Vergangenheit, Gegenwart und Zukunft von GnuPG

Werner Koch

39. DAFTA — Köln

19. November 2015

Übersicht

Wir schreiben das Jahr 1991

PGP-2

- Phil Zimmermann schreibt erste öffentliche Verschlüsselungssoftware.
- Wesentlich verbessert von Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA Patent
- Problem 2: IDEA Patent
- Problem 3: Exportkontrolle

Wir schreiben das Jahr 1991

PGP-2

- Phil Zimmermann schreibt erste öffentliche Verschlüsselungssoftware.
- Wesentlich verbessert von Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA Patent
- Problem 2: IDEA Patent
- Problem 3: Exportkontrolle

Wir schreiben das Jahr 1991

PGP-2

- Phil Zimmermann schreibt erste öffentliche Verschlüsselungssoftware.
- Wesentlich verbessert von Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA Patent
- Problem 2: IDEA Patent
- Problem 3: Exportkontrolle

Wir schreiben das Jahr 1991

PGP-2

- Phil Zimmermann schreibt erste öffentliche Verschlüsselungssoftware.
- Wesentlich verbessert von Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA Patent
- Problem 2: IDEA Patent
- Problem 3: Exportkontrolle

Wir schreiben das Jahr 1991

PGP-2

- Phil Zimmermann schreibt erste öffentliche Verschlüsselungssoftware.
- Wesentlich verbessert von Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA Patent
- Problem 2: IDEA Patent
- Problem 3: Exportkontrolle

5 Jahre später

1996 PGP Inc. gegründet

1997 DH Patent abgelaufen, PGP-5 veröffentlicht.

1997 IETF Arbeitsgruppe für OpenPGP gegründet.

1998 PGP Inc. von NAI gekauft.

1998 RFC-2440 veröffentlicht.

2002 NAI stellt Support für PGP ein.

2007 RFC-4880 veröffentlicht.

2012 RFC-6637 veröffentlicht (ECC Erweiterung)

IN Kongreß 1997

Start

Zurück

Vorträge des Kongreß 97

des Individual Network e.V.

27. und 28. September 1997

Samstag, 27. September 1997		
Zeit	Security	New Technologies
9:00-9:30	Heiko Schlichting Keynote	
9:30-10:30	Norbert Pohlmann Firewall-Technologien	Werner Almesberger ATM und Linux
10:30-11:30	T. Zieschang Security und Chipcards	Dave S. Miller Linux on Sparc
11:30-12:30	M. Klische, DCS AG Biometrische Personenidentifikation	Stephen R. van den Berg SPAM, procmail, cucipop
12:30-13:30	Mittagessen	
13:30-14:30	Andreas Bäß Status DPN	Bruce Perens, Pixar Inc. Debian GNU/Linux
14:30-15:30	Arttu Huhtiniemi, SolidTech Database and JAVA	Xlink
15:30-16:00	Pause	
16:00-17:00	Gerhard Unger Secure Computing	Bettina Kauth, DFN-NOC Status des B-WiN
17:00-18:00	Richard Stallman GNU Current Projects, Ethico-Political issues of free software	
20:00-offen	Buffet Geselliger Abend	
Sonntag, 28. September 1997		
Zeit	Security	New Technologies
9:30-10:30	Jörg Ladwein Security Dynamics	Jan Vekemans, Vasco Internet-AcessKey
10:30-11:30	Lutz Donnerhacke CA+PGP-Keys	
11:30-13:00	Brunch	
13:00-14:00	Thomas Hetschold, GMD Secude	K. Schröter, DOCconnect AG DOCconnect, Med. Network
14:00-15:00	Alan Cox IPv6	Progressive Networks Live Video
15:00-16:00	D. James Bidzos Präsident der RSA Inc.	

GnuPG

g10 / GnuPG

„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden."

- PGP-5 keine Freie Software.
- Dezember 1997: g10 als PGP-2 Ersatz:
  - Keine patentierten Verfahren
  - Als Unix Werkzeug entworfen
- Frühjahr 1998: Name auf GnuPG geändert; nun OpenPGP.

g10 / GnuPG

„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden."

