

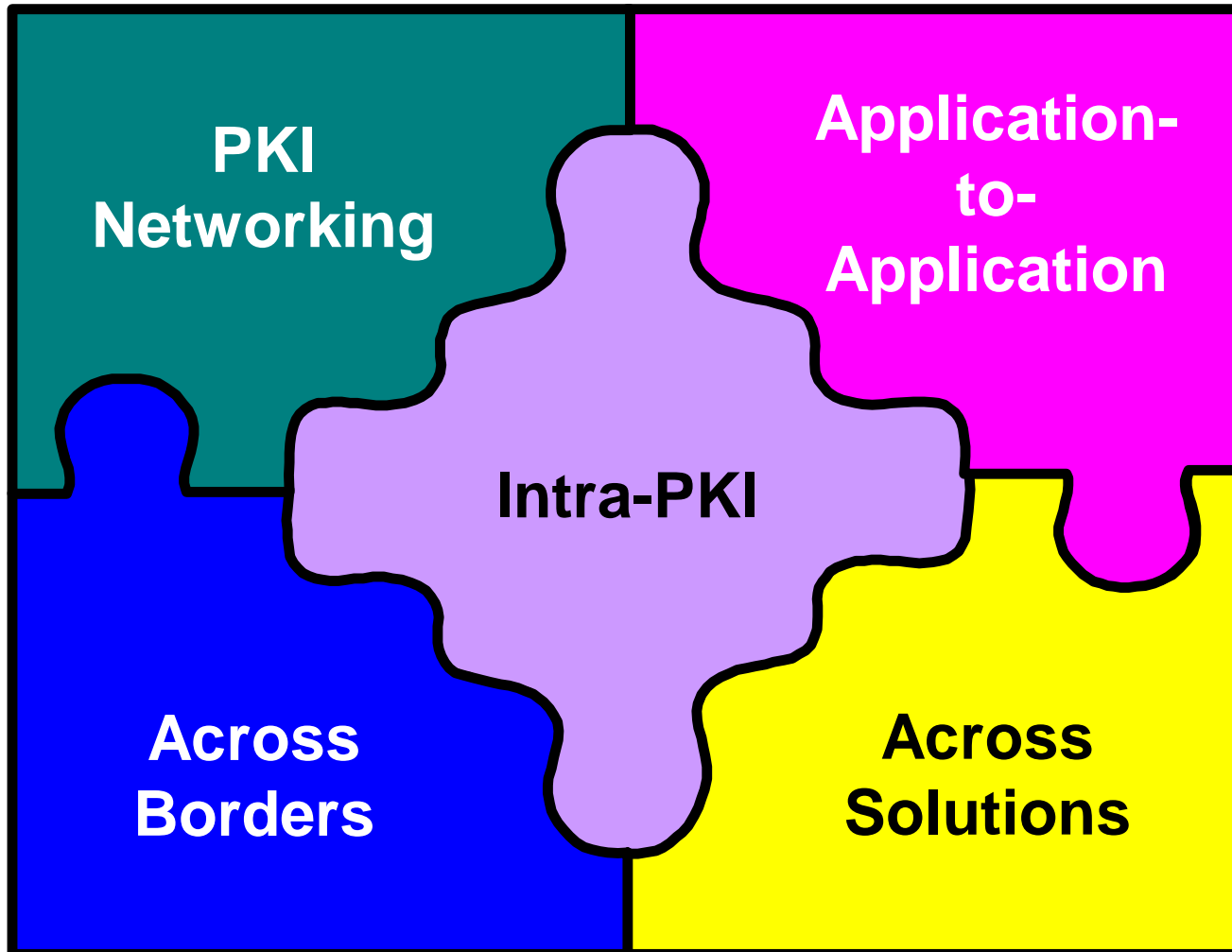


Entrust and Interoperability

Chris Voice
Product Management

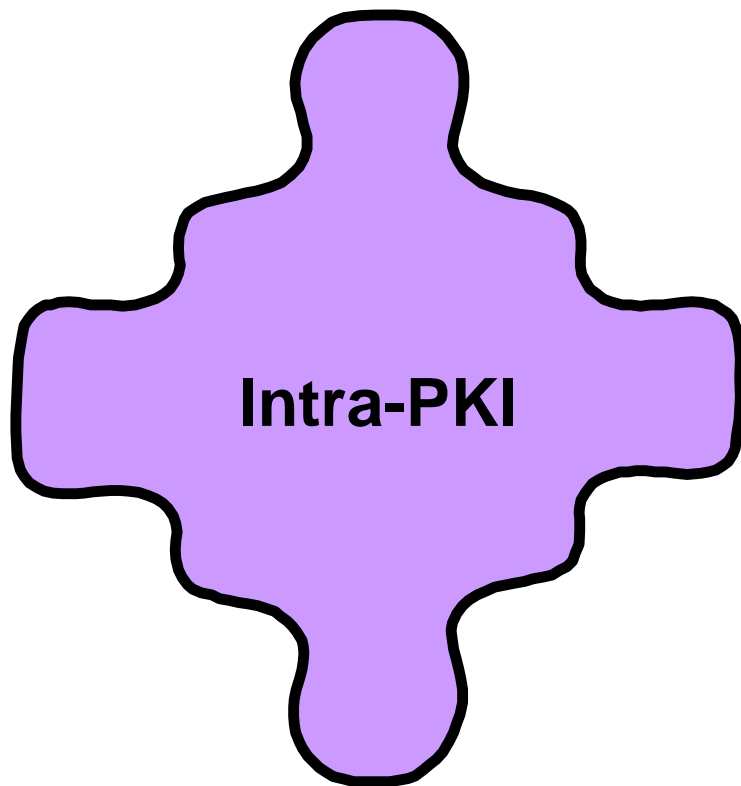


Interoperability Framework





Intra-PKI Issues



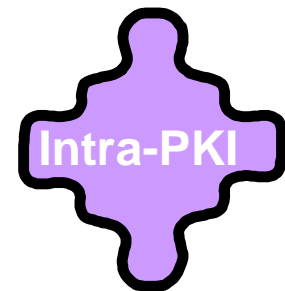
- Certificate format
- Key/cert request & management
- Flexible architecture
- Algorithms
- Certificate repository
- Certificate revocation
- Security hardware
- Platforms





Certificate Format

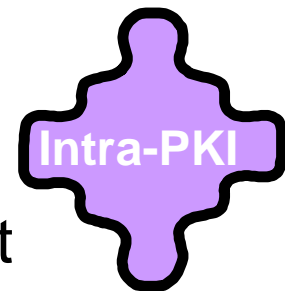
- X.509v3 since 1996
 - PKIX certificate profile
- Support flexible certificate formats using X.509v3 extensions
 - Defined by Entrust customers
 - Issued by Entrust/PKI
 - Processed by Entrust desktop engines
 - Issued by other vendors' certificate servers
 - Processed by Entrust desktop engines
 - compatibility with applications
 - e.g., Microsoft vs. Netscape browsers





Keys + Certificates

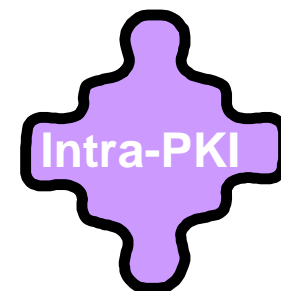
- Certificate request protocols
 - PKCS #10 and PKCS #7
 - PKIX-CMC
 - When it becomes a standard
 - Secure Electronic Transmission (SET™)
- Key and certificate management protocols
 - PKIX-CMP
 - Interop testing with IBM and Baltimore
 - Reference source code from IBM
 - Reference implementation from US Gov't (NIST)





