GENERAL DYNAMICS
C4 Systems

Microsoft vs. Red Hat

A Comparison of PKI Vendors

Outline

- Definitions
- Issue #1: RedHat vs. Microsoft CA
- Issue #2: Cross Domain Flows
- Issue #3: Core PKI Domain
- Recommendation

Definitions

User or Enrollment Officer - The entity that requests an X509 v3 certificate. Both vendors provide URL access to the CA for the purposes requesting a certificate.

PKI Approving Agent - The entity that approves and issues the X509 v3 certificate. This entity is needed if auto enrollment is not used.

OCSP - Online Certificate Status Protocol is an application protocol used query the status of the validity of a certificate.

CRL - Certificate Revocation List is a product of the CA and is a signed list of serial numbers and revocation dates of all revoked certificates. Both CAs produce CRLs.

MiniCRL - Mini Certificate Revocation List is a CoreStreet proprietary condensed version of a CRL. Usually 200-400 byte in size. Handy in low bandwidth situations.

Air Gap - A method to transfer data from one domain to another not using network connectivity.

Issue #1: Microsoft vs. Red Hat

Microsoft provides a CA service with all of its family of servers: 2000, 2003 and 2008. This service is included free, has been in use since the introduction of Server 2000, and is widely used in industry and in government. TVE R2 is using a Microsoft CA in its ESS.

This has prompted an analysis of whether LCSS SR 3 TacPKI should switch from a RedHat CA to a Microsoft CA for compatibility.

The following slides detail the differences between token provisioning using both CAs.

Token Provisioning

Token provisioning is the process of

- Assigning a token to an end user
- Generating the public/private key pair
- Generating a certificate request
- Retrieving the certificate from the Authority
- Importing the certificate to the token device.

Red Hat Token Provisioning

End User or enrollment officer

- Logs onto a client machine in the PKI domain
- Opens a web browser and enters the URL for the CAs End-user certificate services
- Fills-in required information and submits a request for a user certificate

PKI Approving Agent

- Logs onto a client machine in the PKI domain
- Opens a web browser and enters the URL for the CA Agent services
- Locates and reviews/issues the certificate

End User or enrollment officer

- Logs back into the client machine and uses the same browser and URL then imports the Certificate into the browser.
- From the browser the certificate is located and exported to the desktop in PKCS# 12 format.
- Launches eToken PKI application and imports the certificate chain onto the eToken device. Device ready for the end user.

Microsoft Token Provisioning

User or enrollment officer

- Logs on to a client machine in the PKI domain
- From a browser connects to the MS CA via URL
- Submits a request for a certificate

PKI Approving Agent

- Logs into the CA and opens the Certification Authority Snap-in and reviews/approves the request (issues the cert).

User or enrollment officer

- Opens the browser and imports the certificate into the browser.
- The certificate is exported to the desktop in PKCS #12 format. Launches eToken PKI Client to import user certificate to eToken device.
- The eToken is ready to be used.

Microsoft Data Flows

- Microsoft CA publishes its CRLs and user certificates to Active Directory (AD)
- The TVA consumes the CRL and user certificates from the AD
- The TVA publishes OCSP response lists and miniCRLs
- The TVA can be configured as an OCSP responder
- The responders consume OCSP response lists and miniCRLs
- The Responders provide status responses to domain Desktop Validation Clients (DVC)
- All status requests and responses occur over Https connections

Pros & Cons of Microsoft CA with AD

Pros:

- Microsoft CA functionality is included with the Server 2000, 2003, 2008 OS
- There are many MS servers in the current architecture that could be a CA.
- MS CA uses Active Directory to store certs, CRLs and user info.
- No duplicate identity information user information
- MS CA can be configured to use other LDAP Directories
- ESS is using MS CA and AD for TVE attestation purposes
- No Red Hat products are necessary
- Currently supports CoreStreet PKI components
- Common MMC interface to MS CA is well know to system administrators
- AD exists in each domain currently.

Cons:

- MS CA administration required in all affected domains
- The additional purchase of eToken Token Management System (TMS) is suggested, but not critical. Used to manage token assignment, enrollment, and certificate import.

