

eMail-Verschlüsselung für Einsteiger

Kai 'zeus' Kostian <zeus@ctdo.de>

Chaostreff Dortmund

Chaos BBQ Weekend 2011

09.07.2011



Über mich

- Kai aka. zeus - zeus@ctdo.de
- Mitte 20 und häufig im Chaostreff-Dortmund anzutreffen und an allem interessiert, was nach Technik riecht



Index

- 1 Generelles Vorwissen zum Thema
- 2 Bedarf und Anwendungen von Verschlüsselung und Signaturen
- 3 Funktionsweise im Detail
- 4 Chain of Trust - Das Vertrauensmodell
- 5 Verschlüsselung mobil ?!?
- 6 Anwendung im täglichen Leben - So sieht die Praxis aus
- 7 Fragen und Antworten
- 8 Ende



Kryptographie kurz erklärt

- Wird seit dem Römischen Reich zur Übermittlung von geheimen Informationen genutzt (z.B. Schlachtpläne)
- Die Anfänge: Caesar-Chiffre (Schlüssel "C"):
 - DiesisteinKlartext
 - GLHVLVWHLQNODUWHAW
- Durchbruch der Verschlüsselung seit der Enigma(1918): DES(1975), RSA(1977), AES(1998), ...
- Verschiedene Verfahren: Symmetrische und Asymmetrische Schlüsselverfahren



Kryptographie kurz erklärt

- Wird seit dem Römischen Reich zur Übermittlung von geheimen Informationen genutzt (z.B. Schlachtpläne)
- Die Anfänge: Caesar-Chiffre (Schlüssel "C"):
 - DiesisteinKlartext
 - GLHVLVWHLQNODUWHAW
- Durchbruch der Verschlüsselung seit der Enigma(1918): DES(1975), RSA(1977), AES(1998), ...
- Verschiedene Verfahren: Symmetrische und Asymmetrische Schlüsselverfahren



Kryptographie kurz erklärt

- Wird seit dem Römischen Reich zur Übermittlung von geheimen Informationen genutzt (z.B. Schlachtpläne)
- Die Anfänge: Caesar-Chiffre (Schlüssel "C"):
 - DiesisteinKlartext
 - GLHVLVWHLQNODUWHAW
- Durchbruch der Verschlüsselung seit der Enigma(1918): DES(1975), RSA(1977), AES(1998), ...
- Verschiedene Verfahren: Symmetrische und Asymmetrische Schlüsselverfahren



Kryptographie kurz erklärt

- Wird seit dem Römischen Reich zur Übermittlung von geheimen Informationen genutzt (z.B. Schlachtpläne)
- Die Anfänge: Caesar-Chiffre (Schlüssel "C"):
 - DiesisteinKlartext
 - GLHVLVWHLQNODUWHAW
- Durchbruch der Verschlüsselung seit der Enigma(1918): DES(1975), RSA(1977), AES(1998), ...
- Verschiedene Verfahren: Symmetrische und Asymmetrische Schlüsselverfahren



Wie eMail funktioniert

- Elektronische Post seit 1984
- Getrennte Server für Empfang (POP3 - veraltet, und IMAP) und Versand (SMTP) einer eMail
- eMails bestehen aus Header- und Body-Teil
- Verschlüsselte Kommunikation nur bis zum Provider ohne Zusatzsoftware möglich
- eMails passieren im "Klartext" meist einige bis einige dutzend Server



Wie eMail funktioniert

- Elektronische Post seit 1984
- Getrennte Server für Empfang (POP3 - veraltet, und IMAP) und Versand (SMTP) einer eMail
- eMails bestehen aus Header- und Body-Teil
- Verschlüsselte Kommunikation nur bis zum Provider ohne Zusatzsoftware möglich
- eMails passieren im "Klartext" meist einige bis einige dutzend Server



Wie eMail funktioniert

- Elektronische Post seit 1984
- Getrennte Server für Empfang (POP3 - veraltet, und IMAP) und Versand (SMTP) einer eMail
- eMails bestehen aus Header- und Body-Teil
- Verschlüsselte Kommunikation nur bis zum Provider ohne Zusatzsoftware möglich
- eMails passieren im "Klartext" meist einige bis einige dutzend Server



Wie eMail funktioniert

- Elektronische Post seit 1984
- Getrennte Server für Empfang (POP3 - veraltet, und IMAP) und Versand (SMTP) einer eMail
- eMails bestehen aus Header- und Body-Teil
- Verschlüsselte Kommunikation nur bis zum Provider ohne Zusatzsoftware möglich
- eMails passieren im "Klartext" meist einige bis einige dutzend Server

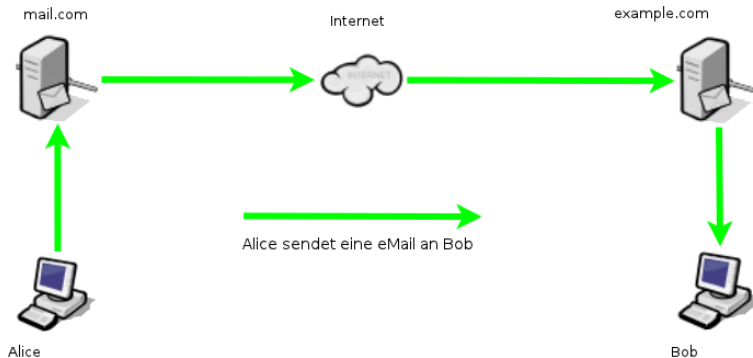


Wie eMail funktioniert

- Elektronische Post seit 1984
- Getrennte Server für Empfang (POP3 - veraltet, und IMAP) und Versand (SMTP) einer eMail
- eMails bestehen aus Header- und Body-Teil
- Verschlüsselte Kommunikation nur bis zum Provider ohne Zusatzsoftware möglich
- eMails passieren im "Klartext" meist einige bis einige dutzend Server



