

More secure with less "security"

Tobias Mueller

Stef Walter



GNOME™

Board of Directors

The GNOME Foundation is run by a [Board of Directors](#), which is elected annually by the GNOME community, as the GNOME Membership, to carry out much of the GNOME Foundation's tasks.

The meetings of the Board of Directors are posted publicly on the [foundation-list mailing list](#) and on the [Minutes wiki](#) page for easier access.



Emmanuele Bassi



Joanmarie Diggs



Ekaterina Gerasimova



Tobias Mueller



Andreas Nilsson



Sriram Ramkrishna




Marina Zhurakhinskaya

~313337 USD p.a.





 Friends of GNOME donations

\$19993.9. \$6 to go!

[Donate now!](#)

application containment
enhanced disk encryption support
Tor integration
user control over diagnostic reporting features
robust VPN routing
application integration with system-wide privacy settings
control how GNOME devices are identified on networks
anti-phishing features for Web, the GNOME browser



GNOME Love

GNOME3

FUCK YOU



“the user”



hu·man

[hyoo-muhn or, often, yoo-]

“Filtering out extraneous
information is one of the basic
functions of consciousness”

— Barry Schwarz

freedom \neq choice

**IF YOU FORCE THE USER TO BE A
PART OF A SECURITY SYSTEM**



YOU'RE GONNA HAVE A BAD TIME

The extent of the human's
involvement in security prompts
is to identify themselves

Experts?

the worst possible time to ask
a user a risky question?

when they're trying
to do something else.



worse than random chance.

Prompts are
dubious

Security prompts are
wrong

Interrupting the user to make a
permanent security decision is
EVIL

Untrusted connection



This connection is untrusted. Would you like to continue anyway?

The identity provided by the chat server cannot be verified.

The certificate is self-signed.

► **Certificate Details**

☐ Remember this choice for future connections

Cancel

Continue

The software is not signed by a trusted provider.



The software is not signed by a trusted provider.
Do not update this package unless you are sure it is safe to do so.

Malicious software can damage your computer or cause other harm.
Are you **sure** you want to update this package?

Close

Force install



Abrt found a new update which fix your problem. Please run before submitting bug: `pkcon update --repo-enable=fedora --repo-repo=updates-testing tracker-0.14.1-1.fc17`. Do you want to continue with reporting bug?

No

Yes

GAME

OVER

MAN

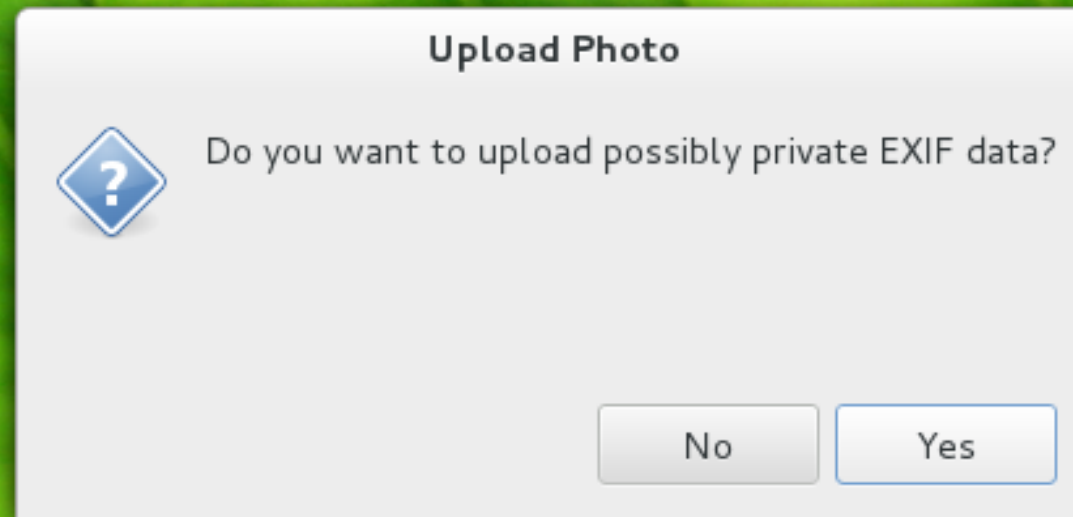
Stop interrupting

Let the user express
their intent...

... and make security decisions
based on intent.

Example: Portals





Example: EXIF

Photos



Kressbronn, Baden-Württemberg, Germany

09-Sep-2012 15:34

Fix(ing) it!

