ILM WORKSHOP

Sponsored by IBM Advanced Technical Support
Washington Systems Center
Gaithersburg, Maryland

Open Cryptographic Services Facility

Mary Sweat
IBM Washington Systems Center
Gaithersburg, MD 20879
sweatm@us.ibm.com

Trademarks

IBM @server zSeries

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

eNetwork DFSMS/MVS IMS/ESA* RAMAC
geoManager DFSMSdfp IP PrintWay RMF
AD/Cycle DFSMSdss IPDS RS/6000
ADSTAR DFSMShsm Language Environment S/390*
AFP DFSMSrmm Multiprise S/390 Parallel
APL2 DFSORT MQSeries Enterprise Server
APPN* Enterprise System/3090 MVS/DFP SecureWay
BookManager Enterprise System/4381 MVS/ESA StorWatch
BookMaster Enterprise System/9000 Network Station Sysplex Timer*
S/370 ES/3090 NetSpool System/390
CallPath ES/4381 OfficeVision/MVS SystemView
CallPath CICS/MVS ES/9000 Open Class SOM
CICS* ESA/390 OpenEdition SOMobjects
CICS/ESA* ESCON* OS/2 SP
CICS/MVS First Failure OS/390(*) VisualAge
CICSPlex Support Technology Parallel Sysplex* VisualGen*
COBOL/370 FlowMark Print Services VisualLift*
DataPropagator FFST Facility VTAM
DisplayWrite GDDM PrintWay WebSphere*
DB2* ImagePlus ProductPac 3090
DB2 Universal Intelligent Miner PR/SM 3890/XP
Database IBM*, IBM logo* QMF z/OS
DFSMS IMS RACF z/VM
FICON VM/ESA* zSeries
z/Architecture

* Registered trademarks of IBM Corporation

Trademarks

IBM @server zSeries

The following are trademarks or registered trademarks of other companies.

DFS is a trademark of Transarc Corporation
Lotus, Notes, and Domino are trademarks or registered trademarks of Lotus Development Corporation
LINUX is a registered trademark of Linus Torvalds
Penguin (Tux) complements of Larry Ewing
Tivoli is a trademark of Tivoli Systems Inc.
Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries
UNIX is a registered trademark of The Open Group in the United States and other countries.
Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.
SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

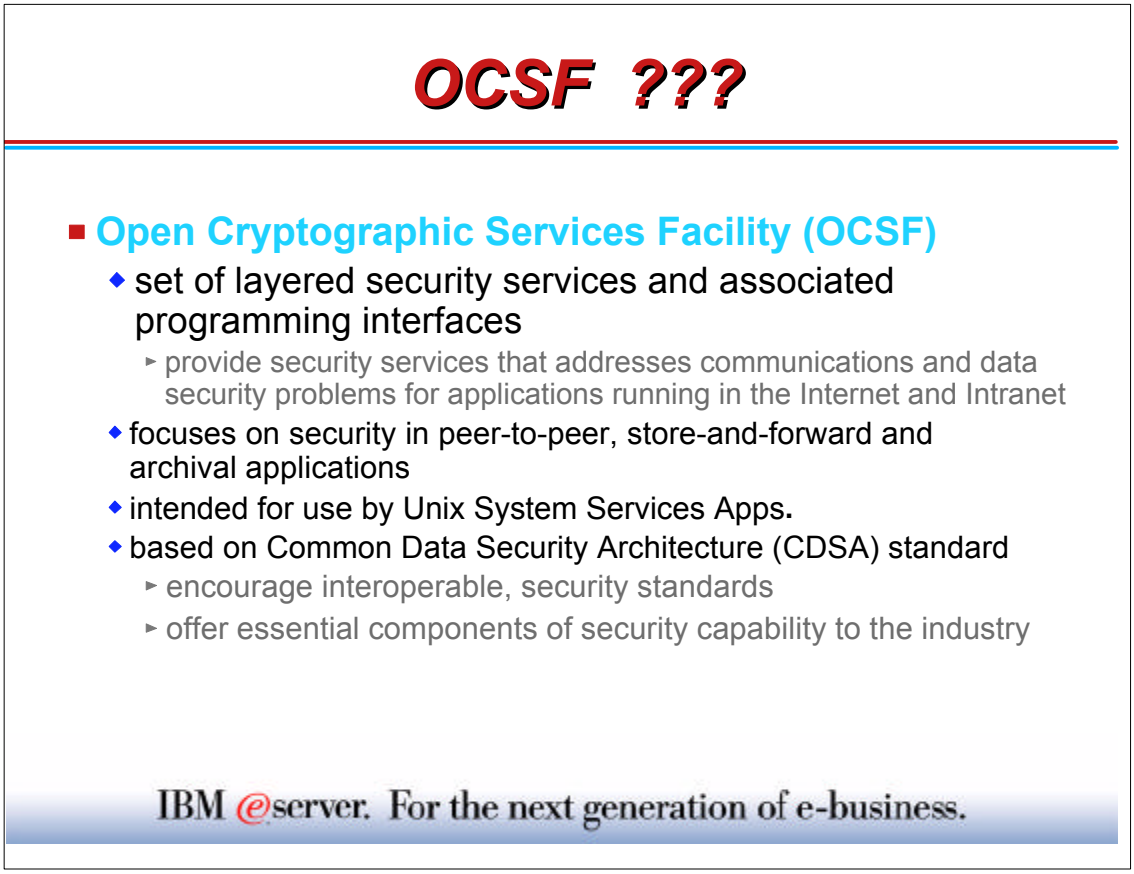
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