eMail mit Alice und Bob



Wie eMail-Verschlüsselung funktioniert - Ein Überblick

- PGP - Pretty Good Privacy (1991) - Programm zur Beschreibung des Schlüsselmodells
 - Bis Ende der 90er unter Kriegswaffengesetz in USA - mittlerweile von McAfee aufgekauft
- OpenPGP (1998) - Offener Standard und Beschreibung des Verfahrens basierend auf PGP v.5
- GnuPG (1998) - Freies Programm auf Basis des Standards von OpenPGP
- Web of Trust (Keine zentrale Zertifizierungsinstanz)



Wie eMail-Verschlüsselung funktioniert - Ein Überblick

- PGP - Pretty Good Privacy (1991) - Programm zur Beschreibung des Schlüsselmodells
 - Bis Ende der 90er unter Kriegswaffengesetz in USA - mittlerweile von McAfee aufgekauft
- OpenPGP (1998) - Offener Standard und Beschreibung des Verfahrens basierend auf PGP v.5
- GnuPG (1998) - Freies Programm auf Basis des Standards von OpenPGP
- Web of Trust (Keine zentrale Zertifizierungsinstanz)



Wie eMail-Verschlüsselung funktioniert - Ein Überblick

- PGP - Pretty Good Privacy (1991) - Programm zur Beschreibung des Schlüsselmodells
 - Bis Ende der 90er unter Kriegswaffengesetz in USA - mittlerweile von McAfee aufgekauft
- OpenPGP (1998) - Offener Standard und Beschreibung des Verfahrens basierend auf PGP v.5
- GnuPG (1998) - Freies Programm auf Basis des Standards von OpenPGP
- Web of Trust (Keine zentrale Zertifizierungsinstanz)



Wie eMail-Verschlüsselung funktioniert - Ein Überblick

- PGP - Pretty Good Privacy (1991) - Programm zur Beschreibung des Schlüsselmodells
 - Bis Ende der 90er unter Kriegswaffengesetz in USA - mittlerweile von McAfee aufgekauft
- OpenPGP (1998) - Offener Standard und Beschreibung des Verfahrens basierend auf PGP v.5
- GnuPG (1998) - Freies Programm auf Basis des Standards von OpenPGP
- Web of Trust (Keine zentrale Zertifizierungsinstanz)



Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 2048 bit) und sicherem Passwort
 - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
 - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
 - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
 - Praktische Alternative zum Schlüsseltausch: Keyserver
 - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
 - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)



Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 2048 bit) und sicherem Passwort
 - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
 - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
 - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
 - Praktische Alternative zum Schlüsseltausch: Keyserver
 - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
 - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)



Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 2048 bit) und sicherem Passwort
 - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
 - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
 - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
 - Praktische Alternative zum Schlüsseltausch: Keyserver
 - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
 - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)



Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 2048 bit) und sicherem Passwort
 - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
 - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
 - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
 - Praktische Alternative zum Schlüsseltausch: Keyserver
 - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
 - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)



Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 2048 bit) und sicherem Passwort
 - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
 - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
 - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
 - Praktische Alternative zum Schlüsseltausch: Keyserver
 - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
 - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)



Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 2048 bit) und sicherem Passwort
 - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
 - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
 - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
 - Praktische Alternative zum Schlüsseltausch: Keyserver
 - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
 - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)



Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 2048 bit) und sicherem Passwort
 - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
 - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
 - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
 - Praktische Alternative zum Schlüsseltausch: Keyserver
 - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
 - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)



Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 2048 bit) und sicherem Passwort
 - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
 - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
 - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
 - Praktische Alternative zum Schlüsseltausch: Keyserver
 - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
 - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)



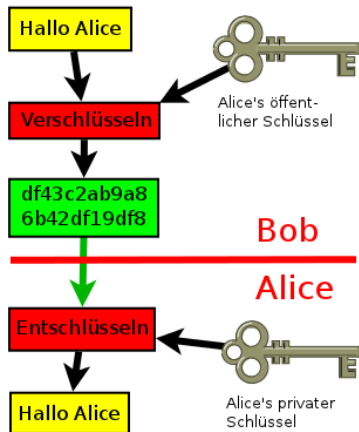
Vorraussetzungen

- Schlüsselerzeugung mit OpenPGP bei ausreichender Schlüssellänge (z.B. 2048 bit) und sicherem Passwort
 - 2 Schlüssel werden erzeugt; 1 privater und 1 öffentlicher
 - Der öffentliche Schlüssel muss an alle künftigen Kommunikationspartner weitergegeben werden
 - Der private Schlüssel sowie das Passwort **DARF NIEMALS** weitergegeben werden
- Schlüsselaustausch am besten persönlich vornehmen
 - Praktische Alternative zum Schlüsseltausch: Keyserver
 - Schlüsselserver dienen zum Austausch von Public-Keys mit automatischer Synchronisation untereinander
 - **Achtung: Verifikation von Schlüsseln ist bei Nutzung von Keyservern wichtiger denn je !!**
- Verifizierung von Schlüsseln entweder persönlich oder über alternative Kanäle (z.B. Fingerprint am Telefon vorlesen)

