground
- Conversations https://conversations.im/
- GlobalPlatformPro https://github.com/martinpaljak/GlobalPlatformPro
- K9 Mail https://k9mail.github.io/about.html
- OpenKeychain https://www.openkeychain.org/
- openpgp Applet von Joeri Richterhttps://github.com/jderuiter/javacard-openpgpcard
- openpgp Applet von Yubikey https://github.com/Yubico/ykneo-openpgp
- Password Store https://github.com/zeapo/Android-Password-Store/

III. Lösungs-Idee: Smartcards

Schnell kamen wir auf die Idee die besteheneden Probleme mit einer Smartcard zu lösen. Da eine Smartcard einerseits den privaten Schlüssel schützt, ermöglicht die Smartcard andererseits, dass der private Schlüssel ohne größerem Aufwand an verschiedenen Geräten verwendet wird. Dabei erfordert die Verwendung einer Smartcard weder die Eingabe längerer Passwörter noch müssen die Schlüssel über mehrere Geräte synchronisiert werden.

Wir brauchen eine Smartcard. Was muss sie können? Nach einer kleinen Umfrage im Hackerspace haben wir die folgenden Spezifikationen festgelegt:

Es sollte möglich sein

- E-Mails mit GnuPG zu verschlüsseln und
- mindestens einen kompatiblen Instant Messenger geben.

Weiterhin sollte die Smartcard am

- PC und
- Smartphone verwendet werden können.

Wünschenswert ist auch die Möglichkeit einen

- Password Safe zu entsperren sowie
- 2FA- bzw. OTP-Logins durchzuführen.

Daneben sollte es möglich sein,

- die Smartcard um Funktionalitäten zu ergänzen, um für spätere Anforderungen zu genügen und
- die Smartcard sollte so offen und frei wie nur möglich sein.

Alle primären Funktionen können durch eine GnuPG-kompatible Smartcard abgedeckt werden. Um diese jedoch auch an einem Smartphone verwenden zu können, sollte NFC zur Verfügung stehen.

Damit die Smartcard für jeden in der Gruppe erschwinglich ist, haben wir uns ein Kostenlimit von 20 g€esetzt.

IV. Wo bekommen wir jetzt so eine Smartcard her?

Diese Aufgabe stellte sich als größte Herausforderung dar und nimmt daher den größten Teil dieser Arbeit ein. Im Folgenden werden unsere Stationen und Unwegbarkeiten

bei der Beschaffung eine GnuPG-kompatiblen Smartcard aufgezeigt.

Wenn man nach GnuPG-kompatiblen Smartcards sucht, findet man zuerst die Karten von **ZeitControl**. Dabei handelt es sich um eine Implementierung auf der Basis der Basic Zeitcontrol Smartcards. Leider ist diese Entwicklung komplett proprietär und für Privatpersonen nicht erhältlich, daher scheidet Zeitcontrol für unsere Betrachtung aus.

Yubico bietet mit dem **Yubikey Neo** eine GnuPG-kompatible Smartcard im praktischen Format mit USB- und NFC-Schnittstelle an. Das von Yubikey Neo verwendetete Java Card Applet ist eine angepasste Version des von Joeri de Ruiter veröffentlichten Quellcodes. Allerdings kostet diese Smartcard 49 ,€ was weit über unserem Limit liegt.

Nitrokey wird von einen Startup aus Berlin entwickelt und vertrieben. Nitrokey hat keine NFC-Schnittstelle und ist somit nicht für die Verwendung mit Smartphones geeignet.

Es gibt noch weitere Implementierungen auf der Basis von **Java Smartcards**. Diese Implementierungen sind meist Open Source und somit für jederman zugänglich. Auch lassen sich auf einer Java Smartcard mehrere Applets nebeneinander betreiben, somit ist es möglich die Smartcard um funktionen für 2 Faktor authentifikation oder x509 funktionalitäten zu erweitern. Daher haben wir uns entschieden, unsere Smartcard auf Basis einer Java Smartcard mit NFC zu erstellen.

Bei unseren ersten Recherchen im Internet haben wir verschiedene **Händler in Deutschland und der EU** gefunden. Bei diesen Händlern haben die passenden Smartcards oft weit über 20 g€ekostet. Dies war jedoch über oder an unserem Limit und wir suchten weiter nach günstigeren Anbietern.

Wir versuchten unser Glück bei einem netten **Händler aus China**, King Security Co. ltd. Dabei ist es uns aufgefallen, dass fast auschließlich Java Smartcards mit Magnetstreifen (Kartentyp J2A040) angeboten werden. Es scheint so, als würden die meisten Käufer dieser Java Smartcards, diese nicht für die Verschlüsselung ihrer Daten verwenden und wir uns mit dem Beschaffen solcher Karten in nicht ganz legalen Kreisen bewegen. Trotz des Umstandes haben wir uns entscheiden diese Karten zu bestellen, da sie weit aus günstiger als in europäischen Shops waren. Die Karten kosten 8 p€ro Stück inklusive Versand und Zollgebühren.

Nach mehreren Wochen Wartezeit war es dann endlich so weit und wir hatten unsere ersten Java Smartcards in den Händen. Doch nach kurzen Testen uns Spielen mit den Karten kam die Ernüchterung: Unser netter Händler aus China hatte die Karten so unvorteilhaft vorpersonalisiert, dass wir nicht im Stande waren unser GnuPG-Applet aufzuspielen bzw. zu verwenden. Die Karte erlaubte nur das T = 0 Protokoll.

