

# **Global Information Assurance Certification Paper**

# Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

# Interested in learning more?

Check out the list of upcoming events offering "Security Essentials Bootcamp Style (Security 401)" at http://www.giac.org/registration/gsec Common Data Security Architecture – (CDSA) For SANS GIAC Level One Security Essentials GSEC Practical Assignment

> Document Version Document Version Date Document By

1.0 1<sup>st</sup> March, 2001 Michael Yeung

### TABLE OF CONTENTS

INTRODUCTION		
1.0 WHATISCDSA?	<u></u>	
1.1 System Security Services 1.2 The Common Security Service Manager (CSSM) 1.3 Security Add -in Modules		
20 HOW IS CDSABEIN G USED?		5
2.1 INTERACTION BETWEEN CSP AND APPLICATIONS		
3.0 HOW CDSA ADDRESSES A UTHENTICITY, INTEG RI TY, AND	CONFIDENTIAL ITY?	6
<ul> <li>3.1 CRYPTOGRAPHY SERVICE PROVIDER</li> <li>3.1.1 AP Is that support Data confidentiality:</li> <li>3.1.2 AP Is that support Data integrity:</li> <li>3.1.3 AP Is that facilitate authentication via public/private key managen</li> <li>3.2 CERTIFICATE LIBRARY SERVICES</li> <li>3.2.1 AP Is that support Certificate Operations</li> <li>3.2 API that support Certificate operations</li> </ul>	nent :	
An WILLAT A DE THE DOC SIDLE ENTRE TRENDS OF CDC 42		
REFERENCE S		10

# Introduction

Common Data Security Architecture (CDSA) is an open and extensible software framework that addresses security requirements of applications such as e -commerce, communication, and digital content distributi on.

This paper aims to provide a general understanding of CDSA and to describe how CDSA addresses the three basic concerns of Internet security:

- 1) Authenticity
- The ability to verify the parties on both ends of a communication link
- 2) Integrity
- The ability to verify that all data transmitted and received has not been tampered with or changed 3) Confidentiality

The ability to ensure that all transmitted data over a communication link cannot be read by unintended parties

In order to achieve these objectives, this p aper will address the following questions:

- What is CDSA?
- How is CDSA being used? (two scenarios)
- How CDSA addresses Authenticity, Integrity, and Confidentiality?
- What are the possible future trends of CDSA?

# 1.0 What is CDSA?

CDSA is an open and extensible software framework and API specification that address communication and data security requirements. CDSA was originally developed by Intel Architecture Lab (IAL). The specification was refined through the Open Group standards process with companies such as Hewlett - Packard, IBM, JP Morgan, Motorola, Netscape, Trusted Information Systems, and Shell Companies. CDSA was adopted by the Open Group in 1977 as an open specification. The objectives of CDSA are:

- 1. Encourage interoperable, horizontal security standa rds
- 2 Offer essential components of security capability to the industry at large

In order to achieve these objectives, CDSA was designed with the following architectural principals:

- 1. A layered service provider model CDSA consists of a set of horizontal la yers of services. Each layer builds on services provided by the layer below it.
- 2. Open Architecture

CDSA is fully disclosed for peer review and went through the Open Group Standards Process

3. Modularity and Extensibility Each layer is made up of individual mo dules. New modules can be added as needed and therefore support extensibility

The overview of CDSA is illustrated as follows:



The diagram shows that CDSA is made up of three basic layers:

- System Security Services
- The Common Security Services Manager (CSSM)
- Security Add -in Modules

### 1.1 System Security Services

System Security Services are between applications and CSSMservices. Software at this layer provides a high level abstraction of security services such as secure e -mail, secure file systems, or secure communications. Applications can invoke the CSSM APIs directly, or use these layered services to access security services on a platform.

#### 1.2 The Common Security Service Manager (CSSM)

CSSM provides a set of core services that are common to all c at egories of security services. CSSM defines five basic categories of services:

#### Cryptographic Service Provider (CSP) modules

CSPs perform cryptographic operations such as bulk encrypting, digesting, and digital signatures.

#### Trust Policy (TP) modules

TPs implement policies defined by authorities and institutions and set the level of trust required to carry out specific actions (such as issuing a check or gaining access to confidential intellectual property).

#### Certificate Library (CL) modules

CLs manage c ertificatés and revocation lists, and access to remote signing capabilities such as Certification Authorities (CA).

