Gluing Together Desktop Crypto

Stef Walter
Gluing Together Desktop Crypto

Stef Walter

Three steps to Collabora
Three steps...

1. Store keys and certificates interoperably
2. Make consistent trust decisions
3. Refer to keys and certificates in a standard way
Spock warns: “Be careful with glue”
Key Storage
What is a key store?

What makes it different?

Application → Sign Y using key X → Signed data Y → Key Store
PKCS#11
PKCS #11 Concepts

PKCS #11 module

Application + crypto library

PKCS #11 module

Slots and Tokens == Key Stores
Support for PKCS#11

Decent Support:
- GnuTLS
- GNOME Keyring
- Java (SUN)
- Mozilla's NSS
- OpenSC
- OpenSSH
- OpenVPN
- QCA (QT)
- TrueCrypt

Work in Progress
- GLib
- OpenSSL

Patches Available:
- GnuPG

... and many others
p11-kit: Solves PKCS#11 on the Desktop

1. Using the same PKCS#11 modules more than once in the same process.

2. Configuration: A standard way to lookup which modules are installed and enabled.

... and other handy things ...
PKCS#11 Module Configuration

System
/etc/pkcs11

- Global Config
  pkcs11.conf

- Smart Card Driver
  modules/smart-card

User
~/.pkcs11

- User Config
  pkcs11.conf

- Power user module
  modules/kssl-storage

- Keyring module
  modules/gnome-keyring
PKCS#11 Configuration Lockdown

System
/etc/pkcs11

Global Config
pkcs11.conf

Smart Card Driver
modules/smart-card

Keyring module
modules/gnome-keyring
PKCS#11 Module Configuration

User

~/.pkcs11

User Config
pkcs11.conf

Power user module modules/kssl-storage
Library: p11-kit

http://p11-glue.freedesktop.org/p11-kit.html
Three steps...

- Store keys and certificates interoperably
- Make consistent trust decisions
- Refer to keys and certificates in a standard way
'Trust'
'Trust'

What does that even mean?
Trust Assertions

Each Trust Assertion makes a positive or negative assertion about level of trust in a subject.
Trust Assertions

Subject → Level of Trust → Purpose
eg: Certificate Trust Anchor

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "Family Members Root CA G2" for the following purposes?

- Trust this CA to identify web sites.
- Trust this CA to identify email users.
- Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate
eg: Pinned Certificate Exception

Certificate

Trusted

Server: ca.cert.org

Subject

Level of Trust

Purpose
eg: SSH Known Host

```
sten@stef-laptop:~$ ssh thewalter.net
The authenticity of host 'thewalter.net (94.75.203.101)' can't be established.
Are you sure you want to continue connecting (yes/no)? 
```
eg: Certificate Revocation List

Serial+Issuer
Subject

Distrusted
Level of Trust

Any
Purpose
Spec: Trust Assertions in PKCS#11

http://p11-glue.freedesktop.org/trust-assertions.html
Three steps...

1. Store keys and certificates interoperably
2. Make consistent trust decisions
3. Refer to keys and certificates in a standard way
How do you refer to Keys and Certs?
PKCS#11 URIs

pkcs11:object-type=private;
object=MyKey;
token=Magic%20Token;
id=%69%97%5c
PKCS#11 URIs

pkcs11:object=blah;...

pkcs11:object=blah;...
RFC: PKCS#11 URI Scheme

Three steps...

- Store keys and certificates interoperably
- Make consistent trust decisions
- Refer to keys and certificates in a standard way
Any questions?

http://p11-glue.freedesktop.org

p11-glue@lists.freedesktop.org

- Thanks to everyone who contributed!