Mastering Digital Certificates: The Keys for Creating a Streamlined Experience

BC125

Jan Prihoda Product Owner, Broadcom

Chip Mason Product Manager, Broadcom

Mastering Digital Certificates: The Keys for Creating a Streamlined Experience

Creating and managing certificates for z/OS can be daunting, with missteps leading to delayed deployments, unplanned outages and unnecessary complexity for administrators. In this session we'll explore the key concepts and discuss strategies and best practices for simplifying certificates. We'll also introduce a new toolkit designed to streamline the initial certificate experience when installing mainframe software.

UNDERSTANDING CERTIFICATES

Digital certificates establish privacy and foster trust

A digital certificate is a set of electronic credentials for

- **Authentication**: Verifies the identity of the certificate holder
- **Encryption**: Secures communication by encrypting data
- **Non-Repudiation**: Provides evidence that a transaction occurred
- **Trust**: Establishes trust between parties in online interactions

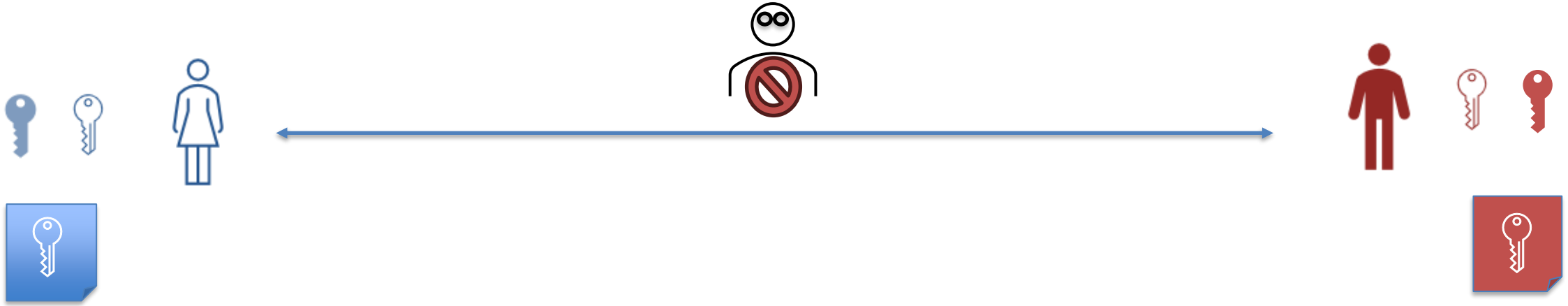
A **digital cert** contains a **public key** and is tied to a **private key** that is kept secret

Digital Certificates Are Encrypted Files

- Part of Public Key Infrastructure (PKI), they provide a method for sharing a public key and validating the issuer.
- Used for encryption, verification, and proof of origin, and to prevent tampering.
- An encrypted file that contains details on the service using the certificate, the issuer as well as the validating parties, provided in a ‘chain of trust’.
- The certificate must be defined appropriately for its use: A signing certificate can not be used as a TLS certificate, as it not valid for that use. A certificate for one website can not be used for another website*

Public Key Infrastructure Ensures Trust Everywhere

- Challenge: You need to communicate with someone who is remote, but you want to make sure that the person you are communicating with is really that person.



- PKI: Private Key/Public Key pair:
  - Share the Public Key, Hold the Private Key
  - Encrypt a file with the Public Key, and only the Private Key can unencrypt: RSA
  - Only person who can decrypt is my target

BUT, How do I TRUST its really you?

CA Certificate Authority – ID Card Issuer of Internet

- Certificate Authorities are like the ID card issuers of the Internet
  - We trust State DMV/ US State Dept that ID is authentic.
  - Browsers trust most external CAs

Bills
Tax Record
SSN
Other ID

Proof of Identity

URL
Domain
Corp Records
Email

Broadcom, Inc.

