BAE SYSTEMS

Security Services Freeware Library

8 April 2005

BAE SYSTEMS

Security Services Freeware Libraries

BAE SYSTEMS

BAE Systems Security Services Objectives

- Provide freeware reference implementations of:
  - X.509 v3 certification path building and verification
  - Rule Based Access Control
  - IETF S/MIME v3 security protocol
  - Abstract Syntax Notation.1 (ASN.1) encoding and decoding (Distinguished Encoding Rules (DER), Basic Encoding Rules (BER), and Packed Encoding Rules (PER))
- Provide unencumbered source code for libraries
- Provide modular, high-level, portable interface:
  - Minimizes effort required by application developers to meet security requirements
  - Allows developers to use only the libraries required for their particular application

BAE SYSTEMS

BAE Systems Security Services Libraries

- Certificate Management Library (CML)
  - Builds and validations X.509 certification paths and certificate revocation lists (CRLs)
  - Provides local cert/CRL storage functions
  - Provides remote directory retrieval via Lightweight Directory Access Protocol (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 and authorizations as per SDN.801
  - Uses X.509 Public Key Certificates and Attribute Certificates
  - Meets Defense Message System (DMS), DoD Bridge Certification Authority Demo, Canadian MMHS Requirements
- Enhanced SNACC (eSNACC) Abstract Syntax Notation.1 (ASN.1)
  - Performs Encoding and Decoding using Distinguished Encoding Rules (DER) and Packed Encoding Rules (PER)

