Certificate Revocation Checking in DoD PKI

Kevin Heald
DOD PKE Tech Lead
http://www.DoDPKE.com
(703)824-5365
Kevin_Heald@sra.com

DOD PKE OCSP Pilot

- Uses Corestreet and Akamai to provide a highly available and reliable OCSP solution
- Corestreet RTC Validation Authority pre-generates responses signed by a trusted key
- Responses are then pushed to Corestreet OCSP Responders on the Akamai network
- Responders then respond to user requests
- 25,000 User Pilot
- Limited amount of commercial client licenses
  - Developing in-house OCSP client for DOD use

Timeline

- Pilot was initiated in August 2003
- Pilot went live October 20, 2003
- Pilot set for 180 Day trial period
  - If the pilot is deemed successful (meets all success criteria) efforts will go into building an enterprise offering

Why?

- Recognized the need for more revocation checking options
  - Challenges of current solutions (CRLs)
  - The more options we can provide for revocation checking the better
- Needed to be up quickly
- Cost effective
- New DOD Net-Centric Focus
- Test out ASP hosted net-centric offerings
  - Akamai model

OCSP Pilot Benefits

- OCSP requires less bandwidth
  - 2-3k per OCSP request
- Akamai will automatically route requests to the closest responder
  - Provides for quicker responses
  - Prevents outages due to peering disputes
  - Allows for a more flexible solution
- No local OCSP responder required
  - Network-centric model (through Akamai)
  - Investigating the possibility of providing separate OCSP responders for special cases
- Costs to DOD Enterprise are significantly cheaper than traditional OCSP
  - Corestreet responders do not sign responses
  - Key storage and signing adds significant costs

OCSP Pilot Realities

- The OCSP Pilot will NOT solve for every revocation checking scenario
  - Example are environments that do not have reliable reach-back capability due to low-bandwidth
  - SIPRNET
- Akamai is not deployed on DOD networks
  - This will effect networks not connected to the Internet
  - Exploring the possibility of adding this capability to these networks
- DOD does not issue OCSP signing certificates
  - A self signed certificate is being used for the pilot
- IECA CRLs are not yet included in the pilot
  - Working on adding this capability
  - IECA CDPs should still work

Nonce

- NONCE realities
  - Larger deployments of PKI with millions of certificates need to rely on less frequent status updates.
  - Without Nonces, OCSP infrastructures can get current freshness of each response by utilizing the “thisUpdate” and “nextUpdate” response fields.
  - Validity duration of an OCSP response will match times for the CRL that was used to determine cert status, and freshness security will match CRL-based validation.
- Nonce based deployments have their place
  - High value transactions
  - Small PKI environments can deploy multiple responders that can receive very frequent updates of certificate status changes
  - Relying party decision
- Security also plays a key role in decision process for not using a Nonce-based infrastructure

Pilot Requirements

- Relying party application must have Internet connectivity
  - Akamai network is currently only on the Internet
  - Working on getting the Akamai network onto DOD networks
- OCSP capable application
  - For most Windows applications a third party client is required
  - A small number of OCSP clients are available for the pilot.
- Install the OCSP Pilot signing certificate
  - Self Signed certificate for the pilot
  - Available on DODPKE.com

What’s Next

- Look into Roll-out possibilities for Enterprise
- Bring Akamai into NIPR, SIPR, etc
- IECA inclusion
- DOD issued OCSP certs
- Make DOD CRLs available on Akamai network
  - LDAP
  - HTTP
  - HTTPS