- PGP-5 keine Freie Software.
- Dezember 1997: g10 als PGP-2 Ersatz:
  - Keine patentierten Verfahren
  - Als Unix Werkzeug entworfen
- Frühjahr 1998: Name auf GnuPG geändert; nun OpenPGP.

g10 / GnuPG

„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden."

- PGP-5 keine Freie Software.
- Dezember 1997: g10 als PGP-2 Ersatz:
  - Keine patentierten Verfahren
  - Als Unix Werkzeug entworfen
- Frühjahr 1998: Name auf GnuPG geändert; nun OpenPGP.

Auswahl der Algorithmen

- Ursprungsversion (g10)
  - Elgamal ersetzt RSA (signieren und verschlüsseln).
  - Blowfish für symmetrische Verschlüsselung.
  - IDEA+RSA als Plugin zu PGP-2 Kompatibilität in einigen Ländern.
- OpenPGP hat Unterschlüssel
  - DSA für Signaturen, Elgamal zur Verschlüsselung.
  - 3DES oder CAST5 zur symmetrische Verschlüsselung.
  - RSA im September 2000 hinzugefügt
- GnuPG und PGP-{5,6,7}
  - Zusammenarbeit mit Hal Finney und Jon Callas.
  - Informale Interoperabilitättests.
  - Testen von neuen Features.

Auswahl der Algorithmen

- Ursprungsversion (g10)
  - Elgamal ersetzt RSA (signieren und verschlüsseln).
  - Blowfish für symmetrische Verschlüsselung.
  - IDEA+RSA als Plugin zu PGP-2 Kompatibilität in einigen Ländern.
- OpenPGP hat Unterschlüssel
  - DSA für Signaturen, Elgamal zur Verschlüsselung.
  - 3DES oder CAST5 zur symmetrische Verschlüsselung.
  - RSA im September 2000 hinzugefügt
- GnuPG und PGP-{5,6,7}
  - Zusammenarbeit mit Hal Finney und Jon Callas.
  - Informale Interoperabilitättests.
  - Testen von neuen Features.

Auswahl der Algorithmen

- Ursprungsversion (g10)
  - Elgamal ersetzt RSA (signieren und verschlüsseln).
  - Blowfish für symmetrische Verschlüsselung.
  - IDEA+RSA als Plugin zu PGP-2 Kompatibilität in einigen Ländern.
- OpenPGP hat Unterschlüssel
  - DSA für Signaturen, Elgamal zur Verschlüsselung.
  - 3DES oder CAST5 zur symmetrische Verschlüsselung.
  - RSA im September 2000 hinzugefügt
- GnuPG und PGP-{5,6,7}
  - Zusammenarbeit mit Hal Finney und Jon Callas.
  - Informale Interoperabilitättests.
  - Testen von neuen Features.

GnuPG-2

- g10^{code} gegründet in 2001.
- Ausschreibung zur Implementierung von S/MIME gewonnen.
  - zusammen mit Intevation (Osnabrück)
  - und KDAB (Berlin).
- ...Start von GnuPG-2 (2003)
  - Modularisiert
  - Separate Krypto-Bibliothek
  - Bibliothek mit GnuPG API (gpgme)

GnuPG-2

- g10^{code} gegründet in 2001.
- Ausschreibung zur Implementierung von S/MIME gewonnen.
  - zusammen mit Intevation (Osnabrück)
  - und KDAB (Berlin).
- ...Start von GnuPG-2 (2003)
  - Modularisiert
  - Separate Krypto-Bibliothek
  - Bibliothek mit GnuPG API (gpgme)

GnuPG-2

- g10^{code} gegründet in 2001.
- Ausschreibung zur Implementierung von S/MIME gewonnen.
  - zusammen mit Intevation (Osnabrück)
  - und KDAB (Berlin).
- ...Start von GnuPG-2 (2003)
  - Modularisiert
  - Separate Krypto-Bibliothek
  - Bibliothek mit GnuPG API (gpgme)

