Digital signature

- دلایل استفاده / مزایا
- انواع پروتکل ها
  - POP3/IMAP/SMTP
  - OpenPGP
  - S/MIME
  - PEM
  - SMEmail
- ابزار ها
  - FireGPG
  - Gmail S/MIME
  - PHPki

دلایل استفاده / مزایا

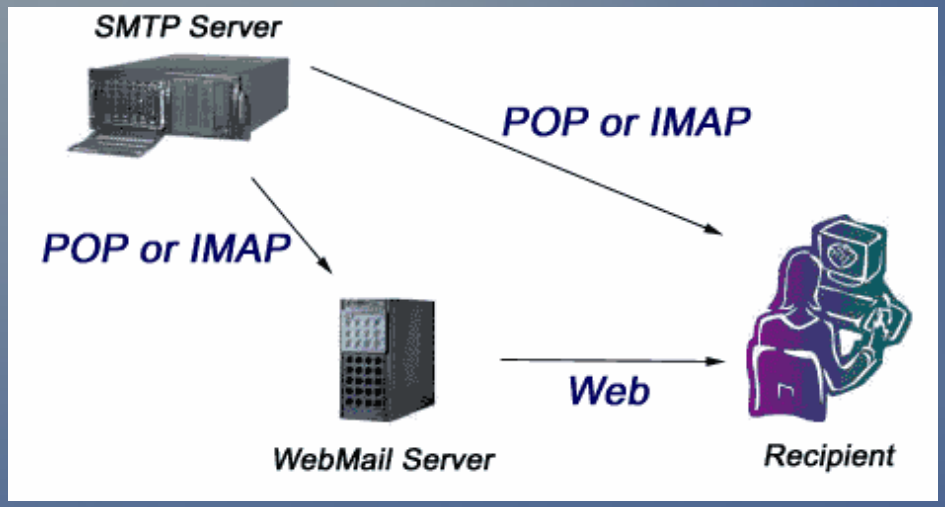
دلایل استفاده

- احراز هویت
- جامعیت
- انکار ناپذیری
- محرامانگی

مزایا امضای دیجیتال

- عدم امکان کپی برداری
- عدم امکان جعل و الحاق

انواع پروتکل ها



POP3/IMAP/SMTP

DKIM(public-key) ,SPF –

OpenPGP (RFC 2440) ✓

PGP 5 ✓

S/MIME ✓

S/MIME certificates ✓

PEM ✓

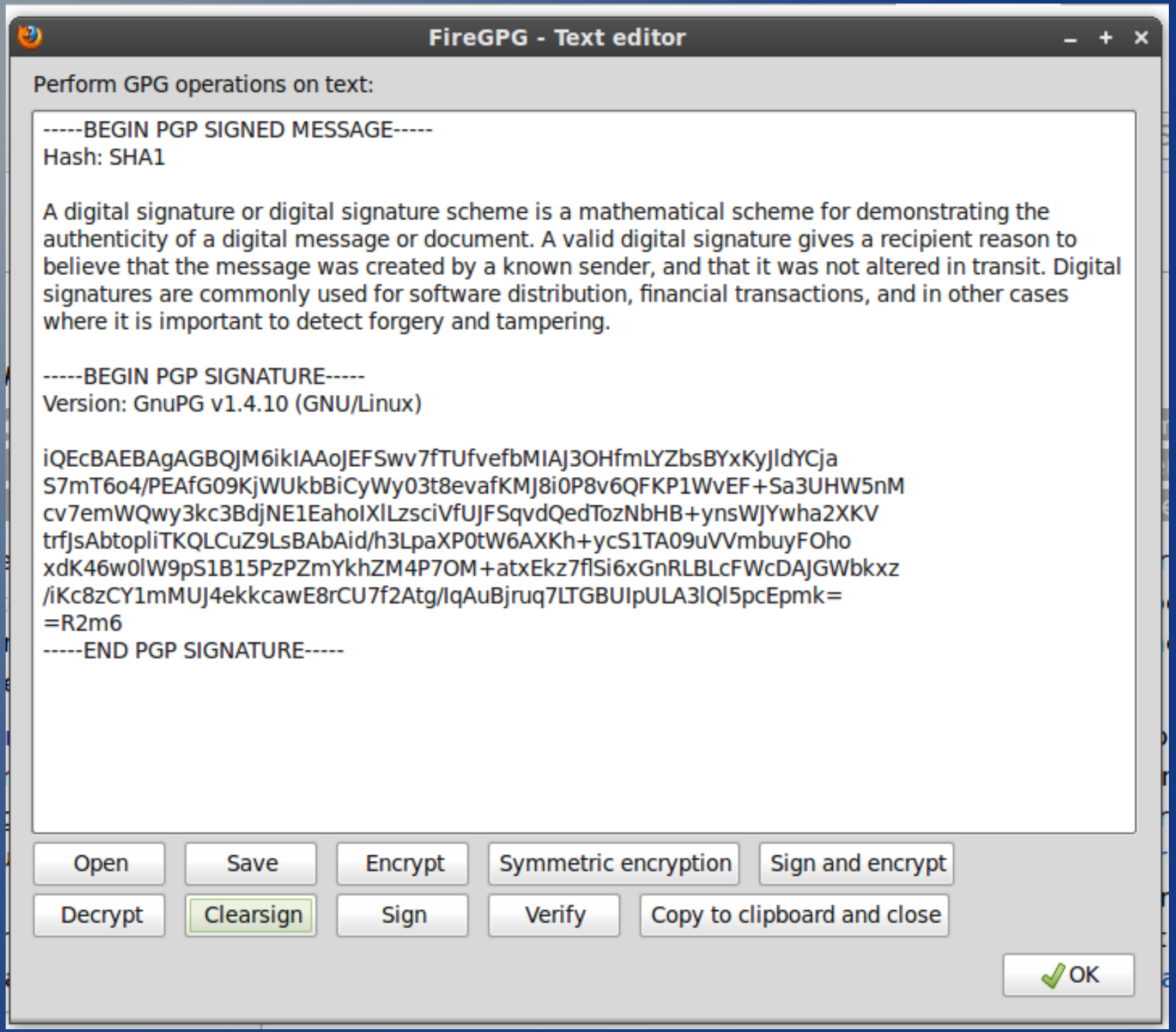
Privacy-Enhanced Mail ✓

SMEmail ✓

A New Protocol for the Secure E-mail in Mobile Environments –

ابزار ها

- FireGPG ✔
  - discontinued –
- Gmail S/MIME ✔
  - Verification is not supported –
- PHPki ✔
- Outlook / Thunderbird ✔
- Smart Card ✔