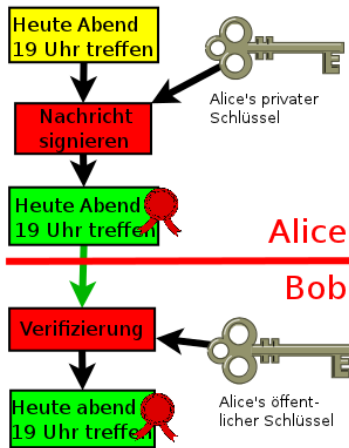


eMail-Verschlüsselung mit Alice und Bob

Verschlüsselung einer Mail



Signierung und Verifikation



Privater Bereich

- Der typische "Liebesbrief" und ähnliches
- Vertrauen durch Schweigepflicht bei Ärzten, Psychiatern, Geistlichen, Beratungsstellen, etc.
- Schutz vor Behörden und staatlicher Repression
- Kann ich meinem Gegenüber vertrauen, dass er/sie auch wirklich er/sie ist ?



Privater Bereich

- Der typische "Liebesbrief" und ähnliches
- Vertrauen durch Schweigepflicht bei Ärzten, Psychiatern, Geistlichen, Beratungsstellen, etc.
- Schutz vor Behörden und staatlicher Repression
- Kann ich meinem Gegenüber vertrauen, dass er/sie auch wirklich er/sie ist ?



Privater Bereich

- Der typische "Liebesbrief" und ähnliches
- Vertrauen durch Schweigepflicht bei Ärzten, Psychiatern, Geistlichen, Beratungsstellen, etc.
- Schutz vor Behörden und staatlicher Repression
- Kann ich meinem Gegenüber vertrauen, dass er/sie auch wirklich er/sie ist ?



Privater Bereich

- Der typische "Liebesbrief" und ähnliches
- Vertrauen durch Schweigepflicht bei Ärzten, Psychiatern, Geistlichen, Beratungsstellen, etc.
- Schutz vor Behörden und staatlicher Repression
- Kann ich meinem Gegenüber vertrauen, dass er/sie auch wirklich er/sie ist ?



Geschäftlicher Bereich

- Wirtschaftlicher Bedarf an Vertrauenswürdigkeit, da häufig viel Geld im Spiel ist
- Schutz vor der Konkurrenz
- Leaking !!!



Geschäftlicher Bereich

- Wirtschaftlicher Bedarf an Vertrauenswürdigkeit, da häufig viel Geld im Spiel ist
- Schutz vor der Konkurrenz
- Leaking !!!



Geschäftlicher Bereich

- Wirtschaftlicher Bedarf an Vertrauenswürdigkeit, da häufig viel Geld im Spiel ist
- Schutz vor der Konkurrenz
- Leaking !!!



Hoheitlicher Bereich

- Da ist noch viel viel mehr Geld im Spiel...
- Schutz vor anderen Staaten und Nationen
- Sicherstellung der Geheimniswahrung kann ggf. über Leben und Tod sowie über Krieg und Frieden entscheiden
- Hier ist Leaking noch deutlich brisanter als bei Firmen (siehe WikiLeaks) !!



Hoheitlicher Bereich

- Da ist noch viel viel mehr Geld im Spiel...
- Schutz vor anderen Staaten und Nationen
- Sicherstellung der Geheimniswahrung kann ggf. über Leben und Tod sowie über Krieg und Frieden entscheiden
- Hier ist Leaking noch deutlich brisanter als bei Firmen (siehe WikiLeaks) !!



Hoheitlicher Bereich

- Da ist noch viel viel mehr Geld im Spiel...
- Schutz vor anderen Staaten und Nationen
- Sicherstellung der Geheimniswahrung kann ggf. über Leben und Tod sowie über Krieg und Frieden entscheiden
- Hier ist Leaking noch deutlich brisanter als bei Firmen (siehe WikiLeaks) !!



Hoheitlicher Bereich

- Da ist noch viel viel mehr Geld im Spiel...
- Schutz vor anderen Staaten und Nationen
- Sicherstellung der Geheimniswahrung kann ggf. über Leben und Tod sowie über Krieg und Frieden entscheiden
- Hier ist Leaking noch deutlich brisanter als bei Firmen (siehe WikiLeaks) !!



Bedarf an Vertrauenswürdigkeit - Fazit

• Das Fazit

- 1. Je peinlicher oder persönlicher eine Information, desto mehr Bedarf an Schutzwürdigkeit
- 2. Je brisanter die Informationen, desto mehr Bedarf an Schutzwürdigkeit
- 3. Je teurer es ist, wenn Informationen in die falschen Hände gelangen, desto mehr Bedarf an Schutzwürdigkeit



Bedarf an Vertrauenswürdigkeit - Fazit

- Das Fazit

- 1. Je peinlicher oder persönlicher eine Information, desto mehr Bedarf an Schutzwürdigkeit
- 2. Je brisanter die Informationen, desto mehr Bedarf an Schutzwürdigkeit
- 3. Je teurer es ist, wenn Informationen in die falschen Hände gelangen, desto mehr Bedarf an Schutzwürdigkeit



Unterschied https:// und eMail-Verschlüsselung

- https ersetzt eMail-Verschlüsselung **NICHT**
- https schützt vor Account- und Identitätsdiebstahl
- eMail-Verschlüsselung schützt vor Manipulation, vor Mitlesern und ermöglicht Authentifizierung des Kommunikationspartners
- beides sind **ERGÄNZENDE** Verfahren, **NIEMALS** eMail-Verschlüsselung ohne https bzw. TLS/SSL benutzen!!!