Flexible Architecture

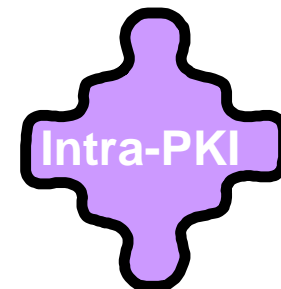
- “Flexible” architecture required for interop
 - Handles certificate request protocols from different types of “devices”
 - Provides flexibility and responsiveness in a changing environment
- Entrust/WebConnector™
 - Netscape, Microsoft, Apache, ...
- Entrust/VPNConnector™
 - Cisco + other VPN vendors
- Entrust/CommerceConnector™
 - All SET™ vendors





Algorithms

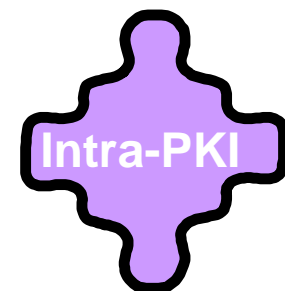
- PKI must be algorithm-independent
 - Provide customer choice
 - Policy (securely) determines which algorithms users can use
- Public-key algorithms
 - RSA, DSA, Diffie-Hellman, Elliptic-curve
- Symmetric algorithms
 - Triple-DES, DES, CAST, RC2, IDEA
- Hashing algorithms
 - SHA-1, MD5, RIPEMD





Certificate Repository

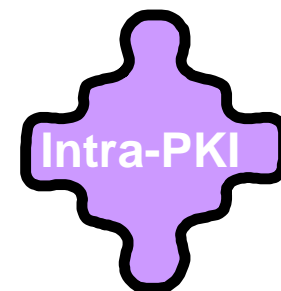
- PKI must be directory-independent
 - Provide customer choice
 - LDAP support since 1994
 - PKIX LDAP Schema specification
- Customers working with Directory products from the following vendors:
 - PeerLogic, Siemens, Novell, Control Data, Netscape, ZOOMIT, DCL, etc. ...





Certificate Revocation

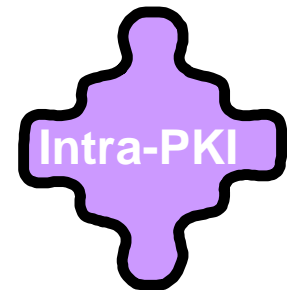
- Support for CRLs since 1994
 - X.509v2 CRL format with PKIX profile
- Invented CRL Distribution Points to provide scalable revocation systems (part of PKIX)
 - Free patent licensed by Microsoft, IBM, and others
- Support interoperability with systems that only have a single CRL (e.g., VeriSign)
- OCSP:
 - Entrust is a co-author
 - Partner Valicert providing OCSP solution





Security Hardware

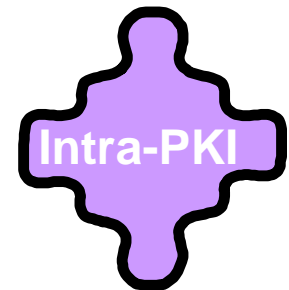
- Support PKCS #11 interface for CA hardware since 1997
 - Stronger security for CA private keys over software-only solutions
 - Provide customer choice
- Chrysalis-ITS
 - FIPS 140-1 Level 3
- Other vendor support including Atalla, Racal, etc...





Platforms

- PKI must be platform-independent
 - Provide customer choice
 - Infrastructure and desktop software
- Windows
 - 3.1, 95, 98, NT4, 2000
- HP-UX
- Solaris
- AIX
- Macintosh
- Java





PKI Networking™ Issues



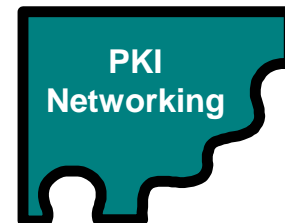
PKI Networking

CA networking
(cross-certification)
Policy networking
Directory networking
Revocation networking
Algorithms & key pairs



