



BALTIMORE

www.baltimore.com



BALTIMORE[™]
www.baltimore.com

Baltimore's Participation in the DoD BCA Phase II Demonstration

August 2, 2001

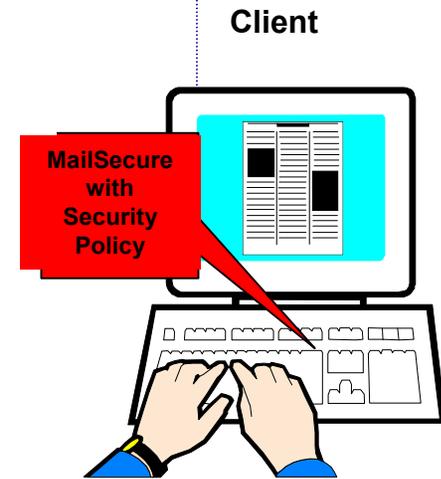
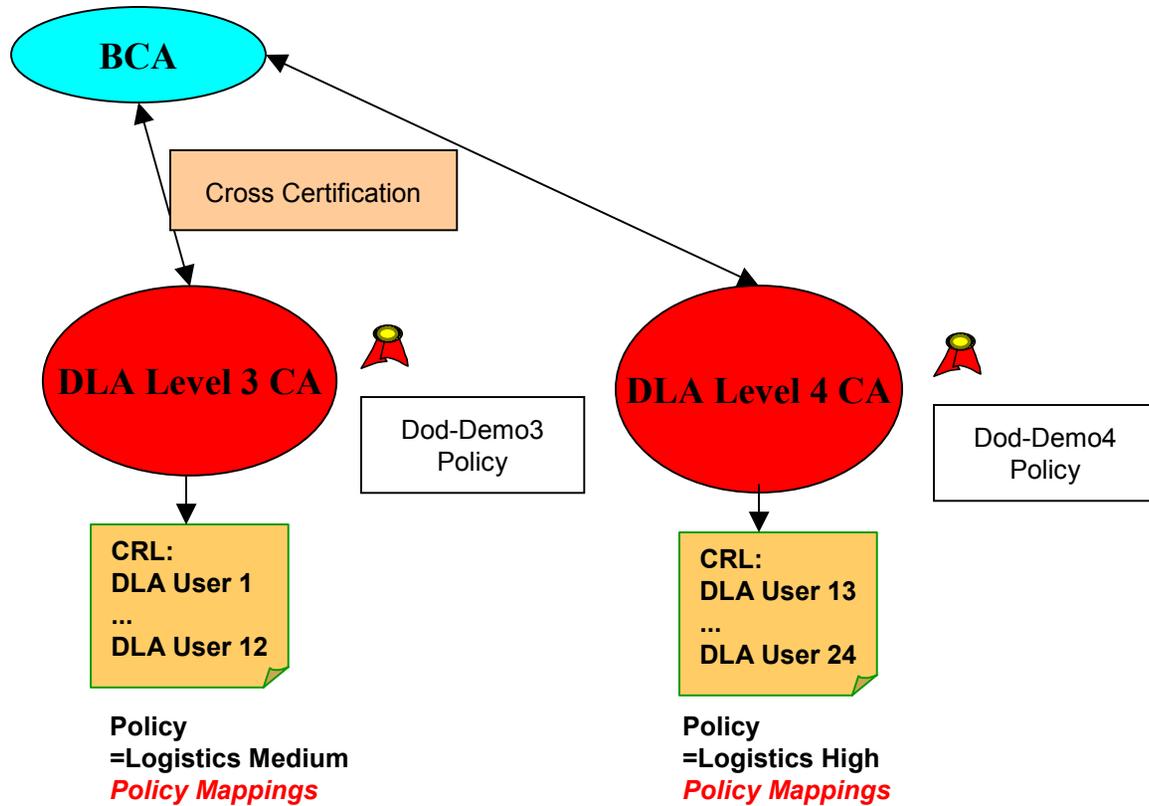
www.baltimore.com the global leader in e|security

CONFIGURATION



- Baltimore's UniCERT PKI product used to create 2 DLA CAs
- DLA CAs individually cross-certified with the Bridge CA
- Cross-certification included policy mapping using multiple OIDs
- CRLs provided for certificate validation
- End User Certificates issued under DLA Subtree
- End User Certificates used to exchange email messages and connect to access-controlled web server
- Used Baltimore's Client S/MIME Email Software, MailSecure, for secure messaging

Baltimore Configuration



*MailSecure Enhanced
to Provide All
Functional
Requirements*

MAILSECURE (Standard)



- Client Side of Baltimore's Suite of E-mail Security Applications
- Plug-in application to standard mail clients
- Provides full set of security functions using PKI standards
- Provides central administration - Security Policy defines security settings
- Includes verification of X.509 certificate paths containing certificates signed using RSA/MD5, RSA/SHA-1 and DSS crypto-algorithms

BCA Version of MAILSECURE



The following enhancements added to BCA version of MailSecure:

- Compliance with Technical Interoperability Profile (TIP)
- Integration with Certificate Path Development Library, capable of developing certificate paths from generated, non-hierarchical trust graphs
- Verification of X.509 certificate paths containing cross certificates

MAILSECURE Enhancements (Cont.)



