Bridge Certification Authority
Interoperability Test Suite (BITS)

23 January 2002

John.Pawling@GetronicsGov.com
Overview

- Requirements
- Objectives
- BITS Test Data and Documents
- Freeware BITS Test Data Generation Tool
- BITS Technical Support
Managing BCA Interoperability

- BCA Establishes Trust Paths Between PKIs
- Organizations Need to Retain Security Control
  - Limit / Prevent Transitive Trust
  - Maintain Level of Assurance
- X.509 Provides Tools to Meet These Needs
  - Name Constraints
  - Certificate Policies
  - Certificate Policy Mapping
Name Constraints

- Standard Extension to X.509 Certificates
- CA Certificates Can Include Name Constraints
  - Regulate Certificates Accepted Through Path
  - Can Specify Permitted or Excluded Names
- Names constraints checks performed by relying party certification path validation software

CA1

- Permitted: Army
- Excluded: DLA

This Relying Party Will
- Accept the Army Cert
- Reject the DLA Cert
Certificate Policies

- Standard Extension to X.509 Certificates
- Each certificate asserts one or more certificate policies
- Certificate policies identify assurance level of certificate (ex: high, medium, low)
- Certificate policies identify acceptable uses of certificate (ex: DOD Class 4 for classified processing)
- Certificate policy mapping guides relying parties in determining acceptability of “foreign” certificates
BCA Demo Phase II Architecture

Demo BCA [Cygnacom]

- Demo CA [Baltimore]
- Demo Top CA and Hierarchy [SETECS] (Not used)
- Demo CAs [Spyrus]

- Demo Root CA [Motorola]
- Demo Intermed CA [Spyrus]

- Demo CA [Motorola]

Mesh Infrastructure [Entrust]

CA

- Outlook MailSecure (CPDL)

Outlook (Entrust Express)

S/MIME V3

Eudora (CPDL, CML, SFL, ACL, SPYRUS Card)

Attribute Authority (Cygnacom)

Chained Directory System
BCA Demo Phase II Standards

- ITU 2000 X.509 Recommendation
- RFC 2459 X.509 PKI Certificate & CRL Profile
- S/MIME v3 Secure Messaging (RFCs 2630, 2632, 2633)
- RFC 822 SMTP Messaging
- RFC 2045 MIME
- RFC 2253 LDAP v3 for Client - Directory Interface
- RSA/MD5 or DSA/SHA-1 for Signatures
Phase II BCA Interoperability Demonstration Final Report describes BCA concepts, PKI architecture, cross-certification relationships, test cases, and test results for demo.

Final Report appendix contains complete set of matrices illustrating results of interoperability testing conducted as part of demo effort.

Final Report available from these web sites:

<http://www.anassoc.com/BCA.html>
<http://bcatest.atl.getronicsgov.com/>
A primary BCA Demo objective is to encourage vendors to provide commercial products that include capabilities required for BCA environment such as:

- Building cert paths in cross-certified PKIs
- Name Constraints
- Certificate Policies
- Certificate Policy Mapping
Commercialization Strategy

- DOD is providing freeware security libraries and test support at no cost to vendor to reduce investment required to enhance/test products to provide capabilities required for BCA environment.

- Under DOD contract, Getronics is providing security services freeware, documentation & technical support at no cost to vendor.

- Under DOD contract, Getronics is providing BITS test data, documentation, facilities & technical support at no cost to vendor.

- Under DOD contract, Cygnacom is providing freeware Certification Path Development Library.
BITS Objectives

BITS includes standard set of tests cases, procedures, data that can be used to determine a product’s degree of interoperability with BCA Demo Phase II architecture including:

- developing certification paths in cross-certified PKI environment;
- validating certification paths;
- implementing S/MIME in an interoperable way

Includes certs & CRLs equivalent to those created by various products for BCA Demo Phase II

Includes test cases and procedures that exercise features tested in BCA Demo Phase II (except for access control and border directory concept)
BITS Objectives (cont’d)

- Includes certification paths that product should be able to successfully validate
- Includes certification paths that product should reject or, in some cases, prompt user before proceeding
- Initial goal is to support testing of S/MIME applications, but BITS certification path test data can be used to test any PKI-enabled application

**BCA Interoperability Test Description** documents test cases, procedures, data

- Includes subset of test cases documented in **Phase II BCA Interoperability Demo Final Report**
BITS Test Cases

 BITS includes test cases that exercise majority of RFC 2459 cert path validation reqts