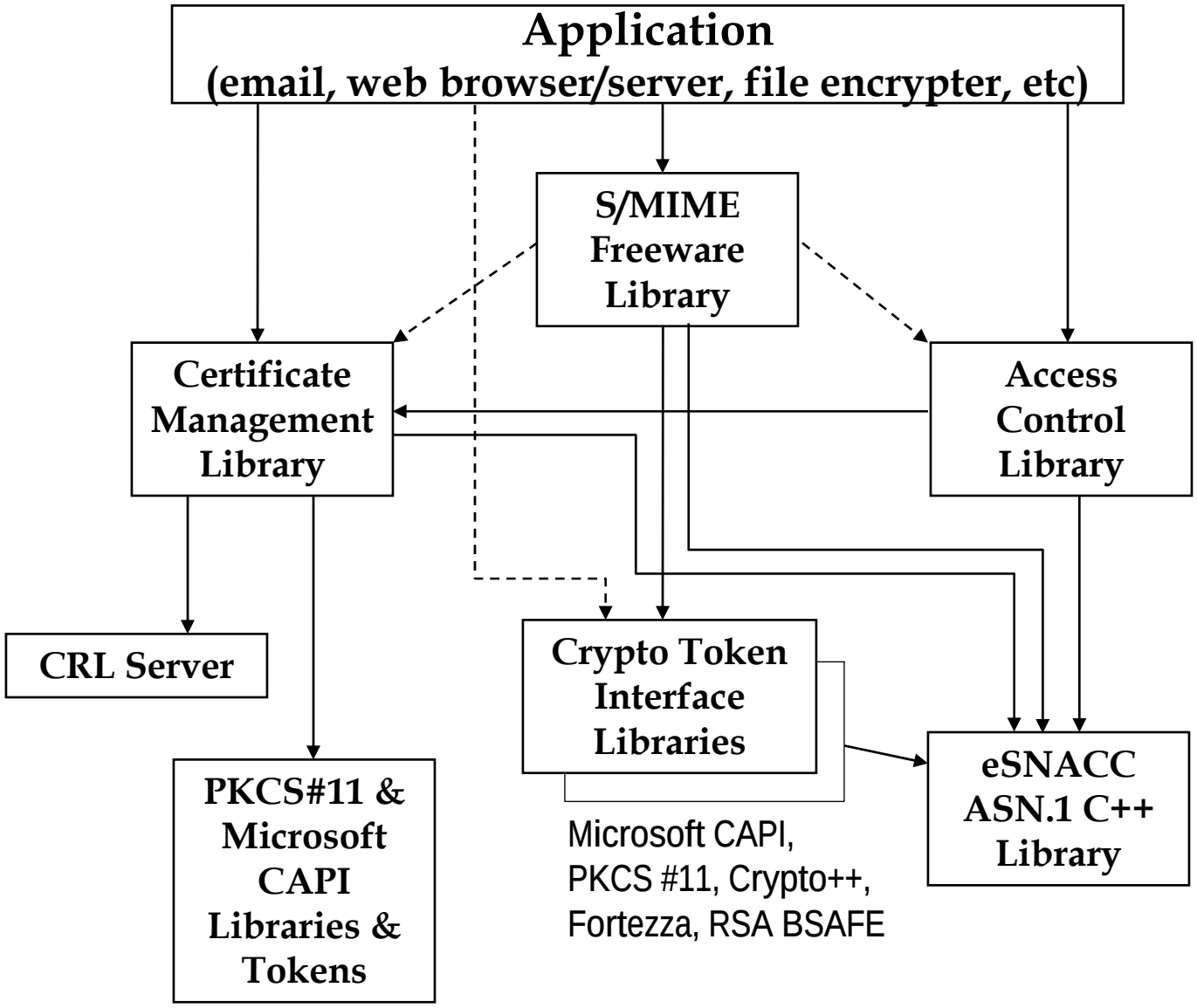
BAE SYSTEMS

BAE Systems Freeware Availability

- S/MIME Freeware Library
  - <http://www.DigitalNet.com/knowledge/sfl_home.htm>
- Certificate Management Library
  - http://www.digitalnet.com/knowledge/cml_home.htm>
- Access Control Library
  - <http://www.DigitalNet.com/knowledge/acl_home.htm>
- eSNACC ASN.1 Toolkit
  - <http://www.DigitalNet.com/knowledge/snacc_home.htm>
- For all BAE Systems freeware libraries, unencumbered source code is freely available to all. BAE Systems freeware can be used without paying any royalties or licensing fees. There is a public license associated with each freeware library.

BAE SYSTEMS

Security Services Freeware Architecture



BAE SYSTEMS

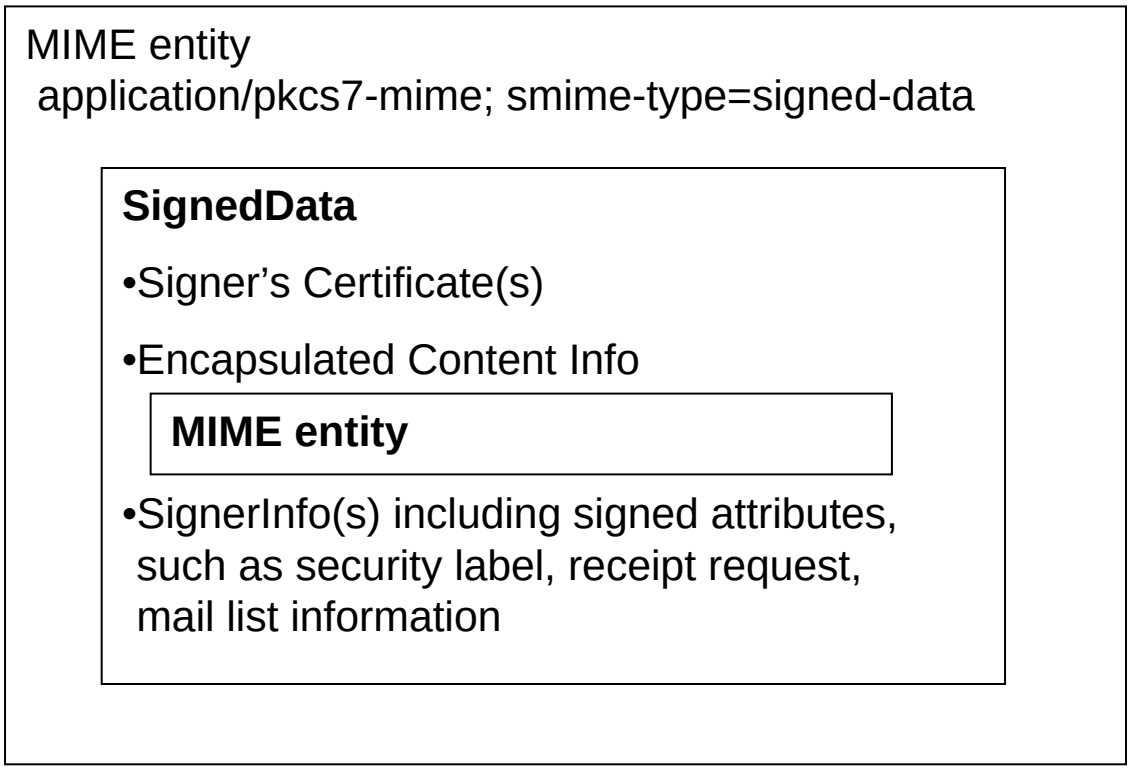
S/MIME Freeware Library (SFL)