CA Networking

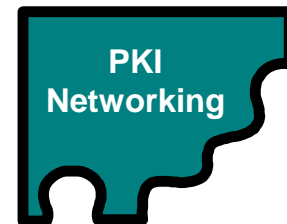
- Network structure
 - Hierarchical or distributed
- Cross-certificate format
 - Support X.509v3
 - Support flexible cross-certificate formats using X.509v3 extensions
 - Defined by Entrust customers
 - Issued by Entrust/Authority™
 - Processed by Entrust desktop engines
- Establish cross-certificates with PKIX-CMP or PKCS #10/#7





Policy Networking

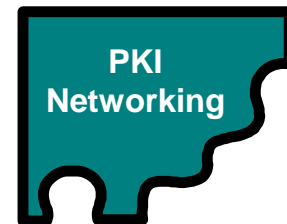
- Cross-certificates can contain:
 - Policy constraints
 - Policy mappings
 - Name constraints
 - Path length constraints
- Entrust desktop engines provide checking to ensure security policy is applied consistently across applications and platforms





Directory Networking

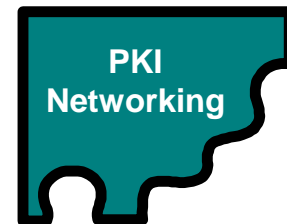
- Distributed directory systems in order to share certificates and revocation information across organizations
- Support via LDAP and X.500 since 1994
 - Replication, shadowing, chaining, etc... to distribute data





Revocation Networking

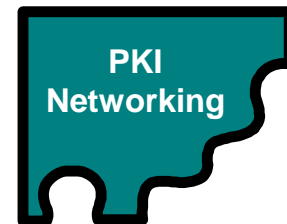
- Supported through LDAP + X.500
 - Distributed directory systems
- Scalability through X.509v2 standards-compliant CRLs with Distribution Points
- Standards-compliant ARLs (cross-certificate revocation lists) with Distribution Points





Algorithms + Key Pairs

- CA signature algorithms
 - RSA
 - DSA
- Single- or multi-key-pair systems





Application-to-Application Issues

Application-
to-
Application

Data formats & protocols
Algorithms
Key pairs





Data Formats + Protocols

- File formats
 - S/MIME since 1997
 - PEM since 1995
- Online authentication, integrity, and confidentiality protocols
 - IPSec (IKE)
 - SSL
 - SPKM



Application-
to-
Application



Algorithms

- Public-key algorithms
 - RSA, DSA, Diffie-Hellman, Elliptic-curve
- Symmetric algorithms
 - Triple-DES, DES, CAST, RC2, IDEA
- Hashing algorithms
 - SHA-1, MD5, RIPEMD
- Full suite maximizes interop with other vendors
 - Microsoft, Netscape, Baltimore, ...

Application-
to-
Application





Key Pairs

- Support for interoperability with:
 - Single-key-pair systems
 - Baltimore, Netscape, Microsoft, ...
 - Multi-key-pair systems
 - Microsoft Exchange/Outlook, ...

Application-
to-
Application





Across-Solutions Issues



Single login
Key storage & mobility
Policy
PKI networking
Key & cert management
Repository & revocation
Developer tools





Single Login

- Single login and security credentials across:
 - E-mail
 - E-forms
 - Web
 - VPN + remote access
 - ERP
 - Disk encryption
 - Smart cards, biometrics, software profiles





Key Storage + Mobility

- Support key storage options
 - Software profiles
 - Smart cards
 - Biometrics
- PKCS #11
 - Provides customer choice
- Mobility through:
 - Smart cards
 - Central storage and retrieval of keys





PKI Networking

- CA networking
- Directory networking
- Revocation system networking
- Policy networking





Policy

- Algorithms
 - Enforce which algorithms are used for encryption
 - But maintain full suite of algorithms for decryption (for interoperability)
- Passwords
 - Composition and update rules
- Key storage protection
 - Automatic logoff timeout
- Revocation checking
 - Caching or instantaneous