IBM considers a product "Year 2000 ready" if the product, when used in accordance with its associated documentation, is capable of correctly processing, providing and/or receiving date data within and between the 20th and 21st centuries, provided that all products (for example, hardware, software and firmware) used with the product properly exchange accurate date data with it. Any statements concerning the Year 2000 readiness of any IBM products contained in this presentation are Year 2000 Readiness Disclosures, subject to the Year 2000 Information and Readiness Disclosure Act of 1998.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.



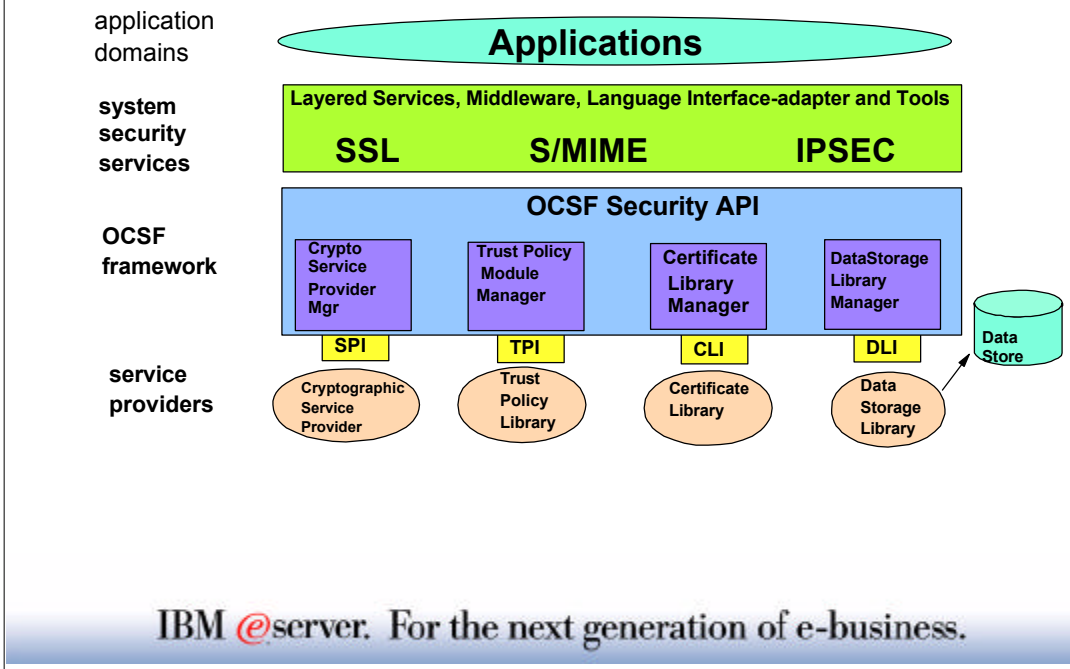
- OCSF provides security services that addresses communications and data security problems for applications running in the Internet and Intranet
- CDSA was developed to address multiple security needs, such as confidentiality, integrity, authentication and non-repudiation.

