Open Source Crypto and Mozilla

Frank Hecker
hecker@mozilla.org

http://www.hecker.org/mozilla/open-source-crypto-and-mozilla.pdf

Topics for Today

- Brief history of Mozilla and crypto
- Export control issues for open source crypto
- Mozilla crypto architecture
- Current status of Mozilla crypto development
- Near-term roadmap for Mozilla crypto
- Longer-term possibilities for crypto in Mozilla
- Information sources

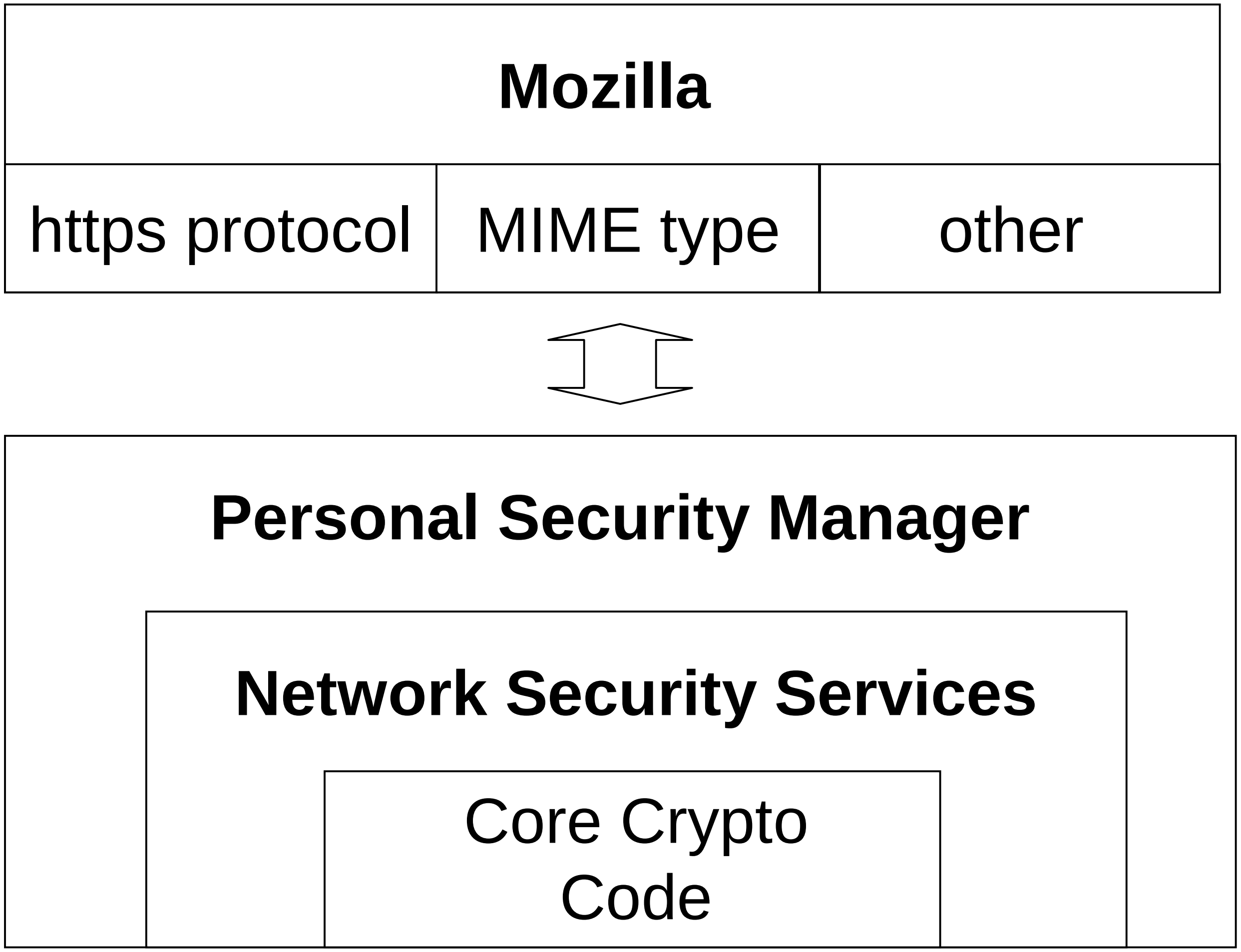
Brief history of Mozilla crypto

- SSL was invented at Netscape and implemented in Netscape Navigator 1.0
- Netscape security/crypto library was later used in servers, extended for S/MIME, etc.
- Partial source code was released in January 2000 under MPL/GPL, minus proprietary RSA code
- Mozilla support for “128-bit” SSL available since M14 through a binary-only add-on from iPlanet
- Goal is full open source implementation for Mozilla SSL, S/MIME, and other functions, including independently-developed features

US crypto export control

- Open source has special exemption
  - No permission required to export open source
  - Can make available for unrestricted download
- Remaining issues
  - Must notify US government of export
  - Risks in working with developers from some nations (Iraq, Iran, Cuba, North Korea, etc.)
  - Commercial products based on open source may still require US government paperwork