Portierung nach Windows

- Experimenteller Port in 1998.
- Vollständiger Port in 2000.
  - Aufgrund eines Projekts des BMWi
- Gpg4win wurde 2006 veröffentlicht
- GnuPG-2 war nicht für eine Windows Portierung vorgesehen
  - . . . wir haben es dann aber doch geschafft.
- Zirka 4000 Gpg4win 2.x Downloads am Tag

Portierung nach Windows

- Experimenteller Port in 1998.
- Vollständiger Port in 2000.
  - Aufgrund eines Projekts des BMWi
- Gpg4win wurde 2006 veröffentlicht
- GnuPG-2 war nicht für eine Windows Portierung vorgesehen
  - . . . wir haben es dann aber doch geschafft.
- Zirka 4000 Gpg4win 2.x Downloads am Tag

Portierung nach Windows

- Experimenteller Port in 1998.
- Vollständiger Port in 2000.
  - Aufgrund eines Projekts des BMWi
- Gpg4win wurde 2006 veröffentlicht
- GnuPG-2 war nicht für eine Windows Portierung vorgesehen
  - . . . wir haben es dann aber doch geschafft.
- Zirka 4000 Gpg4win 2.x Downloads am Tag

Portierung nach Windows

- Experimenteller Port in 1998.
- Vollständiger Port in 2000.
  - Aufgrund eines Projekts des BMWi
- Gpg4win wurde 2006 veröffentlicht
- GnuPG-2 war nicht für eine Windows Portierung vorgesehen
  - . . . wir haben es dann aber doch geschafft.
- Zirka 4000 Gpg4win 2.x Downloads am Tag

Portierung nach Windows

- Experimenteller Port in 1998.
- Vollständiger Port in 2000.
  - Aufgrund eines Projekts des BMWi
- Gpg4win wurde 2006 veröffentlicht
- GnuPG-2 war nicht für eine Windows Portierung vorgesehen
  - . . . wir haben es dann aber doch geschafft.
- Zirka 4000 Gpg4win 2.x Downloads am Tag

Übersicht

Branches

- Version 2.1 (“modern”)
  - Veröffentlicht im November 2014.
  - Neue Features (z.B. TOFU).
- Version 2.0 (“stable”)
  - Befindet sich im Maintenance-Modus
  - Kleinere Änderungen als Hilfe zur Migration nach 2.1.
- Version 1.4 (“classic”)
  - Für alte Daten und Schlüssel sowie Plattformen wie VMS etc.
  - Hat weiterhin PGP-2 Support.
  - Kleinere Änderungen als Hilfe zur Migration nach 2.1.

Branches

- Version 2.1 (“modern”)
  - Veröffentlicht im November 2014.
  - Neue Features (z.B. TOFU).
- Version 2.0 (“stable”)
  - Befindet sich im Maintenance-Modus
  - Kleinere Änderungen als Hilfe zur Migration nach 2.1.
- Version 1.4 (“classic”)
  - Für alte Daten und Schlüssel sowie Plattformen wie VMS etc.
  - Hat weiterhin PGP-2 Support.
  - Kleinere Änderungen als Hilfe zur Migration nach 2.1.

Branches

- Version 2.1 (“modern”)
  - Veröffentlicht im November 2014.
  - Neue Features (z.B. TOFU).
- Version 2.0 (“stable”)
  - Befindet sich im Maintenance-Modus
  - Kleinere Änderungen als Hilfe zur Migration nach 2.1.
- Version 1.4 (“classic”)
  - Für alte Daten und Schlüssel sowie Plattformen wie VMS etc.
  - Hat weiterhin PGP-2 Support.
  - Kleinere Änderungen als Hilfe zur Migration nach 2.1.

OpenPGP IETF Working Group

Mär 2008 Abgeschlossen nach RFC-4880

Jun 2015 Re-chartered

Sep 2015 (rough) Consensus über Updates von RFC-4880.

Feb 2016 Erster WG I-D for RFC-4880bis.

Jul 2016 RFC-4880bis WG I-D Final Call.

