

IWFST 2005
International Workshop on Future Software Technology 2005
November 8 – 10, 2005 in Shanghai, China

Trusted Key Server
OpenPKSD TKS

Hironobu SUZUKI
hironobu@openpkd.org
hironobu@h2np.net

Who am I


- Co-chairman and COO of FSIJ
 - Free Software Initiative of Japan
- Unix Expert
 - Over 20 years professional career
 - Software consultant, President of my own company
- Part-time teacher in some colleges
 - Waseda Univ. Senshu Univ. and Jissen Women Univ.
- My own Free Software project and research project
 - OpenPKSD.ORG project
 - WCLSCAN project

What Is OpenPGP

- OpenPGP is a public key cryptography technology specification as defined RFC2440
- OpenPGP provides encryption, decryption, digital signature and others
- PGP is cryptographic tool that was developed by Philip Zimmermann
- GNUPG has been developed by GNU Privacy Guard project.

Why We Need It?

- Verify file for distribution
 - To distribute collect file
 - To avoid Trojan horse
- Source code exchange
 - Between trustworthy developers
- Example
 - Debian developer community uses OpenPGP among them



Public key infrastructure is required to build trustful distribution

Public Key Scheme

- Alice generates a pair of public key and secret key
- Alice sends a public key Bob
- Bob make text encrypt using Alice's public key and bob sends encrypted text to Alice
- Only Alice can decrypt using her own secret key

Digital Signature Scheme

- Alice generates a pair of sign key and verify key
- Alice sends a verify key to bob
- Alice signs on Alice's data using Alice's sign key and send signed data to bob
- Bob can verify Alice's signed data using Alice's verify key

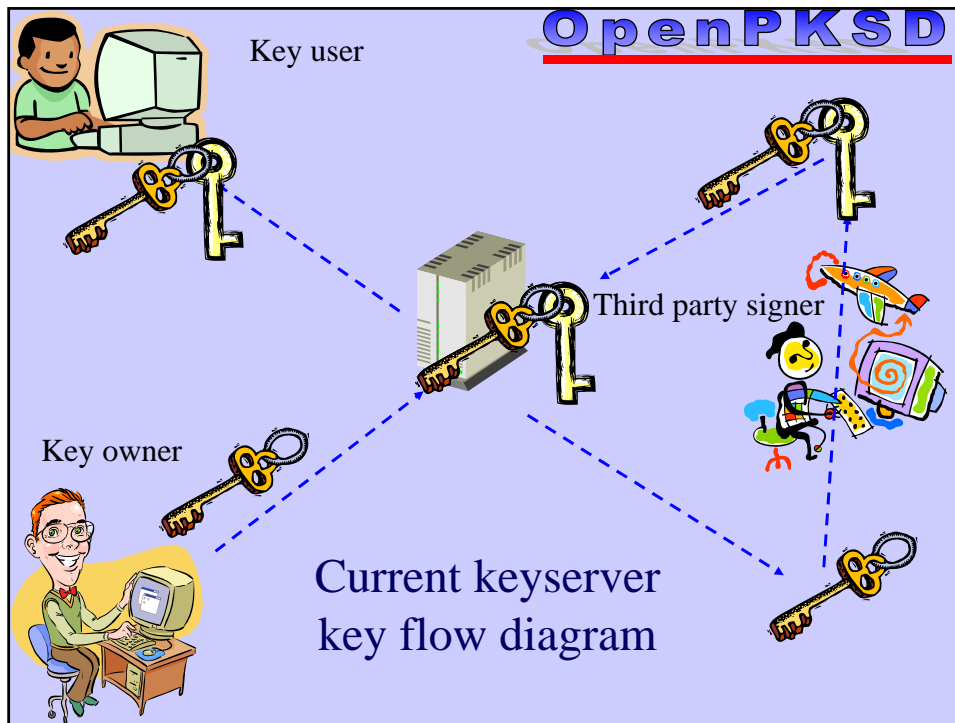
Where Is Alice's Public/Verify Key?

- Email
 - Do you want to send email again, again and again?
- Personal website
 - Not too bad
- Keyserver
 - Easy to find it
 - Pgp public key servers have been available since 1994
 - OpenPKSD that is ruby version of keyserver has been available at <http://openpkd.org> since 2002