- SFL is freeware implementation of IETF S/MIME v3 RFC 3852 Cryptographic Message Syntax (CMS)
- CMS is becoming the standard security protocol for protecting data communicated across the Internet
- RFC 2634 Enhanced Security Services (ESS) specs that provide Message Security Protocol (MSP)-equivalent security features
- SFL supports the use of RFC 3850 (Certificate Handling) and RFC 3581 (Message Specification)
- Used SFL to successfully process and product sample data in “Examples of S/MIME Messages”

BAE SYSTEMS

S/MIME v3 Signed Data

- Provides integrity, authentication, non-repudiation security services through digital signatures



BAE SYSTEMS

SFL

- Protects any type of data (not just MIME)
- Algorithm independent: SFL is used with external crypto libraries that provide a variety of crypto algorithms
- Uses eSNACC freeware library to perform all ASN.1 encoding (including DER) and decoding of CMS and ESS objects
- Uses CML to ASN.1 decode X.509 certificates, CRLs, etc.
- Can be configured to use CML to build and validate X.509 certification paths
- Can be configured to use ACL to perform SDN.801 rule based access control processing
- Does not build/process MIME headings

BAE SYSTEMS

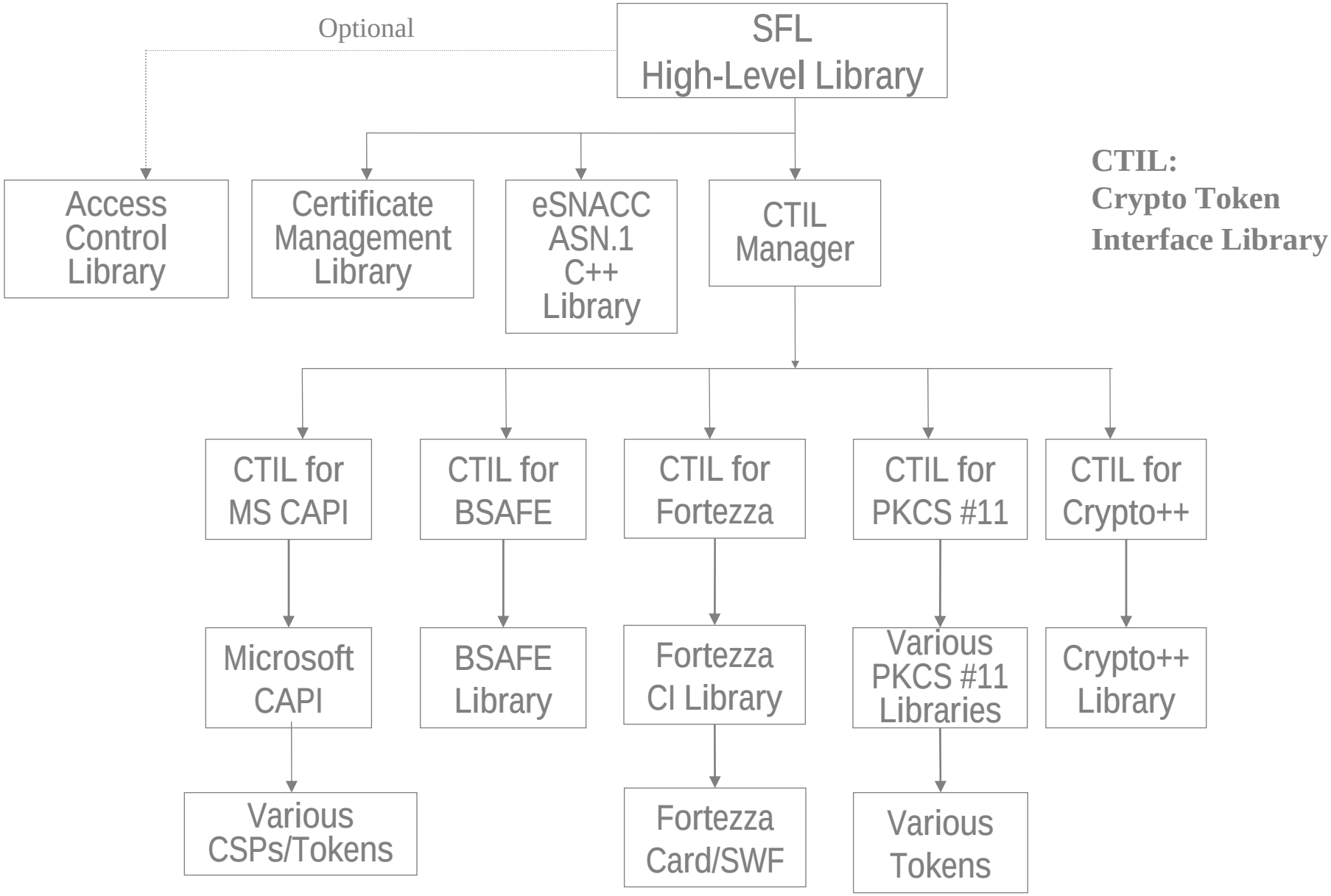
SFL *(continued)*

Implements optional RFC 2634 security services:

- Signed receipts – provides authenticated proof of delivery (similar to registered mail)
- Security labels – provides the capability to label data with sensitivity values (e.g., company proprietary; private medical information)
- Mail list information – supports the secure distribution of messages by mail list servers
- Signing Certificate Attribute – identifies signer's certificate(s), ACs and certificate policies

SFL Architecture

BAE SYSTEMS



CTIL:
Crypto Token Interface Library

BAE SYSTEMS

SFL Components

- SFL High Level Library
  - Builds and processes CMS and ESS objects independent of the crypto library in use
  - Provides full C++ API and limited C API
- eSNACC ASN.1 Library
  - Implements ASN.1 Distinguished Encoding Rules
- Crypto Token Interface Libraries (CTIL)
  - Isolates the SFL High Level classes from the specifics of the cryptographic token processing
  - Calls the cryptographic token functions to perform the Encrypt, Decrypt, Sign, and Verify operations

BAE SYSTEMS

