

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

gnupg.org



- Il progetto GnuPG
- Caratteristiche tecniche
- Il Backend
- I Front-End
- La crittografia del GnuPG
- La release attuale 1.0.4
- Confronto con il PGP
- Lo standard OpenPGP (RFC2440)

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

Il progetto GnuPG



Il progetto tedesco GnuPG (GNU Privacy Guard) nasce nel 1997 per opera di Werner Koch, sviluppatore indipendente interessato alla crittografia OpenSource.

L'obiettivo del progetto è la realizzazione di un engine crittografico, alternativo al Pgp, totalmente open source basato su algoritmi crittografici standard e non proprietari.

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

Il progetto GnuPG



Basato su di un sistema di crittografia "ibrido", simile al Pgp, con algoritmi simmetrici (crittografia tradizionale) e asimmetrici (crittografia a chiave pubblica).

Rappresenta, allo stato attuale, un vero e proprio engine crittografico in grado di cifrare/decifrare, firmare ed autenticare file e messaggi di posta elettronica (standard MIME).

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

Caratteristiche tecniche



- Standard OpenPgp
- Piena compatibilità con Pgp 2
- Decifra, verifica msg Pgp 5,6,7
- Supporto algoritmi crittografici ElGamal, DSA, RSA, AES, 3DES, Blowfish, Twofish, CAST5, MD5, SHA-1, RIPE-MD-160 e TIGER
- Supporto modulare per nuovi algoritmi crittografici
- Gestione delle date di scadenza per chiavi e firme

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

Caratteristiche tecniche



- Gestione forzata degli User Id standard
- Supporto multi-lingue: English, Danish, Dutch, Esperanto, French, German, Japanese, Italian, Polish, Portuguese (Brazilian), Portuguese (Portuguese), Russian, Spanish e Swedish
- Sistema di help on-line
- Supporto integrato per HKP keyserver (wwwkeys.pgp.net).
- Supporto opzionale per la gestione di messaggi anonimi

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

Sistemi operativi supportati



GNU/Linux with x86, alpha, mips, sparc64, m68k or powerpc CPUs

FreeBSD with x86 CPU works fine.

OpenBSD works fine (x86 CPU?). **NetBSD** works fine (x86 CPU?).

AIX v4.3,

BSDI v4.0.1 with i386,

HPUX v9.x, v10.x and v11.0 with HPPA CPU,

IRIX v6.3 with MIPS R10000 CPU,

MP-RAS v3.02,

OSF1 V4.0 with Alpha CPU,

OS/2 version 2.

SCO UnixWare/7.1.0.

SunOS, Solaris on Sparc and x86,

USL Unixware v1.1.2,

Windows 95 and **WNT** with x86 CPUs.

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

Il Backend



- Sistema compatto a linea di comando
sintassi: `gpg [options] [files]`
- Funzionalità ed interfaccia simile al Pgp.
- Utilizzabile come engine per applicazioni crittografiche.
- Gestione ottimizzata del flusso dati input/output (standard pipe).

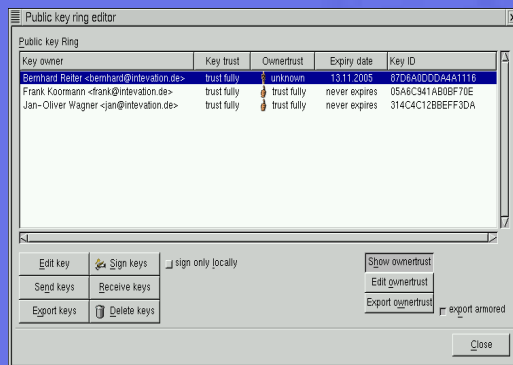
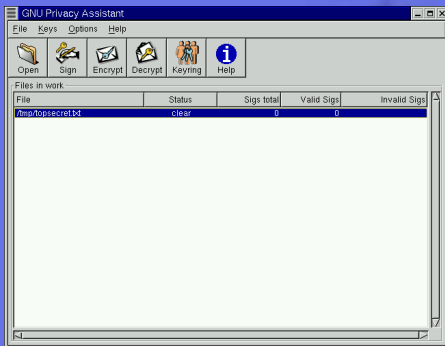
"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)



Il Front-End

Esistono diverse interfacce per GnuPG, la più famosa è GPA GNU Privacy Assistant, basata su GIMP Tool Kit (GTK).



Altri front-end: Seahorse (Gnome), GnomePgp (Gnome), Geheimniss (Kde), TkPgp, pgpgpg (interprete di script pgp per gnupg), Mutt (gnupg email), MailCrypt (Emacs), pgp4pine, pgpenvelope, exmh, etc.

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

La crittografia del GnuPG



Basata su algoritmi standard non proprietari (possibilità di espansione con moduli software).

Gli algoritmi di default sono:

- ElGamal/DSA (asimmetrici) utilizzati per la generazione delle chiavi, la cifratura/ decifratura dei dati e la firma digitale (DSA)
- Blowfish (simmetrico) per la cifratura "veloce" dei dati

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

La crittografia del GnuPG



Simile al Pgp con un sistema crittografico "ibrido".

Al posto dell'RSA per la cifratura della chiave random è presente l'ElGamal (passaggio matematico dalla teoria dei numeri primi ai logaritmi discreti).

Al posto dell'IDEA per la cifratura "veloce" dei dati e dei msg su chiave random di sessione c'è il Blowfish più performante.

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

La release attuale 1.0.4



La release attuale, la 1.0.4 rilasciata il 17 Ottobre 2000, rappresenta un security update importante.

Release stabile.

Si tratta di una versione nata dopo 2 anni di sviluppo con un'architettura crittografica modulare con più di 20 algoritmi implementati.

Dalla versione 1.0.3 è presente il supporto dell'algoritmo RSA

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

Il confronto con il Pgp



PGP:

Architettura crittografica chiusa (DSS, RSA, IDEA...).

Software proprietario della PGP Inc. - NAI Inc.

Presenza di features "poco trasparenti"
vedi ultimo bug sulle ADK.

GNUPG:

Architettura aperta (algoritmi modulari)

Software non proprietario (libero), licenza GPL.

Ottimizzazione del codice, engine leggero,
features essenziali

"Il progetto GnuPG e la crittografia Open Source"

Enrico Zimuel (cerin0@olografix.org)

Lo standard OpenPgp (RFC2440)

Primo standard crittografico completo con filosofia open source.



Standard aperto per la cifratura/decifratura dei dati, firma digitale, autenticazione, gestione delle chiavi pubbliche/private

Tentativo di affermare uno standard libero per applicazioni crittografiche in un ottica di difesa delle libertà digitali

Perchè solo le istituzioni o grandi aziende possono utilizzare strong encryption?