

OpenPGP-Smartcards auf dem Campus

Jan Tobias Mühlberg

[<muehlber@fh-brandenburg.de>](mailto:muehlber@fh-brandenburg.de)

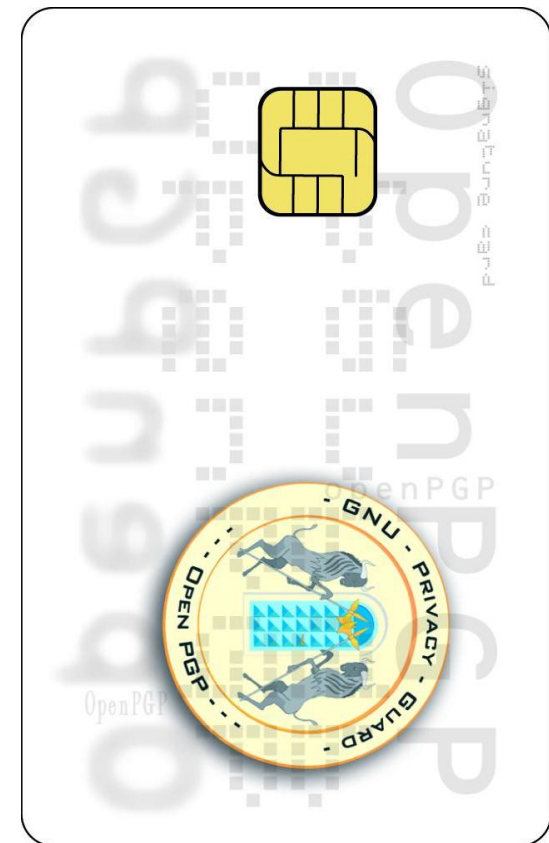
Brandenburg an der Havel, den 23. November 2004

Gliederung

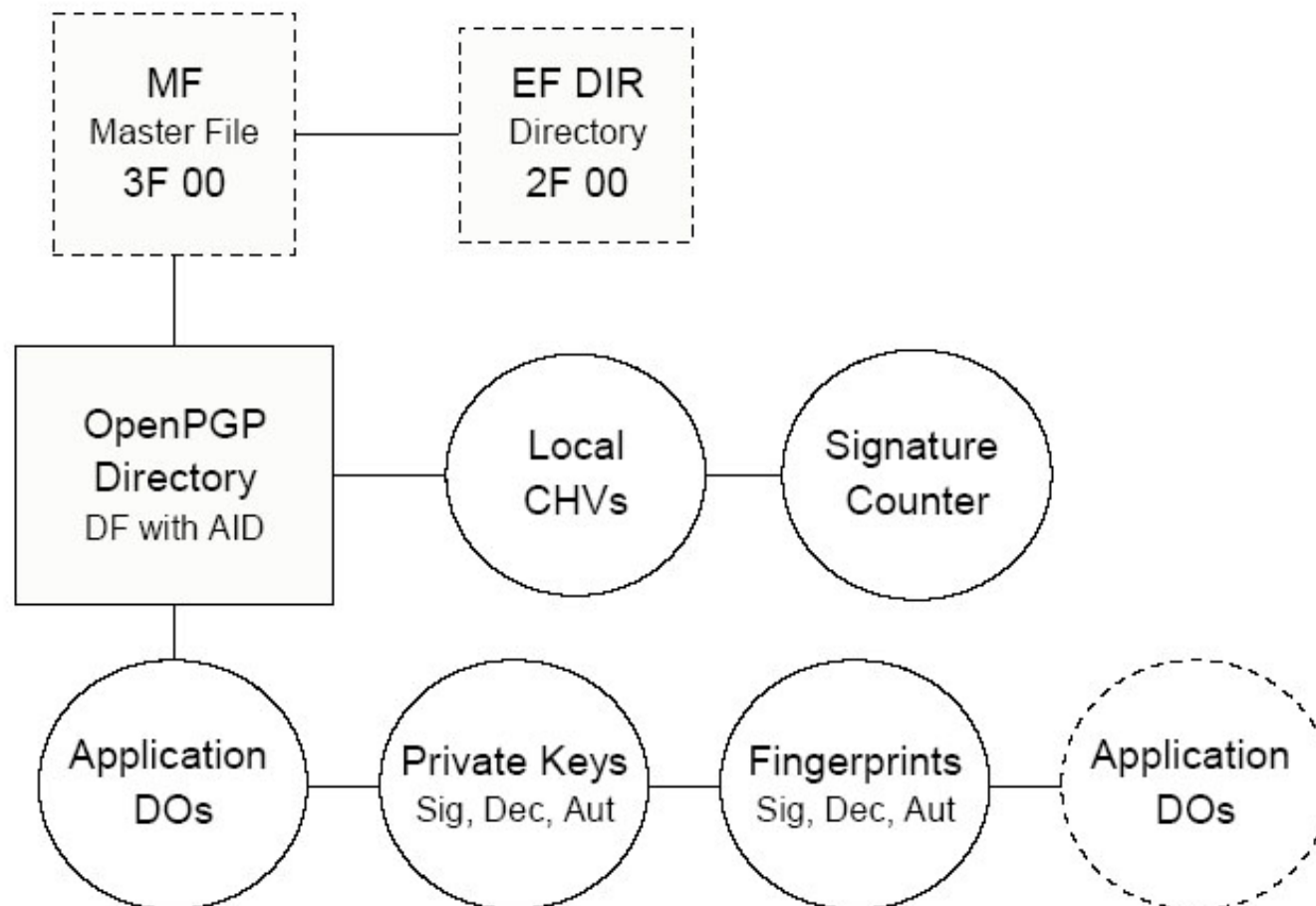
1. Die OpenPGP-Smartcard
2. Funktionsumfang der Karte
3. Einsatzmöglichkeiten
4. Quellen