Pros & Cons of RedHat CA

Pros:

- Purchased, configured and installed in SOSPI for proof of concept demo
- Licenses exist to extend current architecture into the SBU domain
- No direct user contact with servers, functions are executed via URL network access

Cons:

- Administration is cumbersome and configuration is complex
- User information duplicated between AD and the LDAP directory server
- Red Hat Linux required for CA and Directory
- Is not compatible with eToken Token Management System

Issue #2: Cross Domain Flows

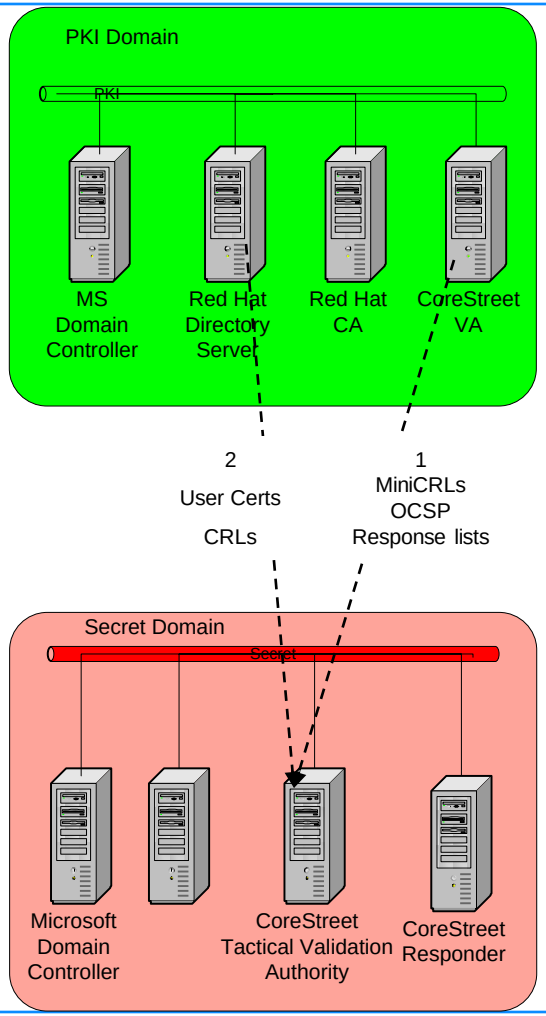
Currently in SOSPI there are no PKI directory servers in the Secret/SBU domains

