GnuPG: Past, Present, and Future

Werner Koch

DebConf15 — Heidelberg
August 16, 2015

GnuPG

Outline

PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.
- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions

PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions

PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.
- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions

PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions

PGP-2 and the year was 1991

- First public available crypto tool by Phil Zimmermann.
- Heavily improved by Branko Lankester, Colin Plumb, Derek Atkins, Hal Finney, Peter Gutmann, et al.

- Problem 1: RSA patent
- Problem 2: IDEA patent
- Problem 3: Export restrictions

PGP-5 and OpenPGP

- 1996: PGP Inc founded
- Spring 1997: DH patent expired, PGP-5 released
- Autumn 1997: OpenPGP WG chartered
- Spring 1998: PGP Inc bought by NAI (ceased support in 2002)
- Autumn 1998: RFC-2440 published
- Autumn 2007: RFC-4880 published

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 was non-free
  - even PGP-2 not DFSG compatible
- December 1997: g10 as free PGP-2 replacement
  - No patented algorithms
  - Designed as Unix tool
- Spring 1998: Name now GnuPG, protocol now OpenPGP.

GnuPG

g10 / GnuPG

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

- PGP-5 was non-free
  - even PGP-2 not DFSG compatible
- December 1997: g10 as free PGP-2 replacement
  - No patented algorithms
  - Designed as Unix tool
- Spring 1998: Name now GnuPG, protocol now OpenPGP.

g10 / GnuPG

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

- PGP-5 was non-free
  - even PGP-2 not DFSG compatible
- December 1997: g10 as free PGP-2 replacement
  - No patented algorithms
  - Designed as Unix tool
- Spring 1998: Name now GnuPG, protocol now OpenPGP.

Algorithm selection

- Initial version
  - Elgamal simply replaced RSA (sign+encrypt)
  - Blowfish as symmetric cipher
  - IDEA as plugin for PGP-2 compatibility in some countries.
- OpenPGP introduced subkeys
  - DSA for signatures, Elgamal for encryption.
  - 3DES and CAST5 for symmetric cipher.
  - RSA added in September 2000
- GnuPG and PGP-{5,6,7}
  - Worked with Hal Finney and Jon Callas
  - Informal interop testings
  - Testing of new features

Algorithm selection

- Initial version
  - Elgamal simply replaced RSA (sign+encrypt)
  - Blowfish as symmetric cipher
  - IDEA as plugin for PGP-2 compatibility in some countries.
- OpenPGP introduced subkeys
  - DSA for signatures, Elgamal for encryption.
  - 3DES and CAST5 for symmetric cipher.
  - RSA added in September 2000
- GnuPG and PGP-{5,6,7}
  - Worked with Hal Finney and Jon Callas
  - Informal interop testings
  - Testing of new features

GnuPG-2

- g10^{code} founded in 2001
- Bid accepted to implement S/MIME
- . . . birth of GnuPG-2 (2003)
  - modularized
  - separated crypto library
  - library (gpgme)

GnuPG-2

- g10^{code} founded in 2001
- Bid accepted to implement S/MIME
- . . . birth of GnuPG-2 (2003)
  - modularized
  - separated crypto library
  - library (gpgme)

GnuPG-2

- g10^{code} founded in 2001
- Bid accepted to implement S/MIME
- . . . birth of GnuPG-2 (2003)
  - modularized
  - separated crypto library
  - library (gpgme)

GnuPG in Debian

```
g10 (0.2.7-1) unstable; urgency=low

  * Initial release.

 -- James Troup <jjtroup@...>  Fri, 20 Feb 1998
```

- gpgv written in 2000 to prepare for signed packages
- 4 years later integrated into apt
- GnuPG-2 packaged in 2004

GnuPG in Debian

```
g10 (0.2.7-1) unstable; urgency=low

  * Initial release.

 -- James Troup <jjtroup@...>  Fri, 20 Feb 1998
```

- gpgv written in 2000 to prepare for signed packages
- 4 years later integrated into apt
- GnuPG-2 packaged in 2004

GnuPG in Debian

```
g10 (0.2.7-1) unstable; urgency=low

  * Initial release.

 -- James Troup <jjtroup@...>  Fri, 20 Feb 1998
```

- gpgv written in 2000 to prepare for signed packages
- 4 years later integrated into apt
- GnuPG-2 packaged in 2004

