Freie Universität Berlin

Cryptographic Identities on a Mobile Platform

The CryptID infrastructure on Android

Florian Schmid

Motivation

„Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. [...]“

Edward Snowden (The Guardian, 17.06.2013)

Problembeschreibung

- Verschlüsselung (von Kommunikation) wenig verbreitet
- Änderung der Kommunikationskultur
- bisherige Public-Key-Infrastrukturen zentralisiert oder schwierig zu nutzen

Ziele

- Applikation für Mobilsysteme
- dezentrale Public-Key-Infrastruktur
- verifizierte aktuelle Kontaktdaten
- Schlüsselaustausch
- Schnittstelle für andere Applikationen
- gute Benutzbarkeit

Grundlagen

- Peer-to-Peer-Netzwerk *MissingLink* als Public-Key-Infrastruktur
- Austausch von CryptIDs über QR-Codes
- Speicherung der Kontaktdaten mit Signatur des Besitzers

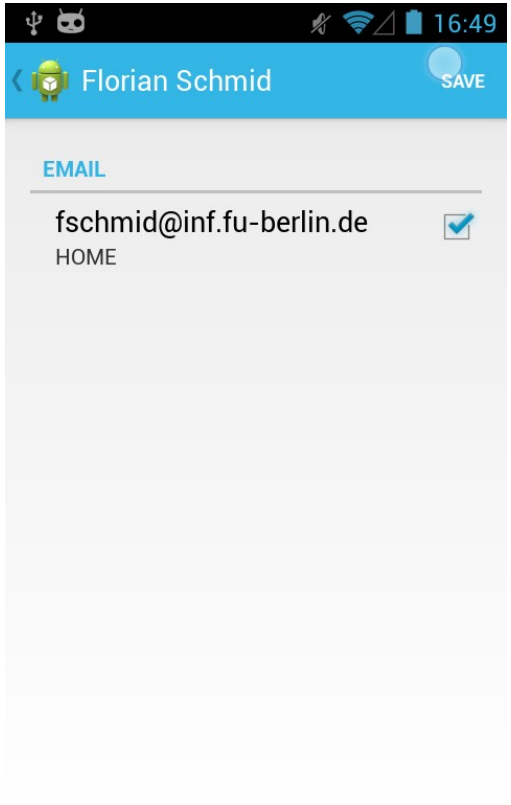
Trivia:

cryptid

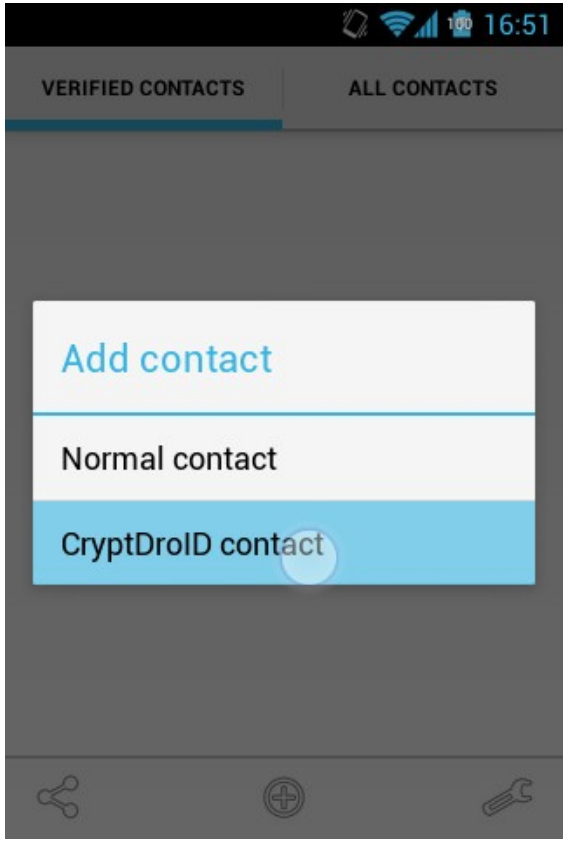
> an animal whose existence or survival is disputed or unsubstantiated, such as the yeti.