Target architecture has PKI directory servers in the Secret/SBU domains

Current Cross Domain Activities

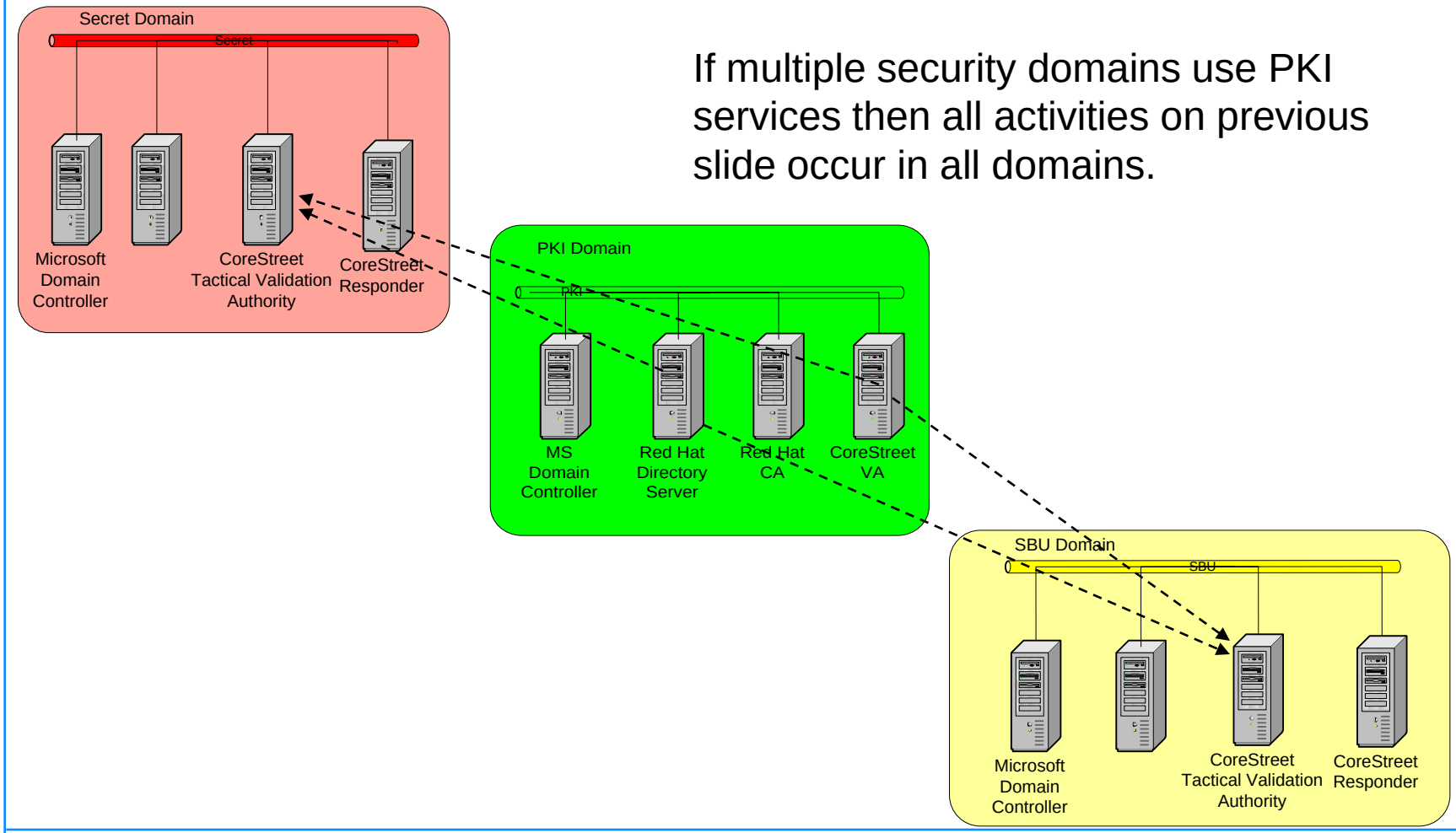
Core PKI High Level Activities include:

- Certificate Authority (CA) publishes user certificates and Certificate Revocation Lists (CRLs) to the directory
- Validation Authority (VA) consumes the user certificates and CRL and publishes MiniCRLs and OCSP response lists
- Transferring PKI data to the secret domain is performed via air gap. There are two different methods that accomplish this.
  1. Copy OCSP response lists and MiniCRLs from the VA to transfer media then copy OCSP responses and MiniCRL to the secret TVA
  2. Copy CRLs and user certs from the LDAP directory to the transfer media then copy CRLs and user certs to secret TVA to produce MiniCRL and OCSP Responses



GENERAL DYNAMICS
C4 Systems

Current Cross Domain Activities Cont.



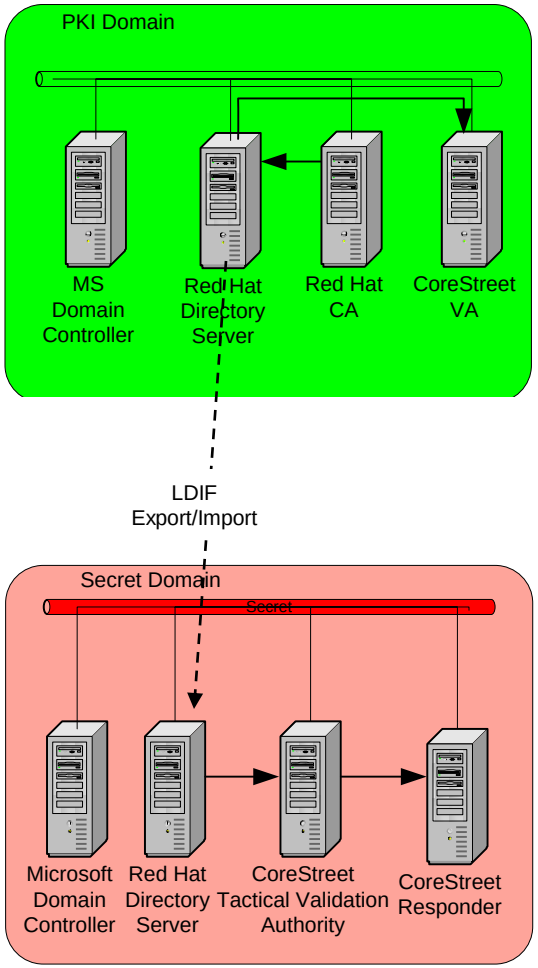
If multiple security domains use PKI services then all activities on previous slide occur in all domains.