Unterschied https:// und eMail-Verschlüsselung

- https ersetzt eMail-Verschlüsselung **NICHT**
- https schützt vor Account- und Identitätsdiebstahl
- eMail-Verschlüsselung schützt vor Manipulation, vor Mitlesen und ermöglicht Authentifizierung des Kommunikationspartners
- beides sind **ERGÄNZENDE** Verfahren, **NIEMALS** eMail-Verschlüsselung ohne https bzw. TLS/SSL benutzen!!!



Unterschied https:// und eMail-Verschlüsselung

- https ersetzt eMail-Verschlüsselung **NICHT**
- https schützt vor Account- und Identitätsdiebstahl
- eMail-Verschlüsselung schützt vor Manipulation, vor Mitlesern und ermöglicht Authentifizierung des Kommunikationspartners
- beides sind **ERGÄNZENDE** Verfahren, **NIEMALS** eMail-Verschlüsselung ohne https bzw. TLS/SSL benutzen!!!



Unterschied https:// und eMail-Verschlüsselung

- https ersetzt eMail-Verschlüsselung **NICHT**
- https schützt vor Account- und Identitätsdiebstahl
- eMail-Verschlüsselung schützt vor Manipulation, vor Mitlesern und ermöglicht Authentifizierung des Kommunikationspartners
- beides sind **ERGÄNZENDE** Verfahren, **NIEMALS** eMail-Verschlüsselung ohne https bzw. TLS/SSL benutzen!!!



GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern **UND** Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

Vorteile:

- Überprüfbarkeit der Authentizität von Schlüsseln durch Fingerprints
- Überprüfbarkeit einer Nachricht auf Manipulation durch Signaturen
- Erweiterung von "Vertrauen" durch Keysigning (gegenseitiges Unterschreiben von Schlüsseln)
 - Verschiedene Vertrauensebenen - Ein wesentlicher Bestandteil der Chain of Trust / des Web of Trust



GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern **UND** Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

Vorteile:

- Überprüfbarkeit der Authentizität von Schlüsseln durch Fingerprints
- Überprüfbarkeit einer Nachricht auf Manipulation durch Signaturen
- Erweiterung von "Vertrauen" durch Keysigning (gegenseitiges Unterschreiben von Schlüsseln)
 - Verschiedene Vertrauensebenen - Ein wesentlicher Bestandteil der Chain of Trust / des Web of Trust



GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern **UND** Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

Vorteile:

- Überprüfbarkeit der Authentizität von Schlüsseln durch Fingerprints
- Überprüfbarkeit einer Nachricht auf Manipulation durch Signaturen
- Erweiterung von "Vertrauen" durch Keysigning (gegenseitiges Unterschreiben von Schlüsseln)
 - Verschiedene Vertrauensebenen - Ein wesentlicher Bestandteil der Chain of Trust / des Web of Trust



GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern **UND** Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

Vorteile:

- Überprüfbarkeit der Authentizität von Schlüsseln durch Fingerprints
- Überprüfbarkeit einer Nachricht auf Manipulation durch Signaturen
- Erweiterung von "Vertrauen" durch Keysigning (gegenseitiges Unterschreiben von Schlüsseln)
 - Verschiedene Vertrauensebenen - Ein wesentlicher Bestandteil der Chain of Trust / des Web of Trust



GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern **UND** Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

Vorteile:

- Überprüfbarkeit der Authentizität von Schlüsseln durch Fingerprints
- Überprüfbarkeit einer Nachricht auf Manipulation durch Signaturen
- Erweiterung von "Vertrauen" durch Keysigning (gegenseitiges Unterschreiben von Schlüsseln)
 - Verschiedene Vertrauensebenen - Ein wesentlicher Bestandteil der Chain of Trust / des Web of Trust



GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern **UND** Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

Vorteile:

- Überprüfbarkeit der Authentizität von Schlüsseln durch Fingerprints
- Überprüfbarkeit einer Nachricht auf Manipulation durch Signaturen
- Erweiterung von "Vertrauen" durch Keysigning (gegenseitiges Unterschreiben von Schlüsseln)
 - Verschiedene Vertrauensebenen - Ein wesentlicher Bestandteil der Chain of Trust / des Web of Trust



GPG, PGP, GnuPG... und andere P und G's...

- Asymmetrisches Schlüsselverfahren mit Passwörtern **UND** Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

Vorteile:

- Überprüfbarkeit der Authentizität von Schlüsseln durch Fingerprints
- Überprüfbarkeit einer Nachricht auf Manipulation durch Signaturen
- Erweiterung von "Vertrauen" durch Keysigning (gegenseitiges Unterschreiben von Schlüsseln)
 - Verschiedene Vertrauensebenen - Ein wesentlicher Bestandteil der Chain of Trust / des Web of Trust



GPG, PGP, GnuPG... und andere P und G's...