Key & Cert Management

- Key backup and recovery
- Support for non-repudiation
- Automatic and transparent key update
- Different algorithms for different functions
 - e.g., DSA for digital signature in the US Government means another algorithm is required for key transfer





Repository & Revocation

- Common directory
 - Reduces management costs
- Common revocation system
 - Consistency across solutions





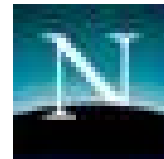
Developer Tools

- No-cost, open Toolkits
 - Demonstrated interoperability with Entrust, Microsoft, Netscape, Verisign, and Baltimore
 - Full development PKI
- Support standard protocols and APIs
 - PKCS, PKIX, S/MIME SSL, IPSec, LDAP
 - GSS-API, Java JDK
- Across platforms
 - Windows, Macintosh, UNIX, Java





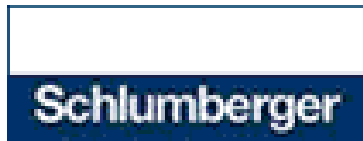
Across Solutions



CHECK POINT™
Software Technologies Inc.



How the world shares ideas.



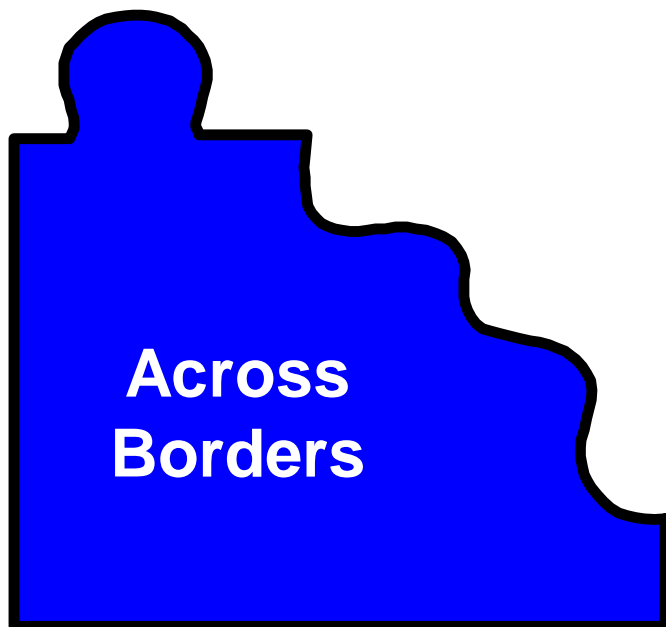
Recent Technologies
Bell Labs Innovations



+ more...



Across Borders Issues



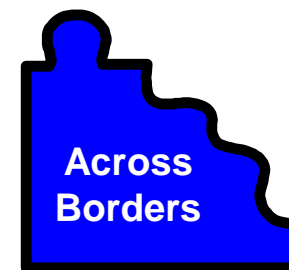
Algorithms
Open Toolkits





Algorithms

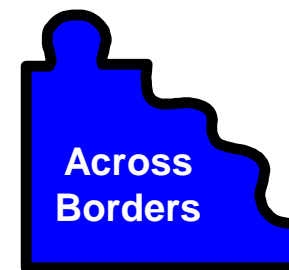
- Public-key algorithms
 - RSA, DSA, Diffie-Hellman, Elliptic-curve
- Symmetric algorithms
 - Triple-DES, DES, CAST, RC2, IDEA
- Hashing algorithms
 - SHA-1, MD5, RIPEMD
- Local algorithm support for interoperability





