RSA Validation Solution
Agenda

• Need for Certificate Validation
• Certificate Validation
  — CRLs
  — OCSP
• RSA Validation Solution
  — RSA Validation Manager
  — RSA Validation Client
• Summary
Agenda

• Need for Certificate Validation
• Certificate Validation
  — CRLs
  — OCSP
• RSA Validation Solution
  — RSA Validation Manager
  — RSA Validation Client
• Summary
Need for Certificate Validation

• How can servers & applications know if users trying to access information have valid certificates?

• How can users receiving signed e-mail know the status of the sender’s certificate?

• How do businesses provide high level of assurance for transactions using digital certificates?
Need for Certificate Validation

• To ensure high levels of trust organizations need to validate digital certificates
  — Digital certificates can expire, be revoked or be suspended

• Organizations need an efficient and reliable method to check the validity of certificates with every transaction.

• Long standing method to determine certificate status is certificate revocation lists (CRLs)
Agenda

• Need for Certificate Validation
• Certificate Validation
  — CRLs
  — OCSP
• RSA Validation Solution
  — RSA Validation Manager
  — RSA Validation Client
• Summary
Certificate Validation
Certificate Revocation Lists (CRLs)

Certificate Authority
(RSA or other)

Web Application

LDAP Directory

Fetch CRLs

Certificate Status?

CRLs
Certificate Validation
Challenges with CRLs

• Two significant challenges of CRLs:
  — Accuracy of information
  — Distribution/scalability

• Bottleneck in validation process prevents accurate and timely certificate validation
Certificate Validation: CRLs Deployment Issues
Certificate Validation: CRLs Deployment Issues

Certificate Status is checked at Server or Desktop

Web Applications

Certificate Authorities (RSA or other)

User-to-User Interaction

LDAP Directory (ABC Co.)

LDAP Directory (123 Co.)

LDAP Directory (XYZ Co.)

123 Co. CA

ABC Co. CA

XYZ Co. CA

Authentication  Access Management  Encryption  Digital Signatures
Certificate Validation: CRLs Deployment Issues

Certificate Status is checked at Server or Desktop

Web Applications

Certificate Authorities (RSA or other)

ABC Co. CA

123 Co. CA

XYZ Co. CA

User-to-User Interaction

Fetch CRLs (XX MBs)

LDAP Directory (ABC Co.)

LDAP Directory (123 Co.)

LDAP Directory (XYZ Co.)
Agenda

- Need for Certificate Validation
- Certificate Validation
  - CRLs
  - OCSP
- RSA Validation Solution
  - RSA Validation Manager
  - RSA Validation Client
- Summary
Certificate Validation:
Online Status Checking Protocol (OCSP)

- IETF industry standard to address the challenges with CRLs

- How it works:
  - When a user attempts to access a server, OCSP sends a request for certificate status information.
  - The server sends back a response of "current", "expired," or "unknown."
  - The OCSP protocol specifies the nature of communication between the server (which contains the certificate status) and the client application (which is informed of that status)
Agenda

• Need for Certificate Validation
• Certificate Validation
  — CRLs
  — OCSP
• RSA Validation Solution
  — RSA Validation Manager
  — RSA Validation Client
• Summary
RSA Validation Solution
Business Benefits

• Ensures high levels of trust & assurance of transactions
  — Resolves CRL performance and scalability issues
  — Protects organizations from security breaches with invalid certificates

• Detailed auditing for increased accountability and protection

• RSA Validation Client seamlessly integrates real-time status checking into MS Windows applications

• Interoperable with third-party Certificate Authorities

• Certificate validation critical for secure Web services
Agenda

• Need for Certificate Validation
• Certificate Validation
  — CRLs
  — OCSP
• RSA Validation Solution
  — RSA Validation Manager
  — RSA Validation Client
• Summary
RSA Validation Manager
Overview

• Industry standards-based OCSP server:
  — RFC 2560 (PKIX OCSP)
  — CONOPS (US Gov’t)
  — Identrus (Financial Services)
• Highly scalable, enterprise-ready certificate status checking
• Interoperability with Keon CA and third party standards-compliant CAs
• Interoperability with third party OCSP clients
• Platform Support:
  — Solaris 8
Certificate Validation:
Certificate Status Checking with OCSP
Certificate Validation: Certificate Status Checking with OCSP
RSA Validation Manager
Key Features – Administration and Security

• Easy Administration
  — Command line administration for task automation
  — Local and remote web-based administration
  — Centralized aggregate of CRLs & delta CRLs published by single or multiple CAs