GnuPG in Debian

```
g10 (0.2.7-1) unstable; urgency=low

  * Initial release.

 -- James Troup <jjtroup@...>  Fri, 20 Feb 1998
```

- gpgv written in 2000 to prepare for signed packages
- 4 years later integrated into apt
- GnuPG-2 packaged in 2004

Port to Windows

- Experimental port to Windows in 1998
- Final port to Windows in 2000
  - Thanks to grant from the German government
- Gpg4win published in 2006
- GnuPG-2 was not designed to be ported
  - . . . but we did it anyway
- Surprising number of Gpg4win users

Port to Windows

- Experimental port to Windows in 1998
- Final port to Windows in 2000
  - Thanks to grant from the German government
- Gpg4win published in 2006
- GnuPG-2 was not designed to be ported
  - . . . but we did it anyway
- Surprising number of Gpg4win users

Port to Windows

- Experimental port to Windows in 1998
- Final port to Windows in 2000
  - Thanks to grant from the German government
- Gpg4win published in 2006
- GnuPG-2 was not designed to be ported
  - . . . but we did it anyway
- Surprising number of Gpg4win users

Port to Windows

- Experimental port to Windows in 1998
- Final port to Windows in 2000
  - Thanks to grant from the German government
- Gpg4win published in 2006
- GnuPG-2 was not designed to be ported
  - . . . but we did it anyway
- Surprising number of Gpg4win users

Port to Windows

- Experimental port to Windows in 1998
- Final port to Windows in 2000
  - Thanks to grant from the German government
- Gpg4win published in 2006
- GnuPG-2 was not designed to be ported
  - . . . but we did it anyway
- Surprising number of Gpg4win users

Outline

Branches

- Version 2.1 ("modern")
  - Released November 2014
  - Fixing remaining bugs
  - Adding last features
  - In experimental
- Version 2.0 ("stable")
  - Just maintained.
  - Minor changes to help migration to 2.1.
- Version 1.4 ("classic")
  - Supported to help with old data and keys.
  - Keeping PGP-2 support.
  - Minor changes to help migration to 2.1.

Branches

- Version 2.1 (“modern”)
  - Released November 2014
  - Fixing remaining bugs
  - Adding last features
  - In experimental
- Version 2.0 (“stable”)
  - Just maintained.
  - Minor changes to help migration to 2.1.
- Version 1.4 (“classic”)
  - Supported to help with old data and keys.
  - Keeping PGP-2 support.
  - Minor changes to help migration to 2.1.

Branches

- Version 2.1 (“modern”)
  - Released November 2014
  - Fixing remaining bugs
  - Adding last features
  - In experimental
- Version 2.0 (“stable”)
  - Just maintained.
  - Minor changes to help migration to 2.1.
- Version 1.4 (“classic”)
  - Supported to help with old data and keys.
  - Keeping PGP-2 support.
  - Minor changes to help migration to 2.1.

OpenPGP WG timeline

Mar 2008 Concluded after RFC-4880

Jun 2015 WG re-chartered

Sep 2015 WG (rough) consensus on updates to RFC-4880.

Feb 2016 First WG I-D for RFC-4880bis

Jul 2016 RFC-4880bis WG I-D final call

OpenPGP WG timeline

Mar 2008 Concluded after RFC-4880

Jun 2015 WG re-chartered

Sep 2015 WG (rough) consensus on updates to RFC-4880.

Feb 2016 First WG I-D for RFC-4880bis

Jul 2016 RFC-4880bis WG I-D final call

OpenPGP WG timeline

Mar 2008 Concluded after RFC-4880

Jun 2015 WG re-chartered

Sep 2015 WG (rough) consensus on updates to RFC-4880.

Feb 2016 First WG I-D for RFC-4880bis

Jul 2016 RFC-4880bis WG I-D final call

OpenPGP WG timeline

Mar 2008 Concluded after RFC-4880

Jun 2015 WG re-chartered

Sep 2015 WG (rough) consensus on updates to RFC-4880.