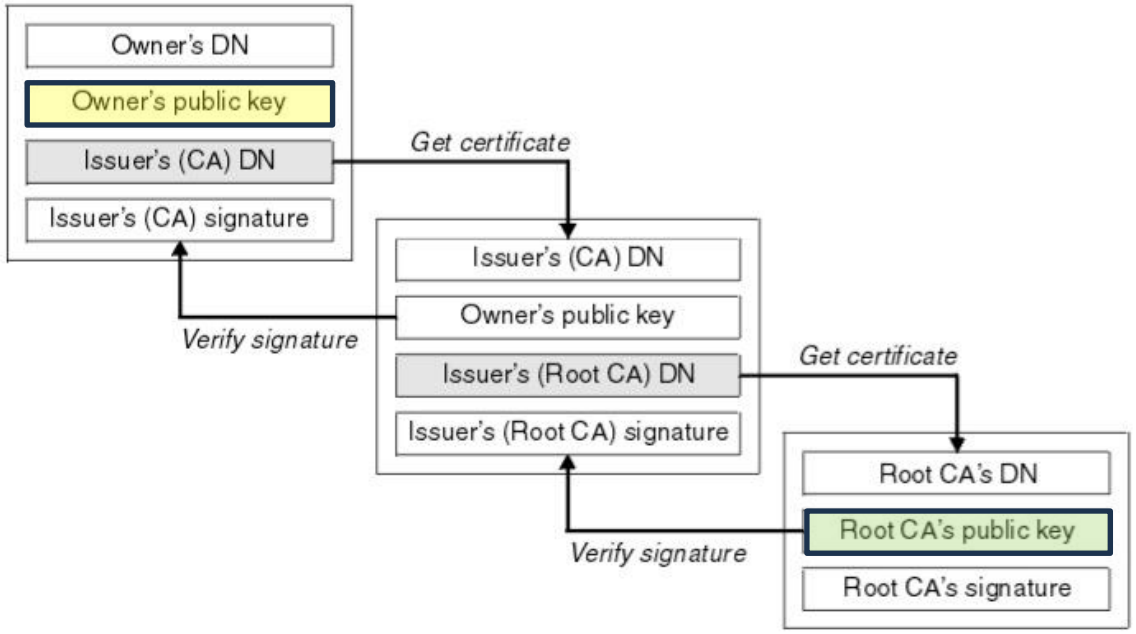
Certificate Authorities

- Let's Encrypt
- GlobalSign
- Comodo
- Sectigo
- GoDaddy
- Digicert
- VeriSign
- Etc.

Certificate

www.broadcom.com

Trust is established via the “Chain of Trust”



End Entity Certificate

(Leaf)

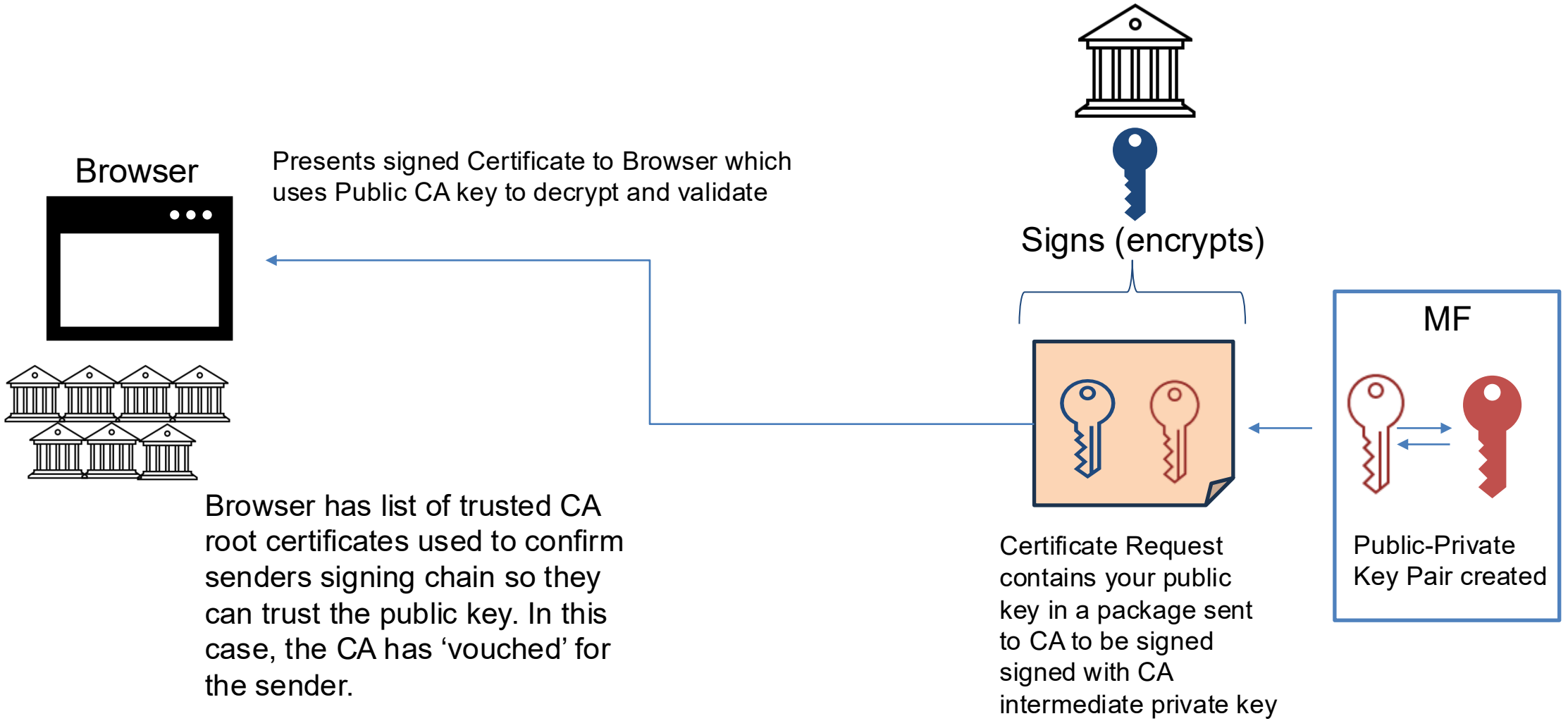
Intermediate Certificate
(often created by CA)