• Enhanced Security
  — HSM Support for FIPS level 3 protection of the private keys
  — SSL enabled requests, responses & administration
  — Digitally signed and unsigned OCSP requests
  — Nonces supported to eliminate replay attacks
  — Instant local revocation of certificates and CAs
  — Detailed audit logs and secure digital signing of audit logs (Q2 '04)
RSA Validation Manager
Key Features – Scalability and Performance

• Synchronization between servers
  — Eliminates need to distribute CRL to every OCSP Server
  — Allows Low bandwidth distribution of updates

• Caching Configurability
  — Grace period for expired CRLs
  — Enables quicker response time

• Supports multiple CAs simultaneously
  — Designate specific signer to sign OCSP responses
  — Specify the status source used to obtain status

• Supports Multiple Signers
  — Each Signer can have multiple certificates to serve different CAs

• Supports Multiple Status Sources
  — Can “Fetch” CRL/deltaCRL/ARL from an LDAP directory or manually import
  — Can “Forward” or “Proxy’ requests to another OCSP responder
Checking Status with OCSP: Scalability & High Assurance

Web Applications

Certificate Authorities (RSA or other)

LDAP Directory

CRLs

RSA Validation Manager

Fetch CRLs

OCSP

Synchronization

Third Party OCSP

RSA Validation Manager

Status

Authentication Access Management Encryption Digital Signatures
Checking Status with OCSP: Scalability & High Assurance

Check Status of specific certificate with OCSP

Internet

DMZ

FW

Keyless RSA Validation Manager

Internal Network

FW

RSA Validation Manager Cluster

Authentication

Access Management

Encryption

Digital Signatures
## RSA Validation Manager

### Performance

<table>
<thead>
<tr>
<th>Responder Configuration</th>
<th>Signer</th>
<th>resp/sec</th>
<th>resp/hr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsigned request with nonce</td>
<td>software</td>
<td>209</td>
<td>750,000</td>
</tr>
<tr>
<td>Unsigned request with nonce</td>
<td>nCipher</td>
<td>321</td>
<td>1,150,000</td>
</tr>
<tr>
<td>Signed request with nonce</td>
<td>nCipher</td>
<td>207</td>
<td>745,000</td>
</tr>
<tr>
<td>Unsigned request with no nonce</td>
<td>cached</td>
<td>510</td>
<td>1,800,000</td>
</tr>
</tbody>
</table>

- What Performance level is required for 1,000,000 users?
  
  — Assume that during a peak hour 50% of users use certificates and the average number of uses is 1.5.
  
  — Even with peaks of 50% over mean within the hour one RSA Validation Manager with an HSM can handle the load.
Agenda

• Need for Certificate Validation
• Certificate Validation
  — CRLs
  — OCSP
• RSA Validation Solution
  — RSA Validation Manager
  — RSA Validation Client
• Summary
RSA Validation Client
Overview

• Seamless OCSP client for MS Windows applications:
  — E-mail clients
  — Web browsers & servers
  — Third party MS CAPI compliant applications
• Supports standard RFC 2560 (PKIX OCSP) requests
• Supports signed/unsigned requests & response validation
• Provides full support and management of CRLs/delta/CRLs/ARLs
• Easy to deploy migration path from CRLs to real-time certificate status checking
• Supports multiple CAs and status sources simultaneously
RSA Validation Client

- Client deployable via Microsoft SMS
- Highly configurable to work in heterogeneous environments
- Interoperable with third party OCSP responders & CAs
- Supports local CRLs & OCSP validation to server
- Platform support:
  - Windows 2000
  - XP, NT, 2003 (Q2 2004)
RSA Validation Solution
Adding Value to Microsoft CA

• Validation Client deployable via Microsoft SMS
• Interoperable with MS CA
• Platform support:
  • RSA Validation Client:
    • Windows 2000
    • XP, NT, 2003 (Q2 2004)
  • RSA Validation Server:
    • Windows 2003 & 2000
RSA Validation Solution:
Adding Value to RSA ClearTrust and FIM

ClearTrust on IIS with Validation Client for OCSP

ClearTrust with Custom OCSP WAX (PSO)

FIM – Supports OCSP Today

RSA Validation Manager

Authentication Access Management Encryption Digital Signatures
Summary

• High level of trust and assurance for transactions
• Resolves CRL performance and scalability issues preventing accurate and timely certificate validation
• Scalable solution with high performance and powerful configuration options
• RSA Validation Client provides robust and seamless integration of certificate validation (OCSP and/or CRLs) into MS applications
• Interoperates with third party CAs & OCSP responders
• RSA Security offers the most extensive set of solutions for customers to easily and cost-effectively implement certificate-based applications