Diversinet™

Diversinet Mobile PKI

Federal PKI Technical Working Group

December 11, 2003

Traditional Security Requirements

- Authentication
- Message Integrity
- Non-repudiation
- Confidentiality
- Audit

Security Challenges of Mobile Environment

- Network limitations
  - Lower bandwidth
  - Greater latency
  - Reduced connection stability
  - Unpredictable availability
- Device limitations
  - Relatively less powerful CPUs
  - Relatively less memory
  - Restricted power supply

Approach to Solving Mobile Security Problem

- Clear Need for:
  - PKI “lite”
  - More efficient messaging
  - Real time certificate validation
  - Distributed root key rollover process
  - Push certificate management
  - Push device management

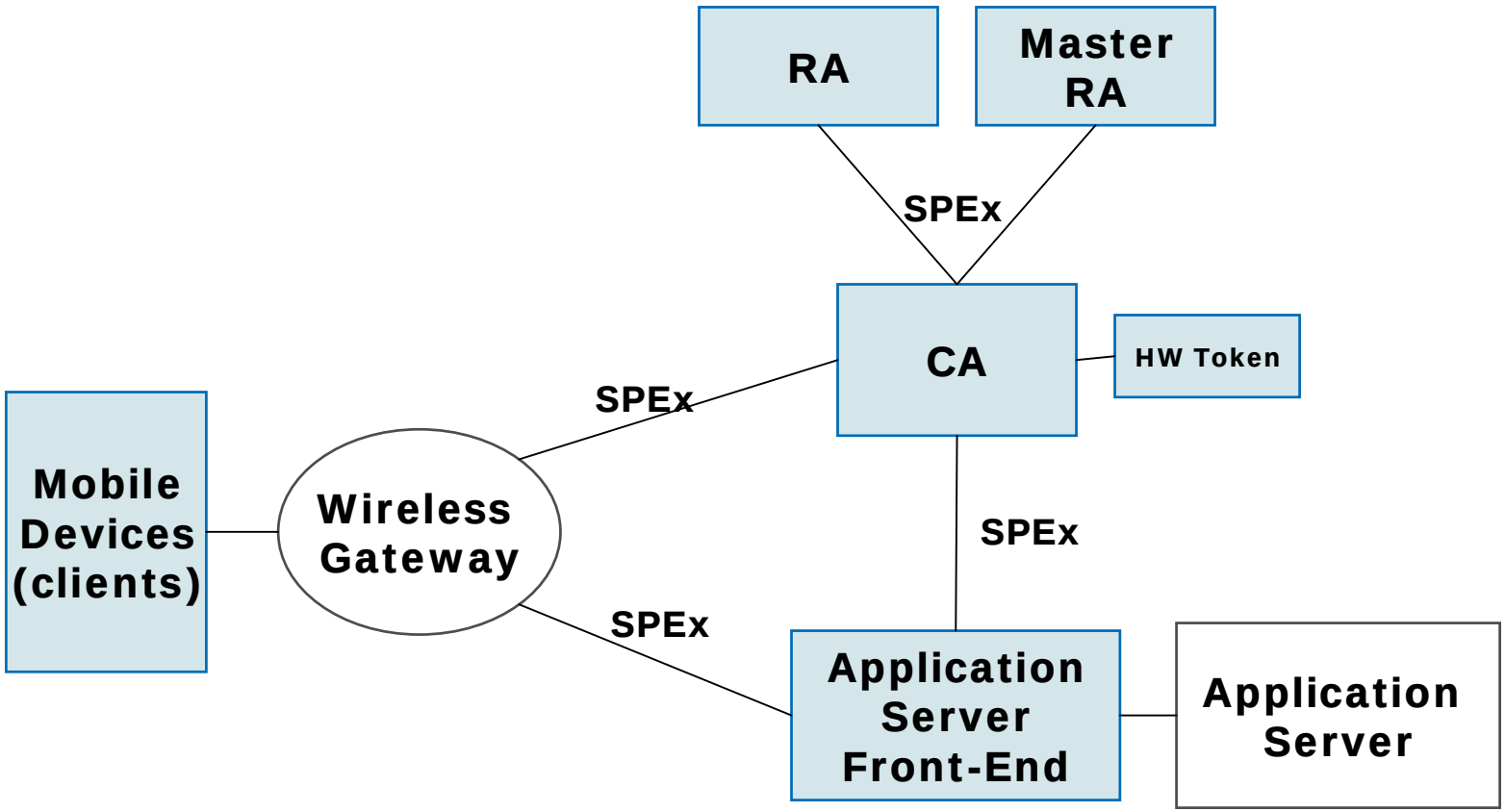
Passport Certificate Server… This is Not Your Mother's PKI.