 BITS does not include complete set of failure test cases for all RFC 2459 cert path validation reqts

 BITS includes test cases focused on:

- name constraints (both permitted and excluded)
- certificate policies
- certificate policy mapping
- certificate revocation using CRLs
- cross certification
- CRL distribution points
- multiple signature algorithms (RSA, DSA) within a path
NIST Test Certification Paths

NIST provides a standard test suite of X.509 certification paths at:
<http://csrc.nist.gov/pki/testing/x509paths.html>

NIST data includes extensive positive & negative test cases for testing these RFC 2459 reqts:

- name chaining
- signature verification
- validity date checking
- basic constraints extension
- key usage extension
Combined NIST & BITS Testing

- Applications should first be tested using NIST test suite to verify basic certification path validation capabilities.

- Applications that are unable to successfully complete NIST cert path tests will not be interoperable with BCA architecture.

- Applications should then be tested using BITS.

- Combination of both sets of test data can be used to perform a comprehensive evaluation of an application’s degree of BCA interoperability.
Certification Path Validation Test Scenarios

- Valid
- Revoked user cert
- Revoked CA cert
- Violates name constraints
- Unacceptable due to lack of acceptable chain of policy mappings
- Process cert path with policy mapping disabled (ex: fail due to unmapped cert policy)
- Process cert path with policy mapping enabled (ex: succeed due to mapped cert policy)
Each cert path validation test case specifies these inputs to cert path processing software:

- Trusted certificate to use (a.k.a. trust anchor)
- Initial-policy-set (one or more Object Identifiers, each representing a certificate policy)
- Initial-explicit-policy indicator value
- Initial-policy-mapping-inhibit indicator value
- Initial-inhibit-policy indicator value
BITs PKI Architecture

Army, Navy, Air Force, rogue DLA

Cross Certification

Justice, FBI, Coast Guard

Figure Key
- End Users
- CA
- Root CA
- Cross Certification
BCA Permits:
- Armed Forces
- Army
- Navy
- Air Force

DLA Prohibits:
- FBI
High Assurance Policies

- DOD Class 4
- BCA High
- Logistics High
- Law Enf. High

Medium Assurance Policies

- Logistics Medium
- BCA Medium
- DOD Class 3
- DISA Policy

**Notation:** B accepts A as equivalent
Example Policy Mapping Flows

- All Mappings “Pass Through” BCA Policies
- DISA User to FBI User:
  - DISA Policy = BCA Medium
  - FBI User accepts DISA Policy as equivalent to Law Enf. Medium through mappings
- DLA4 User to Army User:
  - Logistics High = BCA High
  - Army User accepts Logistics High as equivalent to DOD Class 4 through mappings
BITS Secure Messaging Test Scenarios

- Simulate exchange of signed-only, encrypted-only, signed&encrypted messages between users in different PKIs

- Signed S/MIME messages are provided that require product to validate signer’s cert path

- Test cases specify creation of encrypted S/MIME messages that require product to validate recipient’s cert path

- Encrypted S/MIME messages are provided that can be decrypted using private key provided via PKCS #12 file
Example Cert Path Processing - Send

Sending Application Validates Certification Path

Recipient Encryption Certificate Validated, Message Encrypted

Navy User Signs Message, Retrieves and Validates DLA User Encryption Certificate
Example Cert Path Processing - Receive

Receiving Application Validates Certificate Path

Relying Party’s Trusted CA

DLA 3 CA

CRL: DLA User 20 DLA User 22

DLA User 23

Receiving Application Builds Certificate Path

Armed Forces Root

CRL: AF CA

Army CA

Navy CA

CRL: Navy User 2 Navy User 4

Navy User 5

Navy User
Transmits Encrypted Message
to DLA User

Original Message
(Decrypted, Sig Verified)

DLA User Decrypts Message,
Validates Navy User Signature Cert,
Verifies Message Signature,
and Displays Message

Getronics Government Solutions
1/22/02 BITS Status

- **BCA Interoperability Test Description** document completed and available from BITS web site.
- BITS test data generation & testing tools complete.
- BITS certs, crossCertificatePairs, CRLs generated.
- Majority of verification testing using CML complete, but still resolving errors in test data.
- Now generating & testing: S/MIME msgs, PKCS #12 files.
- We will send e-mail to FPKI TWG mail list when fully tested data and freeware tools are available.
- Getronics goal is to complete testing by 1/31/02.
All BITS certs, crossCertificatePairs, CRLs are available in LDAP directory (data still under test)