Mozilla crypto architecture



Mozilla

https protocol

MIME type

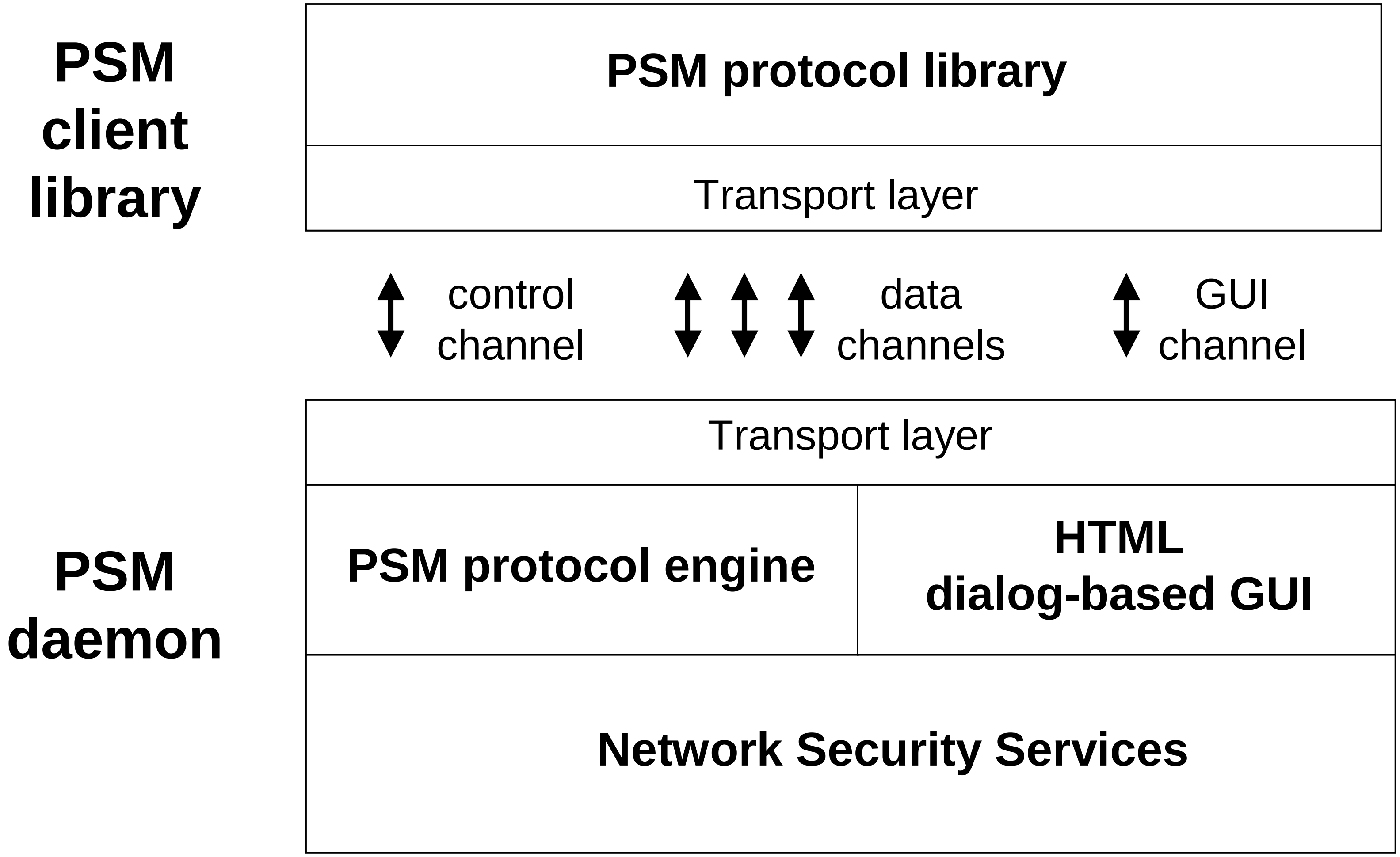
other

Personal Security Manager

Network Security Services

Core Crypto Code

Personal Security Manager



PSM client library

PSM protocol library

Transport layer

control channel

data channels

GUI channel

PSM daemon

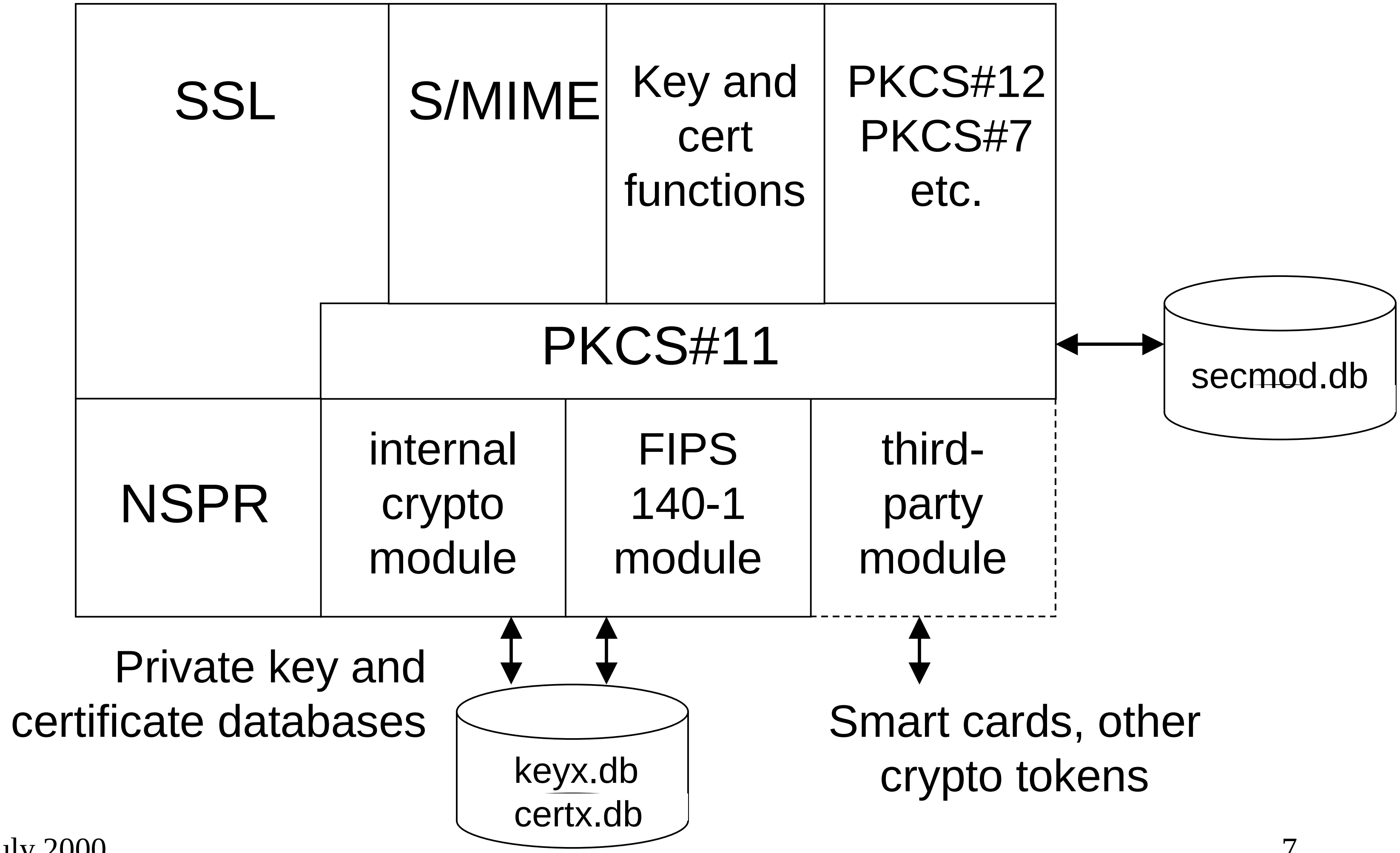
Transport layer

PSM protocol engine

HTML dialog-based GUI

Network Security Services

Network Security Services



SSL

S/MIME

Key and cert functions

PKCS#12
PKCS#7
etc.

PKCS#11

secmod.db

NSPR

internal crypto module

FIPS 140-1 module

third-party module

Private key and certificate databases

keyx.db
certx.db

Smart cards, other crypto tokens

Crypto buzzword compliance

- SSL 2.0/3.0, TLS 1.0 (RSA ciphersuites only)
- 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
- OCSP online certificate validation

Current Mozilla crypto status

- All source code specific to PSM is available
- All NSS code above PKCS#11 is available
- “freebl” API defined below PKCS#11 API but above actual crypto implementation
- NSS can be compiled and built with BSAFE
  - Uses freebl-to-BSAFE code layer
  - PSM can (almost) be built with NSS/BSAFE
- PSM works with Mozilla for SSL support

Near-term Mozilla crypto plans

- Add open source code for remaining crypto
  - Arcfour algorithm
  - Pseudo-random number generator
  - Bignum library (MPI)
  - RSA public key algorithm (after 20 September)
- Add S/MIME toolkit
- Release complete open source NSS (3.1)
- Release buildable open source PSM (1.3?)

Long-term plans, possibilities

- Integration of S/MIME support into mail/news
- Architecture work for PSM, NSS
  - Support for multiple simultaneous applications using PSM
  - Better XPCOM support
  - Expose more crypto-related APIs in Mozilla (including access from JavaScript)
- Independent work for OpenPGP in Mozilla?
- Joint efforts with other crypto projects?

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/
    - extensions/psm_glue
    - security/nss
    - security/psm