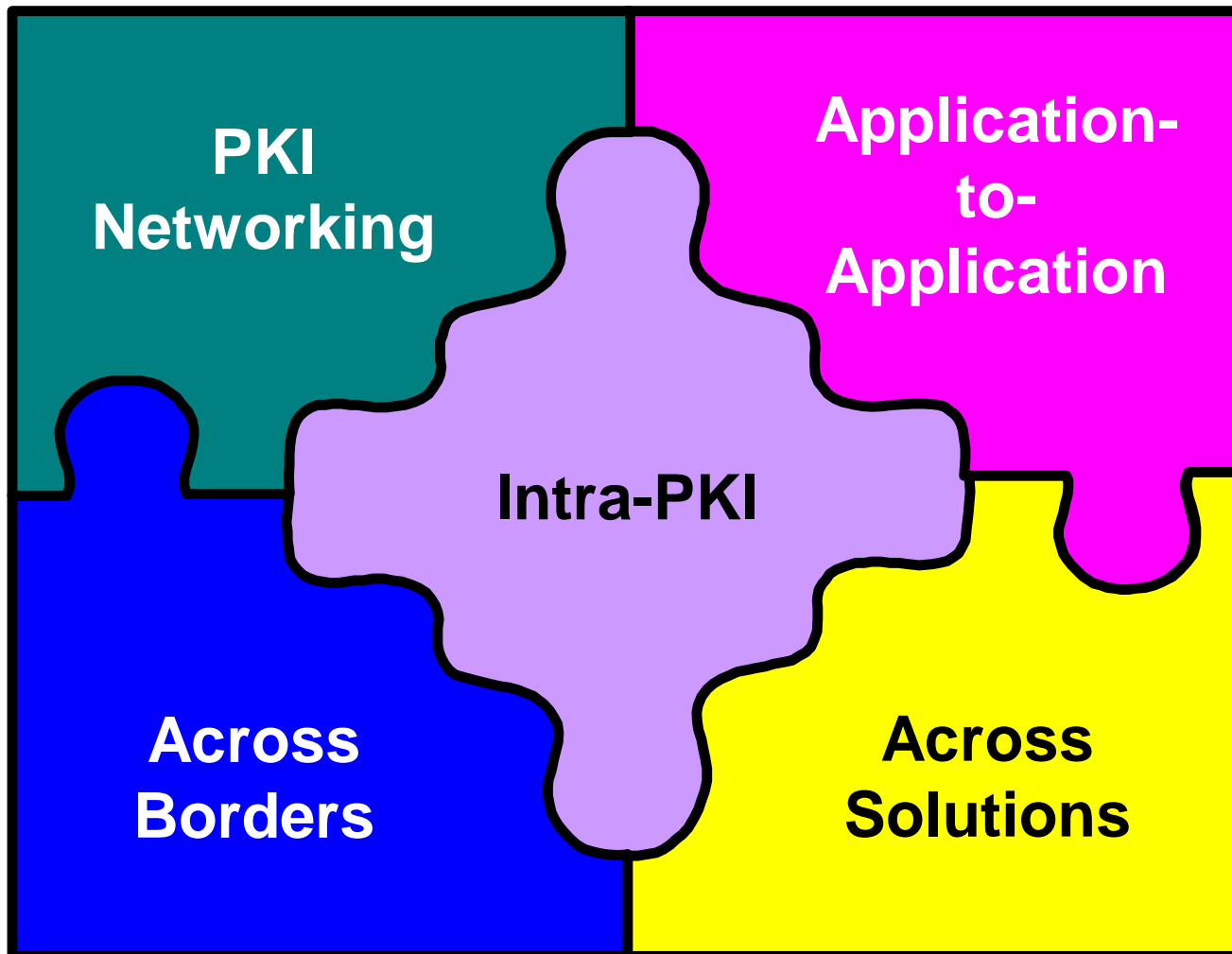
Open Toolkits

- Entrust provides open toolkits
 - Certified under both FIPS 140 and Common Criteria Evaluation
- Entrust-Ready™ applications contain no crypto





Interoperability Framework





Questions?

- For more information on Entrust:
 - Toll-free: 888-690-2424
 - E-mail: entrust@entrust.com
 - Web site: www.entrust.com

Thank you!