Why Do You Care

- **IBM License Manager (ILM) Requires it**
  - must be installed before using ILM
  - used to encrypt and decrypt certificates in ILM
  - no hardware required
  - no additional licenses required

IBM @server. For the next generation of e-business.

OCSF Architecture



- There are four major layers in the OCSF Architecture;
  > Application Domains
  > System Security Services
  > OCSF Framework
  > Service Providers

- Each layer provides services to the layer above it. The lowest layers begin with basic components such as cryptographic algorithms, random numbers and unique identification information.

- The layers build up to digital certificates, key management mechanisms, integrity and authentication credentials, and secure transaction protocols in higher layers.

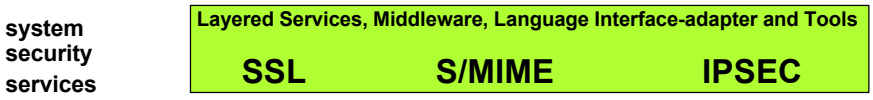
- OCSF also has a service provider interface (SPI) that supports service provider modules which implement building blocks for secure operations

Application Domain Layer

- Implements the application domain services
  - Secure Electronic Transaction (SET)
  - E-Wallet
  - E-mail services
  - License Management
  - file archival services

System Security Services

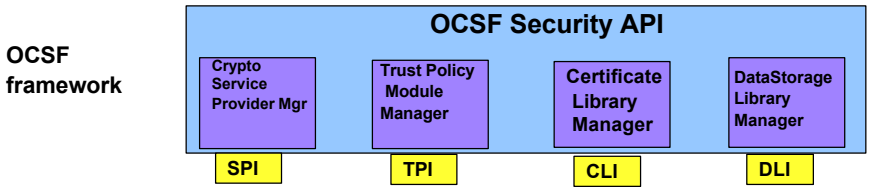
- Implements security protocols that are used by the application domain layer
  - software in this layer may implement cryptographic systems security services such as;
    - Secure Sockets Layer (SSL)
    - Internet Protocol Security (IPSEC)
    - Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - also includes tools and utilities for installing, configuring and maintaining the OCSF Framework and service provider modules



- The System Security Services layer is between the Application Domains layer and the OCSF Framework layer.

OCSF Framework

- **Central component of this architecture**
  - provides mechanisms to dynamically manage service provider modules
  - defines a common security application programming interface (API)
    - used to access services of service provider modules



IBM @server. For the next generation of e-business.

- OCSF Framework layer is the central component in the OCSF architecture; it integrates and manages all the security services.

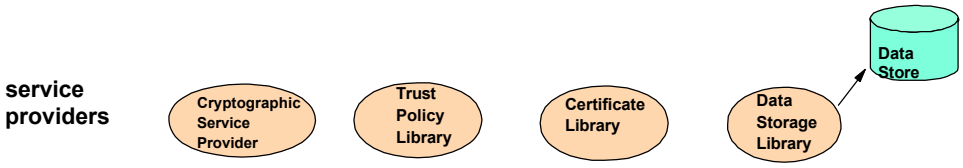
- Applications request security services through the OCSF security API or through system security services implemented in the System Security Services layer. The API supports the development of secure applications and system services and a service provider interface (SPI) that supports service provider modules that implement building blocks for secure operations.

- The OCSF API performs service operations that invoke security operations, such as encrypting data, adding a certificate to a Certificate Revocation List (CRL), or verifying that a certificate is trusted/authorized to perform some action.

- The primary function of this layer is to maintain a state regarding the connections between the application layer code and the service providers underneath.

Service Providers

- Perform the requested security services
- Several provided by IBM
- Additional modules may be available from other software and hardware vendors
- Applications may direct their request to any module that performs the required services



IBM @server. For the next generation of e-business.

- The OCSF Framework does not prescribe or implement any security service. Application specific security services are defined and implemented by service provider modules and layered services.