- Passport CS is optimized for wireless usage
  - Smaller certificate than full X.509 certificate
  - Smaller PKI client on the device – No ASN.1 Encoding
  - Efficient protocols that minimizes # round trips to the server
  - Real time certificate status check
  - An automated process to update root CAs

Overview of Passport Certificate Server

- Unique advantages
  - Supports popular mobile devices: Pocket PC, Palm OS, Symbian, SIM phones, RIM wireless handheld
  - Root Key Rollover
  - Online certificate validation
  - Common Criteria Certification (EAL 2+)
- Other features
  - Anonymous identifiers in a certificate (attributes)
  - Hybrid certificates: RSA, ECDSA
  - Bulk certificate management ops for Registration Authority

Overview of Passport Certificate Server Architecture



High Level Review of Three Critical System Components & Features

- More Efficient Messaging
- Online Certificate Status Check
- Automated Root Key Roll Over

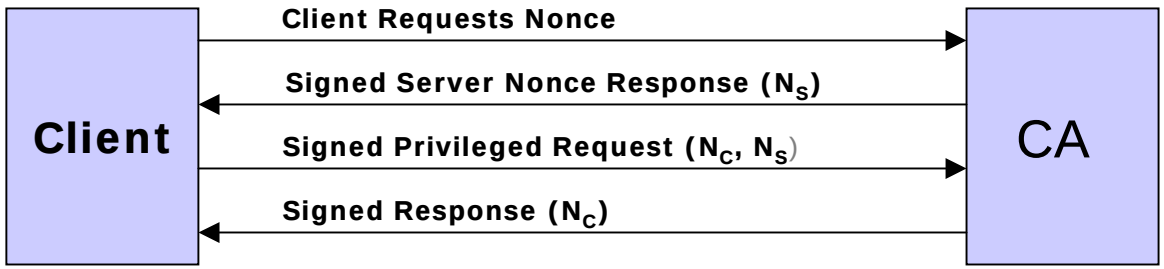
Secure Packet Exchange (SPEx) Protocol

- SPEx is composed of 3 sub-parts:
  - SPEx Secure Data Encoding protocol: a tag, length and value (TLV) encoding system.
  - SPEx Key and Certificate Management Protocol: a protocol for key and certificate management and server administration
  - SPEx Secure Messaging protocol: enables secure end-to-end communication between a client application and a server application
  -
- SPEx is independent of underlying transport protocol
  - (SMTP, HTTP, TCP, SMS)

SPEx Contd.

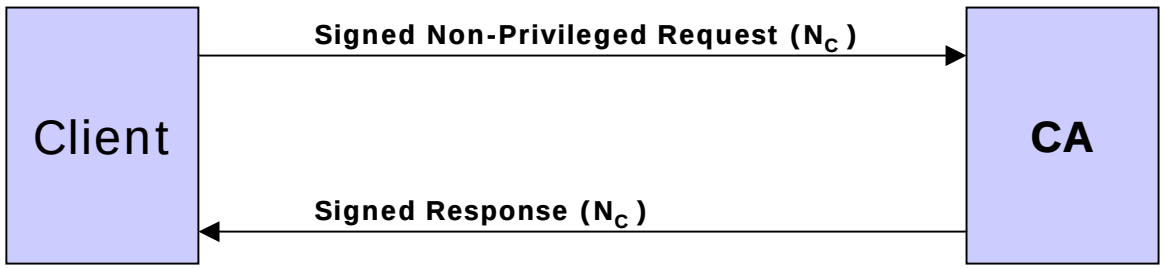
- SPEx supports:
  - certificate life cycle management,
  - online certificate validation,
  - certificate fetch all in a single protocol
  - root key update,
- More efficient than traditional PKI protocols - Fewer passes and characters
- Ideal for low bandwidth, high latency networks and constrained execution environments
- Allows development of full-featured PKI through ultra-minimal-footprint client applications.

