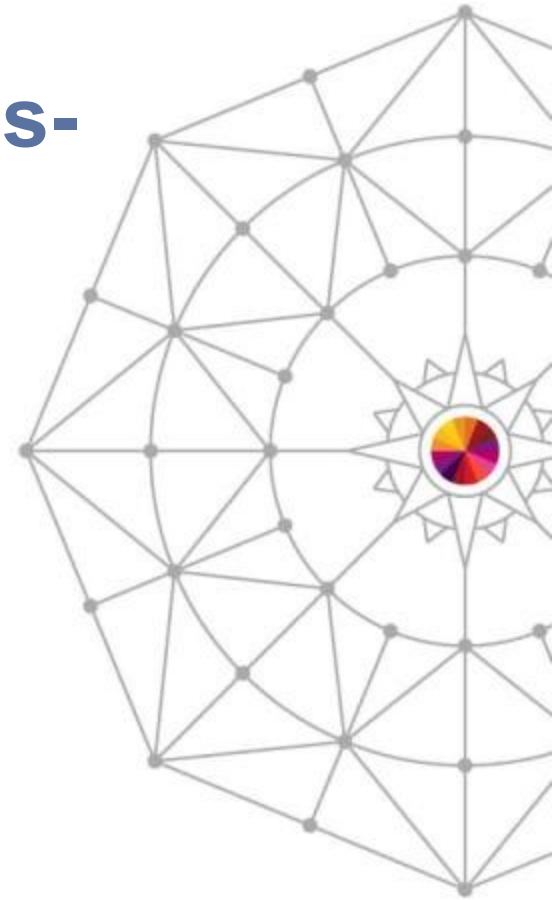
#SHAREorg

SHARE

Sharing Secrets using Encryption Facility - Hands-on Lab

Steven R. Hart
IBM

March 12, 2014
Session Number 14963



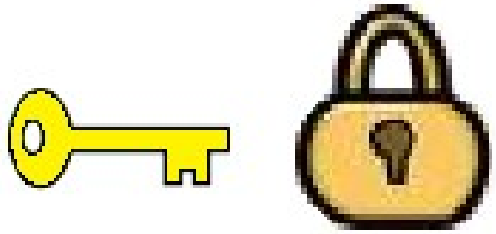
SHARE in Anaheim

Copyright (c) 2014 by SHARE Inc. Except where otherwise noted, this work is licensed under http://creativecommons.org/licenses/by-nc-sa/3.0/

Encryption Facility for z/OS

- Encryption Facility for z/OS is a host based software solution for data encryption

- Encryption Facility for z/OS provides services for:
  - public-key based encryption
  - passphrase-based encryption
  - modification detection of encrypted data
  - data compression
  - importing and exporting of OpenPGP certificates
    - binary or ASCII armor format
  - digital signatures of data



Complete your session evaluations online at www.SHARE.org/AnaheimEval

Encryption Facility for z/OS continued

- Encryption Facility encrypts sensitive data for secure archival and business partner exchange using either a public key or passphrase
- Encrypted data is written to disk or other removable media
- Data can be encrypted in binary or text mode format.
  - Text mode translates the input data to UTF-8 or a local code page.
- Separately licensed product that does NOT come with ICSF or the z/OS base
- Option between 2 encrypted message formats
  - IBM Proprietary Encrypted Message format
    - Provides high performance for z to z encrypted data exchange
  - OpenPGP Message format
    - Provides compatibility between z and distributed systems for encrypted data exchange