- Verification of certificate path policies in accordance with ISO/ITU recommendations X.509
- Includes User Acceptable Policy List - New User Interface that checks policy OIDs in the certificate viewer
- User Configurable Enable/Disable processing of policy mapping
- User Configurable Enable/Disable processing of name constraints

BCA MAILSECURE Performance



Performance slow-down occurs during certificate path processing

To optimize certificate path processing:

- Add credential caching
- Reduce number of times Directory Server is accessed.

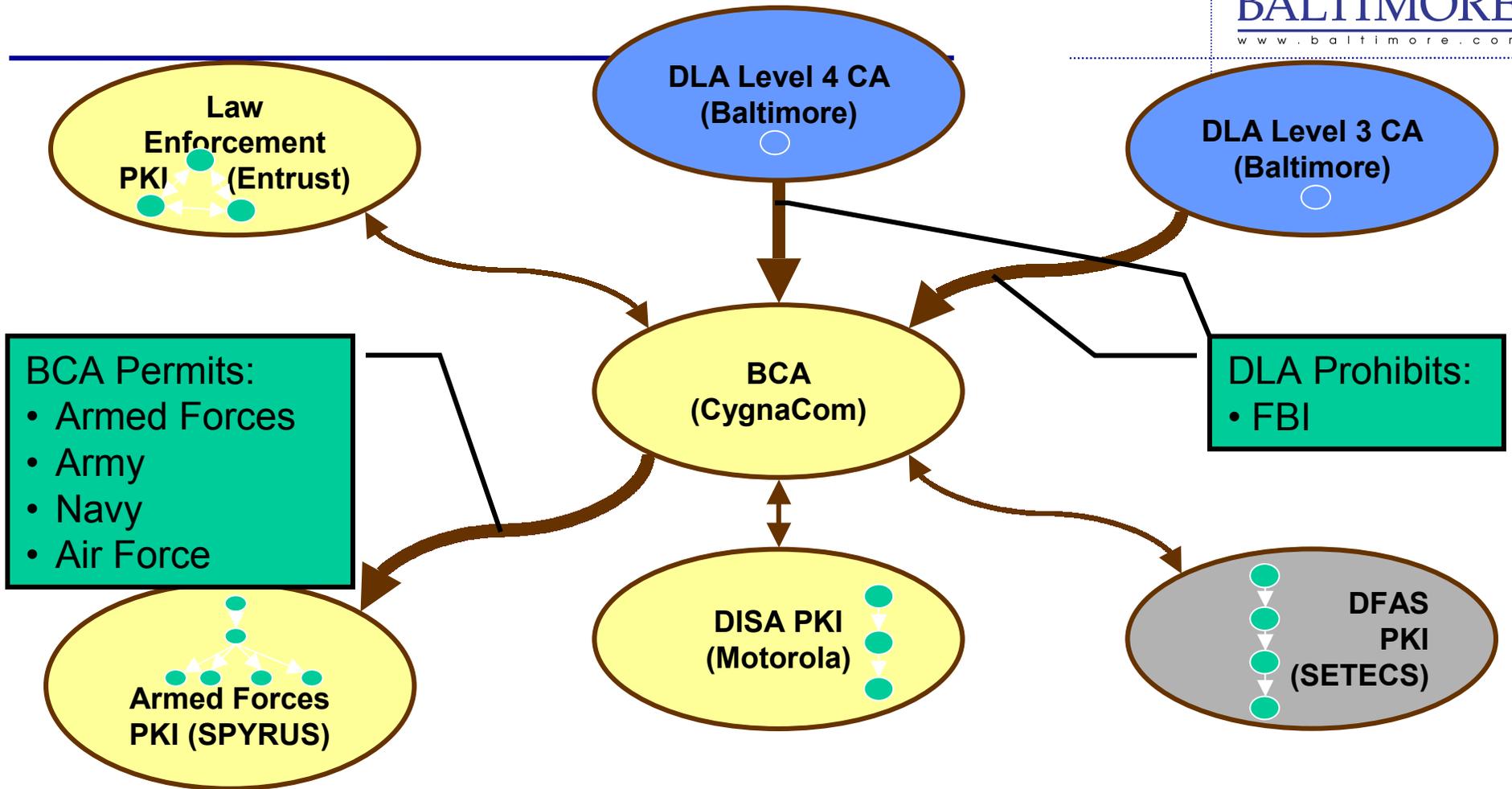
There have been several integration difficulties between CPDL and MailSecure.