SPEx Messaging



1. **Privileged (RBAC) command**

- Requests can be:
  - signed
  - hashed
  - unsigned
  - may contain encrypted sensitive data



2. **Non-privileged command**

Passport CS Client Features

- Thin generic client that can be ported into any wireless platform
- Size is 8K to 500k, depending on device configuration
- Available for devices running Palm OS, Pocket PC, RIM, Symbian, or featuring a SIM card
- Unique GSM/SIM client that is based on SIM Toolkit
- Tool kit allows application developers to easily integrate PKI functions into mobile applications

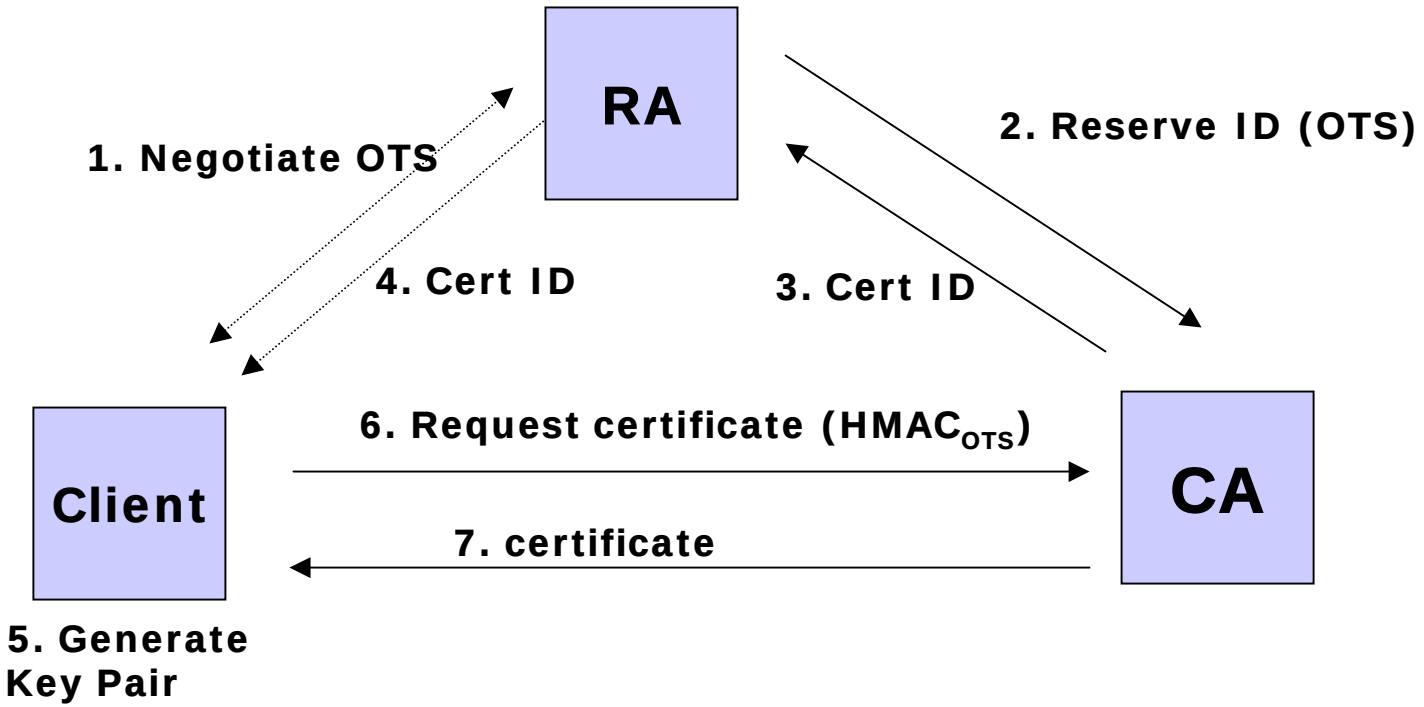
Client Features

- Generates a key pair
  - encrypt and password protect the private key
- Send a certificate request over-the-air to the CA (Equiv PKCS 7/10)
    - Requests secured using one time secret or digital signature
- Retrieve and install a certificate & root
- Accept a new root CA certificate
- Signing & encryption (PKI or Symmetric)

Certificate Registration Process

- Root key set (root cert and rollover keys) installed on device
- RA negotiates an OTS with the mobile user and requests a certificate ID from the CA
- Device generates its key-pair - private key encrypted and password protected (PBE)
- Device authenticates itself to the CA using the OTS and sends its public-key and “publish certificate” request including its reserved ID to the CA
- CA authenticates the message from the mobile and if successful issues a certificate to the mobile
- Mobile validates CS signed response and installs certificate