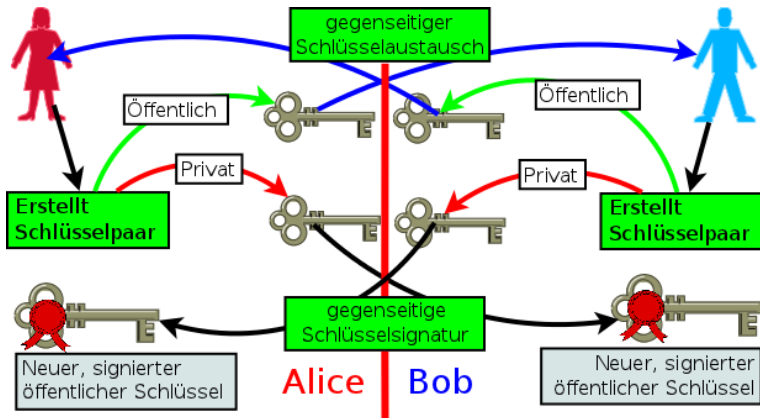
- Asymmetrisches Schlüsselverfahren mit Passwörtern **UND** Schlüsseldateien
- Private- und Public-Keys
- Signatur mit **Private**-Key des Senders
- Verschlüsselung mit **Public**-Key des Empfängers
- Entschlüsselung durch **Private**-Key des Empfängers

Vorteile:

- Überprüfbarkeit der Authentizität von Schlüsseln durch Fingerprints
- Überprüfbarkeit einer Nachricht auf Manipulation durch Signaturen
- Erweiterung von "Vertrauen" durch Keysigning (gegenseitiges Unterschreiben von Schlüsseln)
 - Verschiedene Vertrauensebenen - Ein wesentlicher Bestandteil der Chain of Trust / des Web of Trust



Keysigning mit Alice und Bob



Fingerprints im Detail

- Für Penible: Der Fingerprint ist ein 160-bit SHA-1-Hash des Octets 0x99 über den Public-Key (RFC4880 Kapitel 12.2)
- Key-ID: Die unsignifikantesten (letzten) 64 Bits des Fingerprints
- Hex-Dezimale Notation von Fingerprints und Key-ID's
- Beispiel: Immo Wehrenberg - immo@bundessicherheitsministerium.de

	Fingerprint-Aufbau
Print:	8BFC 303C 1574 5912 23B5 CFDD 5A59 5F09 9B40 9979
ID:	0x 9B40 9979



Fingerprints im Detail

- Für Penible: Der Fingerprint ist ein 160-bit SHA-1-Hash des Octets 0x99 über den Public-Key (RFC4880 Kapitel 12.2)
- Key-ID: Die unsignifikantesten (letzten) 64 Bits des Fingerprints
- Hex-Dezimale Notation von Fingerprints und Key-ID's
- Beispiel: Immo Wehrenberg - immo@bundessicherheitsministerium.de

	Fingerprint-Aufbau
Print:	8BFC 303C 1574 5912 23B5 CFDD 5A59 5F09 9B40 9979
ID:	0x 9B40 9979



Fingerprints im Detail

- Für Penible: Der Fingerprint ist ein 160-bit SHA-1-Hash des Octets 0x99 über den Public-Key (RFC4880 Kapitel 12.2)
- Key-ID: Die unsignifikantesten (letzten) 64 Bits des Fingerprints
- Hex-Dezimale Notation von Fingerprints und Key-ID's
- Beispiel: Immo Wehrenberg - immo@bundessicherheitsministerium.de

	Fingerprint-Aufbau
Print:	8BFC 303C 1574 5912 23B5 CFDD 5A59 5F09 9B40 9979
ID:	0x 9B40 9979



Fingerprints im Detail

- Für Penible: Der Fingerprint ist ein 160-bit SHA-1-Hash des Octets 0x99 über den Public-Key (RFC4880 Kapitel 12.2)
- Key-ID: Die unsignifikantesten (letzten) 64 Bits des Fingerprints
- Hex-Dezimale Notation von Fingerprints und Key-ID's
- Beispiel: Immo Wehrenberg - immo@bundessicherheitsministerium.de

	Fingerprint-Aufbau
Print:	8BFC 303C 1574 5912 23B5 CFDD 5A59 5F09 9B40 9979
ID:	0x 9B40 9979



Fingerprints im Detail

- Für Penible: Der Fingerprint ist ein 160-bit SHA-1-Hash des Octets 0x99 über den Public-Key (RFC4880 Kapitel 12.2)
- Key-ID: Die unsignifikantesten (letzten) 64 Bits des Fingerprints
- Hex-Dezimale Notation von Fingerprints und Key-ID's
- Beispiel: Immo Wehrenberg - immo@bundessicherheitsministerium.de

	Fingerprint-Aufbau
Print:	8BFC 303C 1574 5912 23B5 CFDD 5A59 5F09 9B40 9979
ID:	0x 9B40 9979



Chain of Trust - Teil I : Die Theorie

In der Theorie ist Theorie und Praxis Ein- und Dasselbe

In der Theorie ...

- ...gibt man niemals den Private-Key oder das Passwort weiter (oder vergisst eines von beiden irgendwo...)
- ...Nimmt man für jeden Zweck ein anderes Passwort
- ...benutzt man nur "sichere" Passwörter mit >20 Zeichen, mit Sonderzeichen, Groß- und Kleinbuchstaben und Zahlen
- ...benutzt man nur vertrauenswürdige Hard-& Software und zwar nur in Umgebungen, die man vollständig kontrollieren kann



Chain of Trust - Teil I : Die Theorie

In der Theorie ist Theorie und Praxis Ein- und Dasselbe

In der Theorie ...

