SCrypt - PKCS11 Schnittstelle zu NFC-fähigen Smartphones

Ein asymmetrisches Kryptosystem ermöglicht es viele, der für ein modernes Internet, notwendigen Anforderungen zu erfüllen. Diese Anforderungen auch Schutzziele genannt sind, Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit und Verbindlichkeit. Die Einrichtung eines solchen Systemes bringt allerdings auch einige Hürden mit sich. So muss unteranderem jeder Teilnehmer seinen privaten Schlüssel sicher abspeichern.

Es kann durchaus problematisch sein private Schlüssel auf dem gleichen Rechner, welcher zum verschlüsseln von Daten benutzt wird, zu speichern. Dies kreiert einen Single Point of Failure. Um dieses Problem zu umgehen wurden in den 70iger Jahren sogenannte Smartcards erfunden, Chipkarten auf denen Schlüssel physisch getrennt abgespeichert werden können. So werden Schlüsselmaterial und zu verschlüsselnde Daten nur zum Zeitpunkt der Verschlüsselung zusammengeführt.

In dieser Arbeit soll eine Alternative zu herkömmlichen Smartcards, auf Basis eines Smartphones, entwickelt werden. Hierzu sollen Schlüssel auf dem Gerät gespeichert werden. Diese Schlüssel sollen sicher vor Fremdzugriffen sein und kein Schlüsselmaterial soll jemals das Gerät verlassen. Alle Verschlüsselungsoperationen werden auf dem Smartphone ausgeführt. Die Verbindung zwischen Smartphone und Rechner mit zu verschlüsselden Daten wird über Near Field Communication hergestellt. Zugriff auf Operationen und Schlüssel soll über eine nach PKCS11 standardisierte Schnittstelle auf dem über NFC angebunden Rechner möglich sein. Außerdem sollen Überlegungen angestellt werden, inwiefern die neuen Möglichkeiten die ein Smartphone gegenüber einer Smartcard bietet genutzt werden können.

-motivation: möglichkeiten asmcrypto

- probleme privkey

- neg von SC

- einführung asym cryp

- SChlüssel

- <titel der <arbeit

smartcard emulation

pkcs 11