#### Data Storage Library (DL) modules

DLs provide stable storage for security -related data objects, including certificates cryptographic keys and policy objects.

#### Authorization Computation (AC) modules

ACs define a general authorisation evaluation service that computes whether a set of credentials and samples are authorized to perform a specific operation on a specific object.

#### Elective (EM) M odules

EMs add new and compelling security features not encompassed by the current set of service modules. For example, one new feature that vendors might add to CDSA is biometrics authentication.

In addition, CSSM provides two additional core services:

#### Integrity Services

The integrity services are used by CSSM itself to verify and guarantee the integrity of all the other components within the CSSM environment

#### Security Context Management

CSSM provides context management functions (such as session infor mation) to facilitate applications to utilise the security services

#### 1.3 Security Add -in Modules

This layer is made up of service provider modules that offer basic components — cryptographic algorithms, base certificate manipulation facilities, and storage etc.

# 2.0 How is CDSA being used?

This section attempts to give readers a better understanding of CDSA by providing two perspectives of how CDSA is being used. The first perspective is from a programming point of view — what is sequence of events for an application within CDSA to invoke CSP security services? The second perspective is from a system security services point of view — How can CDSA be used to implement OpenSSL (Open Source Secure Socket Layer)?

#### 21 Interaction between CSP and Applications

Each CSSM module (including CSSM itself and add -ins) must be installed on the system before applications can access it. A typical session of interaction between an application and CSP is outlined as follows:

- 1) The application selects a CSP and requests CSS M to attach to it.
- 2) The CSSM returns a CSP handle to the application that uniquely identifies the pairing of the application thread to the CSP module instance.
- 3) The application establishes a "session," a framework in which the CSP will perform cryptographi c operations.
- 4) The application creates an operation "context," which must exist prior to starting CSP operations and is deleted as soon as possible upon completion of the operation.
- 5) When creating the context, the application specifies an algorithm and may also initialize a session key, pass an initialization vector and/or pass padding information to complete the description of the session.

- 6) A successful return value from the create function to the application indicates the desired CSP is available.
- 7) All cryptographic services requested by applications can now be channeled to the CSP via the CSSM.
- 8) Cryptographic operations might take place:
  - as a single call to perform an operation and obtain a result.
  - as a sequence of calls, starting with an initialization ca II, followed by one or more update calls, and ending with a completion (final) call. Usually, the result is available after the final function completes its execution.
- 9) When security services are no longer needed, the application calls CSSM\_DeleteContext to delete the session's context information and thus terminates the session.

#### 22 Integrating CDS Ainto OpenSSL

While CDSA provides the building blocks for basic security functions, an application may require use of a higher-level set of protocols (among them, SSL, S/MIME, PGP, or SET). These protocols not only provide a higher level structuring for basic security functions, but also ensure cryptographic interoperability among different platforms. Thus, when Internet application developers field their products, they might employ the SSL or S/MIME protocols to ensure interoperability. Broadly speaking, these high -level security protocols safeguard the transmission of e -commerce information and serve as defacto standards of secure communication.

One of these higher -level protocols is OpenSSL. OpenSSL is a security library that implements the SSL protocol and related functionality for use by applications such as Secure Web Servers. The OpenSSL project is a collaborative effort to develop an Open Source tool kit that implements the Secure Socket Layer (SSL), the Transport Layer Security (TLSv1) protocol, and a full strength general -purpose cryptography library. OpenSSL is being maintained by a worldwide community of volunteers.

Through CDSA, OpenSSL would ga in access to a more powerful and complete set of security services; including cryptography, certificate management, trust policies, and secure data storage. In addition, OpenSSL would gain interpretability and extensibility that it does not have now.

As examples how CDSA is being used, the next two sections will outline two approaches that can be used to integrate CDSA with OpenSSL.

#### Option 1: Integrate CDSA into the SSL crypto library

With this approach, the SSL crypto library API implementation is modi fied to invoke functionally equivalent CDSA APIs. This approach is transparent to the applications, i.e. the application would call the same SSL crypto library APIs with the same parameters and return types. However, within the SSL crypto API, calls are routed through CDSA CSP APIs. In short, this approach would involve porting of the appropriate SSL crypto primitives and place CDSA calls in each of these crypto primitives.