- ...gibt man niemals den Private-Key oder das Passwort weiter (oder vergisst eines von beiden irgendwo...)
- ...Nimmt man für jeden Zweck ein anderes Passwort
- ...benutzt man nur "sichere" Passwörter mit >20 Zeichen, mit Sonderzeichen, Groß- und Kleinbuchstaben und Zahlen
- ...benutzt man nur vertrauenswürdige Hard-& Software und zwar nur in Umgebungen, die man vollständig kontrollieren kann



Chain of Trust - Teil I : Die Theorie

In der Theorie ist Theorie und Praxis Ein- und Dasselbe

In der Theorie ...

- ...gibt man niemals den Private-Key oder das Passwort weiter (oder vergisst eines von beiden irgendwo...)
- ...Nimmt man für jeden Zweck ein anderes Passwort
- ...benutzt man nur "sichere" Passwörter mit >20 Zeichen, mit Sonderzeichen, Groß- und Kleinbuchstaben und Zahlen
- ...benutzt man nur vertrauenswürdige Hard-& Software und zwar nur in Umgebungen, die man vollständig kontrollieren kann



Chain of Trust - Teil I : Die Theorie

In der Theorie ist Theorie und Praxis Ein- und Dasselbe

In der Theorie ...

- ...gibt man niemals den Private-Key oder das Passwort weiter (oder vergisst eines von beiden irgendwo...)
- ...Nimmt man für jeden Zweck ein anderes Passwort
- ...benutzt man nur "sichere" Passwörter mit >20 Zeichen, mit Sonderzeichen, Groß- und Kleinbuchstaben und Zahlen
- ...benutzt man nur vertrauenswürdige Hard-& Software und zwar nur in Umgebungen, die man vollständig kontrollieren kann



Chain of Trust - Teil I : Die Theorie

In der Theorie ist Theorie und Praxis Ein- und Dasselbe

In der Theorie ...

- ...gibt man niemals den Private-Key oder das Passwort weiter (oder vergisst eines von beiden irgendwo...)
- ...Nimmt man für jeden Zweck ein anderes Passwort
- ...benutzt man nur "sichere" Passwörter mit >20 Zeichen, mit Sonderzeichen, Groß- und Kleinbuchstaben und Zahlen
- ...benutzt man nur vertrauenswürdige Hard-& Software und zwar nur in Umgebungen, die man vollständig kontrollieren kann



Chain of Trust - Teil II : Die Praxis

Wenn man sagt, dass man einer Sache grundsätzlich zustimmt, so bedeutet es, dass man nicht die geringste Absicht hat, sie in der Praxis durchzuführen. -Otto von Bismarck

In der Praxis...

- ...passieren Fehler eher selten durch schlechte Konzepte oder Technik, sondern durch dessen mangelhafte Umsetzung
- ...ist der Mensch nach wie vor der "Single Point of Failure" in diesem Trustmodell
- ...passieren die meisten GAUs immernoch durch:
 - Dummheit
 - Naivität
 - Faulheit
 - oder Schusseligkeit
- Das ist nun mal die Realität...



Chain of Trust - Teil II : Die Praxis

Wenn man sagt, dass man einer Sache grundsätzlich zustimmt, so bedeutet es, dass man nicht die geringste Absicht hat, sie in der Praxis durchzuführen. -Otto von Bismarck
In der Praxis...

- ...passieren Fehler eher selten durch schlechte Konzepte oder Technik, sondern durch dessen mangelhafte Umsetzung
- ...ist der Mensch nach wie vor der "Single Point of Failure" in diesem Trustmodell
- ...passieren die meisten GAUs immernoch durch:
 - Dummheit
 - Naivität
 - Faulheit
 - oder Schusseligkeit
- Das ist nun mal die Realität...



Chain of Trust - Teil II : Die Praxis

Wenn man sagt, dass man einer Sache grundsätzlich zustimmt, so bedeutet es, dass man nicht die geringste Absicht hat, sie in der Praxis durchzuführen. -Otto von Bismarck

In der Praxis...

- ...passieren Fehler eher selten durch schlechte Konzepte oder Technik, sondern durch dessen mangelhafte Umsetzung
- ...ist der Mensch nach wie vor der "Single Point of Failure" in diesem Trustmodell
- ...passieren die meisten GAUs immernoch durch:
 - Dummheit
 - Naivität
 - Faulheit
 - oder Schusseligkeit
- Das ist nun mal die Realität...



Chain of Trust - Teil II : Die Praxis

Wenn man sagt, dass man einer Sache grundsätzlich zustimmt, so bedeutet es, dass man nicht die geringste Absicht hat, sie in der Praxis durchzuführen. -Otto von Bismarck

In der Praxis...

- ...passieren Fehler eher selten durch schlechte Konzepte oder Technik, sondern durch dessen mangelhafte Umsetzung
- ...ist der Mensch nach wie vor der "Single Point of Failure" in diesem Trustmodell
- ...passieren die meisten GAUs immernoch durch:
 - Dummheit
 - Naivität
 - Faulheit
 - oder Schusseligkeit
- Das ist nun mal die Realität...



Chain of Trust - Teil II : Die Praxis

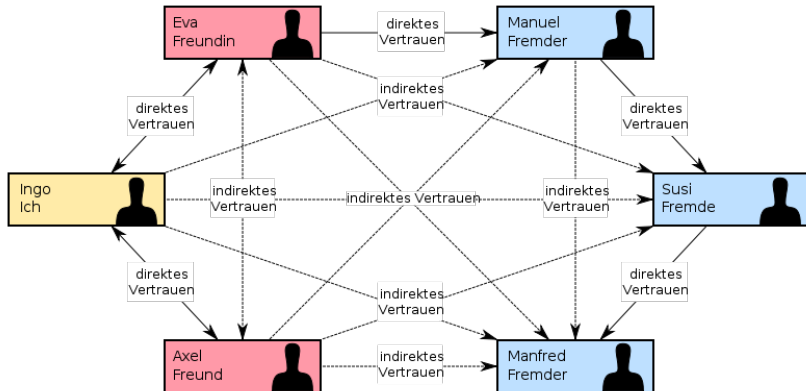
Wenn man sagt, dass man einer Sache grundsätzlich zustimmt, so bedeutet es, dass man nicht die geringste Absicht hat, sie in der Praxis durchzuführen. -Otto von Bismarck

In der Praxis...