Nach Beanstandung und einigen E-Mail-Ping-Pong, konnten wir unseren Händler überzeugen uns noch einmal Karten zuzusenden. Wieder ein paar Wochen später hatten wir die neuen Karten und haben natürlich sofort geprüft, wie diese diesmal vorpersonalisiert sind. Dabei stellten wir erstaunt fest, dass wir dieses Mal kommplett nicht vorpersonalisierte Karten bekommen hatten. Uns dämmerte, dass unsere erste Vermutung für was diese Karten eigentlich angeboten werden, wahrscheinlich richtig war.

Da unser Hackerspace ca. einmal im Jahr eine Cryptoparty organisiert, hielten wir es für eine gute Idee, den Besuchern die Konzepte und Verwendung von Smartcards näher zubringen. Da all die Theorie ohne praktische Anwendungsmöglichkeiten nicht hilft, suchten wir nach einem Sponsor für Java Smartcards. Ein mittelständischen Unternehmen in der Nähe von Eisenach mit dem Namen **CARDAG Deutschland GmbH** hatte sich bereit erklärt unsere Cryptopartys mit Java Smartcards zu sponsorn. Dadurch können wir auf unseren Cryptopartys den Besuchern die Verwendung von Smartcards zum Verschlüsseln und Authentifizieren zeigen und ihnen die eingerichtete Smartcard auch gleich unentgeldlich mitgeben.

Da die Spenden bis jetzt immer recht großzügig waren, haben wir bei uns noch einige Smartcards übrig und würden diese auch gerne für eure Hackerspaces und Projekte zur Verfügung stellen.

V. Initialisieren der Karte

Nun da wir unserer Java Smartcards haben, wollen wir diese auch mit Leben befüllen. Dies gestaltet sich mit den nicht vorpersonalisierten Karten aus China als nicht so schwierig, da die nötigen Befehle zum Personalisieren von dem chinesischen Händler mitgeliefert wurden. Ansonsten wäre dies ein echtes Problem, da die Befehle zum Personalisieren nicht öffentlich sind.

Zuerst haben wir die Smartcards mit globalPlatform vorbereitet, dabei wurden die Karten personalisiert und die nötigen PINs gesetzt. Als Applet haben wir uns für die openSource-Variante von Yubico entscheiden, da diese die größte Kompatibilität mit Programmen und Apps bereitstellt. Dann hielten wir endlich unsere erste GnuPG-kompatible Smartcard für unseren Hackerspace in den Händen.

VI. Was haben wir bis jetzt erreicht?

Unsere ersten Karten (von dem chinesischen Händler) konnten wir leider wegen fehlendem NFC-Interface nur am PC mit einem Lesegerät verwenden. Die Dual-Interface-Karten von CARDAG Deutschland GmbH sind für unsere Ansprüche besser geeignet. Mit diesen Karten konnten wir erstmals die Funktionen an unseren Smartphones testen. Dabei hat uns sehr überrascht, dass es schon einige Apps in den verschiedenen App-Stores gibt, die mit der Smartcard genutzt werden können. Darunter befinden sich Apps zur E-Mail-Verschlüsselung, Dateiverschlüsselung und Passwort-Safes sowie Instant Messenger (siehe **??**). Da wir die Karte selbst initialisieren, haben wir Zugriff auf alle Funktionen der Karte und können somit auch weitere Applets aufspielen.

VII. Ausblick

Da die Kosten für eine Smartcard stark von der Menge der Bestellung abhängt, ist es sinnvoll, die Bestellungen vieler einzelnen Personen zusammenzufassen. Aus diesem Grund haben wir uns entschlossen, eine Firma zu gründen, um dies zu tun. Dies ermöglicht uns die Smartcard-Hardware zu einem günstigen Preis abzugeben und möglichst vielen Menschen die Möglichkeit zu geben, ihre privaten Schlüssel komfortabel zu schützen. Außerdem planen wir die Karten in mehreren Varianten anzubieten, um möglichst viele Anwendungsfälle bedienen zu können.

Natürlich gehen wir nicht davon aus, dass dies ein Produkt für jederman ist. Unsere Zielgruppe sind Menschen, die bereits Verschlüsselung nutzen und diese nun auch mit Smartcards verwenden möchten. Wir versuchen die Hürde für diese Personen so gering wie möglich zu gestalten.

Variante	1	2	3
NFC	✓	✓	
Kontakte	✓		✓
ADMIN-PIN	✓	✓	✓
Einfacher Druck	✓	✓	✓
Geplanter Preis in €	15	10	10

Als weiteren wichtigen Teil dieser Firma soll eine Webseite entstehen, die mit detallierten Anleitungen das Erstellen von GnuPG-Smartcards vereinfachen soll. Zusätzlich planen wir best practice Beschreibungen für die Verwendung von Smartcards mit GnuPG auf PCs sowie Smartphones.

Eine weitere Einschränkung besteht derzeit in der maximalen Größe des privaten Schlüssels auf der Smartcard. Diese liegt zurzeit bei unseren Karten noch bei 2048 Bit. Dies gilt zwar zurzeit für viele Anwendungen als sicher, aber die Möglichkeit größere Schlüssel zu verwenden, ist wünschenswert. Seit 2017 gibt es Java Smartcards, die theoretisch RSA-Operationen mit privaten Schlüsseln mit einer Größe von 4096 Bit unterstützen (Version JCOP 3). Sobald wir diese Smartcards haben, wollen wir das Yubico Applet für 4096 Bit Schlüssel erweitern. Hierfür suchen wir jede Unterstützung, die wir bekommen können.