CoreStreet’s Distributed Certificate Validation

Randy Bowman
Principal Systems Engineer
Corestreet Ltd. Federal Team

rbowman@corestreet.com
Cell: (301) 254-3858
Agenda

• About CoreStreet
• CoreStreet Products and Services
• Technology Basics
• Distributed Certificate Validation
• DISA Validation System Facts & Readiness
• Vision
## CoreStreet in a Nutshell

<table>
<thead>
<tr>
<th>What We Make:</th>
<th>Massively scalable software for validating people, documents, computers, devices, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Founded:</td>
<td>October 2001</td>
</tr>
<tr>
<td>Employees:</td>
<td>35</td>
</tr>
<tr>
<td>Headquarters:</td>
<td>Cambridge, MA</td>
</tr>
<tr>
<td>IP:</td>
<td>16 issued patents + 18 filed patents</td>
</tr>
<tr>
<td>Target Markets:</td>
<td>Government, financial services, healthcare sectors.</td>
</tr>
<tr>
<td>Customers:</td>
<td>Identrus, three major federal agencies, two Global 1000 companies</td>
</tr>
<tr>
<td>Funding:</td>
<td>Privately funded</td>
</tr>
</tbody>
</table>
Our Products

RTC-Client

RTC-VA

Computer Security

Physical Access

Document Mgmt.

Real Time Credential Foundation

• "Shrink-wrapped" product
• Certificate validation and revocation
• Fully OCSP compatible

Applications developed on the RTCF to demonstrate real-world capabilities.

• Developer-facing application framework
• Lets developers add RTC capabilities to existing application or build custom solutions

© Copyright 2004 CoreStreet, Ltd.
First Some Definitions

- **Identity** “the qualities of a person that make them different”
  - Name, age, date of birth, physical features

- **Authentication** is proving your claimed identity
  - The picture on your driver’s license

- **Authorization** is granting privileges (process)
  - Privilege to drive, pass to enter military base

- **Credentials** are “evidence of one’s relationship or privileges”
  - Driver’s license represent relationship with state that issued it

- **Validation** is verifying your credentials are in good standing
  - Your relationship to the credentialing authority is still in good standing
  - Your privilege to drive has not been revoked
It’s a 2 Step Process!

Today, more than ever, there is a critical need to:

• Positively identify people, and then
• Decide if they should be allowed access to a place, device or function

Secure access therefore reduces to answering two critical questions:

1. Are you who you say you are? (Authentication)
2. Are you suppose to be doing what you are trying to do, right now? (Validation)
Certificate Validation Examples

SSL Web Service

VPN

Document Signing

Secure Email

Secure IM

Secure Wireless
Validation Choices Today

• Certificate Revocation Lists (CRLs)
  – Traditional CRLs
  – MiniCRLs

• Online Certificate Status Protocol (OCSP)
  – Traditional OCSP
  – Distributed OCSP
CRL

Certificate Authority

CRLs

Directory Server

Advantages
• Easy to manage for small numbers
• Works with all issued certificates
• Industry standard

Disadvantages
• Large bandwidth to the clients
• Does not scale

Clients

requires trust
(physical and data security)
CRL Problem #1: Scalability

• CRLs grow to unmanageable sizes
  – DoD CRLs already at 2-7 Megabytes Each (nearly 40MB)
  – Download times of 7-14 minutes
  – Current 17% revocation rate expected to grow

• CRLs need to be distributed to every relying party application
  – All data goes to all applications

Bottom line:

CRLs Do Not Scale!
CRL Problem #2: Performance

Need CRLs for all accepted certificates:

Federation explodes performance problem

From: Alice @ CIA
From: Bob @ DoJ
From: Chuck @ DoD
From: Dave @ DHS
OCSP: Market Acceptance

Native OCSP:
- Microsoft Windows (Longhorn)
- Identrus
- Netscape / Mozilla Communicator
- Sun ONE Identity Server
- RIM Blackberry PDA
- Compaq iPAQ
- Netegrity SiteMinder
- Oblix Netpoint
- Silanis Approvet
- Arcot Adobe Acrobat signing
- Elock Assured Office
- IBM DSMS
- Ascertina PDF Signer
- Conclusive TrustLogic
- Lexign ProSigner
- Gemplus eSigner
- CMG WAP Gateway
- Cisco Local Director, VPN
- Netscreen VPN
- Cyberguard VPN
- VeriSign

OCSP libraries/plug-ins:
- CoreStreet
- Alacris
- ValiCert
- Ascertina
- AssuredBytes
- Kyberpass
- SyTrust
- RSA Keon and BSAFE
- Authentica

Plug-ins support:
- Microsoft Outlook
- MS Outlook Express
- MS Internet Explorer
- MS IIS
- Apache web server
- Netscape/AOL/Sun servers
- Microsoft VPN
- MS Office XP
- Eudora (via Authentica)
- Peoplesoft (via Authentica)
- SAP (via Authentica)
- Lotus Notes (via Authentica)
Traditional OCSP

Advantages
- Small bandwidth to clients
- Works with issued certificates
- Industry standard