Complete your session evaluations online at www.SHARE.org/AnaheimEval

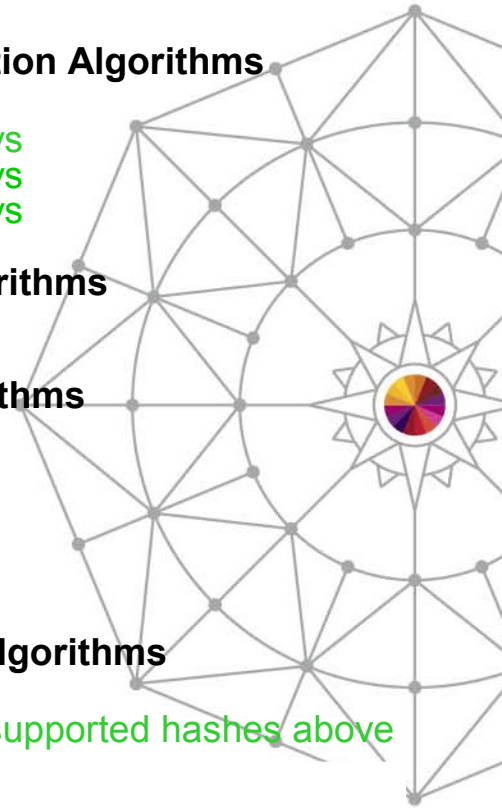
EF OpenPGP Support

- OpenPGP is a widely accepted, open standard for handling encryption of data files and messages
  - OpenPGP is a file format for exchanging encrypted data. It is not an encryption algorithm.
  - OpenPGP is standardized in IETF and has been adopted as the format for encrypted files by a wide-range of open-source and commercial products
  - OpenPGP does not define how encryption keys should be managed
  - OpenPGP allows a wide range of choices for key exchange and trust model
  - OpenPGP provides additional flexibility and interoperability for tape exchanges with external business partners and vendors
  - OpenPGP allows customers to exchange an encrypted, compressed, and/or digitally signed file with business partners who have an installed OpenPGP client running on z/OS and other operating systems

Complete your session evaluations online at www.SHARE.org/AnaheimEval

EF OpenPGP Support continued

- Provides at a minimum, support for all Mandatory/Must Do's identified in the OpenPGP standard (RFC 4880).
- This includes support for the following:
  - **Public key encryption of session key**
  - **Passphrase base encryption of session key**
    - string-2-key specification completed implemented
  - **Digital signatures of data**
  - **Compression of data**
  - **Importing/exporting OpenPGP certificates**
  - **RSA, ElGamal, and DSA key generation**
  - **Use of partial data packets**
  - **ASCII Armor for OpenPGP certificates**
  - **Asymmetric Encryption Algorithms**
    - RSA
    - ElGamal
  - **Symmetric Encryption Algorithms**
    - Triple DES
    - AES 128 bit keys
    - AES 192 bit keys
    - AES 256 bit keys
    - Blowfish
  - **Compression Algorithms**
    - ZIP
    - ZLIB
  - **Digest/Hash Algorithms**
    - SHA-1
    - MD5
    - MD2
    - SHA-256
    - SHA-384
    - SHA-512
  - **Digital Signature Algorithms**
    - DSA w/ SHA1
    - RSA w/ all the supported hashes above



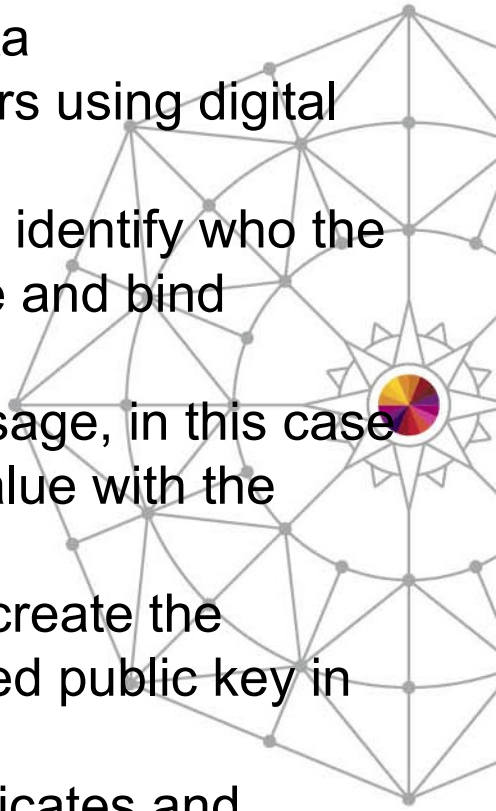
Legend/Notes:

GREEN: Functions that can use ICSF/H/W crypto. H/W crypto requires the correct environment and require a Crypto module to be installed.

Complete your session evaluations online at www.SHARE.org/AnaheimEval

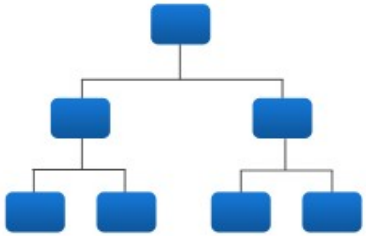
Digital Certificates

- Encryption Facility can use public-keys to encrypt data
- Public-keys are exchanged between business partners using digital certificates
- Digital certificates contain a public key, information to identify who the key belongs to, and a digital signature to authenticate and bind together the public key with the identity information.
- Digital Signatures are made by taking a hash of message, in this case the digital certificate, and then encrypting the hash value with the signers private key.
- Only the signer has the private key that was used to create the signature. Business partners must have the associated public key in order to verify the signature.
- Encryption Facility can be used with both X.509 certificates and OpenPGP Certificates.