- CPDL only uses DN to identify trust points, not always a unique identifier
- CPDL has “C” API and can be integrated into mail clients but not optimal for C++ projects and Object Oriented Design

NAME CONSTRAINTS



BALTIMORE™
www.baltimore.com



DLA CA's Certificate Configured to Include Name Constraints Extension Preventing Communication With FBI Issued Certificates

DEMONSTRATION



Baltimore, using its own secure email client, MailSecure, successfully:

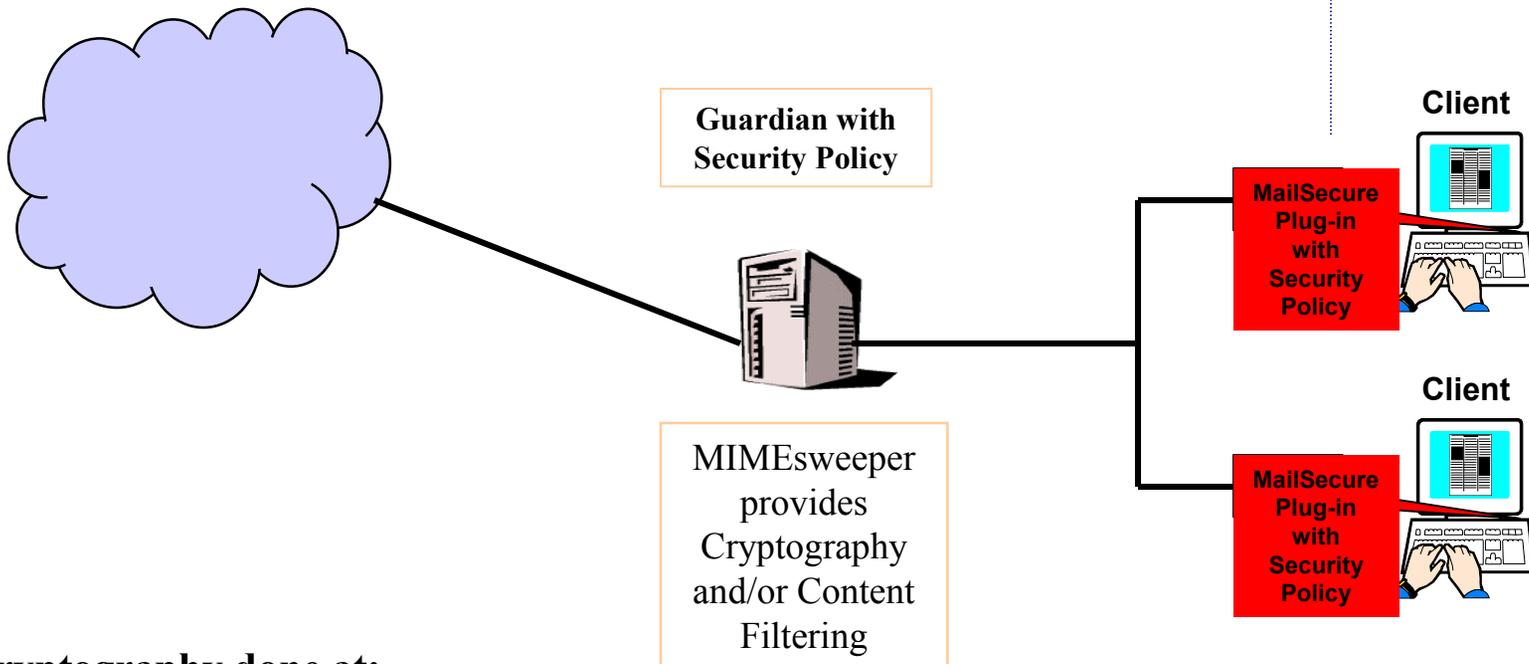
- Received encrypted and signed email from both SPYRUS and Entrust end users
- Decrypted received email from both SPYRUS and Entrust end users
- Denied receipt of email sent by the FBI issued certificate displaying “Name Constraints Error”

MAILSECURE Roadmap



- MailSecure integrated with content filtering (MIMEsweeper)
- Long term modification is expected to include credential caching integrated into Baltimore toolkits
- Also, Certificate Path Validation is expected to be integrated into Baltimore toolkits

MailSecure and MIMESweeper



Cryptography done at:

- **Client with MailSecure**
- **Server with MIMESweeper**
- **Both Client and Server - message is also sent to Guardian where it is processed**

LESSONS LEARNED



Participating in this effort, working with different PKI architectures has caused Baltimore to make changes to core application programs.

- UniCERT now allows policy mapping in cross certificates even if policies being mapped are not in certificate policy extension
- UniCERT now allows policy mapping with multiple certificate policies

DBCA SUMMARY



This has been a very rewarding experience for Baltimore Technologies and we look forward to the continued support of this effort.

We are honored to have participated in this collaborative effort proving interoperability among leading PKI systems.

www.baltimore.com