#### Options 2: Replace SSL crypto library with CDSA

With this approach, all the SSL cry ptolibrary calls will be replaced with functionally equivalent CDSA APIs. This approach is not transparent to the applications, i.e. the application source would need to be modify to call CDSA APIs instead of SSL cryptolibrary APIs to perform crypto oper ations. In short, this approach would by pass the existing SSL cryptolibrary all together.

# 3.0 How CDSA addresses Authenticity, Integrity, and Confidentiality?

Although all the CSSM modules contribute to authenticity, integrity and confidentiality, the p rincipal modules that address these are the Cryptography Service Provider (CSP) module and Certificate Library Services (CL) module.

The objective of this section is that by going into more details about how these two modules supports authenticity, integrity and confidentiality that the readers would gain yet another level of understanding of CDSA.

#### 3.1 Cryptography Service Provider

A CSP (whether software and/or hardware -based) provides data encryption/decryption, digital signatures, cryptographic hash ing, key generation, random -number generation services. A CSP supports confidentiality, integrity and authenticity by providing a set of comprehensive APIs.

#### 3.1.1 APIs that support Data confidentiality:

- 1. Data encryption APIs
  - CSP\_Encry ptData ()

This function n encrypts all data contained in the set of input buffers using information in the context. CSP\_EncryptDataInit ()

This function initializes the staged encrypt function.

CSP\_EncryptDataUpdate()

This function continues the staged encryption process over all data in the set of input buffers. CSP\_EncryptDataFinal ()

This function finalizes the staged encryption process by returning any remaining cipher text not returned in the previous staged encryption call.

2 Data decryption APIs (with similar functional description as CSP\_EncryptData\*)

- CSP\_DecryptData()
- CSP\_DecryptDatalnit()

CSP\_DecryptDataUpdate()

CSP\_DecryptDataFinal ()

### 3.1.2 APIs that support Data integrity:

- 1. Sign Data APIs
  - CSP\_SignData ()

This function signs all data contained in the set of input b uffers using the private key specified in the context.

CSP\_SignDataInit ()

This function initializes the staged sign data function. For staged operations, a combination operation selecting both a digesting algorithm and a signing algorithm must be specifie d.

CSP\_SignDataUpdate ()

This function continues the staged signing process over all data contained in the set of input buffers. Signing is performed using the private key specified in the context.

CSP\_SignDataFinal ()

This function completes the final stage of the sign data function.

- 2 Verify Data APIs (with similar functional description as CSP\_SignData\*) CSP\_Verify Data () CSP\_Verify DataInit () CSP\_Verify DataUpdate () CSP\_Verify DataFinal ()
- Digest Data APIs (A message digest is the result of a hash operation on an arbitrary series of bits) *CSP\_Digest Data ()* ODD\_Diment Data (hit h)
  - CSP\_DigestDataInit ()

CSP\_DigestDataUpdate ()

CSP\_DigestDataFinal ()

CSP\_DigestDataClone()

This function clones a given staged message digest context with its cryptographic attributes and intermediate result.

- 4. APIs that support MAC (Message Authentication Code A function that produces fixed length output from variable -length input and a key. Might be hash -based, cipher -based, or stream -cipher based) CSP\_GenerateMac ()
  - CSP\_GenerateMacInit()
  - CSP\_GenerateMacUpdate()
  - CSP\_GenerateMacFinal ()
  - CSP\_VerifyMac ()
  - CSP\_VerifyMacInit ()
  - CSP\_VerifyMacUpdate ()
  - CSP\_VerifyMacFinal()

### 3.1.3 APIs that facilitate authentication via public/private key management:

#### CSP\_GenerateKey ()

This function generates a symmetric k ey.

CSP\_GenerateKeyPair()

This function generates an asymmetric key pair. (One public, one private)

CSP\_WrapKey ()

This function wraps the supplied key using the context. (Key wrapping/unwrapping means Encryption/decryption of a key. The key can be a symmetric key or private key of a public/private key pair)

CSP\_UnwrapKey()

This function unwraps the supplied key using the context.

CSP\_DeriveKey ()

This function derives a new symmetric key using the context and/or information from the base key in the context.

CSP\_QueryKeySizeInBits ()

This function gets the logical and effective size of a key. The logical size of the key is the number of bits in the key data for a symmetric key, or the size of the key component commonly used to reference the size of an asymmetric key. The effective size of a key is the number of bits in a key that are actually used in the cryptographic operation.