- ...passieren Fehler eher selten durch schlechte Konzepte oder Technik, sondern durch dessen mangelhafte Umsetzung
- ...ist der Mensch nach wie vor der "Single Point of Failure" in diesem Trustmodell
- ...passieren die meisten GAUs immernoch durch:
 - Dummheit
 - Naivität
 - Faulheit
 - oder Schusseligkeit
- Das ist nun mal die Realität...



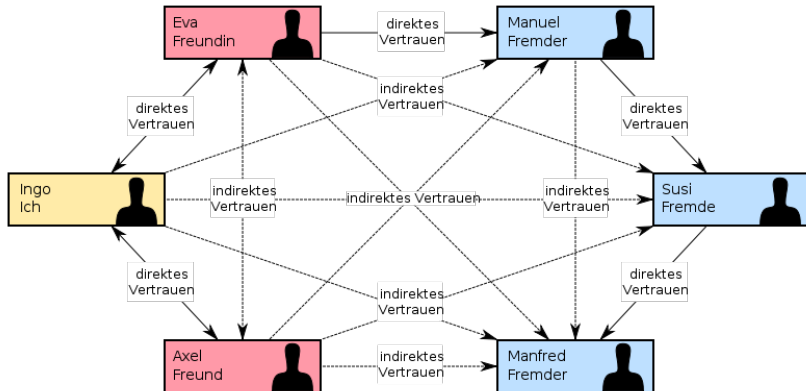
Web of Trust - Vertrauensketten



- Schaffung von Vertrauensketten durch direktes und indirektes Vertrauen
- Kurz gesagt: Ich vertraue Jedem, dem von Jemandem vertraut wird, dem ich vertraue



Web of Trust - Vertrauensketten



- Schaffung von Vertrauensketten durch direktes und indirektes Vertrauen
- Kurz gesagt: Ich vertraue Jedem, dem von Jemandem vertraut wird, dem ich vertraue



Backups

- Backups von privaten Schlüsseln anzufertigen ist **UNERLÄSSLICH**
- Der goldene Weg: Auf Papier ausdrucken, und im Schliessfach/Tresor lagern, am besten redundant
 - Problem: bei Verlust/Verlegen des Keys ist das abtippen mühselig (etwa 1 Din-A4 Seite voller kryptischer Zeichen)
- Fazit: Jedes Konzept hat seine Schwächen



Backups

- Backups von privaten Schlüsseln anzufertigen ist **UNERLÄSSLICH**
- Der goldene Weg: Auf Papier ausdrucken, und im Schliessfach/Tresor lagern, am besten redundant
 - Problem: bei Verlust/Verlegen des Keys ist das abtippen mühselig (etwa 1 Din-A4 Seite voller kryptischer Zeichen)
- Fazit: Jedes Konzept hat seine Schwächen

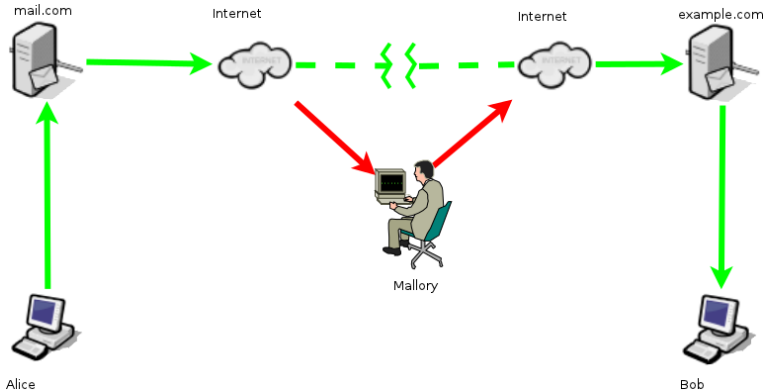


Backups

- Backups von privaten Schlüsseln anzufertigen ist **UNERLÄSSLICH**
- Der goldene Weg: Auf Papier ausdrucken, und im Schliessfach/Tresor lagern, am besten redundant
 - Problem: bei Verlust/Verlegen des Keys ist das abtippen mühselig (etwa 1 Din-A4 Seite voller kryptischer Zeichen)
- Fazit: Jedes Konzept hat seine Schwächen



Man-in-the-Middle Attacke



Ist nur mit Vorsicht zu genießen

Verschlüsselung mobil, tragbar und bequem auf dem USB-Stick ist zwar möglich, aber nicht ratsam, denn man bricht die Chain of Trust:

- man hat das "Zielsystem" seltenst auch nur halbwegs unter Kontrolle (z.B. Keylogger)
- man kann nicht abschätzen, wo Private-Key oder Passwort vielleicht landen
- gestohlene Identitäten sind besonders tragisch, wenn sich der "Dieb" auch noch authentifizieren kann
- halbwegs sicherer weg für alle, die, Warnungen ignorieren wollen:
 - verschlüsselter USB-Stick (oder CD) mit Keys drauf
 - am besten als bootbares Live-System
 - **DAS ALLES HILFT TROTZDEM NICHTS GEGEN MANIPULIERTE TASTATUREN ODER FIES AUSGERICHTETE KAMERAS!!**