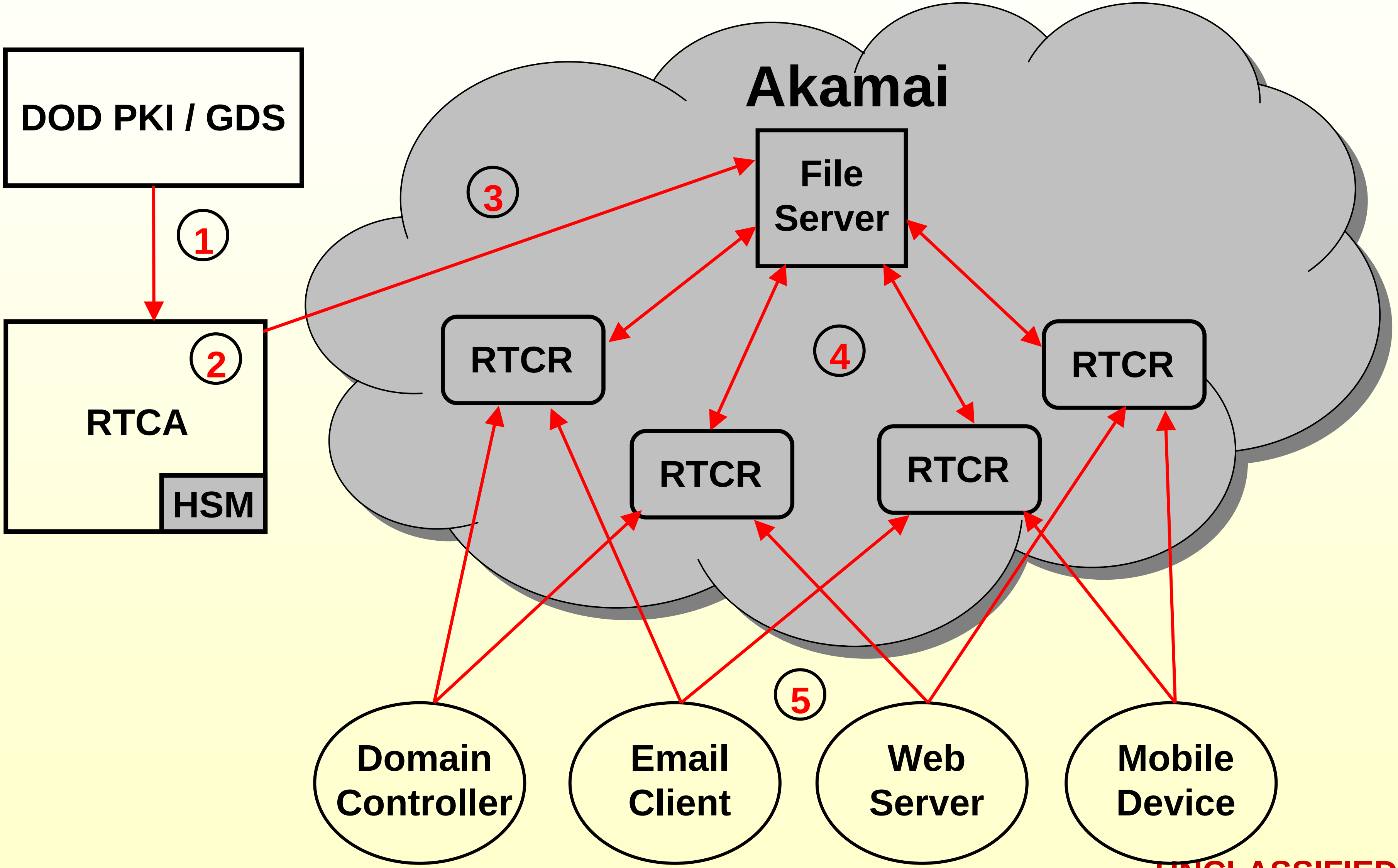
Revocation Checking Options in DOD

- Regular CRL checking
- Local CRL Caching Solution (updating as necessary)
- Locally deployed OCSP
- DOD PKE OCSP Pilot
- Continuing to look for new ways to provide revocation information for relying parties

Questions?

Backup Slides

OCSP Pilot Picture



Pilot Data and Facts

- Vendor/contractor makeup: CoreStreet, Akamai, Chrysalis, SRA
- Number of certificates available for validation: over 8.5 million
- Number of licensed users: 25,000 users
- Number of CAs being supported: 19
- Number of CRLs being supported: 19
- Size of largest CRL supported: over 5 MBytes
- Number of certificates issued by CA with largest CRL: over 1.5 million
- Number of Responders deployed: 20
- Number of Responder sites: 10

Pilot Data and Facts Cont’

- Number of certificate statuses per signature: 20
- Time to generate largest list of proofs (1.5 million certs): 15 minutes at 20 certs per signature
- Compressed size of largest proof list: 1 MBytes
- Time to upload the compressed proof list from Validation Authority (at SRA) to Akamai control server: 2 minutes
- Time to distribute compressed proof list from Akamai control server to each of the responders (do in parallel): 30 sec
- Time to uncompress and index largest proof list at the responder: 30 sec
- Size of uncompressed and indexed largest proof list at responder: 54 MBytes
- Size of response to relying party: 2.7kBytes at 20 certs per signature
- Measured average response time (from client to Akamai responder and back to client): 60 millisecond
- Tested capacity of responder: greater than 1,000 requests per second