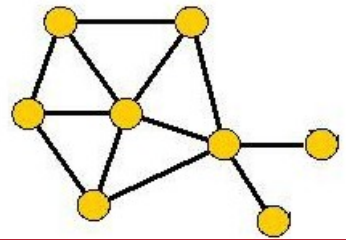
Complete your session evaluations online at www.SHARE.org/AnaheimEval

X.509 vs. OpenPGP Certificates



- X.509 uses a hierarchical authentication model
  - Each X.509 certificate contains 1 digital signature, either self signed or signed by a CA
  - A root Certificate Authority (CA) is established and trusted as a self signed certificate
  - Other certificates are signed by a CA within the hierarchy

- OpenPGP uses a decentralized authentication model
  - Each OpenPGP certificate can be self signed and can contain multiple signatures from other keys
  - OpenPGP sub-keys are all signed by the Primary key to bind together the Primary and sub-keys
  - Encryption Facility for z/OS provides an option to sign your OpenPGP certificates with a CA.



Complete your session evaluations online at www.SHARE.org/AnaheimEval

EF configured with ICSF and RACF

- EF configured with ICSF
  - When configured with ICSF, EF can generate new RSA key pairs in ICSFs PKDS
  - EF can also use pre-existing RSA key pairs in ICSF PKDS
  - EF can use and generate clear keys and secure keys (with the use of cryptographic coprocessors) in ICSFs PKDS
- EF configured with RACF
  - EF can use pre-existing RSA key pairs connected to a RACF Keyring
  - RACDCERT must be used to generate the RSA key pairs as EF only has read access of RACF keyrings
- EF configured with RACF and ICSF
  - EF can use pre-existing RSA key pairs connected to a RACF Keyring that point to private keys protected in ICSFs PKDS
  - RACDCERT must be used to generate the RSA key pairs as EF only has read access of RACF keyrings

Complete your session evaluations online at www.SHARE.org/AnaheimEval

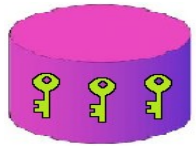
EF configured without ICSF and RACF

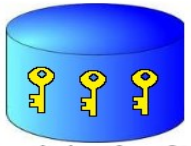
- EF configured without ICSF and RACF
  - When not configured with ICSF and RACF, EF can use the Java Cryptographic Extension (JCE) and a Java keystore within Unix System Services to perform software based cryptography.

Complete your session evaluations online at www.SHARE.org/AnaheimEval

Key Management with EF

- OpenPGP keyring
  - Stores OpenPGP certificates containing public keys
  - Resides in the Unix System Services file system
- Native Key store
  - Stores X.509 certificates, public keys and private keys



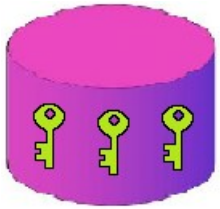


z/OS	Java Keystore (JCEKS)	RACF Keyring (JCERACFKS)	ICSF PKDS (JCECCAKS)	RACF and ICSF (JCECCARACFKS)
Hardware Cryptography			✓	✓
Integration with existing audit and access control		✓	✓	✓
Password Protected	✓		✓	

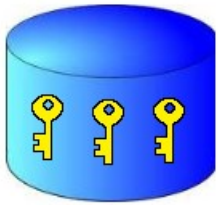
Complete your session evaluations online at www.SHARE.org/AnaheimEval

Exchanging Encrypted Data

z/OS



OpenPGP Keyring contains public keys



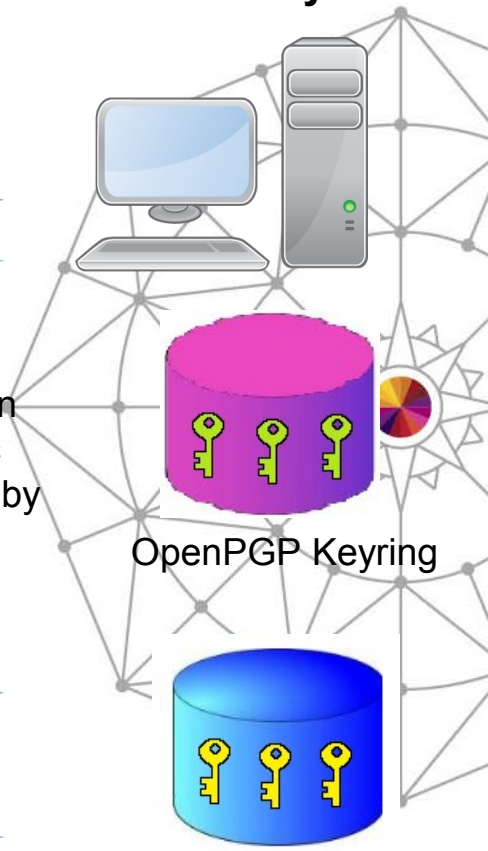
Private keys are in the local keystore (ICSF, RACF, JCEKS)

Either public keys, via digital certificates, or a passphrase is exchanged between business partners.