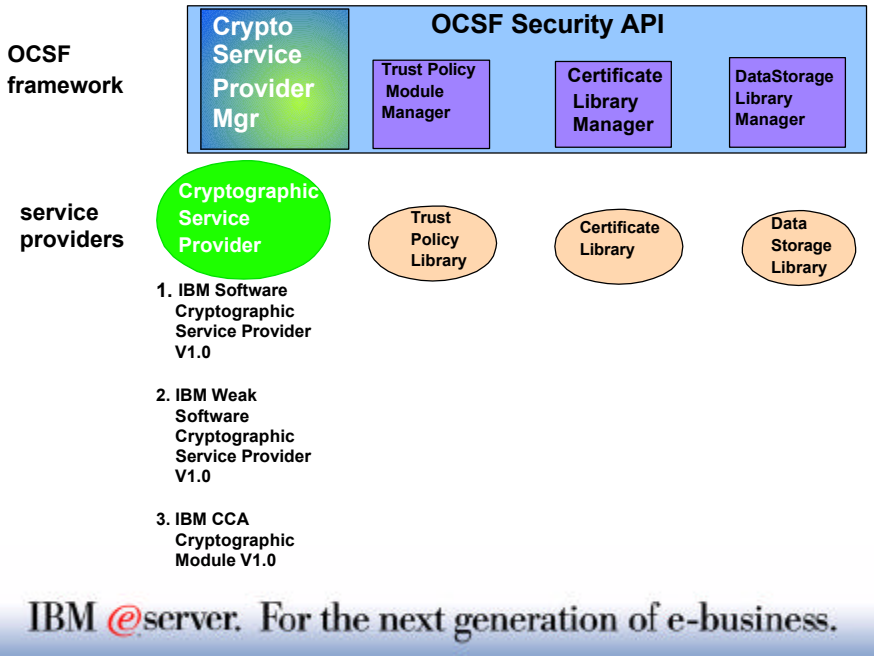
- OCSF defines a common API for accessing the services provided by service provider modules. OCSF redirects application API calls to the selected service provider modules that will perform the request.

- OCSF manages a registry that records the logical name of each service provider module that is installed on the system, information required to locate the service provider, and some data describing the algorithms implemented by the service provider.

- Before a service provider module can be used it must be installed in the OCSF by recording its services with the OCSF Framework.

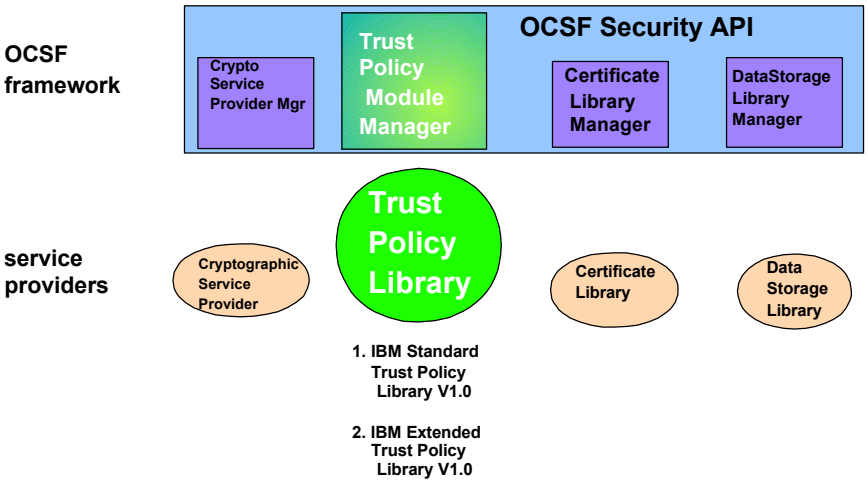
- Applications can query the OCSF Framework registry to obtain information on;
  > modules installed on the system
  > capabilities and functions implemented by those modules

