libpkix: Bringing High Quality Certificate Handling to the Masses

Presentation to the FBCA Path Discovery and Validation Technical Working Group
June 3, 2004

Steve Hanna, Sun Microsystems, Inc.

Outline

- What is libpkix?
- Why libpkix?
- libpkix in detail
- Proposal
- Q&A

What is libpkix?

- C library for X.509 certificate handling
  - Building certificate chains
  - Validating certificate chains

Why libpkix?

Primary Obstacles to PKI Deployment and Usage

1) Software Applications Don't Support It
2) Costs Too High
3) PKI Poorly Understood
4) Too Much Focus on Technology, Not Enough on Need
5) Poor Interoperability

Source: OASIS PKI TC August 2003 Survey
http://www.oasis-open.org/committees/pki/pkiobstaclesaugust2003surveyreport.pdf

Why libpkix?

- We need strong PKI support in applications
  - Standards-compliant
  - Reliable
  - Interoperable
  - Bridge CA compatible
- Application vendors will add such support if
  - Revenue boost substantially exceeds costs
  - NIST draft rec, J GPKI => revenue impact
  - Strong Open Source library => lower development costs

Why isn't CML enough?

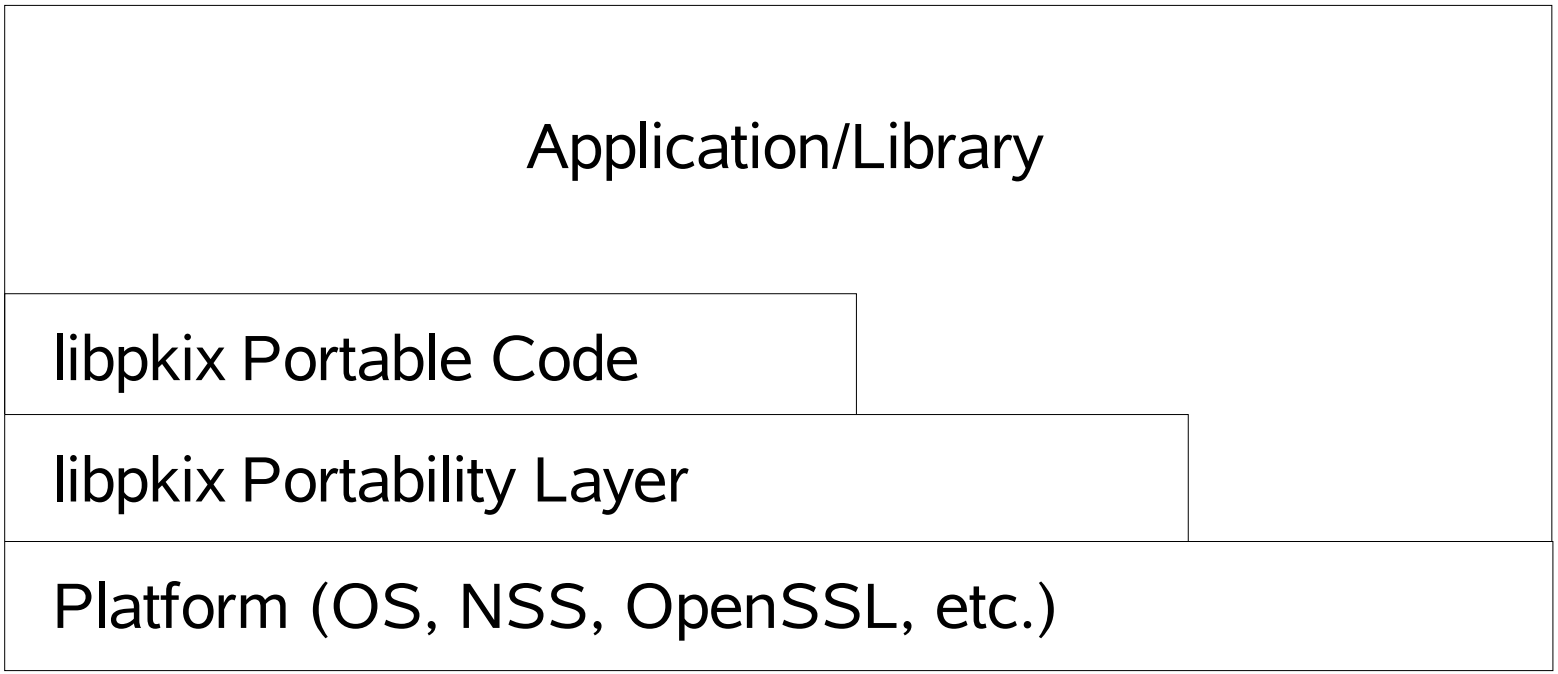
- Application developer requirements
  - Efficient
  - Thread-hot
  - Small
  - Minimal application code changes

Source: Mozilla NSS Team, OpenSSL Team

libpkix Features

- Standards-compliant (RFC 3280, etc.)
- Supports Bridge CA and any other topology
- Easy to use
- Portable
- Efficient (Thread-hot)
- Extensible
- Designed to plug easily into any code base: Mozilla, OpenSSL, etc.
- Still under development

libpkix Architecture



libpkix APIs

- PKIX_ValidateChain()
- PKIX_BuildChain()
- PKIX_CollectCerts()

- Support Functions

Development Team

- Sun Labs Internet Security Research Group
  - Created CertPath libraries (in JDK 1.4 & later) which pass PKITS tests
  - Authors of NDSS '01 paper on path building
  - Ongoing PKI research: R&D Workshop, etc.
  - Active in IETF PKIX WG, OASIS PKI TC, etc.
- Dartmouth PKI Lab
  - PKI Research and Deployment
  - Dozens of Papers and Prototypes
  - Years of Deployment Experience
  - Responsible for HEBCA

Applications

- NSS
  - Mozilla
  - Sun servers
  - Netscape servers
- OpenSSL
- Others in discussions

Implementation Status

- Architecture Complete
- APIs Complete
- Basic NSS Portability Layer Working
- Starting on Basic Path Validation

Current Schedule

- Fall 2004 – Basic Path Validation
- Summer 2005 – Full Path Validation
- Summer 2006 – Full Path Building
- Summer 2007 – Certificate Collection
- Later – Optional Features
  (CRL DP, segmented CRLs, etc.)

Proposal

- Accelerate by adding one full-time engineer at Dartmouth PKI Lab for one year
- Cost: $100,000
- Benefit: Accelerated Schedule
  - Spring 2005 – Full Path Validation
  - Fall 2005 – Full Path Building

For More Info

- Read libpkix Architecture
- Read libpkix Programmer's Guide
- Email steve.hanna@sun.com

Q&A