Crypto Token Interface Libraries (CTIL)

- Microsoft CAPI CTIL: Uses Microsoft CAPI v2.0 that provides access to variety of underlying Crypto Service Providers, crypto tokens, and crypto algorithms
- PKCS #11 CTIL: Provides access to PKCS #11-compliant crypto libraries; tested with Litronic Maestro, GemPlus, DataKey PKCS #11 libraries
- Crypto++ CTIL: Calls freeware Crypto++ library providing 3DES, E-S D-H, SHA-1, DSA, RSA, etc.
- BSAFE CTIL: Calls RSA BSAFE library providing RSA algorithms, such as RSA, RC2, MD5
- FORTEZZA CTIL: Calls FORTEZZA CI library using FORTEZZA card/Software FORTEZZA providing SKIPJACK, Key Exchange Algorithm, SHA-1, DSA

BAE SYSTEMS

SFL Interoperability Testing

- SFL S/MIME v2 interoperability testing: SFL used to exchange signedData and evelopedData messages with Microsoft Internet Explorer Outlook Express 4.01, Netscape Communicator 4.X, Entrust and Baltimore MailSecure S/MIME v2 products.

- SFL S/MIME v3 interoperability testing: Tested the majority of features in RFCs 3852 (CMS), 2631 (D-H), and 2634 (ESS), as well as some of the features in RFC 3850 (Cert) and 3851 (Msg). SFL does not support every S/MIME v3 optional feature and does not build/process MIME headers.

- Used SFL to successfully process and produce sample data in “Examples of S/MIME Messages”. Complete test drivers and test data available as part of SFL release. SFL-generated data in drivers and test data available as part of SFL release. SFL-generated data in Examples I-D such as: signed receipts, countersignatures, security labels, equivalent labels, mail list info, signing certificate attribute.

BAE SYSTEMS

SFL Interoperability Testing *(continued)*

- S/MIME v3 interoperability testing between SFL and Microsoft successfully tested almost all signedData and envelopedData features. Included DSA, 3DES, E-S, D-H, RSA, and FORTEZZA algorithms. For example, SFL (using Crypto++) exchanged E-S D-H protected envelopedData. Almost all ESS features tested (signed receipts)
- SFL can produce and process SFL-supported features in IETF S/MIME v3 interoperability testing matrix. SFL-generated sample objects illustrating each supported feature in the matrix are provided as part of SFL release.
- SFL interoperability testing is automated using test drivers and configuration files so it can be easily repeated and modified.

