Mozilla Crypto/PKI Support

Frank Hecker
hecker@hecker.org

http://www.hecker.org/mozilla/mozilla-crypto-pki.pdf

Topics for today

- The Mozilla project
- Mozilla, Firefox, and Thunderbird
- Brief Firefox demonstration
- Mozilla crypto and PKI support
- Q&A

The Mozilla project

- Goal: develop innovative open source standards-based Internet client software
  - Originally initiated by Netscape in 1998
- Now run by the Mozilla Foundation
  - Non-profit with funding from AOL and others
  - Staffed by key long-time Mozilla contributors
  - Also does custom consulting, development
- Contributions from wider community
  - Volunteer developers, QA teams, etc.
  - Distributors of Mozilla-based products

Mozilla products

- Mozilla Suite
  - Combined browser/mail client/HTML editor/...
- Firefox (in development)
  - Next generation web browser
  - Designed for speed, ease of use
- Thunderbird (in development)
  - Next generation email client
  - Design goals same as Firefox

Firefox and Thunderbird features

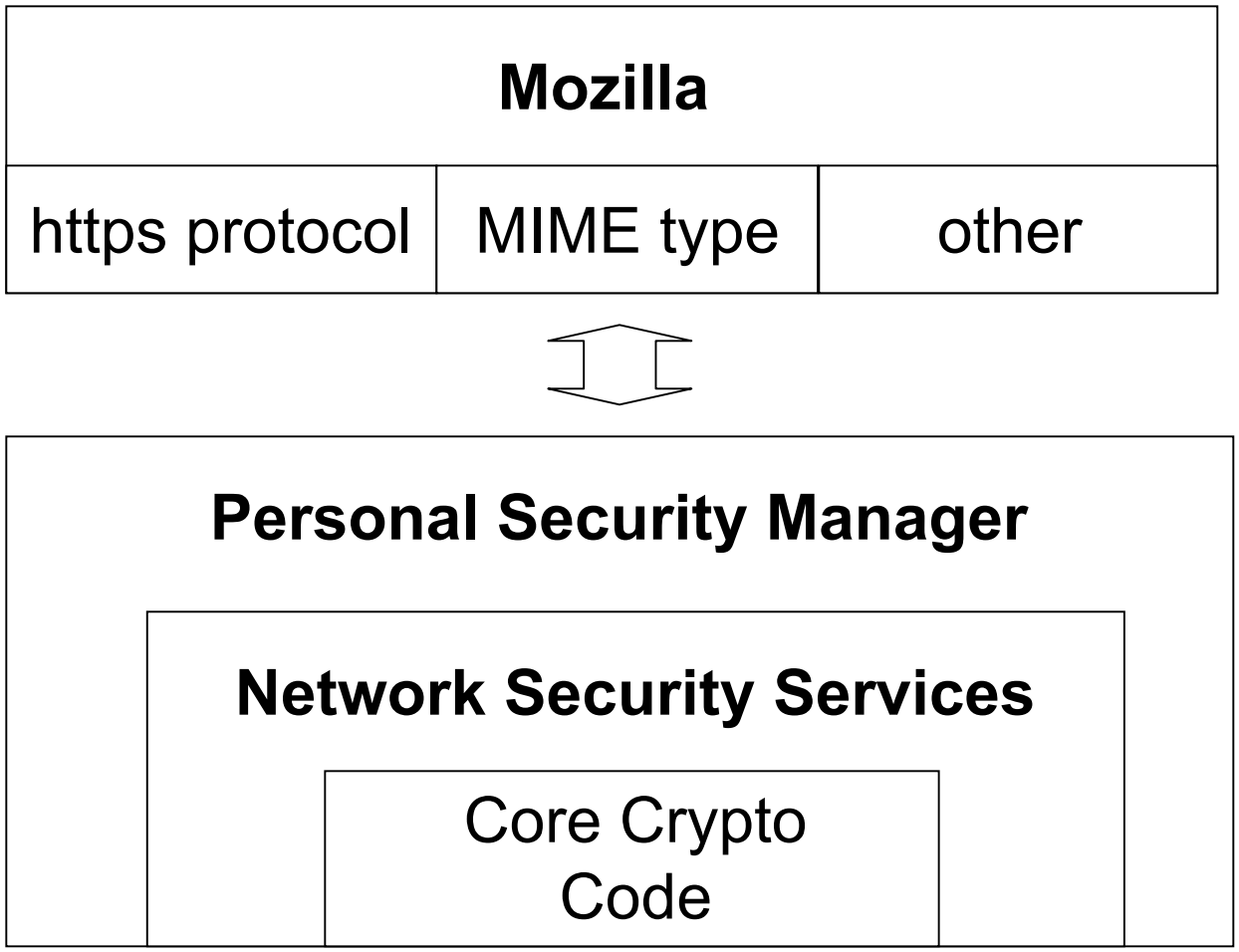
- Cross platform
  - Windows, Linux, Mac OS X, plus many others
- Firefox
  - Popup blocking, tabbed browsing, simple UI
- Thunderbird
  - POP, IMAP, SMTP
  - Spam filtering, multiple identities
- Extensible
  - Can add features through optional downloads