Feb 2016 First WG I-D for RFC-4880bis

Jul 2016 RFC-4880bis WG I-D final call

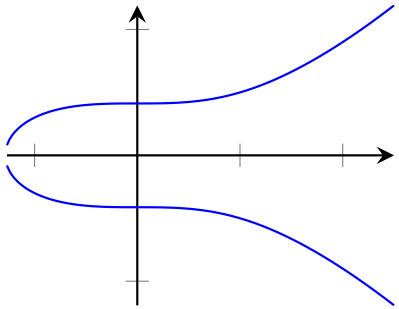
OpenPGP WG timeline

Mar 2008	Concluded after RFC-4880
Jun 2015	WG re-chartered
Sep 2015	WG (rough) consensus on updates to RFC-4880.
Feb 2016	First WG I-D for RFC-4880bis
Jul 2016	RFC-4880bis WG I-D final call

RFC-4880bis goals

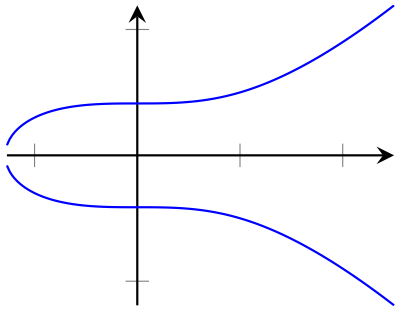
- Potential inclusion of curves recommended by the Crypto Forum Research Group (CFRG)
- A symmetric encryption mechanism that offers modern message integrity protection (AEAD)
- Revision of mandatory-to-implement algorithms and deprecation of weak algorithms
- An updated public-key fingerprint mechanism

Elliptic curve cryptography



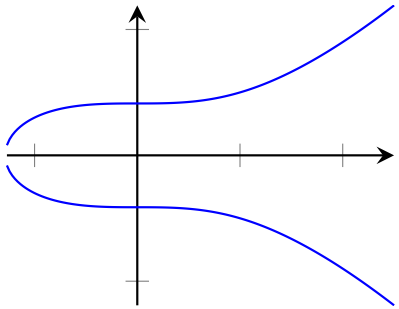
- RFC-6637 specifies ECC for OpenPGP.
  - NIST curves,
  - but allows other curves (e.g. Brainpool).
- 2.1 implements this since 2011.
- NIST curves are somewhat suspect.
- We want curves with better repudiation:
  - ECDH with Curve25519,
  - EdDSA using Ed25519,
  - Maybe CFRG suggested curves

Elliptic curve cryptography



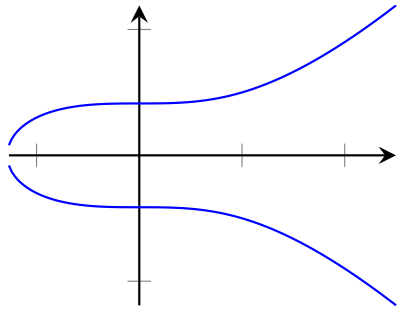
- RFC-6637 specifies ECC for OpenPGP.
  - NIST curves,
  - but allows other curves (e.g. Brainpool).
- 2.1 implements this since 2011.
- NIST curves are somewhat suspect.
- We want curves with better repudiation:
  - ECDH with Curve25519,
  - EdDSA using Ed25519,
  - Maybe CFRG suggested curves

Elliptic curve cryptography



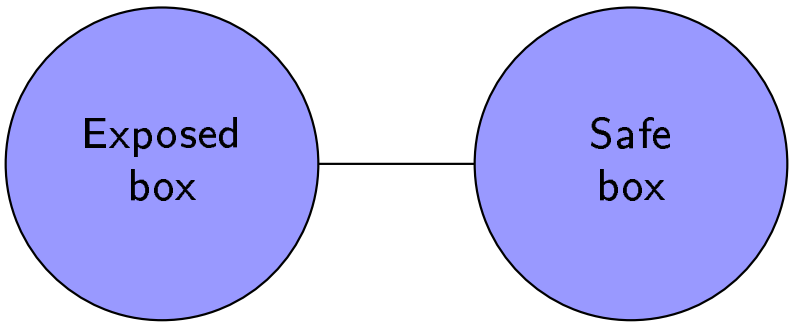
- RFC-6637 specifies ECC for OpenPGP.
  - NIST curves,
  - but allows other curves (e.g. Brainpool).
- 2.1 implements this since 2011.
- NIST curves are somewhat suspect.
- We want curves with better repudiation:
  - ECDH with Curve25519,
  - EdDSA using Ed25519,
  - Maybe CFRG suggested curves