Cryptographic Module



- The Cryptographic Module Manager administers the Cryptographic Service Providers (CSPs) modules and defines a common application programming interface (API) for accessing CSP modules. All cryptography functions are implemented by the CSPs.
- The security services SPI defined by this module are certificate-based.
- CSPs are modules equipped to perform cryptographic operations and to securely store private keys.
  Cryptographic services offered by OCSF are;
  > Bulk Encryption Algorithms
  > Digital Signature Algorithms
  > Cryptographic hash algorithm
  > Unique identification number
  > Random number generator
  > Secure key storage
  > Customer facilities unique to the CSP
- CSPs provide encrypted storage for private keys and variables, they must also deliver key management services.
- Portions of the IBM Software Cryptographic Service Provider and the IBM Weak Software Cryptographic Service Provider contains software code provided by RSA Data Security, Inc. Prior to marketing, selling or distributing applications developed by you, that use this module, you must obtain a license from RSA for that application.
- Option 1 allows you to use the encryption algorithms for Triple DES, DES, RC2, RC4 or RC5. For triple DES you must have OCSF Security Level 3 feature applied. Strength of the encryption algorithm depends on the OCSF Policy Modules and the OCSF feature installed. The Policy module defines the cryptographic algorithms and the associated strengths that can be used.
- Option 2 allows you to use the encryption algorithms for RC2, RC4 or RC5. The option only allows for 40 bit cryptographic strengths and 512 bits for RSA and DSA requests.
- Option 3 specifies that are you are using the z/OS hardware encryption and Integrated Cryptographic Service Facility.

Trust Policy Module



- The Trust Policy (TP) Module Manager administers the TP modules that may be installed on the local system and defines a common application programming interface (API) for these libraries.

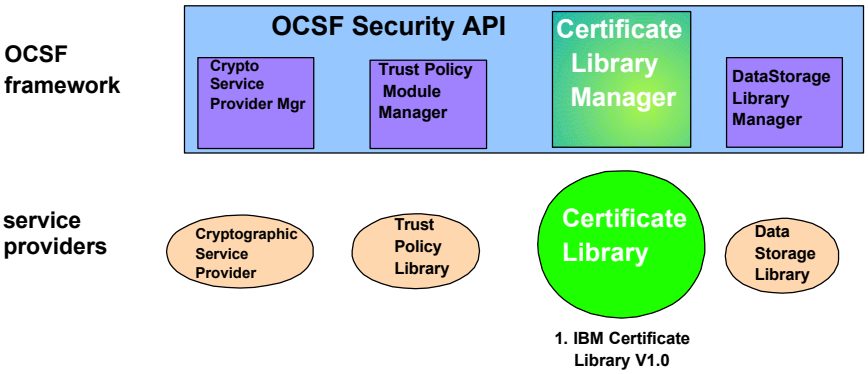
- The TP API allows applications to request security services that require policy review and approval as the first step in performing the operation. Operations include verifying trust in the following;
  > a certificate for signing or revoking another certificate
  > a user or user-agent to perform an application-specific action
  > the issuer of a Certificate Revocation List (CRL)

- The TP modules implement policies defined by a Certificate Authority. Policies define the level of trust required before certain action can be performed.

- Option 1 provides a service for verifying chains of X.509 certificates (version 3).

- Option 2 validates X.509 version 3 certificates and CRLs, using two types of

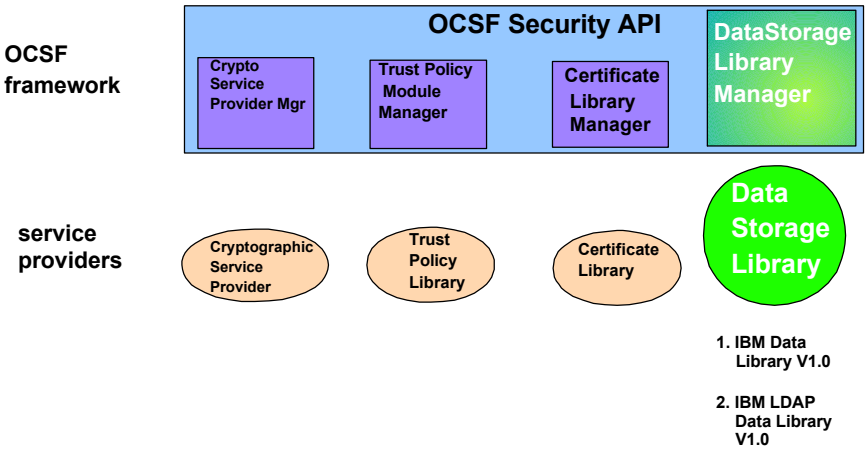
Certificate Library Module



IBM @server. For the next generation of e-business.