OpenPGP IETF Working Group

Mär 2008	Abgeschlossen nach RFC-4880
Jun 2015	Re-chartered
Sep 2015	(rough) Consensus über Updates von RFC-4880.
Feb 2016	Erster WG I-D for RFC-4880bis.
Jul 2016	RFC-4880bis WG I-D Final Call.

OpenPGP IETF Working Group

Mär 2008	Abgeschlossen nach RFC-4880
Jun 2015	Re-chartered
Sep 2015	(rough) Consensus über Updates von RFC-4880.
Feb 2016	Erster WG I-D for RFC-4880bis.
Jul 2016	RFC-4880bis WG I-D Final Call.

OpenPGP IETF Working Group

Mär 2008	Abgeschlossen nach RFC-4880
Jun 2015	Re-chartered
Sep 2015	(rough) Consensus über Updates von RFC-4880.
Feb 2016	Erster WG I-D for RFC-4880bis.
Jul 2016	RFC-4880bis WG I-D Final Call.

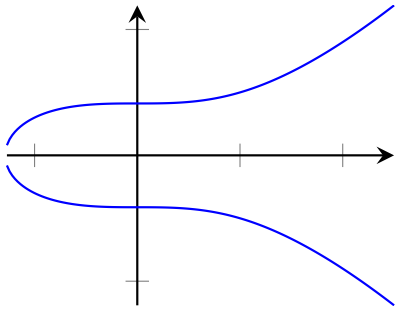
OpenPGP IETF Working Group

Mär 2008	Abgeschlossen nach RFC-4880
Jun 2015	Re-chartered
Sep 2015	(rough) Consensus über Updates von RFC-4880.
Feb 2016	Erster WG I-D for RFC-4880bis.
Jul 2016	RFC-4880bis WG I-D Final Call.

RFC-4880bis Ziele

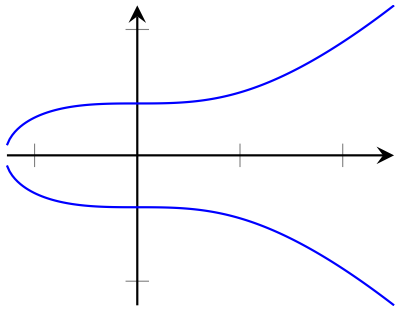
- Zusammenfassung der relvanten 3 OpenPGP RFCs.
- Neue Kurven wie von der Crypto Forum Research Group (CFRG) empfohlen.
- Symmetrische Verschlüsselung mit modernem Integritätsschutz (AEAD).
- Revision der MUST Algorithmen and Verbannung von schwachen Algorithmen (MD5, SHA-1).
- Neues Fingerprint Verfahren.

Elliptic curve cryptography



- RFC-6637 beschreibt ECC für OpenPGP.
  - NIST Kurven,
  - andere Kurven auch möglich (z.B. Brainpool).
- GnuPG 2.1 implementiert dies seit 2011.
- NIST Kurven sind etwas suspekt.
- Wir wollen Kurven mit besserer Repudation:
  - ECDH mit Curve25519,
  - EdDSA mit Ed25519,
  - die vom CFRG vorgeschlagenen Kurven.

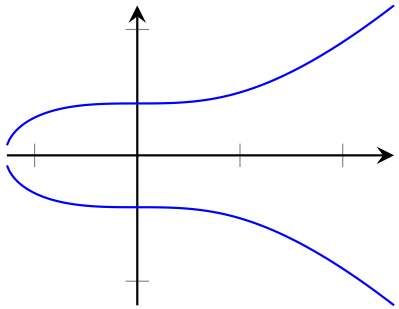
Elliptic curve cryptography



- RFC-6637 beschreibt ECC für OpenPGP.
  - NIST Kurven,
  - andere Kurven auch möglich (z.B. Brainpool).
- GnuPG 2.1 implementiert dies seit 2011.
- NIST Kurven sind etwas suspekt.
- Wir wollen Kurven mit besserer Repudation:
  - ECDH mit Curve25519,
  - EdDSA mit Ed25519,
  - die vom CFRG vorgeschlagenen Kurven.