Since more than 90% of Cryptographic Operations APIs were listed above with simplified descriptions, the reader should now have a pretty good idea about the functionality of the CSP module.

# 3.2 Certificate Library Services

Authenticity can be supported via the certificate infrastructure. A certificate is a mechanism for establishing identity. The primary purpose of a Certificate Li brary (CL) module is to perform syntactic manipulations on a specific certificate format, and its associated certificate revocation list (CRL) format. These manipulations cane be grouped into 2 categories:

- Certification Operations
- CertificateRevocationListOperations.

# 3.2.1 APIs that support Certificate Operations

#### CL\_Cert Sign ()

This function sign a certificate using the private key and signing algorithm specified in a context Handle.

CL\_Cert Verify ()

This function verifies that the signed certificate h as not been altered since it was signed by the designated signer.

CL\_Cert Create Template ()

This function allocates and initializes memory for an encoded certificate template output. The initialization process includes encoding all certificate field values according to the certificate type and certificate encoding supported by the certificate library module.

#### CL\_CertGetFirstFieldValue()

This function returns the value of the certificate's first field (design at ed by the data structure CSSM\_OID Cert Field)

CL\_CertGetNextFieldValue()

This function returns the value of a certificate field, when that field occurs multiple times in a certificate. CL\_CertAbortQuery ()

This function terminates a results handle used to access multiple certificate fields.

CL\_Cert GetKey Info ()

This function returns the public key and integral information about the key from the specified certificate. CL\_Cert GetAll Fields ()

This function returns a list of the values stored in the input certificate.

CL\_CertDescribeFormat()

This function returns a list of the values this certificate library module uses to name and reference fields of a certificate.

# 3.2.2 APIs that support Certificate Revocation List Operations

CL\_CrlCreateTemplate()

This function creates an unsigned, memory -resident CRL. Fields in the CRL are initialized.

CL\_CrISet Fields ()

This function will set the fields of the input CRL to the new values, specified by the input.

CL\_CrIAddCert ()

This function revokes the input certificate by adding a record representing the certificate to the CRL CL\_CrlRemoveCert ()

This function reinstates a certificate by removing it from the specified CRL.

CL\_CrlSign ()

This function signs a CRL using the private key and signing algorithm. The result is a signed, encoded certificate revocation list.

CL\_Crl Verify ()

This function verifies that the signed CRL has not been altered since it was signed by the designated signer.

CL\_IsCertInCrl ()

This function searches the CRL for a record corresponding to the certificate.

CL\_CrlGetFirstFieldValue()

This function returns the value of the CRL's first field (designated by the CSSM\_OID CrlField).

CL\_CrlGetNextFieldValue()

This function returns the value of a CRL field, when that field occurs multiple times in a CRL

CL\_CrIAbort Query ()

This function terminate s the query initiated

CL\_CrIDescribeFormat ()

This function returns a list of the values this certificate library module uses to name and reference fields of a CRL.

As with the CSP module, the simplified API descriptions listed above should give the reade r a deeper understanding of the CL module functionality.

# 4.0 What are the possible future trends of CDSA?

Currently, CDSA Version 2 specification has been adopted by The Open Group. Intel developed a reference implementation of the CDSA Version 2 specific ation for Windows\* 95, Windows 98, and Windows NT\* 4.0 and Linux. Various vendors such as Hewlett -Packard, IBM have already implemented and committed to CDSA.

A stream of development to be expected is that more and more high -level security services/proto cols such as S/MIME, SET, and PGP will be integrated with CDSA.

Currently, the CDSA APIs are specified and implemented in the Clanguage. Given the widely adopted JAVA platform, it is not unreasonable to expect a JAVA package that defines the JAVA classe s and interfaces to CSSM-defined services.

Another stream of development to be expected is the integration or collaboration of CDSA with other technologies such as LDAP. For example, the Data Storage Library of CSSM can use LDAP as the supporting infrastructure for storing data objects. In addition, the Trust Policy module can also use LDAP to centrally store and manage policies.

In conclusion, CDSA has gained wide acceptance as an open standard. It is expected that CDSA will continue to be a framework for developing security applications and services for the fores eeable future.