Each side can then encrypt data using their business partners public key or the passphrase. A symmetric session key is actually used to encrypt the data. When using public keys, the session key is randomly generated and wrapped by each public key separately. When using passphrase, the passphrase is used to generate the session key using an S2K algorithm.

Each side can now send their partner encrypted data.

z/OS or Distributed System



OpenPGP Keyring

Private keystore

Complete your session evaluations online at www.SHARE.org/AnaheimEval

Recent Enhancements

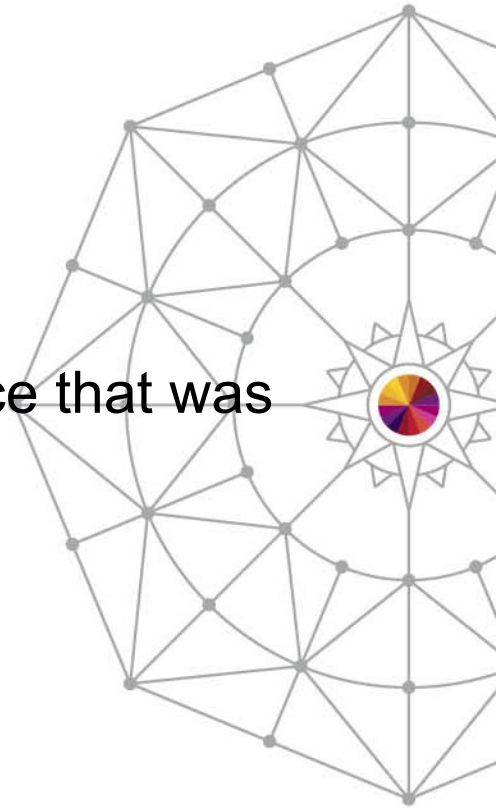
- RFC 4880 Compatibility
- Speculative Key ID Support
- Batch Key Generation and Batch Public Key Export
- Symmetrically Encrypted Integrity Protected Data Packet
- Notation Data Sub-packets containing raw binary data
- IBM 31-bit SDK for z/OS, Java Technology Edition, Version 7
- zEnterprise Data Compression (zEDC) Support

Complete your session evaluations online at www.SHARE.org/AnaheimEval

Latest Level of EF Service

- The latest level of EF service contains:
  - all enhancements listed in the previous slide
  - all fixes that have been delivered in APARs
  - supersedes all previous levels of EF

- All EF customers should apply this level of service that was made generally available February 3, 2014:
  - **APAR OA43923 / PTF UA72268**



Complete your session evaluations online at www.SHARE.org/AnaheimEval

EF OpenPGP Command Syntax

All Encryption Facility for OpenPGP commands have the following syntax. **-homedir** must appear before all the options, all the options must appear before the commands, and the commands must appear before the arguments.

java -jar CSDEncryptionFacility.jar [-homedir name] [options] commands [args]

where:

- **homedir** name is the name of the directory that contains the configuration file ibmef.config that contains specified options to use with the command.
- **options** is the name of one or more options to use on the command line and always starts with -. These option values override values in the configuration file.
- **commands** is the name of one or more commands and always starts with -.
- **arguments** specifies one or more targets of the command, for example, file name, certificate, alias, and so forth.

Complete your session evaluations online at www.SHARE.org/AnaheimEval

Reference

- Encryption Facility for z/OS V1.2 User's Guide
  http://publibz.boulder.ibm.com/epubs/pdf/csdd1125.pdf

- Encryption Facility for OpenPGP zEnterprise Data Compression (zEDC) Support - APAR OA43869

ftp://public.dhe.ibm.com/eserver/zseries/zos/ef/pdf/OA43869.pdf

- Encryption Facility for z/OS web page

http://www-03.ibm.com/systems/z/os/zos/tools/encryption_facility/

Complete your session evaluations online at www.SHARE.org/AnaheimEval