GENERAL DYNAMICS
C4 Systems

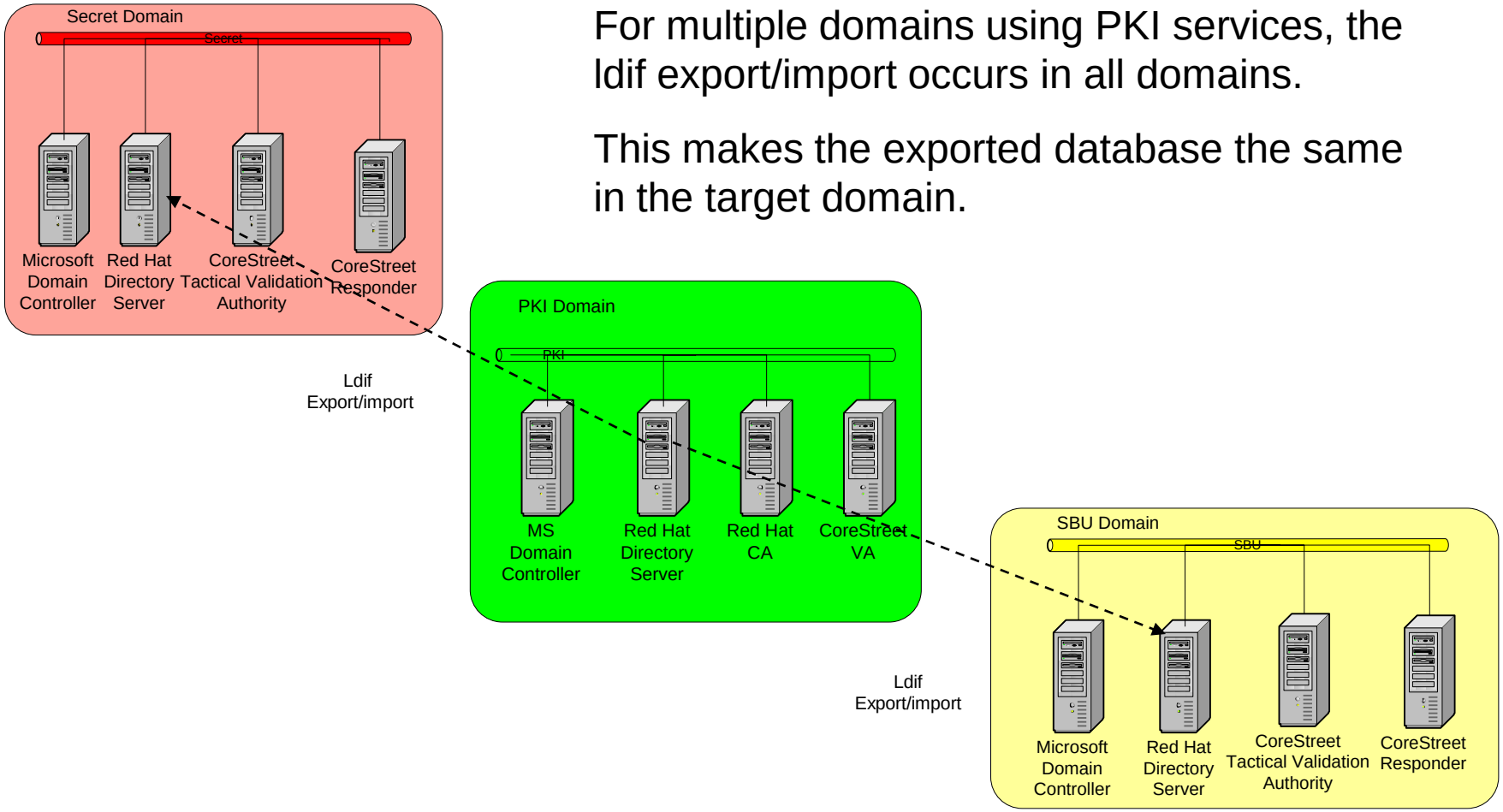
Directory Server in Secret Domain

Adding a Red Hat directory in the secret domain provides for data transfer of one file for air gap transfer to the Secret domain.