GnuPG

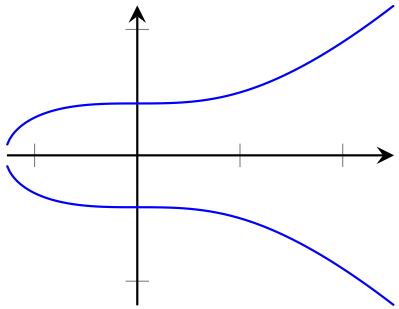
Elliptic curve cryptography



- RFC-6637 beschreibt ECC für OpenPGP.
  - NIST Kurven,
  - andere Kurven auch möglich (z.B. Brainpool).
- GnuPG 2.1 implementiert dies seit 2011.
- NIST Kurven sind etwas suspekt.
- Wir wollen Kurven mit besserer Repudation:
  - ECDH mit Curve25519,
  - EdDSA mit Ed25519,
  - die vom CFRG vorgeschlagenen Kurven.

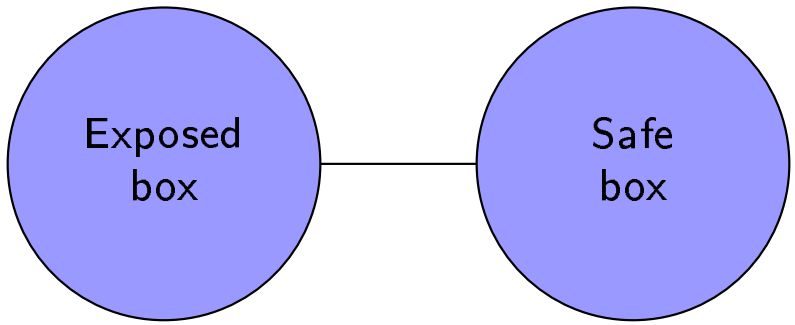
GnuPG

Elliptic curve cryptography



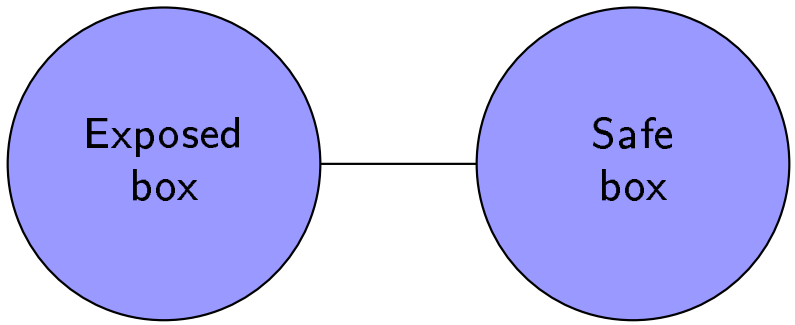
- RFC-6637 beschreibt ECC für OpenPGP.
  - NIST Kurven,
  - andere Kurven auch möglich (z.B. Brainpool).
- GnuPG 2.1 implementiert dies seit 2011.
- NIST Kurven sind etwas suspekt.
- Wir wollen Kurven mit besserer Repudation:
  - ECDH mit Curve25519,
  - EdDSA mit Ed25519,
  - die vom CFRG vorgeschlagenen Kurven.

Exkurs: Remote Use



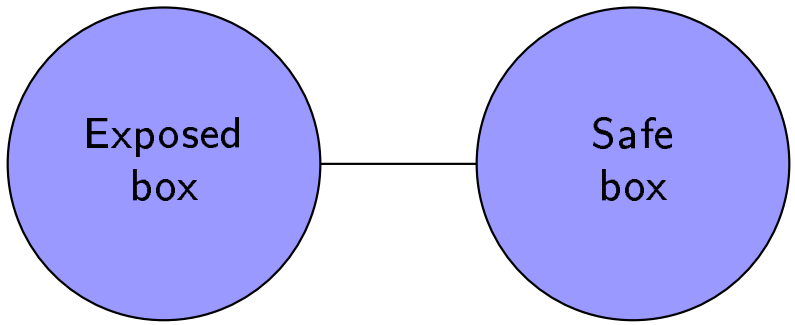
- Mittels ssh's Socket Forwarding:
  - gpg-agent läuft auf dem "sicheren" Rechner,
  - gpg läuft auf dem "exponierten" Server.
- Siehe auch `--extra-socket`, `--browser-socket`.