Disadvantages
- Requires secured responders
- Expensive to scale
- Slow response time to client
- Single point of failure
- Failover issues

Certificate Authority

Validation Authority (Responders)

CRL

OCSP Response

Clients

= requires trust
(physical and data security)
Traditional OCSP “Hard Questions”

• How many OCSP responders to deploy?
  – Cost issue

• Where to put the OCSP responders?
  – Cost and security issue

• How to use OCSP in tactical environments?
  – Security and rapid response issue

• How does a relying party application trust the response it receives from an OCSP responder?
  – Security and operational issue
Validation Solution Goals

- High Performance
- High Availability
- Truly Scalable
- Secure
- Cost effective

How to provide Distributed Validation that is cost effective and secure?
Design Principle

Separate the security sensitive data and trusted operations from the delivery process of providing certificate status to relying party applications.
Distributed OCSP

Advantages
- Uses unsecured responders
- Cost Effective
- Small bandwidth to clients
- Response 20X faster than T-OCSP
- Works with issued certificates
- Industry standard
- Scales to 10s millions of users
- No impact to client apps
- No impact to CA infrastructure
- Single key to manage
- Inherently more secure

Pre-signed OCSP Responses

RTC Authority

Certificate Authority

CRL

= requires trust (physical and data security)
Answers to “Hard Questions”

• How many OCSP responders to deploy?
  – As many as needed

• Where to put the OCSP responders?
  – Close to users

• How to use OCSP in tactical environments?
  – Set up responder, provide connectivity

• How does a relying party application trust the response it receives from an OCSP responder?
  – Short-lived certs from one Validation Authority
True Scalability

Revocation Request

Traditional OCSP

Distributed OCSP

LDAP

requires trust (physical and data security)
Distributed OCSP, Managed

**DISA Validation System Facts**

- Live on October 16, 2003
- # Certs supported > 12 million
- # CAs/CRLs supported = 19 + 1
- # Responders = 20
- # Global sites = 10
- Ave response time = 65 millisecs
- Responder capacity > 1,000 r/sec
- System accessed by users from:
  - 8 foreign countries
  - 19 different states

---

RTCAuthority

Pre-signed OCSP Responses

Responders

OCSP Response

= requires trust
(physical and data security)
Valid Response

The Certificate for:

CHRISTINE BOWMAN

has been Validated and is:

Good

Time to Validate: 0.431 seconds

Certificate

Serial Number
0x7405E

Issued: 10/22/2003
Expires: 10/21/2006

CRL

Revocation Reason
Not Revoked

Freshness
10 Hours, 13 Minutes, 17 Seconds

Contact

Email
christine.bowman@langley.af.mil

Send Whitepaper
Contact Me
Revoked Response

The Certificate for:

Matthew Arntt

has been Validated and is:

Revoked

Time to Validate: 0.43 seconds

Details

Certificate
Serial Number: 0x4983D
Issued: 7/10/2002
Expires: 7/10/2005

CRL
Revocation Reason: Unspecified
Freshness: 18 Hours, 38 Minutes, 55 Seconds

Contact
Email: matt_arntt@bra.com

© Copyright 2004 CoreStreet, Ltd.
Signed Email Checks Signer and CA
Web Server Certs Validated
Code Signing w/ Status Unknown
Operational Readiness

• **Performance**
  – Operational correctness, response time, data “freshness”

• **Availability**
  – 100% up time (improved SLA), successful upgrades, global users

• **Scalability**
  – 20 CAs, 12 million certs, > 1,000 rqst/sec/responder, ECA added

• **Security**
  – Secure against Intrusion, DoS, Replay attacks, in NIAP evaluation

• **Interoperability**
  – JITC certified, work with multiple CAs, clients, applications

• **Cost effectiveness**
  – Infrastructure cost savings versus traditional OCSP > 70%
• Questions about Today?
• Let’s Share the Vision!

rbowman@corestreet.com
Distributed OCSP, Mixed

RTC Authority

CRL

Local Deployment

Local Responder

(e.g. nightly at 2am)

Responders

OCSP Response

(C) Copyright 2004 CoreStreet, Ltd.
Distributed OCSP with Privileges

Certificate Authority

RTC Authority

Pre-signed OCSP Responses

Responders

OCSP Response

Certificate #1234:
- Is a Pilot
- Is not an Inspector

Signed: RTC Authority

TSA

James M. Loy

requires trust
(physical and data security)
Merging Physical and Logical Access

CA₁

LDAP

CA₂

VA

Location₁

Local Responder

Local Access Manager

Location₂

Local Responder

Local Access Manager

© Copyright 2004 CoreStreet, Ltd.
MiniCRL

How It Works

- VA sends a segmented and highly compressed (30X average) CRL to each responder.
- Responder sends individual segments to client.

Advantages

- Smallest bandwidth between VA and responders
- Small bandwidth between responder and clients
- No trusted responders required
- Scales to 100s of millions of users
- Computationally simple (no signing per transaction)
- Works with all issued certificates

Disadvantages

- Not yet adopted as an industry standard
- New client plug-in required

© Copyright 2004 CoreStreet, Ltd.