- An ldif export / import from the PKI to the secret directory server provides the TVA with a source of user certs and CRLs
- TVA consumes CRLs and user certs from the directory and publishes its own MiniCRL and OCSP response lists



Directory Server in Secret Domain Cont.



For multiple domains using PKI services, the ldif export/import occurs in all domains.

This makes the exported database the same in the target domain.

GENERAL DYNAMICS
C4 Systems

Benefits

Directories in the Secret/SBU domains provide the following benefits:

- Ease of use – importing individual certificates into the TVA is very time consuming
- Less data that needs to go cross domains

If we choose to go with a Microsoft CA, then a directory (AD) already exists in each domain

Issue #3: Core PKI Domain

Original purpose for PKI domain was to have certificates classified as “vanilla” so that they could then be exported into both Secret and SBU domains

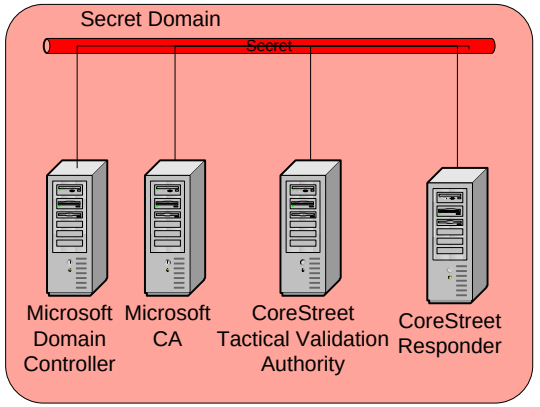
Because we are using certificates for signing emails, the certificates must be bound to an email address. Therefore, there is no way to make a domain agnostic certificate. The current architecture requires separate certificates for the Secret and SBU domains

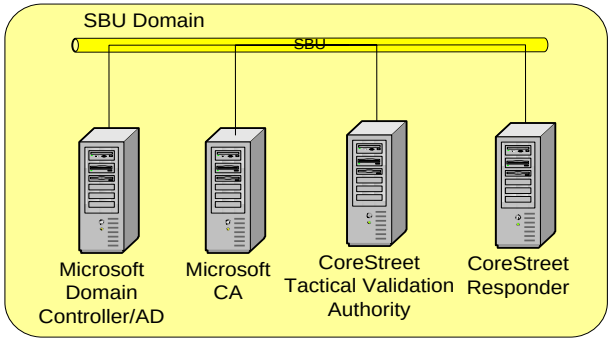
Question then arises whether we should remove the PKI domain and have a separate CA in both the Secret and SBU domains to manage domain specific certificates

Cross Domain Activities with Multiple CAs

TacPKI data flows between domains with respect to validating signatures is reduced with the introduction of a CA in each domain.

If signed message traffic crosses domains and signature validation is required, then there will be a need for a CDS.





GENERAL DYNAMICS
C4 Systems

Token Provisioning without PKI domain

Token provisioning using PKCS #12 is the method used for SoSPI. The CA is not connected to a reachable network.

The addition of a tactical CA in a security domain allows for a cleaner provisioning process than using PKCS#12 files.

Token Management System is an application server/client package from eToken that is a management tool covering full token life cycle.

eToken TMS

The Token Management System (TMS) manages the eToken throughout the entire lifecycle from Assignment thru EOL

Benefits:

- Integrates with Microsoft CA
- Can be configured for end user self enrollment
- Need one license for each PKI domain
- Loads the certificate directly to the token
- User certificate renewal
- Public/Private key pair generated on the token

Issue Consolidation & Recommendation

Due to these issues, the recommendation is to do the following:

- Switch to a Microsoft CA and use AD for directory services
- Get rid of the PKI domain and have a CA/AD in each domain requiring certificate services
  - There is already a Microsoft Server (where Certificate Services could be turned on) and AD in each domain
- Use the eToken TMS to manage certificates