Firefox / Thunderbird Demo

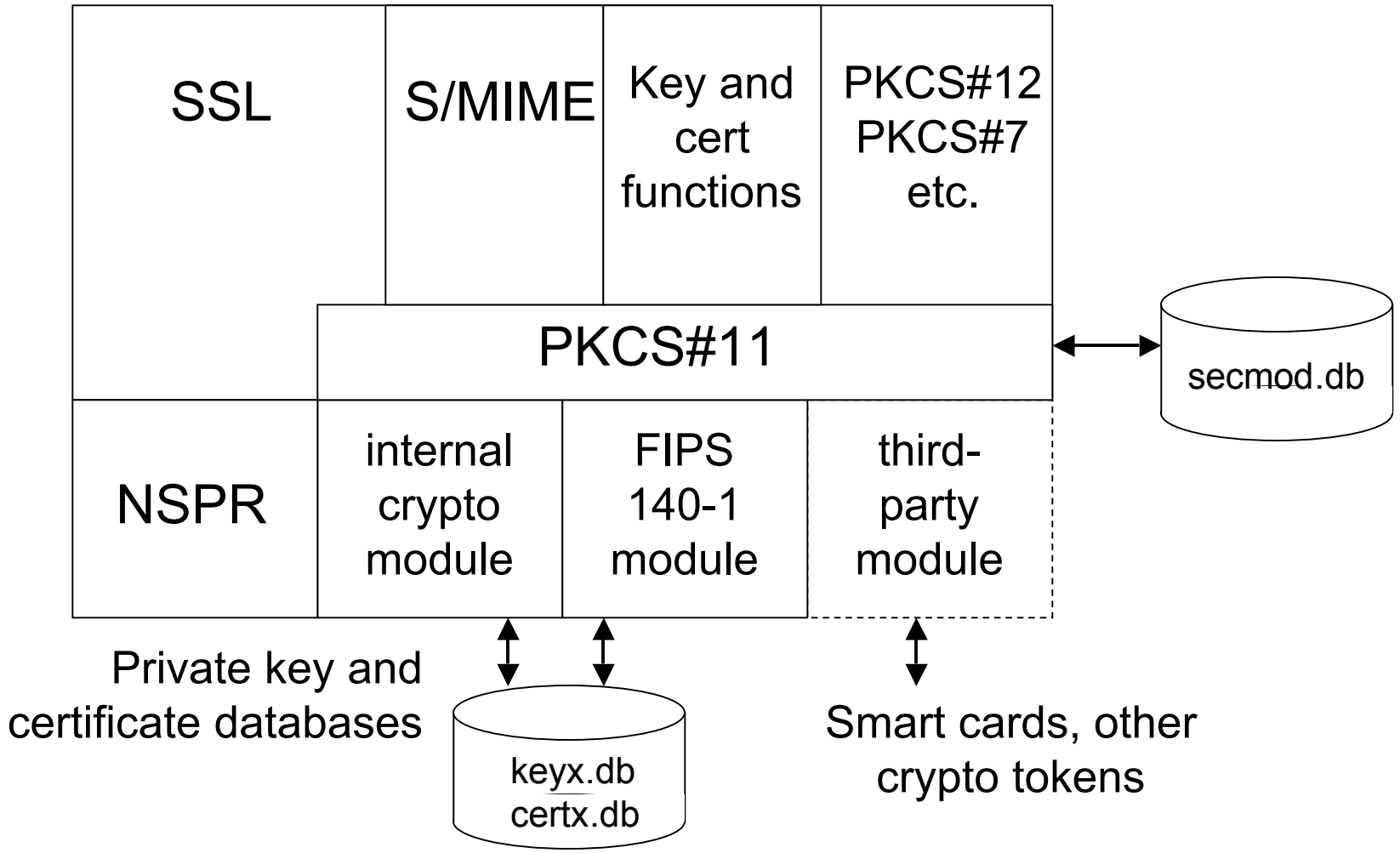
Mozilla crypto-related features

- SSL/TLS support
  - Web browsing (HTTP over SSL)
  - Email protocols (POP, IMAP, SMTP over SSL)
  - Directory search (LDAP over SSL)
- S/MIME support
  - Encrypted and/or signed email
- Digitally-signed code
  - Signed JavaScript and Java
  - Signed Firefox/Thunderbird extensions (.xpi)

Mozilla crypto architecture



Network Security Services



Crypto buzzword compliance

- SSL 2.0/3.0, TLS 1.0
- RC4, DES, 3DES, AES algorithms
- S/MIMEv3 (commonly-used features)
- PKCS#11 2.01 API for third-party hardware or software crypto modules (smart cards, etc.)
- Support for "dual-key" operation
  - Separate keys, certificates for signing, encryption
- CMC certificate request protocols
- CRL checking
- OCSP online certificate validation

But more needs to be done…

- Better UI for certificate, PKI operations
  - Overly-complex, not well integrated
  - Confusing warning dialogs, error messages
- Improved CRL and OCSP support
  - CRL/OCSP checking not enabled by default
  - Must download CRLs "by hand" initially
- No support for advanced PKI features
  - Cross-certification
- Revalidation for FIPS 140-2?

For more information

- Mozilla crypto newsgroup
  - netscape.public.mozilla.crypto
- PSM/NSS project pages
  - http://www.mozilla.org/projects/security/pki/
- Mozilla source tree
  - http://lxr.mozilla.org/mozilla/source/
    - security/nss
    - security/manager

Q&A