# References

Common Security: CDSA and CSSM, Version 2 (with corrigenda) http://www.opengroup.org/security/cdsa/index. htm

Intel Common Data Security Architecture – Technical Overview http://www.intel.com/ial/security/tech.htm

Intel Common Data Security Architecture – Frequently Asked Questions http://www.intel.com/ial/security/faq.htm

Integrating CDSA into OpenSSL (CDSA Engineering Release 3.1.2) http://developer.intel.com/ial/security/documentation.htm

A Comparison of CDSA to Cryptoki http://cs.rc.nist.gov/niss.c/1999/program/rd11.htm

"Common Data Security Architecture (CDSA)" "Common Data Security Architecture (CDSA) Tutorial", "Integrity Services" "CSSM Core Services" "SSL and CDSA" http://develope r.intel.com/ial/security/documentation.htm

Common Data Security Architecture (CDSA) White Paper http://docs.hp.com/hpux/internet/index.html

Virtual Private Network (VPN) Security http://www.sans.org/infosecFAQ/encryption/VPN\_sec.htm

# **Upcoming Training**

# Click Here to {Get CERTIFIED!}



Community SANS San Diego SEC401	San Diego, CA	Dec 05, 2016 - Dec 10, 2016	Community SANS
Community SANS St Louis SEC401	St Louis, MO	Dec 05, 2016 - Dec 10, 2016	Community SANS
SANS Cyber Defense Initiative 2016	Washington, DC	Dec 10, 2016 - Dec 17, 2016	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201612,	Dec 13, 2016 - Feb 02, 2017	vLive
Community SANS Marina del Rey SEC401	Marina del Rey, CA	Jan 09, 2017 - Jan 14, 2017	Community SANS
SANS Security East 2017	New Orleans, LA	Jan 09, 2017 - Jan 14, 2017	Live Event
SANS SEC401 Hamburg (In English)	Hamburg, Germany	Jan 16, 2017 - Jan 21, 2017	Live Event
Community SANS New York SEC401	New York, NY	Jan 16, 2017 - Jan 21, 2017	Community SANS
Community SANS Chantilly SEC401	Chantilly, VA	Jan 23, 2017 - Jan 28, 2017	Community SANS
SANS Las Vegas 2017	Las Vegas, NV	Jan 23, 2017 - Jan 30, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201701,	Jan 30, 2017 - Mar 08, 2017	vLive
SANS Southern California - Anaheim 2017	Anaheim, CA	Feb 06, 2017 - Feb 11, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Feb 06, 2017 - Feb 11, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Feb 13, 2017 - Feb 18, 2017	Community SANS
SANS Munich Winter 2017	Munich, Germany	Feb 13, 2017 - Feb 18, 2017	Live Event
Community SANS Seattle SEC401	Seattle, WA	Feb 13, 2017 - Feb 18, 2017	Community SANS
SANS Scottsdale 2017 - SEC401: Security Essentials Bootcamp	Scottsdale, AZ	Feb 20, 2017 - Feb 25, 2017	vLive
SANS Scottsdale 2017	Scottsdale, AZ	Feb 20, 2017 - Feb 25, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Feb 20, 2017 - Feb 25, 2017	Community SANS
Community SANS Minneapolis SEC401	Minneapolis, MN	Feb 27, 2017 - Mar 04, 2017	Community SANS
SANS Dallas 2017	Dallas, TX	Feb 27, 2017 - Mar 04, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Mar 06, 2017 - Mar 11, 2017	Community SANS
SANS San Jose 2017	San Jose, CA	Mar 06, 2017 - Mar 11, 2017	Live Event
Community SANS Chicago SEC401	Chicago, IL	Mar 06, 2017 - Mar 11, 2017	Community SANS
SANS Secure Canberra 2017	Canberra, Australia	Mar 13, 2017 - Mar 25, 2017	Live Event
SANS Secure Singapore 2017	Singapore, Singapore	Mar 13, 2017 - Mar 25, 2017	Live Event
SANS London March 2017	London, United Kingdom	Mar 13, 2017 - Mar 18, 2017	Live Event
SANS Tysons Corner Spring 2017	McLean, VA	Mar 20, 2017 - Mar 25, 2017	Live Event
Mentor Session - SEC401	Orange County, CA	Mar 21, 2017 - Apr 20, 2017	Mentor
SANS Pen Test Austin 2017	Austin, TX	Mar 27, 2017 - Apr 01, 2017	Live Event
SANS Pen Test Austin 2017 - SEC401: Security Essentials Bootcamp Style	Austin, TX	Mar 27, 2017 - Apr 01, 2017	vLive