Elliptic curve cryptography



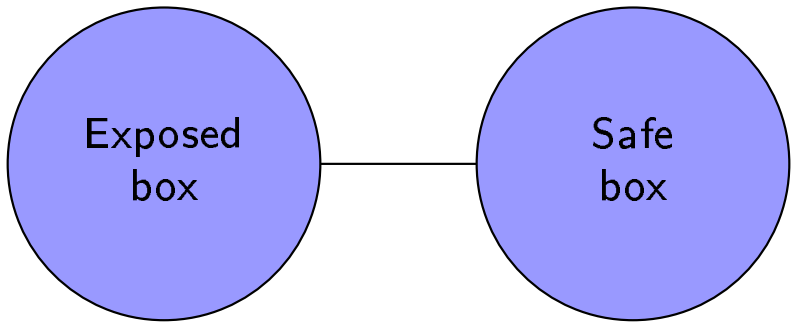
- RFC-6637 specifies ECC for OpenPGP.
  - NIST curves,
  - but allows other curves (e.g. Brainpool).
- 2.1 implements this since 2011.
- NIST curves are somewhat suspect.
- We want curves with better repudiation:
  - ECDH with Curve25519,
  - EdDSA using Ed25519,
  - Maybe CFRG suggested curves

Feature: Remote use



- We use ssh's socket forwarding to
  - run gpg-agent on the "safe" box
  - run gpg on an "exposed" box (server)
- See `--extra-socket`, `--browser-socket`.

Feature: Remote use



- We use ssh's socket forwarding to
  - run gpg-agent on the "safe" box
  - run gpg on an "exposed" box (server)
- See `--extra-socket`, `--browser-socket`.

Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February . . .
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10^{code} into a non-profit
- We are lucky — other projects still suffer.

Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February ...
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10^{code} into a non-profit
- We are lucky — other projects still suffer.

Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February ...
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10^{code} into a non-profit
- We are lucky — other projects still suffer.

Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February ...
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10^{code} into a non-profit
- We are lucky — other projects still suffer.

Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February ...
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10^{code} into a non-profit
- We are lucky — other projects still suffer.

Donations

- 5000 USD/month from the Linux Foundation for 2015
- ProPublica article in February ...
- we received ~300 KEUR in donations
  - Individual
  - Corporate (Stripe, FB)
- No donation campaign right now
  - Tax issues
  - Turning g10^{code} into a non-profit
- We are lucky — other projects still suffer.

How we spend the donations

- Neal Walfield as second full time developer
- Yutaka Niibe does contractual work (e.g. smartcards, ECC)
- Kai Michaelis helps with Enigmail part time
- Me :-)

How we spend the donations

- Neal Walfield as second full time developer
- Yutaka Niibe does contractual work (e.g. smartcards, ECC)
- Kai Michaelis helps with Enigmail part time
- Me :-)

How we spend the donations

- Neal Walfield as second full time developer
- Yutaka Niibe does contractual work (e.g. smartcards, ECC)
- Kai Michaelis helps with Enigmail part time
- Me :-)

How we spend the donations

- Neal Walfield as second full time developer
- Yutaka Niibe does contractual work (e.g. smartcards, ECC)
- Kai Michaelis helps with Enigmail part time
- Me :-)

Special thanks

- David Shaw
- Marcus Brinkmann
- Jussi Kivilinna
- Andre Heinecke
- Debian folks:
  - Andreas Metzler
  - Daniel Kahn Gilmor
  - Daniel Leidert
  - Eric Dorland
  - James Troup
  - Matthias Urlichs
  - Thijs Kinkhorst
- Bug reporters, reviewers, testers, donors, ...

Outline

Vision

- Thanks to Snowden, new demand for encryption
- Gpg and Web-of-Trust are too hard
  - Keysigning parties are for geeks
- New default focus:
  - Mass surveillance (not targetted)
  - Easy to use
- Still supporting targetted users
  - Question of default options

Vision

- Thanks to Snowden, new demand for encryption
- Gpg and Web-of-Trust are too hard
  - Keysigning parties are for geeks
- New default focus:
  - Mass surveillance (not targetted)
  - Easy to use
- Still supporting targetted users
  - Question of default options

Support for TOR and GNUnet

- All network access via a separate module
- New option `--enable-tor` to route everything over TOR
  - challenge: We need a torified resolver
- GNU Naming System (GNS).

Support for TOR and GNUnet

- All network access via a separate module
- New option `--enable-tor` to route everything over TOR
  - challenge: We need a torified resolver
- GNU Naming System (GNS).