BAE SYSTEMS

SFL Test Utilities

- AutoHi: Sophisticated test driver that uses configuration text files to read input data so that SFL test cases can be easily configured and repeated. It exercises all portions of SFL code.
- Report_tool: Test utility that processes and displays contents of MIME encoded messages containing single body part or multi-part CMS components. It performs signature verification operations. It also reads certificates.
- CertificateBuilder: Test utility to generate key material, certificates, Attribute Certificates.

BAE SYSTEMS

SFL Status

- Version 2.5 SFL released April 2005
  - Implements RFC 3852 (CMS) and RFC 3370 (CMS Algorithms)
  - Tested on MS Windows 2000/XP, RedHat Linux and Solaris 2.8
- Future versions may include:
  - Implementing changes to IETF specifications
  - Adding “Certificate Management Messages over CMS” ASN.1 encode/decode functions

BAE SYSTEMS

Certificate Management Library (CML)

- Applications requiring PKI security services can use the CML to meet their X.509 certificate processing requirements
- Builds and validations X.509 certification paths and CRLs as specified in 2000 X.509 Recommendation.
- ASN.1 decodes X.509 Certificates, CRLs, Attribute Certificates, and components thereof.
- Supports both X.509 v3 certificates and FORTEZZA v1 certificates.
- Uses PKC #11 API to support variety of crypto algorithms (such as verifying DSA, ECDSA, & RSA signatures).
- Uses Microsoft Cryptographic API (CAPI) functions to use installed Cryptographic Service Providers.

BAE SYSTEMS

CML *(continued)*

- Robustly builds complex cert paths including cross-certified hierarchical and non-hierarchical PKIs.
- Accompanying Storage and Retrieval Library (SRL) provides local certificate and CRL storage management functions.
- SRL (optionally) provides remote directory retrieval capabilities using LDAP.
- CML was originally developed by U.S. Government.
- CML provides a full C language API and C++ API based on eSNACC ASN.1 C++ classes.

BAE SYSTEMS

CML X.509 Compliance

- Implements majority of 2000 X.509 features and cert path validation requirements:
  - Name Chaining (including multi-valued RDNs)
  - Key Identifier Chaining
  - Signature Verification (using DSA and RSA)
  - Validity Date Checking
  - Revocation Checking (CRLs and OCSP)
  - Name Constraints
  - Basic Constraints
  - Certificate Policies, Mapping, and Constraints
  - Subject and Issuer Alternate Names
  - Key Usage/Extended Key Usage
  - Private Key Usage Period
  - CRL Distribution Points
  - Cross Certificates
  - CRL Extensions and CRL Entry Extensions