Ist nur mit Vorsicht zu genießen

Verschlüsselung mobil, tragbar und bequem auf dem USB-Stick ist zwar möglich, aber nicht ratsam, denn man bricht die Chain of Trust:

- man hat das "Zielsystem" seltenst auch nur halbwegs unter Kontrolle (z.B. Keylogger)
- man kann nicht abschätzen, wo Private-Key oder Passwort vielleicht landen
- gestohlene Identitäten sind besonders tragisch, wenn sich der "Dieb" auch noch authentifizieren kann
- halbwegs sicherer weg für alle, die, Warnungen ignorieren wollen:
 - verschlüsselter USB-Stick (oder CD) mit Keys drauf
 - am besten als bootbares Live-System
 - **DAS ALLES HILFT TROTZDEM NICHTS GEGEN MANIPULIERTE TASTATUREN ODER FIES AUSGERICHTETE KAMERAS!!**



Ist nur mit Vorsicht zu genießen

Verschlüsselung mobil, tragbar und bequem auf dem USB-Stick ist zwar möglich, aber nicht ratsam, denn man bricht die Chain of Trust:

- man hat das "Zielsystem" seltenst auch nur halbwegs unter Kontrolle (z.B. Keylogger)
- man kann nicht abschätzen, wo Private-Key oder Passwort vielleicht landen
- gestohlene Identitäten sind besonders tragisch, wenn sich der "Dieb" auch noch authentifizieren kann
- halbwegs sicherer weg für alle, die, Warnungen ignorieren wollen:
 - verschlüsselter USB-Stick (oder CD) mit Keys drauf
 - am besten als bootbares Live-System
 - **DAS ALLES HILFT TROTZDEM NICHTS GEGEN MANIPULIERTE TASTATUREN ODER FIES AUSGERICHTETE KAMERAS!!**



Ist nur mit Vorsicht zu genießen

Verschlüsselung mobil, tragbar und bequem auf dem USB-Stick ist zwar möglich, aber nicht ratsam, denn man bricht die Chain of Trust:

- man hat das "Zielsystem" seltenst auch nur halbwegs unter Kontrolle (z.B. Keylogger)
- man kann nicht abschätzen, wo Private-Key oder Passwort vielleicht landen
- gestohlene Identitäten sind besonders tragisch, wenn sich der "Dieb" auch noch authentifizieren kann
- halbwegs sicherer weg für alle, die, Warnungen ignorieren wollen:
 - verschlüsselter USB-Stick (oder CD) mit Keys drauf
 - am besten als bootbares Live-System
 - **DAS ALLES HILFT TROTZDEM NICHTS GEGEN MANIPULIERTE TASTATUREN ODER FIES AUSGERICHTETE KAMERAS!!**



Ist nur mit Vorsicht zu genießen

Verschlüsselung mobil, tragbar und bequem auf dem USB-Stick ist zwar möglich, aber nicht ratsam, denn man bricht die Chain of Trust:

- man hat das "Zielsystem" seltenst auch nur halbwegs unter Kontrolle (z.B. Keylogger)
- man kann nicht abschätzen, wo Private-Key oder Passwort vielleicht landen
- gestohlene Identitäten sind besonders tragisch, wenn sich der "Dieb" auch noch authentifizieren kann
- halbwegs sicherer weg für alle, die, Warnungen ignorieren wollen:
 - verschlüsselter USB-Stick (oder CD) mit Keys drauf
 - am besten als bootbares Live-System
 - **DAS ALLES HILFT TROTZDEM NICHTS GEGEN MANIPULIERTE TASTATUREN ODER FIES AUSGERICHTETE KAMERAS!!**



Praxisbeispiel: Thunderbird mit Enigmail-Addon unter Linux

AB HIER KOMMT
EINE GANZ TOLLE
SUPER-LIVE-DEMO



Was Ihr sonst noch so wissen wollt...

Hier ist jetzt Platz für Fragen und Antworten zum Thema

- - -

Diese Vortragsfolien gibt es auch zum Download unter
<http://wiki.ctdo.de/browser/vortraege/gnupg-vortrag/>

- - -

Lizenziert unter Creative Commons Deutsch 3.0 BY-NC-SA
<http://creativecommons.org/licenses/by-nc-sa/3.0/de/>

- - -



Links zum selber Nachlesen

Bild auf Seite 20: http://de.wikipedia.org/wiki/Datei:Web_of_Trust.svg

Links zum Thema:

- <http://www.chaostreff-dortmund.de>
- <http://de.wikipedia.org/wiki/E-Mail-Verschlüsselung>
- http://de.wikipedia.org/wiki/Pretty_Good_Privacy
- <http://de.wikipedia.org/wiki/OpenPGP>
- <http://de.wikipedia.org/wiki/Gnupg>
- http://de.wikipedia.org/wiki/Alice_und_Bob
- http://de.wikipedia.org/wiki/Web_of_trust
- <http://de.wikipedia.org/wiki/Schlüsselserver>
- <http://de.wikipedia.org/wiki/Hexadezimalsystem>
- <http://de.wikipedia.org/wiki/SHA-1>
- <http://tools.ietf.org/html/rfc4880>



Ende des Vortragsteils

Danke das ihr solange durchgehalten habt!