Single LDAP directory includes directory information tree equivalent to that hosted on 6 directory servers for BCA Demo Phase II

Applications can use LDAP to access directory to test their ability to retrieve data required to build cert paths composed of certs from multiple PKIs

LDAP directory is accessible from Internet using: <ldap://bcatest.atl.getronicsgov.com/>

IP address of LDAP server is 199.79.206.5

LDAP server runs default port of 389
BITS "U.S. DoD BCA Technology Demonstration" web site is accessible from Internet using:
<http://bcatest.atl.getronicsgov.com/>

BITS web site provides:
- Zip file containing all test data (certs, CRLs, S/MIME messages, PKCS #12 files); (available soon)
- Instructions for accessing BITS LDAP directory;
- BCA Interoperability Test Description document;
- BCA Demo docs: Briefing, Report, Technical Interop Profile, Cert/CRL Profiles, Directory Profile
- Links to other related web sites
- BITS Freeware Test Utilities (available soon)
- Links to other freeware
Under DOD contract, Getronics will assist vendors with executing BITS tests, answering technical questions, and providing troubleshooting hints

Contact:

John.Pawling@GetronicsGov.com

Richard.Nicholas@GetronicsGov.com
BITTS Freeware Utilities

- **BCA Interoperability Test Description** documents test cases, procedures, data
- Getronics developed freeware test utility to parse Test Description document to automatically generate all test data and post to LDAP directory
- Getronics also developed freeware test utility to use Certificate Management Library to automate validation tests of generated data
- Under DOD contract, Getronics is providing source code for both utilities at no cost to vendors
- Data generation and testing can be easily reproduced or changed by Getronics or third party
Getronics Security Services Libraries

Certificate Management Library (CML)
- Builds and validates X.509 certification paths & CRLs
- Provides local cert/CRL storage functions
- Provides remote directory retrieval via LDAP

S/MIME Freeware Library (SFL)
- Implements IETF S/MIME v3 security protocol
- Security label, signed receipts, mail list support

Access Control Library (ACL)
- Provides Rule Based Access Control using security labels & authorizations as per SDN.801
- Implements Attribute and X.509 Certificates
- Meets DMS, Bridge CA, Canadian MMHS Reqs

Enhanced SNACC
- Implements Abstract Syntax Notation.1 (ASN.1) Distinguished Encoding Rules (DER)
S/MIME Freeware Library

Certificate Management Library

Application (email, web browser/server, electronic forms, etc)

Access Control Library

Crypto Token Interface Libraries

Enhanced SNACC ASN.1 C++ Library

Microsoft CAPI, PKCS #11, Crypto++, Fortezza, Spyrus SPEX/, RSA BSAFE
Gettronics Freeware Availability

- S/MIME Freeware Library
  <http://www.gettronicsgov.com/hot/sfl_home.htm>

- Certificate Management Library
  <http://www.gettronicsgov.com/hot/cml_home.htm>

- Access Control Library
  <http://www.gettronicsgov.com/hot/acl_home.htm>

- Enhanced SNACC – ASN.1 Toolkit supports DER.
  <http://www.gettronicsgov.com/hot/snacc_home.htm>

For all Gettronics freeware libraries, unencumbered source code is freely available to all. Gettronics freeware can be used without paying any royalties or licensing fees. There is a public license associated with each freeware library.
BCA CML/SFL/ACL Success

- BCA Demo Phase II tested cross-certified Entrust, General Dynamics, Baltimore & SPYRUS PKIs
- CML/CPDL successfully used to build & validate certification paths between these PKIs
- CygnaCom integrated SFL/CML/ACL/CPDL into plug-in for Eudora Pro mail client
- Interop testing successful with Baltimore MailSecure & Entrust S/MIME toolkit
- CygnaCom used ACL in Attribute Authority
- CygnaCom used ACL & CML in trusted web server
NIST and Getronics are developing open source S/MIME v3 auto responder using SFL, CML, Enhanced SNACC, CTILs.

NIST plans to host auto responder on NIST website <http://csrc.ncsl.nist.gov/pki/smime/>

Vendors can use facility to determine if products comply with S/MIME v3 specs & NIST profile.

Auto responder processes S/MIME messages sent by tester & provides success/failure feedback.

Auto responder creates signed and/or encrypted S/MIME messages for processing by tester.
Point of Contact

John Pawling
John.Pawling@GetronicsGov.com
Getronics Government Solutions, LLC
141 National Business Pkwy, Suite 210
Annapolis Junction, MD 20701
(301) 939-2739 or (410) 880-6095