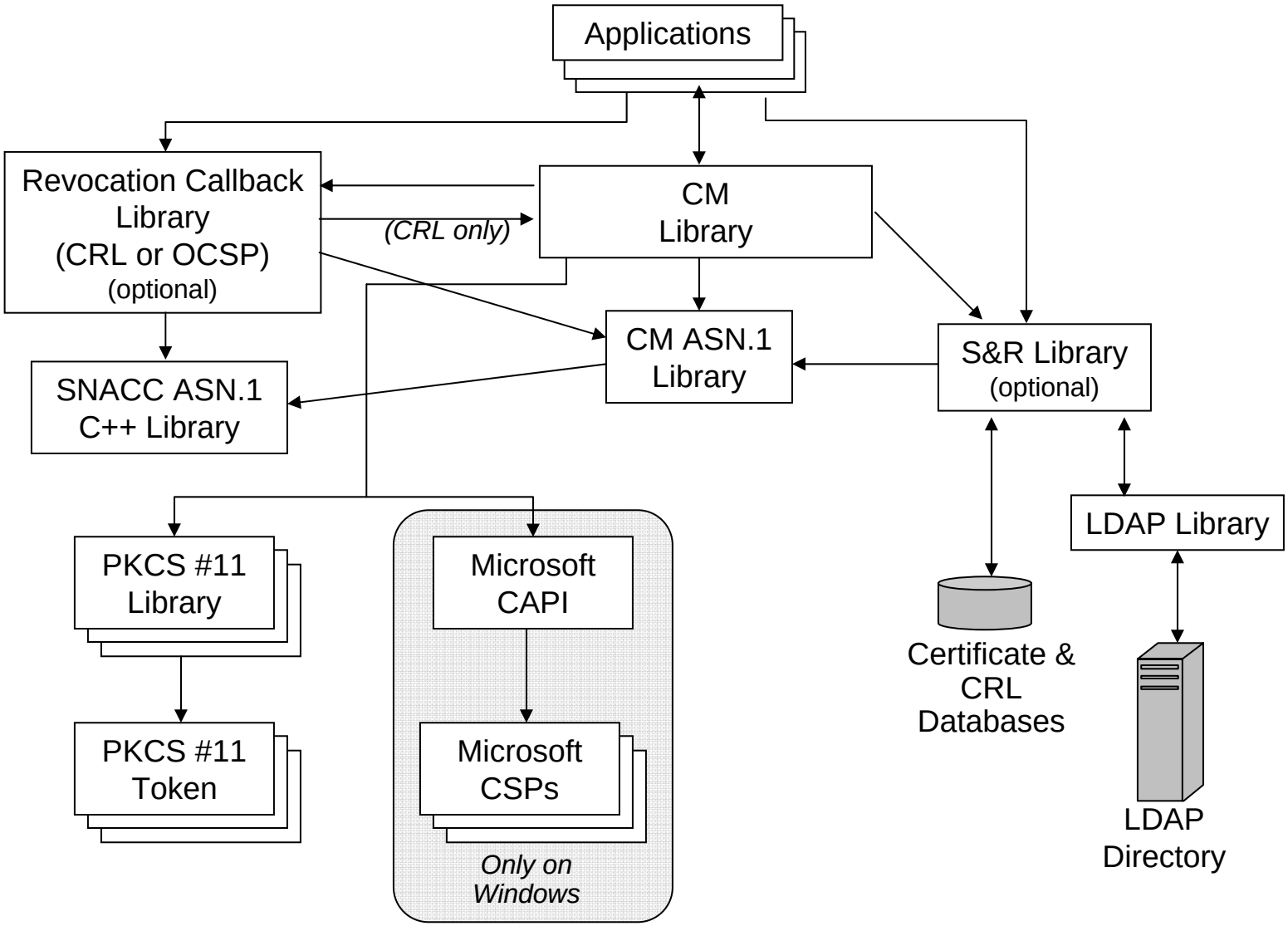
BAE SYSTEMS

CML Compliance

- CML complies with all IETF PKIX requirements in RFC 3280.
- CML meets requirements stated in the SDN.706 Certificate/CRL Profile required by DMS program
- Meets all Federal Bridge Certification Authority (BCA) requirements, such as using cross certificates

BAE SYSTEMS

CML Architecture



BAE SYSTEMS

CML Interoperability Testing

- CML has been thoroughly tested including interoperability testing with a variety of Certification Authority (CA) products.
  - For example, CML has been used to verify certification paths created by VeriSign, Entrust, Microsoft, General Dynamics, Baltimore, Netscape, and SPYRUS CA products.
- CML has been successfully used to build and verify certification paths used in the Federal Bridge Test Hierarchy, which includes cross-certified hierarchical and non-hierarchical PKIs.
- National Institute of Standards and Technology (NIST) provides a standard test suite of X.509 certificate paths
  - http://csrc.nist.gov/pki/testing/x509paths.html
  - Data can be used for testing applications for compliance with RFC 3280 PKIX Certification and CRL Profile.
  - CML was used to successfully process NIST Test Data.

BAE SYSTEMS

PK Interoperability Test Suite (PKITS)

- A free and openly available test resource provided to facilitate vendor development of secure, interoperable PKE software that builds and validations certification paths.
- A comprehensive X.509 path validation test suite that was jointly developed by BAE Systems, NIST, and NSA to cover most of the features specified in X.509 and RFC 3280.
- BAE Systems developed and maintains PKITS web site to provide information and test data
  - http://pkits.atl.digitalnet.com/
- CML has been used to successfully develop and verify the PKITS X.509 certification paths
- Used to support the Federal PKI Working Group interoperability testing including processing cross certs
- NIST posts PKITS as their standard X.509 test suite
  - http://csrc.nist.gov/pki/testing/x509paths.html

BAE SYSTEMS

CML API Overview

- Session Management
  - CML uses session ID to support multiple applications
- Certificate Operations
  - Retrieve, decode, validate CRLs and certs
- Database Management
  - Add, delete, list, retrieve from local database
- Memory Management
  - Functions to free memory allocated by the CML