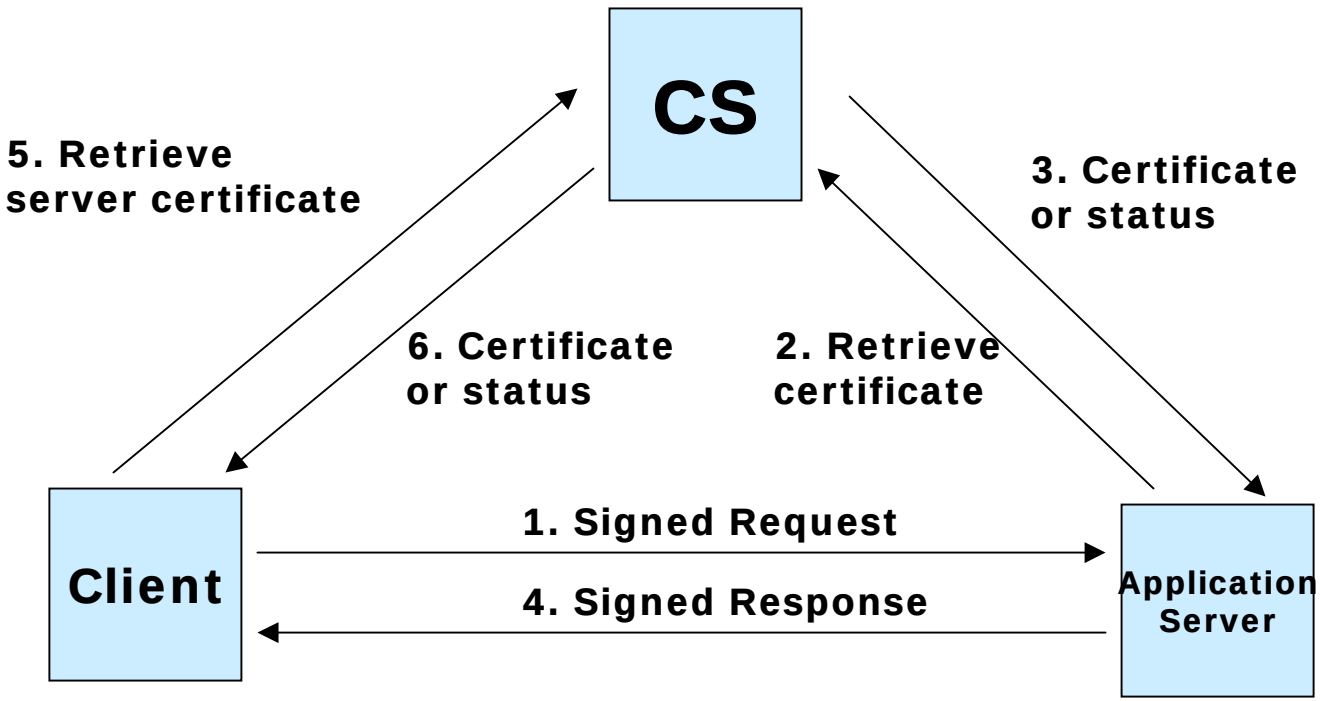
Certificate Registration Process



Certificate Validation Issues

- Current online validation standards
  - OCSP (IETF RFC)
  - SCVP (IETF Draft)
  - WAP and X9.68
- No standards-based protocol to pull and validate in one step