Exkurs: Remote Use



- Mittels ssh's Socket Forwarding:
  - gpg-agent läuft auf dem "sicheren" Rechner,
  - gpg läuft auf dem "exponierten" Server.
- Siehe auch `--extra-socket`, `--browser-socket`.

Exkurs: Remote Use



- Mittels ssh's Socket Forwarding:
  - gpg-agent läuft auf dem "sicheren" Rechner,
  - gpg läuft auf dem "exponierten" Server.
- Siehe auch `--extra-socket`, `--browser-socket`.

Spenden

- 5000 USD/Monat von der Linux Foundation für 2015.
- ProPublica Artikel im Februar ...
- wir erhielten ~300 KEUR an Spenden
  - Individuell
  - Unternehmen (Stripe, FB)
- Wir hatten Glück — andere Projekte sind immer noch unterfinanziert.

Spenden

- 5000 USD/Monat von der Linux Foundation für 2015.
- ProPublica Artikel im Februar ...
- wir erhielten ~300 KEUR an Spenden
  - Individuell
  - Unternehmen (Stripe, FB)
- Wir hatten Glück — andere Projekte sind immer noch unterfinanziert.

Spenden

- 5000 USD/Monat von der Linux Foundation für 2015.
- ProPublica Artikel im Februar ...
- wir erhielten ~300 KEUR an Spenden
  - Individuell
  - Unternehmen (Stripe, FB)
- Wir hatten Glück — andere Projekte sind immer noch unterfinanziert.

Spenden

- 5000 USD/Monat von der Linux Foundation für 2015.
- ProPublica Artikel im Februar ...
- wir erhielten ~300 KEUR an Spenden
  - Individuell
  - Unternehmen (Stripe, FB)
- Wir hatten Glück — andere Projekte sind immer noch unterfinanziert.

Was wir mit unseren Spendne machen

- Neal Walfield als zweiter Vollzeitentwickler
- Yutaka Niibe arbeitet als Freelancer (e.g. Smartcards, ECC)
- Kai Michaelis hilft Teilzeit bei Enigmail.
- Justus Winter als dritter Vollzeitentwickler seit diesem Monat.
- Ich arbeite auch noch mit.

Was wir mit unseren Spendne machen

- Neal Walfield als zweiter Vollzeitentwickler
- Yutaka Niibe arbeitet als Freelancer (e.g. Smartcards, ECC)
- Kai Michaelis hilft Teilzeit bei Enigmail.
- Justus Winter als dritter Vollzeitentwickler seit diesem Monat.
- Ich arbeite auch noch mit.

Was wir mit unseren Spendne machen

- Neal Walfield als zweiter Vollzeitentwickler
- Yutaka Niibe arbeitet als Freelancer (e.g. Smartcards, ECC)
- Kai Michaelis hilft Teilzeit bei Enigmail.
- Justus Winter als dritter Vollzeitentwickler seit diesem Monat.
- Ich arbeite auch noch mit.

Was wir mit unseren Spendne machen

- Neal Walfield als zweiter Vollzeitentwickler
- Yutaka Niibe arbeitet als Freelancer (e.g. Smartcards, ECC)
- Kai Michaelis hilft Teilzeit bei Enigmail.
- Justus Winter als dritter Vollzeitentwickler seit diesem Monat.
- Ich arbeite auch noch mit.

Was wir mit unseren Spendne machen

- Neal Walfield als zweiter Vollzeitentwickler
- Yutaka Niibe arbeitet als Freelancer (e.g. Smartcards, ECC)
- Kai Michaelis hilft Teilzeit bei Enigmail.
- Justus Winter als dritter Vollzeitentwickler seit diesem Monat.
- Ich arbeite auch noch mit.

