

# Gnu Privacy Guard I

Schutz der Privatsphäre  
durch Kryptographie

Öffentliche Schlüssel

Digitale Unterschrift

von Gerhard Öttl  
gerhard.oettl@gmx.at

# Warum Kryptographie?

Kryptographie (die Lehre von der Verrschlüsselung) gewährleistet:

- Vertraulichkeit / Geheimhaltung
  - Individuelles Bedürfnis nach Vertraulichkeit
  - Sensible Daten / Spionageschutz
- Integrität / Schutz vor Veränderung
- Authentizität / Sicherstellung der Datenquelle  
Verträge, Software

# Warum GnuPG?

- frei von Patenten (Algorithmen, Software)
- offizieller Standard (RFC2440 "OpenPGP")  
kompatibel zu PGP 5.x
- Offener Quellcode (Gnu GPL)  
keine Hintertüren, kein "Generalschlüssel"
- unabhängig vom Datenformat  
E-Mail, Text, Bilder, Festplatten, usw
- starke Verschlüsselung  
grosse Schlüssellänge, Public-Key-Verfahren (DSA)

# Grundgedanken

- Sicherheit ist ein Gesamtkonzept und nicht durch eine Einzelmassnahme zu erreichen.
- Es ist immer ein Kompromiss zwischen Sicherheit und Bequemlichkeit zu schliessen.
- Sicherheit bei guten Verschlüsselungsmethoden beruht auf der Geheimhaltung des Schlüssels und nicht auf der Geheimhaltung des Verfahrens.

# Konzepte

- Symmetrische Verschlüsselung
- Public-Key Verschlüsselung
- Hybride Verschlüsselungsverfahren
- Digitale Unterschriften

# Symmetrische Verschlüsselung

- hohe Sicherheit erreichbar  
früher waren 56-Bit Schlüssel üblich, also  $2^{56}$   
72.057.594.037.927.936 Möglichkeiten, jetzt werden  
128-Bit Schlüssel verwendet, das sind  $2^{128}$   
340.282.366.920.938.463.463.374.607.431.768.211.456  
mögliche Schlüssel.
- Problem der Schlüsselübermittlung
- ein Schlüssel pro Gegenüber notwendig  $x*(x-1)/2$

# Public-Key Verschlüsselung

- Schlüsselpaar (geheim / öffentlich)  
jeder Schlüssel des Paares macht die Veränderung des anderen Teiles rückgängig
- verschlüsseln mit öffentlichem Schlüssel von EmpfängerIn / Umkehr mit geheimen Key
- signieren (unterschreiben) mit geheimen Schlüssel von SenderIn / Umkehr mit öffentlichem Key
- grössere Schlüssellängen (ab 1024 Bits)
- komplexere mathematische Algorithmen

# Konzepte

- Symmetrische Verschlüsselung
- Public-Key Verschlüsselung
- Hybride Verschlüsselungsverfahren
- Digitale Unterschriften

# Digitale Unterschriften

- Verschlüsseln der Daten mit dem geheimen Schlüssel
- Daten bzw Dokument im Klartext  
Ermittlung eines Hash-Wertes (Integrität)  
und nur den Hash mit dem geheimen Schlüssel  
verschlüsseln (Unterschrift)
  - ➔Anhängen einer Klartextsignatur
  - ➔Abgetrennte Signatur

# Der eigene Schlüssel

- Erzeugen des Schlüsselpaares (geheim/öffentlich)
  - ➔ Erzeugen einer Widerrufurkunde
- Verschlüsseln und Entschlüsseln von Daten
- Digitale Unterschrift
- Editieren des Schlüssels
  - ➔ Erzeugen einer neuen UID
  - ➔ Erzeugen von Unterschlüsseln
  - ➔ Aktualisieren des Verfallsdatums
  - ➔ Widerrufen von Schlüsselkomponenten

# Schlüssel von anderen

- Schlüsselintegrität / Eigenbeglaubigung
- Austauschen von Schlüsseln
  - Exportieren eines öffentlichen Schlüssels
  - Importieren eines öffentlichen Schlüssels
  - Verwendung von Keyservern
- Beglaubigen anderer Schlüssel
  - durch unsere persönliche Unterschrift
  - durch eine zentrale Stelle
  - durch ein "Web of Trust"
  - Doppelbelegung von "Vertrauen in Unterschrift"

# Prüfung der Identität

- Prüfung der Angaben zur Person, durch (zwei) Lichtbildausweise
- Prüfung des Schlüssels
  - Name
  - Schlüssel-ID
  - Schlüssel-Fingerprint
  - Grösse / Typ

Auf einer Keysigning-Party immer nur anhand von Listen bzw Ausdrucken die Prüfung vornehmen und die Schlüssel ausserhalb der Party austauschen.