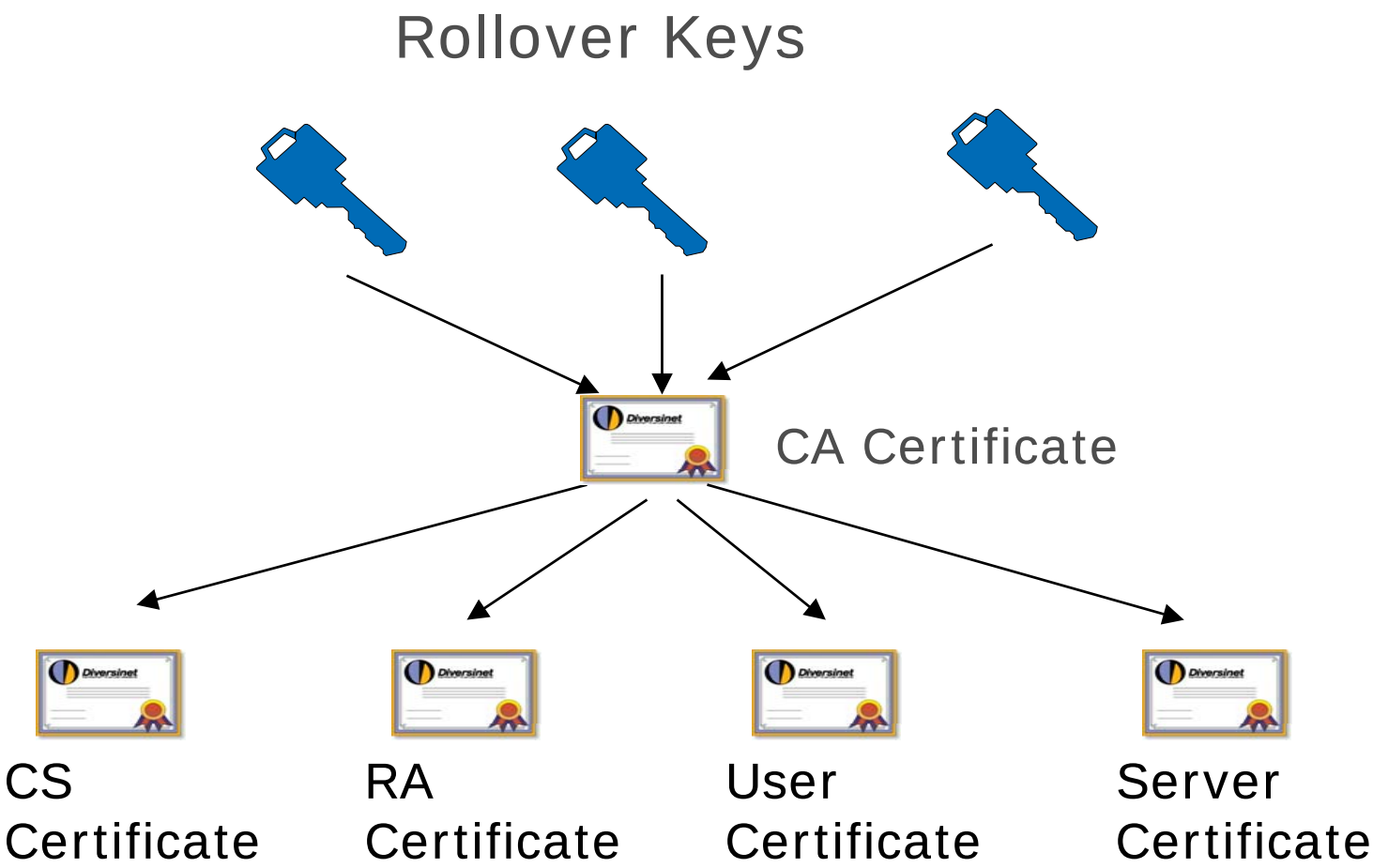
Certificate Validation Message Flows



Root Key Roll Over

- Protects the PKI from root key loss, compromise or expiry (catastrophic loss)
- Three “top level” root certificate rollover keys issued to all devices authenticates the root signing key and distributes security
- Root certificate is the Root CA’s public information signed by each of the root rollover keys
- Root certificate and root rollover keys can be updated by a rollover message signed by two of three root rollover keys

Root Key Roll Over



Root Key Roll Over

Root Key Set

Sequence number
Root certificate
Number of public root rollover keys
Public root rollover key 1
. . .
Public root rollover key *n*

Roll Over Block

Sequence number
Number of new public root rollover keys
New public root rollover key 1
. .
New public root rollover key *n*
Signature of “data block” signed with old private root rollover key 1
. . .
Signature of “data block” signed with old private root rollover key *n*

Root Update Structure

Sequence number
Root certificate
Signature of root certificate signed with current private root rollover key 1
. . .
Signature of root certificate signed with current private root rollover key *n*
Rollover block 1
. . .
Rollover block *m*

Initialisation

Rollover Key Update

Root Certificate Update

Root Key Roll Over Message Flows

Initial Root CA Key

Root CA Key Update

Likely Implementers

- Closed Systems
- Niche Applications

Diversinet Patents

Issued

- Root key rollover process
- Method for Safe Communications
- Permits

Pending

- Payment system and method using tokens
- Communication system and method
- Method of establishing secure communications in a digital network using pseudonymic identifiers
- Method of looking up and validating a digital certificate in one pass (online validation)
- Secure mobile terminal

Q & A

For more information please contact:

J. Scott Lowry
President, Diversinet USA
1101 Pennsylvania Ave,
Washington, DC 20004
202.236.8221
scott@diversinet.com