Bye bye
Certificate
Prompts

Certificate Viewer



Identity: CA Cert Signing Authority

Verified by: CA Cert Signing Authority

Expires: 03/29/2033

☐ Details

Subject Name

O (Organization): Root CA

OU (Organizational Unit): <http://www.cacert.org>

CN (Common Name): CA Cert Signing Authority

EMAIL (Email Address): support@cacert.org



Issuer Name

O (Organization): Root CA

OU (Organizational Unit): <http://www.cacert.org>





Just drop the connection

But but but

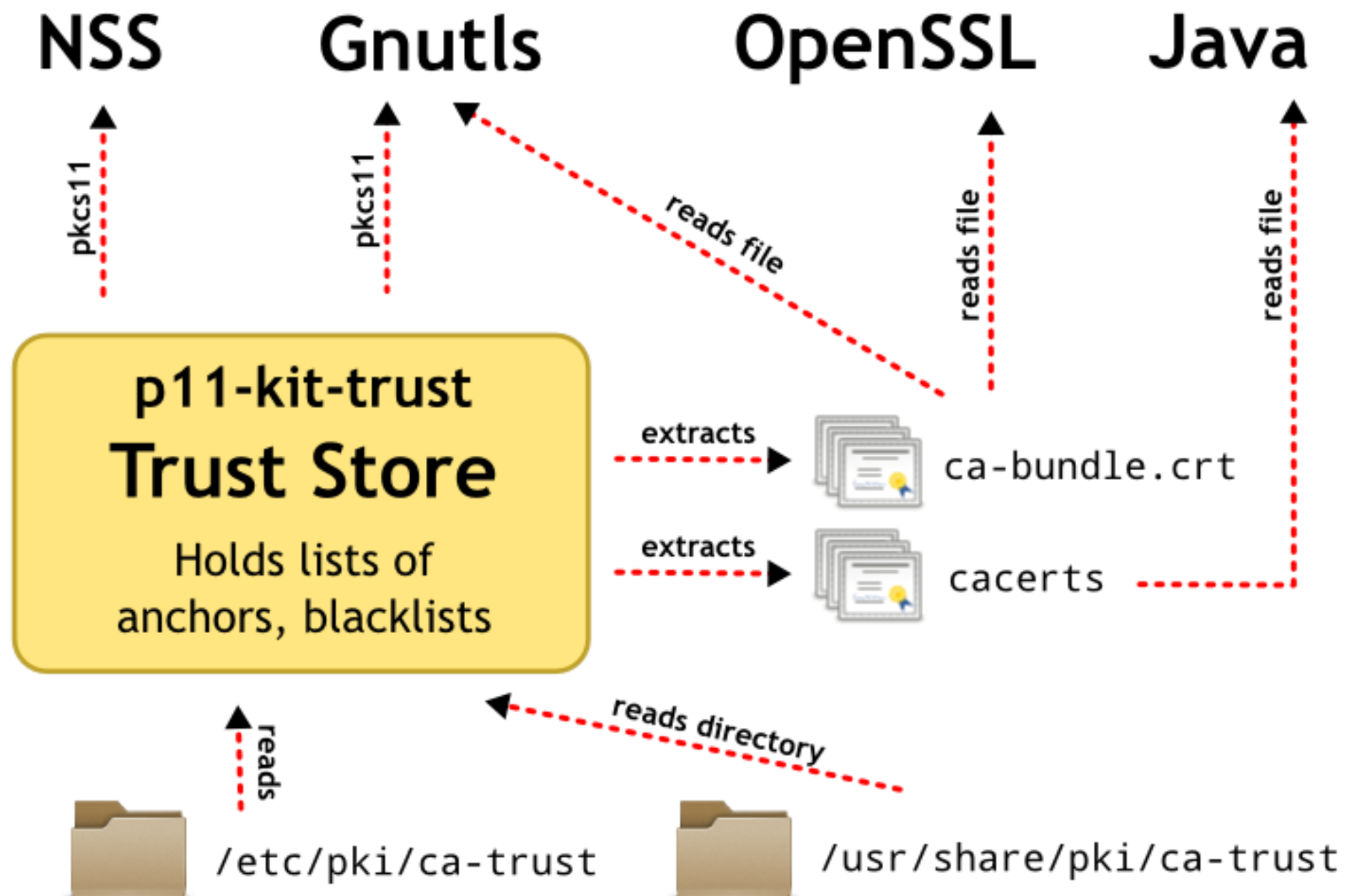
[Configure an Enterprise CA](#)

Can now store anchors

Experts:

Pin certificates to accounts

Shared System Certificates



Command line tools

GUI

real soon now...



NSS, GnuTLS, Java, OpenSC, OpenSSH,
OpenVPN, QCA (QT), GNOME Keyring,
TrueCrypt, GLib, OpenSSL (sorta) ...

Library: p11-kit

<http://p11-glue.freedesktop.org/p11-kit.html>

Go forth and kill

prompts

Ellisons Law:

For every keystroke or click
required to use a crypto feature
the userbase declines by half.

Any Questions?

p11-glue@lists.freedesktop.org
<http://p11-glue.freedesktop.org>

stef@thewalter.net
muelli@hamburg.ccc.de

Credits:

jimmac.musichall.cz

tychay at flickr.com

oliharwood at flickr.com

scradam at flickr.com

bitreaper1 at somethingawful.com

memegenerator.com