Die OpenPGP-Smartcard

- entwickelt von der *g10 code GmbH* und der *PPC Card Systems GmbH*
- von GnuPG seit Mai 2004 unterstützt
- ist über *g10* erhältlich



Funktionsumfang



Funktionsumfang

- Spezifikation entsprechend ISO 7816-3,-4,-8
- 3 unabhängige 1024 bit RSA Schlüssel
(signieren, verschlüsseln, authentifizieren)
- Schlüsselerzeugung auf der Karte oder Import existierender Schlüssel
- Länge der PIN von 6 bis 254 Zeichen; nicht auf Ziffern beschränkt
- Signaturenzähler

Funktionsumfang

- Datenobjekt um die URI des vollständigen OpenPGP-Schlüssels anzugeben
(254 B, RFC1738)
- Datenobjekt für Login spezifische Daten
(2 x 254 B)

Funktionsumfang

- Datenobjekte für Daten des Karteninhabers:
 - Name (39 B, ISO/IEC 7501-1)
 - Sprache (8 B, ISO 639)
 - Geschlecht (1 B, ISO 5218)
- 40 mm * 10 mm beschreibbares Feld auf der Kartenvorderseite

Funktionsumfang

- T=1 Unterstützung nach ISO 7816-3;
kompatibel mit den meisten Lesern
- Spezifikation frei verfügbar und ohne
Einschränkungen nutzbar
- vernünftiger Preis

Einsatzmöglichkeiten

- Authentizität und Vertraulichkeit für interne Zwecke (E-Mail, etc.)
- Rechtssicherheit: Brauchen wir qualifizierte Signaturen?
- Speicherung applikationsspezifischer Daten
- sichere Logins an Workstations

Quellen

- g1 code GmbH: <http://www.g10code.de/>
- Karten-Spezifikation:
<http://www.g10code.de/de/p-card.html>
- OpenPGP Spezifikation/ RFC 2440:
<http://www.faqs.org/rfcs/rfc2440.html>