



Military Traffic Management Command (MTMC)

Transition to Digital Certificates

Paula Mihalek

DSN: 328-3222

Coml: 703-428-3222

manager@eta.mtmc.army.mil



Background

-
- DOD Public Key Infrastructure (PKI) Initiative began in '99
 - PKI is that portion of the security management infrastructure dedicated to the management of keys and certificates used by public key-based security services
 - PKI Implementation
 - DoD Oct 03
 - Army/ETA after FY02
-



Why PKI?

-
- Provides a tighter security environment for the DoD systems
 - Becoming an industry standard
-



What is a digital certificate?

- The digital equivalent of an ID card used in conjunction with a public key encryption system.
 - Certificates are issued by Certificate Authorities (CAs) who can vouch for the individual or organization's identity and ownership of the public key
 - Certificates usually use the X.509 file format
-



What does the certificate contain?



- Data Elements in an X.509 Certificate
 - Version number (certificate format)
 - Serial number (unique value from CA)
 - Algorithm ID (signing algorithm used)
 - Issuer (name of CA)
 - Period of validity (from and to)
 - Subject (user's name)
 - Public key (user's public key & name of algorithm)
 - Digital signature (created with CA's private key)
 - The DOD issued CACs contain additional personal information
-



DOD PKI Components

- Digital certificate authentication required for network, email, and web applications
 - Common Access Cards (CAC) issued to Military/Government personnel containing identity, email and encryption certificates
 - MTMC business partners required to purchase certificates from External Certificate Authorities (ECAs)
 - Certificate Revocation List (CRL) used to identify certificates that have been lost or revoked. This list is updated continuously and widely disseminated to prevent access to DOD systems by unauthorized individuals
-



Digital Certificate Usage with Email



-
- Email will be secured with the DOD PKI initiative through encryption and digital signatures. These components provide confidentiality, integrity, non-repudiation, and authentication.
 - Encryption – translation of data into a secret code
 - Digital Signing - A digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Although the DOD policy has not been finalized, it is expected that digital signing will be required for business correspondence with DOD
-



Implementation for Commercial Partners

- Commercial Partners required to purchase a digital certificate through an External Certificate Authority (ECA) for every employee accessing a DOD application
 - The identity certification process varies depending on the CA and level of certification. Drivers licenses, notarization and fingerprints are examples of documentation to establish identity
 - Must purchase the “identity” and “email” certificate set as a minimum for each user
 - Both “hard” and “soft” certificates are available from ECA vendors
 - “Hard” certificates are stored on a smart card
 - “Soft” certificates are stored on the computer
 - Cost varies - per certificate per year (some CAs offer volume discounts and/or renewal discounts)
 - DOD considers certificate cost a “cost of doing business”
 - The ECA should be notified when an individual loses their certificate or leaves the company so that the certificate can be put on the CRL
-



MTMC-specific Implementation

- Each person accessing a MTMC application through the Electronic Transportation Acquisition (ETA) shall have only one certificate
 - Multi-user scenario:
 - Problem: User currently has multiple user ids to represent multiple organizations or roles
 - Solution: User will have ONE ETA account. ETA will present that user with the organizations/roles that are within their purview and they will choose one to represent for that ETA session
 - Foreign Nationals – infrastructure currently being established to verify identity for certificate distribution
-



Registering Certificates in ETA



- Certificate must be registered with ETA to link certificate serial number with ETA user id
 - Step-by-step process
 - User id and password required for initial certificate registration
- When accessing an ETA application, user will be prompted for certificate.*
- “Identity” certificate should be used for access
- ETA will verify identity and forward user to the application

***(Note: When using the certificate, the user will be prompted for a Personal Identification Number (PIN) by the middleware software on their computer. The PIN is not shared with ETA and should not be confused with a user id/password combination.)**



PKI Web Site



<http://iase.disa.mil/>

<https://eta.mtmc.gov> or <https://eta.mtmc.army.mil>

<http://eca.orc.com/>

<http://www.digsigtrust.com/federal/dod.html>

<http://www.verisign.com/enterprise/government/ieca-dod.html>

Paula Mihalek

DSN: 328-3222

Coml: 703-428-3222

manager@eta.mtmc.army.mil