Support for TOR and GNUnet

- All network access via a separate module
- New option `--enable-tor` to route everything over TOR
  - challenge: We need a torified resolver
- GNU Naming System (GNS).

Tofu

Definition

Trust On First Use: Secure Shell's trust model

- There is a detailed plan for a TOFU design
- Will be available in 2.2
- Will eventually be the default trust model

Tofu

Definition

Trust On First Use: Secure Shell's trust model

- There is a detailed plan for a TOFU design
- Will be available in 2.2
- Will eventually be the default trust model

Tofu

Definition

Trust On First Use: Secure Shell's trust model

- There is a detailed plan for a TOFU design
- Will be available in 2.2
- Will eventually be the default trust model

Tofu

Definition

Trust On First Use: Secure Shell's trust model

- There is a detailed plan for a TOFU design
- Will be available in 2.2
- Will eventually be the default trust model

GPGME

GPGME is a library to access gpg, gpgsm, and gpg-agent.

Planned features:

- Better integrated language bindings
- Support for new gpg features
- Run gpg as a co-process
  - signature verification
  - decryption

GPGME

GPGME is a library to access gpg, gpgsm, and gpg-agent.

Planned features:

- Better integrated language bindings
- Support for new gpg features
- Run gpg as a co-process
  - signature verification
  - decryption

GnuPG release scheduling

- 1.4 releases as needed
  - No ECC support, though.
- 2.0 will reach end-of-life in December 2017.
  - No backport of ECC or other RFC-4880bis stuff.
- 2.1 will be be replaced by 2.2 and declared as stable:
  - Release date: End of this year.
  - Support for Curve25519 encryption.
  - Support for some proposed RFC-4880bis features.
  - ECC key generation needs `--expert` temporarily.
- 2.3 for RFC-4880bis development
  - Certain features will be backported to 2.2

GnuPG release scheduling

- 1.4 releases as needed
  - No ECC support, though.
- 2.0 will reach end-of-life in December 2017.
  - No backport of ECC or other RFC-4880bis stuff.
- 2.1 will be be replaced by 2.2 and declared as stable:
  - Release date: End of this year.
  - Support for Curve25519 encryption.
  - Support for some proposed RFC-4880bis features.
  - ECC key generation needs `--expert` temporarily.
- 2.3 for RFC-4880bis development
  - Certain features will be backported to 2.2

GnuPG release scheduling

- 1.4 releases as needed
  - No ECC support, though.
- 2.0 will reach end-of-life in December 2017.
  - No backport of ECC or other RFC-4880bis stuff.
- 2.1 will be be replaced by 2.2 and declared as stable:
  - Release date: End of this year.
  - Support for Curve25519 encryption.
  - Support for some proposed RFC-4880bis features.
  - ECC key generation needs `--expert` temporarily.
- 2.3 for RFC-4880bis development
  - Certain features will be backported to 2.2

GnuPG release scheduling

- 1.4 releases as needed
  - No ECC support, though.
- 2.0 will reach end-of-life in December 2017.
  - No backport of ECC or other RFC-4880bis stuff.
- 2.1 will be be replaced by 2.2 and declared as stable:
  - Release date: End of this year.
  - Support for Curve25519 encryption.
  - Support for some proposed RFC-4880bis features.
  - ECC key generation needs `--expert` temporarily.
- 2.3 for RFC-4880bis development
  - Certain features will be backported to 2.2

Summary

- 2.1/2.2 will soon be the standard version.
- Solid development team.
- Making mass surveillance expensive.

Thanks for attending.

https://gnupg.org/ftp/blurbs/debconf15_gnupg-past-present-future.org

GnuPG

Summary

- 2.1/2.2 will soon be the standard version.
- Solid development team.
- Making mass surveillance expensive.

Thanks for attending.

https://gnupg.org/ftp/blurbs/debconf15_gnupg-past-present-future.org

GnuPG

Summary

- 2.1/2.2 will soon be the standard version.
- Solid development team.
- Making mass surveillance expensive.

Thanks for attending.

https://gnupg.org/ftp/blurbs/debconf15_gnupg-past-present-future.org

GnuPG

Summary

- 2.1/2.2 will soon be the standard version.
- Solid development team.
- Making mass surveillance expensive.

Thanks for attending.

https://gnupg.org/ftp/blurbs/debconf15_gnupg-past-present-future.org

GnuPG