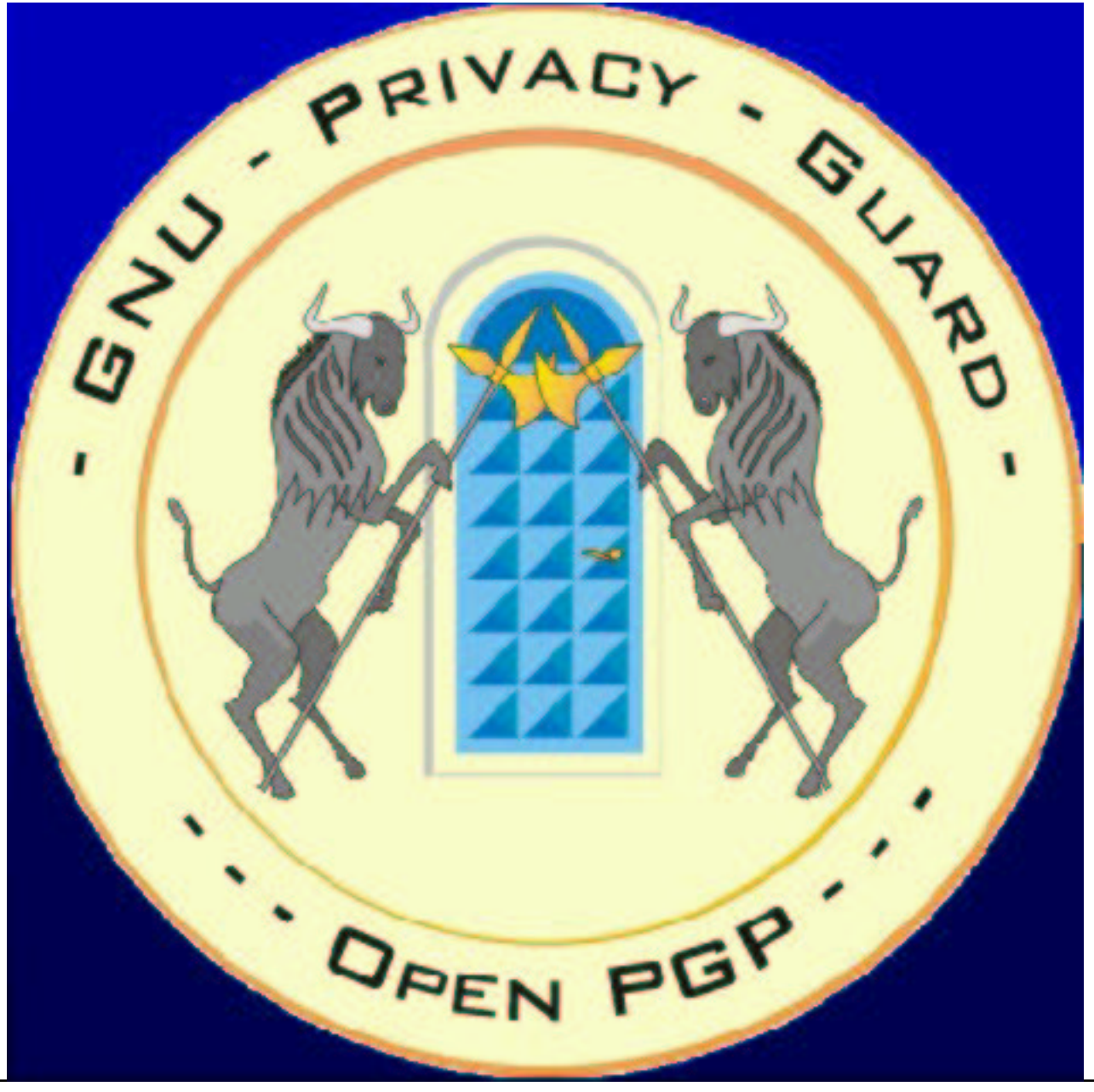
IT Sicherheit und Freie Software

(Saarbrücken, 5. September 2002)



Übersicht

- Free as in Freedom
- Kerckhoff & Cie.
- GnuPG
- Sphinx
- Architektur
- Demonstration

Wir sprechen über Freie Software

- "Freie Software" ist leichter verständlich
- Freie Software ist schwieriger zu missbrauchen
- Freie Software ist wohldefiniert
  - Sie unbegrenzt und für jeden Zweck verwenden zu dürfen.
  - Untersuchen zu dürfen, wie sie funktioniert und sie den eigenen Bedürfnissen anpassen zu dürfen.
  - Sie zu kopieren und an Andere weiter geben zu dürfen.
  - Sie zu verbessern und die Verbesserungen allen zum allgemeinen Wohl zugänglich machen zu dürfen.
- Freie Software bietet zusätzliche Werte

Auguste Kerckhoffs (1835-1903)

"Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvØnient tomber entre les mains de l'ennemi"

(Es ist notwending, daßdas System nicht geheim gehalten wird und ohne Unannehmlichkeiten in die Hände des Feindes fallen kann)

- Im Umkehrschluss fordert man heute, daßdas System öffentlich sein muß, damit Schwachstellen besser erkannt werden.
- Nur Freie Software kann dieses Kriterium erfüllen.
- Es genügt nicht, lediglich öffentliche Algorithmen zu verwenden.

