
Mitretek's PKI Efforts

Federal PKI Steering Committee Meeting Healthcare Working Group

28 March 2001

Mitretek Background

- ☐ Mitretek is a non-profit technology company located in McLean, VA.
- ☐ Mitretek was created by the MITRE corporation in 1995 to house MITRE'S non-FFRDC projects
- ☐ Approximately five hundred professional are currently working on project for most federal departments and agencies
- ☐ Mitretek business practices:
 - Does not compete for projects
 - Usually works for non-profit organizations
 - Has few alliances or partnerships with commercial firms
 - Avoids conflict-of-interest situations

Briefing Contents

- ☐ Mitretek's GSA PKI Efforts
- ☐ Other Federal Non-DHHS Efforts
- ☐ DHHS Activities
- ☐ Activities in the Private Healthcare Sector

GSA – Access Certificates for Electronic Services (ACES)

- ☐ Purpose: To facilitate and secure electronic transactions between eligible agencies and the public using digital signature technologies
- ☐ Means: Multiple Award Schedule contracts for federal agencies
- ☐ Mitretek Roles:
 - Program Design Support
 - Acquisition Support
 - Implementation Support
- ☐ Current Status
 - Contracts awarded
 - Implementation Phase completed
 - Services available to eligible agencies

GSA – Certificate Arbitrator Module (CAM)

- ☐ Purpose: To facilitate interoperability among eligible agencies or applications and multiple CAs who issue digital signature certificates
- ☐ Means: Design, develop, and support a prototype software tool called Certificate Arbitrator Module (CAM)
- ☐ Mitretek Roles:
 - System Design
 - System Development
 - Deployment Support
 - Open Source Management
- ☐ Current Status
 - CAM Services available to eligible agencies
 - Open Source Licensing Agreement in place

GSA – Federal Bridge Certification Authority (FBCA)

- ☐ Purpose: To acquire, implement, and operate an FBCA to enhance interoperability among Federal CAs
- ☐ Means: Design, acquire, implement, operate, and evaluate an FBCA
- ☐ Mitretek Roles:
 - Design Support
 - Acquisition Support
 - Operations Support
- ☐ Current Status
 - Prototype completed
 - EMA Challenge completed
 - Production FBCA nearing completion

Other Federal Non-DHHS PKI Efforts

- 📁 DOJ (JMD, Tax Division, EOUSA, IRS, SSA)
 - PKI prototype project support
- 📁 USPS
 - PKI research and engineering support
- 📁 DoD
 - Class 3 PKI support
- 📁 SEC
 - PKI deployment support
- 📁 NSA
 - Smart Card Protection Profile Evaluation
- 📁 DISA
 - PKI engineering support
- 📁 NOAA
 - PKI engineering support

DHHS PKI Efforts

GCPR Security/PKI Support

- ☐ PKI design for sharing patient information
- ☐ Security policy to support the model
- ☐ Strategy for deploying PKI
- ☐ Consulting support to the GCPR Teams

DHHS PKI Efforts

IHS PKI/Security Support

☐ First stages of a PKI prototype

- Issue Certificates for a small test group
- Test using existing applications (e.g. S/MIME)

☐ Assessment of tokens

- Determine the best options to support strong authentication of users in a mixed environment

The HealthKey Project

Objective	To explore approaches to securing electronic healthcare transactions
Funding	\$2M grant from the Robert Wood Johnson Foundation
Participants	Five states: North Carolina, Massachusetts, Minnesota, Utah, Washington
Results	<ul style="list-style-type: none">☐ Pilot projects to test different security techniques☐ The HealthKey Roadmap – a guide that lays out the major activities that need to occur for widespread secure movement of electronic transactions
Mitretek Role	<ul style="list-style-type: none">☐ Supplying bridge technology to those pilot projects that need this capability