Quelle: http://www.oxforddictionaries.com

Beispielablauf



Beispielablauf

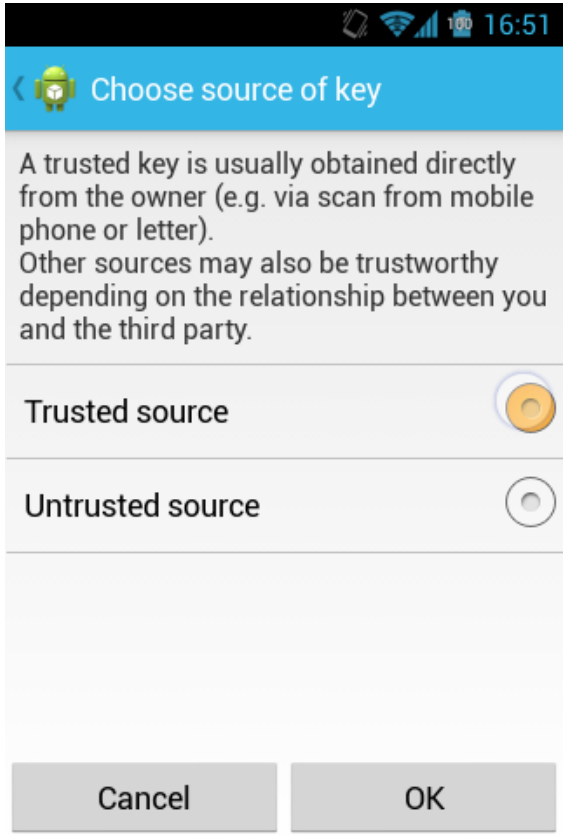


Beispielablauf

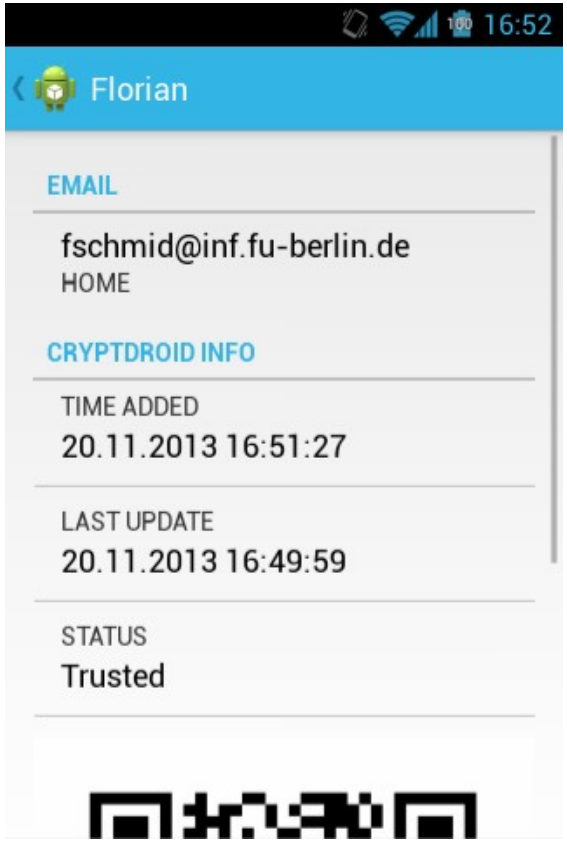
Beispielablauf


```
+-------- CryptId +
|     =E&S==      |
|    ooBSX@ +     |
|     . =o*o      |
|       o . .     |
|        E        |
|                 |
|                 |
|                 |
|                 |
+-----------------+
```

Beispielablauf



Beispielablauf



ToDos

- Verwaltung des Hauptschlüssels nicht implementiert
- funktionell unvollständig im Vergleich zum Standard-Adressbuch
- Nutzertests

Ausblick

„Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. [...]“

Edward Snowden (The Guardian, 17.06.2013)

Ausblick

„Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.

Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it“

Edward Snowden (The Guardian, 17.06.2013)

Ausblick

- Zugriffsschutz für Kontaktdaten
- Verifizierung von Schlüsseln Dritter
- Infrastruktur für weitere Anwendungen
- Portierung auf andere Plattformen

Zusammenfassung

- grundlegende Public-Key-Infrastruktur
- Verbesserungen bezüglich der Funktionalität nötig
- mehrere Erweiterungsmöglichkeiten

Vielen Dank für Ihre Aufmerksamkeit!