Der GNU Privacy Guard

- Vollständige Implementation von OpenPGP.
- Sichert Email und gespeicherte Daten.
- Verbindet digitale Signaturen, Verschlüsselung und Schlüsselverwaltung in einer Anwendung.
- Läuft auf allen POSIX Platformen sowie auf Windows und Mac.
- Flexibel und lange im praktischen Einsatz.

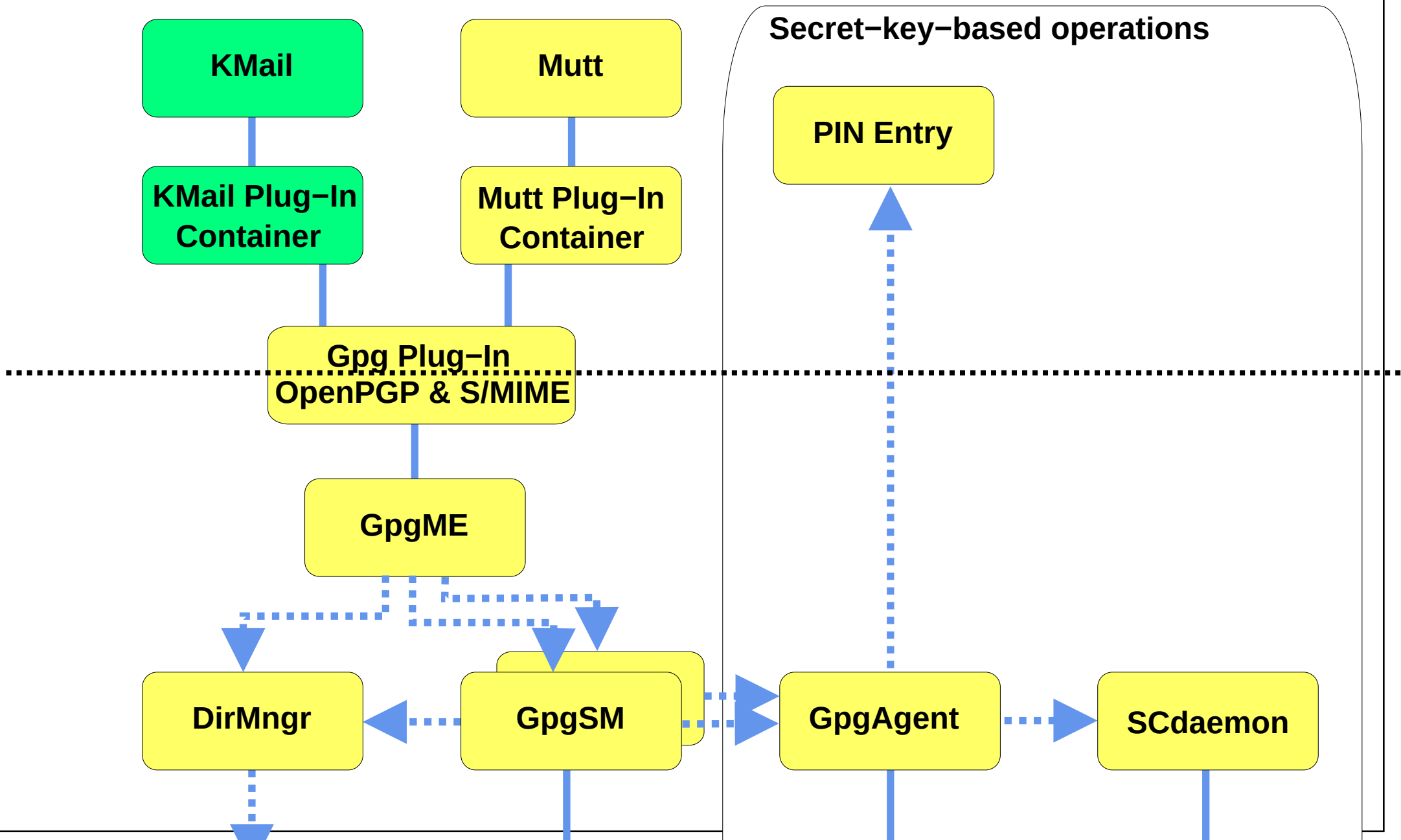
Was ist Sphinx?

- Pilotprojekt for Desktop-zu-Desktop Sicherheit.
- Basiert auf dem S/MIME Standard.
- Sichert Email und gespeicherte Daten.
- Kompatibel mit anderen S/MIME Anwendungen.
- Einheitlicher Standard für Verwaltungen und Bürger.
- Smartcards werden unterstützt.

Das ~gypten Projekt

- Implementierung von Sphinx für POSIX Systeme
- Integration mit GnuPG für OpenPGP
- Einfache Integration in Mailprogramme.
  - KMail (KDE)
  - Mutt (Text basiert)
  - Sylpheed (in Arbeit)
- Ein neues Krypto Framework für GNU/Linux.
- Verfügbar unter der GNU General Public License (GPL).

Architektur



Weitere Informationen

- http://www.gnupg.org/aegypten/
- http://www.bsi.de/aufgaben/projekte/sphinx/
- http://www.fsfeurope.org/documents/whyfs.de.html