- The Certificate Library Module Manager administers the Certificate Libraries (CLs). It defines a common application programming interface (API) for these libraries.
- The API allows applications to manipulate memory-resident certificates and Certificate Revocation Lists (CRLs).
- This API operation includes;
  > creating new certificates and CRLs
  > signing existing certificates and existing CRLs
  > viewing certificates
  > verifying certificates and CRLs
  > extracting values (public keys) from certificates
  > importing/exporting certificates of other data formats
  > revoking certificates
  > reinstating revoked certificates
  > searching CRLs
  > providing pass-through for unique, format-specific certificate and CRL operations
- CL modules manipulate memory-resident certificates and CRLs.
- The IBM supplied module works with options 1 and 2 under the Cryptographic module and it performs X.509 version 3 certificate operations.

Data Library Module



IBM @server. For the next generation of e-business.

- The Data Storage Library Module Manager defines an application programming interface for secure, persistent storage of certificates and Certificate Revocation Lists. The API allows applications to search and select certificates and CRLs and to query information about each data store name, data of last modification, size, etc.

- API operations include;
  > adding new certificates and new CRLs
  > updating existing certificates
  > deleting certificates and CRLs
  > retrieving certificates and CRLs
  > pass-through for unique, module-specific operations

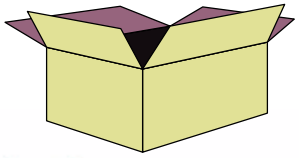
- Data Storage Library modules implement data store operations. It primary purpose is to provide secure, persistent storage, retrieval and recovery of certificates.

- Option 1 provides support for the persistence and retrieval of security-related objects to and from a flat-file database maintained in the local file system.

- Option 2 provides access to generic and security-related objects stored in LDAP-compliant directory server.

OCSF Packaging

- OCSF is part of z/OS 'Cryptographic Services' Element
  - FMID HCRY2A0 - OCSF base
  - FMID JCRY2A6 - OCSF Security Level 3
- C/C++ Compiler and runtime library is used to develop applications using OCSF
- RSA License Required for Production Use



IBM @server. For the next generation of e-business.

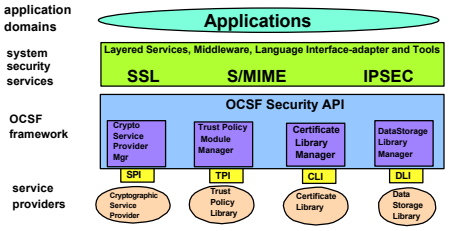
- As of OS/390 2.9 OCSF base and the OCSF Security level 3 are part of the OS/390 base system.
- NO RSA license is required for IBM License Manager, it is already been taken care of by IBM. However, when a customer is writing their own application they will need to obtain a license from RSA.

OCSF Setup

UNIX
HFS

2. **OCSF library authorizations**
- a. program control bits
- b. APF bits

RACF
DB



1. **Security Authorizations**
- a. program control
- b. access to OCSF datasets
- c. OCSF user IDs and permissions

3. **Installation Scripts**

4. **Verification procedures**

- OCSF installation requires some RACF definitions, OCSF library authorization in HFS and the running of installation scripts.

RACF Definitions

- **OCSF resources**
  - CDS.CSSM
    - authorizes the daemon to call OCSF services
  - CDS.CSSM.CRYPTO
    - authorizes the daemon to call a Cryptographic Service Provider (CSP)
  - CDS.CSSM.DATALIB
    - authorizes the daemon to call a Data Library (DL) Service Provider
- **Definitions**
  - define to RACF class FACILITY
  - grant READ authority to person installing OCSF & OCSF applications

Example:
```
RDEF FACILITY CDS.CSSM.CRYPTO
PE CDS.CSSM.CRYPTO CL(FACILITY) ID(ocsfinst) AC(READ)
SETR RACLIST(FACILITY) REFRESH
```


- These profiles must be defined before running any OCSF application or before running the OCSF installation script. If these profiles are not defined, the OCSF services are unavailable.

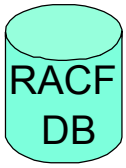
RACF Definitions ....

- **BPX.SERVER**
  - define to RACF class Facility if not already defined
  - user executing the installation scripts requires read access
  - daemon applications require read access

Example : **RDEF FACILITY BPX.SERVER**

PE BPX.SERVER CL(FACILITY) ID(*ocsfinst*) AC(READ)

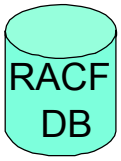
SETR RACLIST(FACILITY) REFRESH



- BPX.SERVER is used when you are using S/390 UNIX security. This profile controls the use of the OS/390 services used by OCSF to determine access authority. Applications using OCSF also require read authority.