Old Style Keyserver

Since 1994

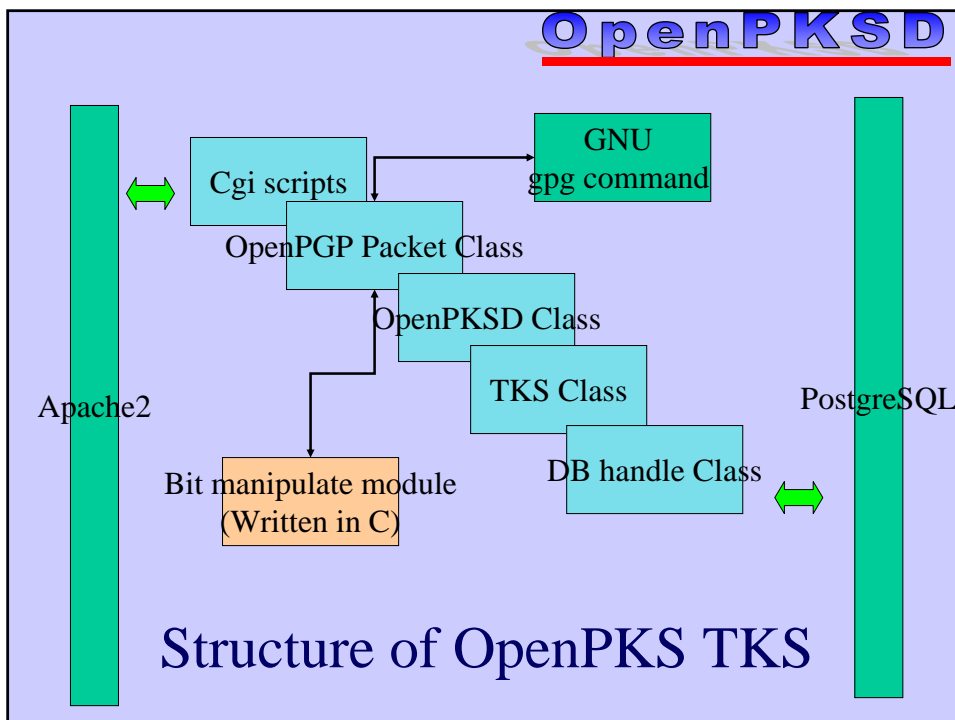
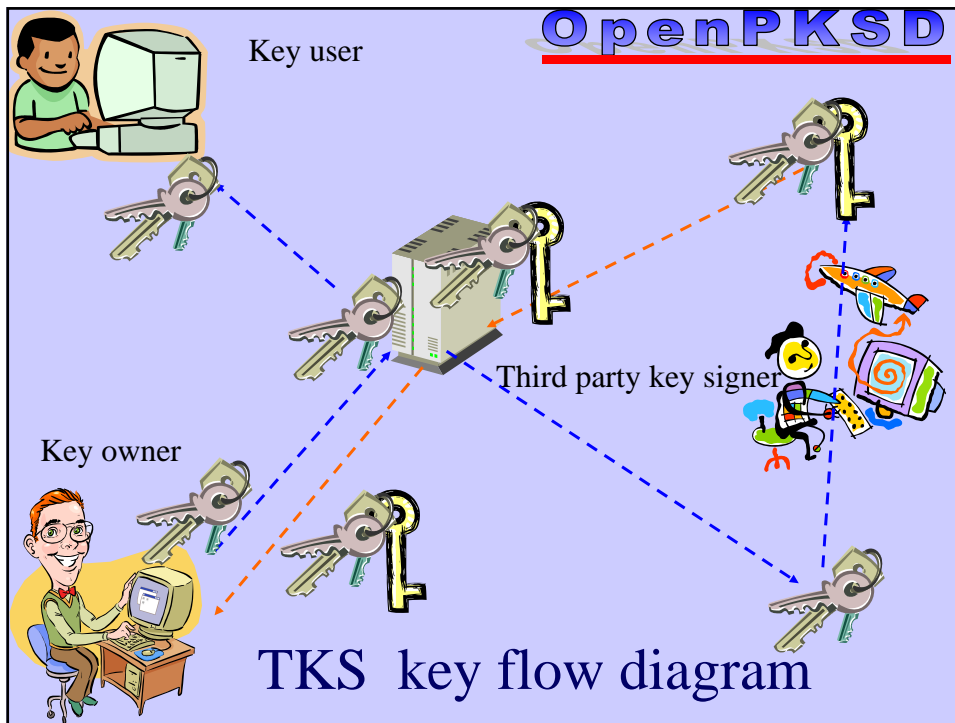
- Alice can't handle her own public key
 - Cathy can put Alice's public key
 - David can put his signature on Alice's public key
 - Alice doesn't want it either



OpenPKSD

OpenPKSD TKS

- Successor of OpenPKSD that is written in Ruby
 - Ruby is good for rapid programming
 - True Object Oriented language
 - I introduced OpenPKSD in Ruby Conference 2002 Seattle
- Public key owners can handle their own key under OpenPKSD TKS (trusted key server)
 - Because TKS has their own public keys
- Free Software
 - Free as in speech not as in beer



Status of OpenPKSD TKS Project

- Prototype developing was started in December 2004 and finished September 2005
- Test site <http://tks.openpkd.org> will be started next few month
- Trusted keyserver service will start in April 2006

Summary

- Digital Signature is strongly required for Free Software/Open Source developers
- OpenPKSD provides public key exchange infrastructure
- OpenPKSD Trusted Keyserver, new version keyserver server system is coming soon.
- Ruby is a strong glue between Apache2, extra-modules and Database and is good for server application