Besonderen Dank

- David Shaw
- Marcus Brinkmann
- Jussi Kivilinna
- Andre Heinecke
- Andreas Metzler
- Daniel Kahn Gilmor
- Daniel Leidert
- Eric Dorland
- Bug-Berichter, Reviewer, Tester, Spender, ...

Übersicht

Vision

- Dank Edward Snowden besteht ein neues Interesse an Verschlüsselung
- Gpg und das Web-of-Trust sind schwierig zu benutzen
  - Keysigning Parties sind für Geeks
- Neuer Standardfocus:
  - Massenüberwachung
  - Einfache Benutzung
- Hochsensible Einsatzbereiche werden weiterhin unterstützt:
  - Per Option.

Vision

- Dank Edward Snowden besteht ein neues Interesse an Verschlüsselung
- Gpg und das Web-of-Trust sind schwierig zu benutzen
  - Keysigning Parties sind für Geeks
- Neuer Standardfocus:
  - Massenüberwachung
  - Einfache Benutzung
- Hochsensible Einsatzbereiche werden weiterhin unterstützt:
  - Per Option.

Vision

- Dank Edward Snowden besteht ein neues Interesse an Verschlüsselung
- Gpg und das Web-of-Trust sind schwierig zu benutzen
  - Keysigning Parties sind für Geeks
- Neuer Standardfocus:
  - Massenüberwachung
  - Einfache Benutzung
- Hochsensible Einsatzbereiche werden weiterhin unterstützt:
  - Per Option.

Vision

- Dank Edward Snowden besteht ein neues Interesse an Verschlüsselung
- Gpg und das Web-of-Trust sind schwierig zu benutzen
  - Keysigning Parties sind für Geeks
- Neuer Standardfocus:
  - Massenüberwachung
  - Einfache Benutzung
- Hochsensible Einsatzbereiche werden weiterhin unterstützt:
  - Per Option.

Support für Tor und GNUnet

- Netzzugriff geschieht über ein dediziertes Modul.
- Die Option `--enable-tor` sendet alles über Tor.
- GNU Naming System (GNS).

Support für Tor und GNUnet

- Netzzugriff geschieht über ein dediziertes Modul.
- Die Option `--enable-tor` sendet alles über Tor.
- GNU Naming System (GNS).

Support für Tor und GNUnet

- Netzzugriff geschieht über ein dediziertes Modul.
- Die Option `--enable-tor` sendet alles über Tor.
- GNU Naming System (GNS).

Tofu

Definition

Trust On First Use: Das Vertrauensmodell der Secure Shell (ssh)

- Erste Implementierung existiert.
- Wird generell in 2.2 vorhanden sein.
- Wird zukünftig das voreingestellte Vertrauensmodell.

Tofu

Definition

Trust On First Use: Das Vertrauensmodell der Secure Shell (ssh)

- Erste Implementierung existiert.
- Wird generell in 2.2 vorhanden sein.
- Wird zukünftig das voreingestellte Vertrauensmodell.

Tofu

Definition

Trust On First Use: Das Vertrauensmodell der Secure Shell (ssh)

- Erste Implementierung existiert.
- Wird generell in 2.2 vorhanden sein.
- Wird zukünftig das voreingestellte Vertrauensmodell.

Tofu

Definition

Trust On First Use: Das Vertrauensmodell der Secure Shell (ssh)

- Erste Implementierung existiert.
- Wird generell in 2.2 vorhanden sein.
- Wird zukünftig das voreingestellte Vertrauensmodell.

GPGME

GPGME ist eine Bibliothek um auf gpg, gpgsm und gpg-agent zuzugreifen.

Features in Planung:

- Verbesserte "Language Bindings"
- Unterstützung neuer gpg Features.
- Gpg wird als Co-Process laufen:
  - Signaturprüfung
  - Entschlüsselung.

GPGME

GPGME ist eine Bibliothek um auf gpg, gpgsm und gpg-agent zuzugreifen.

Features in Planung:

- Verbesserte "Language Bindings"
- Unterstützung neuer gpg Features.
- Gpg wird als Co-Process laufen:
  - Signaturprüfung
  - Entschlüsselung.