- http://www.gnupg.org/related_software/frontends.html ✔
- http://www.flatmtn.com/article/creating-pkcs12-certificates ✔


FireGPG - Text editor
Perform GPG operations on text:
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering.
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.10 (GNU/Linux)
iQEcBAEBAgAGBQJM6ikIAAoJEFSwv7fTUfvefbMIAJ3OHfmLYZbsBYxKyJldYCja
S7mT6o4/PEAfG09KjWUkbBiCyWy03t8evafKMJ8i0P8v6QFKP1WvEF+Sa3UHW5nM
cv7emWQwy3kc3BdjNE1EahoIXlLzsciVfUJFSqvdQedTozNbHB+ynsWJYwha2XKV
trfJsAbtopliTKQLCuZ9LsBAbAid/h3LpaXP0tW6AXKh+ycS1TA09uVVmbuyFOho
xdK46w0lW9pS1B15PzPZmYkhZM4P7OM+atxEkz7flSi6xGnRLBLcFWcDAJGWbkxz
/iKc8zCY1mMUJ4ekkcawE8rCU7f2Atg/IqAuBjruq7LTGBUIpULA3lQl5pcEpmk=
=R2m6
-----END PGP SIGNATURE-----
Open
Save
Encrypt
Symmetric encryption
Sign and encrypt
Decrypt
Clearsign
Sign
Verify
Copy to clipboard and close
OK