BAE SYSTEMS

CML Status

- Version 2.5 CML released April 2005
  - On-Line Certificate Status Protocol (OCSP)
  - Tested on MS Windows NT/98/2000/XP, Linux and Sun Solaris 2.8
- Future versions may include:
  - Enhance CML's CRL server library to run as separate server
  - Implement changes to X.509 and IETF specifications

BAE SYSTEMS

Access Control Library (ACL)

- Provides Access Control Decision Function supporting SDN.801 Partition Rule Based Access Control requirements using:
  - Clearance attribute containing subject's authorizations;
  - Security label indicating sensitivity of data; and
  - Security Policy Information File (SPIF).
- Uses SPIF as part of process of ensuring that subject's authorizations are commensurate with values in security label.
- By using SPIFs, ACL can support a variety of security policies and equivalency mappings between security policy values.
- Checks a security label to ensure it includes a valid combination of security classification and security category values (see SDN.801) as specified in SPIF for security policy identified in label.

BAE SYSTEMS

ACL *(continued)*

- Meets DMS rule based access control requirements
- Verifies Attribute Certificates meet DoD BCA Demo Phase II requirements
- Supports X.509 certificates to meet DMS and Canadian MMHS requirements
- Provides displayable string representation of a security label
- Uses CML to ASN.1 decode X.509 certificates, attribute certificates
- Uses CML to verify signatures as needed
- Optionally, uses CML to build and verify X.509 v3 certification paths
- Optionally, uses LDAP to retrieve security objects
- Provides a high-level C++ language API

BAE SYSTEMS

ACL Status

- Version 2.5 ACL released in April 2005
  - Tested on MS Windows 2000/XP, RedHat Linux, and Sun Solaris 2.8
- Future versions may include:
  - Support for additional requirements such as 2000 X.509 Recommendations, IETF PKIX AC, and alternative access control models

BAE SYSTEMS

eSNACC ASN.1 Software

- BAE Systems enhanced the original SNACC to implement:
  - Distinguished Encoding Rules (DER);
  - Packed Encoding Rules (PER);
  - Support large ASN.1 INTEGERs and multi-byte character strings; and
  - Improve memory usage
- BAE Systems is supporting eSNACC ASN.1 Compiler, C++ library, and C library.
- Implements majority of ASN.1 encoding/decoding rules specified in 1988 X.209 Recommendation.
- Doesn’t support all ASN.1 features, but can be used to produce compliant ASN.1 hex encodings.
- Version 1.7 released in May 2004
- Tested on MS Windows 2000/XP, RedHat Linux, & Sun Solaris 2.8

BAE SYSTEMS

BCA CML/SFL/ACL Success

- DoD BCA Technology Demo tested cross-certified Entrust, General Dynamics, Baltimore, and SPYRUS PKIs. CML successfully used to build and verify cross-certified cert paths between PKIs.
- CygnaCom integrated SFL/CML/ACL/CPDL into a plug-in for Eudora Pro. Interoperability testing successful between SFL/CML/ACL/CPDL/Eudora client, Baltimore Mail Secure and Entrust S/MIME toolkit.
- CygnaCom used ACL in Attribute Authority.
- CygnaCom used ACL & CML in trusted web server.

BAE SYSTEMS

NIST S/MIME v3 Test Facility

- BAE Systems developed open source SMIME v3 auto responder using SFL, CML, eSNACC, CTILs
- NIST hosts auto responder
  - http://csrc.nist.gov/pki/smime/smtest.htm
- Vendors use this facility to determine if products comply with S/MIME v3 specifications and NIST profile
- Auto responder processes S/MIME messages sent by tester and provides feedback regarding success/failure
- Auto responder creates signed and/or encrypted S/MIME messages for processing by tester
- Auto responder generates test key pairs and cert paths for each tester.
  - Can use certs provided by the tester

BAE SYSTEMS

IMC Mail Lists

- Internet Mail Consortium (IMC) has established SFL, CML and eSNACC mail lists for users to provide feedback, report bugs and ask questions.
- Subscription information for mail lists available at:

  <http://www.imc.org/imc-sfl>

  <http://www.imc.org/imc-cml>

  <http://www.imc.org/imc-snacc>

- Please DO NOT send SFL/CML/eSNACC-related messages to IETF mail lists.