Zeitrahmen für neue GnuPG Versionen

- 1.4 Veröffentlichungen bei Bedarf
  - Jedoch ohne ECC Support.
- 2.0 wird im Januar 2018 End-Of-Life erreichen
  - Kein ECC oder RFC-4880bis Erweiterungen.
- 2.1 wird durch 2.2 ersetzt und als stable deklariert:
  - Anfang nächsten Jahres
  - Support für Curve25519.
  - ECC Schlüsselerzeugung wird noch `--expert` erfordern.
- 2.3 für RFC-4880bis Entwicklungen
  - Einige Features werden nach 2.2 zurück portiert.

Zeitrahmen für neue GnuPG Versionen

- 1.4 Veröffentlichungen bei Bedarf
  - Jedoch ohne ECC Support.
- 2.0 wird im Januar 2018 End-Of-Life erreichen
  - Kein ECC oder RFC-4880bis Erweiterungen.
- 2.1 wird durch 2.2 ersetzt und als stable deklariert:
  - Anfang nächsten Jahres
  - Support für Curve25519.
  - ECC Schlüsselerzeugung wird noch `--expert` erfordern.
- 2.3 für RFC-4880bis Entwicklungen
  - Einige Features werden nach 2.2 zurück portiert.

Zeitrahmen für neue GnuPG Versionen

- 1.4 Veröffentlichungen bei Bedarf
  - Jedoch ohne ECC Support.
- 2.0 wird im Januar 2018 End-Of-Life erreichen
  - Kein ECC oder RFC-4880bis Erweiterungen.
- 2.1 wird durch 2.2 ersetzt und als stable deklariert:
  - Anfang nächsten Jahres
  - Support für Curve25519.
  - ECC Schlüsselerzeugung wird noch `--expert` erfordern.
- 2.3 für RFC-4880bis Entwicklungen
  - Einige Features werden nach 2.2 zurück portiert.

Zeitrahmen für neue GnuPG Versionen

- 1.4 Veröffentlichungen bei Bedarf
  - Jedoch ohne ECC Support.
- 2.0 wird im Januar 2018 End-Of-Life erreichen
  - Kein ECC oder RFC-4880bis Erweiterungen.
- 2.1 wird durch 2.2 ersetzt und als stable deklariert:
  - Anfang nächsten Jahres
  - Support für Curve25519.
  - ECC Schlüsselerzeugung wird noch `--expert` erfordern.
- 2.3 für RFC-4880bis Entwicklungen
  - Einige Features werden nach 2.2 zurück portiert.

Zusammenfassung

- 2.1/2.2 wird bald der Standard sein.
- Solides Entwicklerteam.
- Wir machen Massenüberwachung teuer.

Vielen Dank für Ihre Aufmerksamkeit.

https://gnupg.org/ftp/blurbs/dafta15_gnupg-vergangenheit-gegenwart-zukunft.org

GnuPG

Zusammenfassung

- 2.1/2.2 wird bald der Standard sein.
- Solides Entwicklerteam.
- Wir machen Massenüberwachung teuer.

Vielen Dank für Ihre Aufmerksamkeit.

https://gnupg.org/ftp/blurbs/dafta15_gnupg-vergangenheit-gegenwart-zukunft.org

GnuPG

Zusammenfassung

- 2.1/2.2 wird bald der Standard sein.
- Solides Entwicklerteam.
- Wir machen Massenüberwachung teuer.

Vielen Dank für Ihre Aufmerksamkeit.

https://gnupg.org/ftp/blurbs/dafta15_gnupg-vergangenheit-gegenwart-zukunft.org

GnuPG

Zusammenfassung

- 2.1/2.2 wird bald der Standard sein.
- Solides Entwicklerteam.
- Wir machen Massenüberwachung teuer.

Vielen Dank für Ihre Aufmerksamkeit.

https://gnupg.org/ftp/blurbs/dafta15_gnupg-vergangenheit-gegenwart-zukunft.org

GnuPG