

Ngày Phần mềm tự do 28/8/2004, Hà Nội

GnuPG, chữ ký của thời đại

Phan Thái Trung

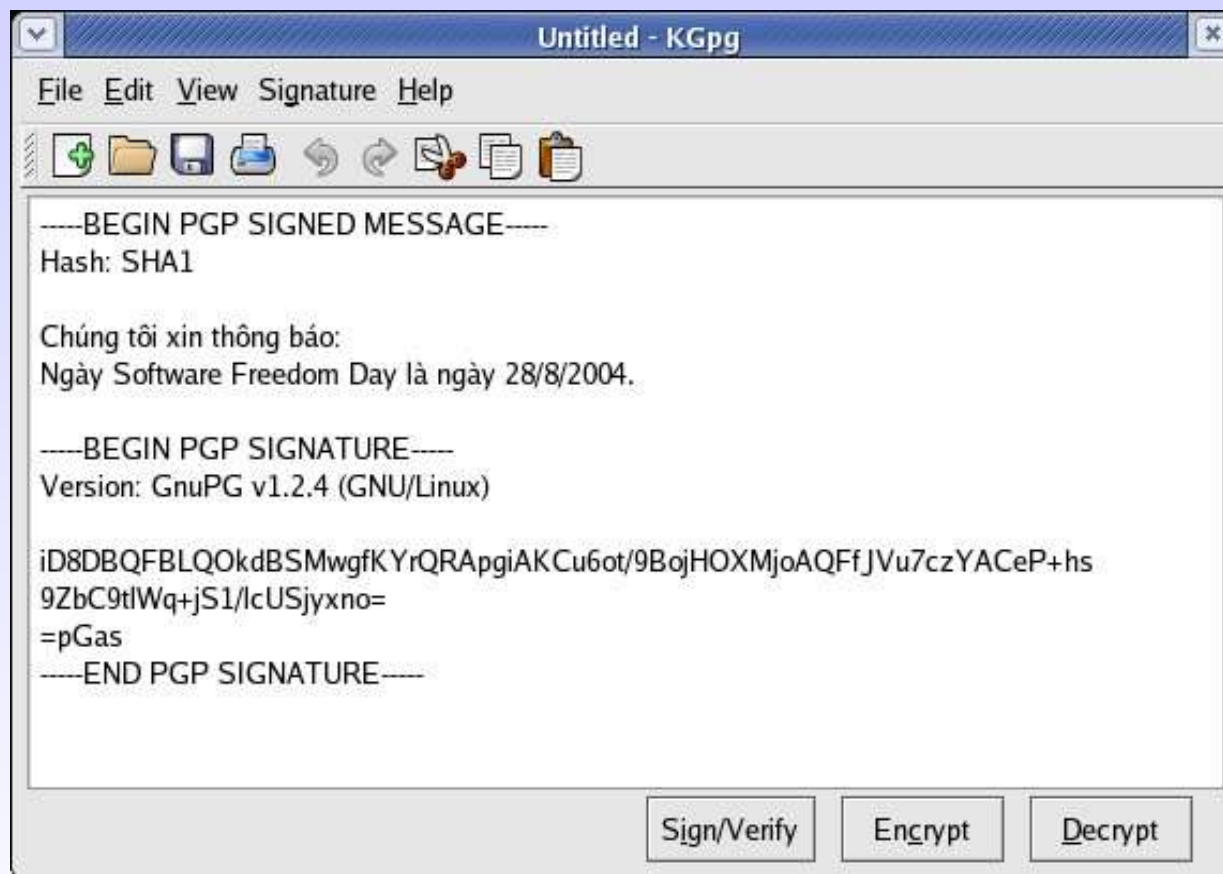
Giới thiệu Chữ ký điện tử

- Định nghĩa Chữ ký điện tử
 - Đơn giản là một đoạn mã xác nhận tính toàn vẹn của nội dung thông điệp và tên người viết nó.
 - Chuẩn GnuPG (GNU Privacy Guard, gnupg.org) trên cơ sở của thuật toán Pretty Good Privacy được tin cậy sử dụng rộng rãi.
- Tại sao cần sử dụng Chữ ký điện tử?
 - Đáp ứng sự tin cậy cho nội dung thông điệp
 - Đáp ứng sự tin cậy về xuất xứ của thông điệp
 - Mã hoá những thông tin nhạy cảm.

Chữ ký GnuPG

- GnuPG được hỗ trợ bởi tổ chức GNU, hợp pháp, nguồn mở, không vướng bản quyền
- Bản chất của chữ ký GnuPG:
 - Độ tin cậy rất cao trong quá trình truyền thông điệp vì không truyền đi mật khẩu bí mật
 - Có hai chuỗi từ khoá: Bí mật và công cộng.
 - **Chữ ký điện tử:** Từ khoá bí mật (mật khẩu) dùng để tạo chữ ký, từ khoá công cộng để cho mọi người khác kiểm tra nó.
 - **Mã hoá thông điệp:** Từ khoá công cộng dùng như một phong thư dán kín thông điệp, từ khoá bí mật sẽ mở phong thư.

GnuPG với vai trò Chữ ký điện tử



Xin cảm ơn!

Xin mời đặt câu hỏi?

Phan Thái Trung
ptt@users.sourceforge.net
<http://nguồnmô.org/phanthaitrung>



This presentation is released under the terms of GNU/Free Document License.

Ngày Phần mềm tự do và nguồn mở 28/8/2004, Trường Đại học Bách Khoa, Hà Nội