# Sorgfalt bei der Bestätigung von Schlüsseln

Unabhängig von Ihrem eigenen Sicherheitsbedürfnis und unabhängig davon, wieviel Wert Sie in die Bestätigungskraft anderer Unterschriften auf Schlüssel legen:

Sie sollten beim Unterschreiben (Beglaubigen) anderer Schlüssel immer mit grosser Sorgfalt vorgehen, oder andernfalls besser gar keine Bestätigungen durchführen, da sich andere unter Umständen auf Ihre Bestätigung verlassen.

# THE END

Ich danke für Ihre Aufmerksamkeit und stehe gerne  
für weitere Auskünfte zur Verfügung

Gerhard Öttl  
gerhard.oettl@gmx.at

# Gnu Privacy Guard II

Schutz der Privatsphäre  
durch Kryptographie

Web of Trust

Sicherer Mailaustausch

von Gerhard Öttl  
gerhard.oettl@gmx.at

# Public-Key Systeme

- passendes Schlüsselpaar (geheim / öffentlich)  
nur beide Schlüssel gemeinsam ergeben Sinn
- digitale Unterschrift (Signatur)
- Web of Trust (Vertrauen / Gültigkeit)
  - ➔ Austausch der Schlüssel
  - ➔ Überprüfung der Identität
  - ➔ Beglaubigung anderer Schlüssel

# Sorgfalt bei der Bestätigung von Schlüsseln

Unabhängig von Ihrem eigenen Sicherheitsbedürfnis und unabhängig davon, wieviel Wert Sie in die Bestätigungskraft anderer Unterschriften auf Schlüssel legen:

Sie sollten beim Unterschreiben (Beglaubigen) anderer Schlüssel immer mit grosser Sorgfalt vorgehen, oder andernfalls besser gar keine Bestätigungen durchführen,

da sich andere unter Umständen auf Ihre Bestätigung verlassen.

# Gültigkeit einer Unterschrift

- durch unsere Beglaubigung
- Automatische Prüfung (Einstellungen)
  - ➔ Anzahl der jeweiligen Vertrauensstufen
    - unbekannt (q)
    - explizit kein Vertrauen (n) [no trust]
    - volles Vertrauen (f) [full trust]
    - teilweises Vertrauen (m) [marginal trust]
  - ➔ Anzahl der Schritte zum überprüften Schlüssel

# Web of Trust (Beispiel)

Alice's Web of Trust:

<b>ID</b>	<b>Unterschrieben von</b>						
	<i>Alice</i>	<b>Berti</b>	<b>Claudia</b>	<b>Doris</b>	<b>Edith</b>	<b>Franz</b>	<b>Gustav</b>
<b>Berti</b>	<i>Alice</i>						
<b>Claudia</b>		Berti		Doris			
<b>Doris</b>	<i>Alice</i>						
<b>Edith</b>			Claudia				
<b>Franz</b>			Claudia	Doris			
<b>Gustav</b>						Franz	

"My Trust" oder 1 Full Trust oder 2 Marginal Trust  
maximal 3 Schritte

# Web of Trust (Zuordnung 5)

Vertrauen in die geleisteten Bestätigungen von:  
Berti (f), Claudia (f), Edith (f), Franz (f)

Vertrauen in die Identität:

<b>Bsp 5</b>	<b>Vertr. Best.</b>	<b>1. Schritt</b>	<b>2. Schritt</b>	<b>3. Schritt</b>	<b>4. Schritt</b>
<b>Berti</b>	f	ja			
<b>Claudia</b>	f		ja (b)		
<b>Doris</b>	q	ja			
<b>Edith</b>	f			ja (c)	
<b>Franz</b>	f			ja (c)	
<b>Gustav</b>	q				<i>ja (f)</i>

# Definition des Sicherheitsbedarfes

Es ist immer ein Kompromiss zwischen Sicherheit und Bequemlichkeit zu schliessen.

- Die Wahl der Schlüssellänge
- Der Schutz des geheimen Schlüssels
- Verfallsdatum und Unterschlüssel
- Verwaltung des Web of Trust
  - ➔ Anzahl der notwendigen Beglaubigungen
  - ➔ Wahl der Pfadlänge
- Aufbau des persönlichen Web of Trust

# THE END

Ich danke für Ihre Aufmerksamkeit und stehe gerne  
für weitere Auskünfte zur Verfügung

Gerhard Öttl  
gerhard.oettl@gmx.at