RACF Definitions ....

- **Activate Program Control**
  - C/C++ Runtime libraries
  - Language environment libraries
  - SYS1.LINKLIB
  - OCSF data set - 'hlq.CRYPTO.SGSKLOAD'
  - ICSF libraries - if used - (not required by IBM License Manager)



Example :

```
SETR WHEN(PROGRAM)  - activate in RACF

RDEF PROGRAM *  ADDMEM('SYS1.LINKLIB'//NOPADCHK) UACC(READ)

RALT PROGRAM * ADDMEM('SYS1.CRYPTO.SGSKLOAD'//NOPADCHK)

SETR WHEN(PROGRAM) REFRESH
```

(* covers all modules in these dataset and places them under program control)

- BPX.SERVER is used when you are using S/390 UNIX security. This profile controls the use of the OS/390 services used by OCSF to determine access authority. Applications using OCSF also require read authority.

OCSF HFS Files

- **OCSF HFS files must be programmed controlled**
  - should already have proper attribute turned on
    - /usr/lpp/ocsf/lib
    - /usr/lpp/ocsf/ivp
    - /usr/lpp/ocsf/bin
    - /usr/lpp/ocsf/addins
- **APF authorization**
  - SMP/E installation of OCSF turns on this attribute

OCSF HFS Files ...

- **Authorization**
  - to view program control and APF bit in HFS user must have access to BPX.FILEATTR.PROGCT

    Example:

    ```
    RDEF FACILITY BPX.FILEATTR.PROGCT
    PE BPX.FILEATTR.PROGCT CL(FACILITY) ID(ocsfinst) ac(read)
    SETR RACLIST(FACILITY) REFRESH
    ```

  - list OCSF libraries and check for program control bit and APF bit
    - **cd /usr/lpp/ocsf/lib**

      ls -E

      -rwxr-xr-x aps- 2 OMVSKERN OMVSGRP 462848 Jul 16 2000 ibmcca.so

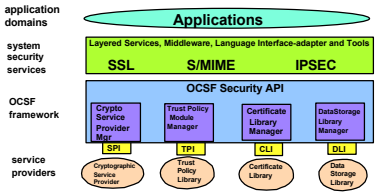
      -rwxr-xr-x aps- 2 OMVSKERN OMVSGRP 598016 Jul 16 2000 ibmcl.so
  - set bits if not present
    - **extattr +p ibmcca.so** or **extattr +a ibmccs.so**

IBM @server. For the next generation of e-business.

- Even though these modules should already have the program control and APF attribute set you should still check them to make sure.
- The AP bits in the second column indicates that the APR bit and the PROGRAM CONTROL bit are turned on. If it was not present then you must set it.

OCSF Scripts

- **Run the OCSF installation script**
  - required for every release of OS/390 and z/OS
  - change to directory /usr/lpp/ocsf/bin
  - run script ocsf_install_crypto
- **Run OCSF verification procedures**
  - change to directory /usr/lpp/ocsf/ivp
  - run ocsf_baseivp
- **Verify correct policy table files are being used**
  - /usr/lpp/ocsf/lib/cssmmanp.dll and /usr/opp/ocsf/lib/cssmusep.dll
    - point to cssmmanp_sl2 and cssmusep_sl2.dll if only OCSF based is used
    - when Security Level 3 is used files should point to cssmmanp_sl3.dll and cssmusep_sl3.dll



- Installation is complete when both scripts run successfully.
- Scripts should be run from a userid with a UID of 0 to ensure you have access to necessary directories.
- Userid running the scripts must have access to the CDS.* profiles and BPX.SERVER
- **NOTE:** Users installing using ServerPac (Full System Replace) path or SystemPac do not need to execute these scripts.

  Customers installing from CBPDO, including those using the Upgrade Package, must run the installation script and the IVP.

Reference

- Open Cryptographic Service Facility Application Developer's Guide and Reference (SG24-5875)
- Common Data Security Architecture standard (http://www.opengroup.org/onlinepubs/009608599/front.htm)