Root Certificate

Why is the chain important?

- The chain of trust proves how you are trusted through others, down to a issuer that is trusted (usually the CA).
  - This is accomplished by a Root Certificate that is trusted and intermediate certificates to verify the trust relationship.
- The client certificate requires the chain to be available to validate authenticity.
- A CA Root private key is used to create an Intermediate which is used to sign all CA certs, then it can be stored away. Lose the Private Key and you do not know which certs are trusted.
- All private keys should be stored in highest security possible, ICSF on mainframe.

A CA is critical to most TLS Certificates



CERTIFICATES ARE A CHALLENGE, ESPECIALLY IN MAINFRAME

Certificate Creation: Many Opportunities to get it Wrong

SSL Certificates

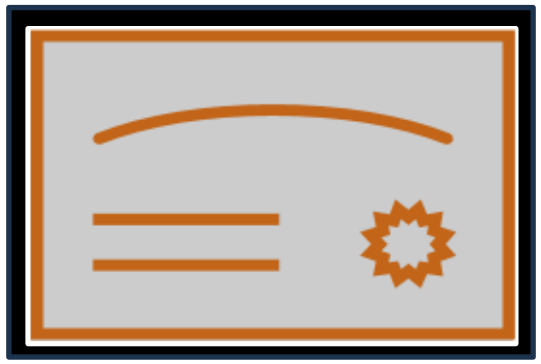
Details

- Certificate Label
- Certificate Owner
- Certificate type
  - Site
  - CertAuth
  - USERID
  - Server
  - Client
  - Signing
- Key Usage
  - Handshake
  - Certsign
  - Dataencrypt
  - Docsign
- Key Type
  - DSA
  - RSA
  - NISTECC
  - BPECC
- Key Size
  - 1024
  - 2048
  - 4096
- Extended Key Usage
  - Client authentication
  - Email protection
  - Encrypting file system
  - File recovery
  - IP security user
  - IPSec IKE
  - IPSec IKE-Intermediate
  - Server authentication
  - Signing KDC responses
  - Smart card logo
- Active Date
- Expiration Date
- Trust
- PKCS Package name

Keystore

- Location
  - Keyring
  - Keystore
- Owner
  - UserID
- ICSF
  - No
  - Yes

Certificate



Subject Name

- Subject CN
- Subject Title
- Subject Organization
- Subject Unit
- Subject City
- Subject State
- Subject Country

Certificate Artifacts

- Package Type
  - PKCS 12
  - PKCS 7
- Certificate Components
  - Root Certificate
  - Intermediate Certificates
  - End Entity Certificate
- Cert Usage
  - SSL/TLS
  - mTLS
  - HTTPS
  - S/MIME
  - POP
  - IMAP
  - LDAP
  - Smart Cards
  - TPM

Subject Alternate Names

- Domains
  - List
- Email addresses
  - List
- IP Addresses
  - List
- URLs
  - List

Manual Certificate Management on the mainframe can be a challenge

```
//ACFBATCH EXEC PGM=ACFBATCH
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
* GENCERT CA Certificate *
GENCERT CERTAUTH.TOMCAT SUBJSDN(CN='TOMCAT-CA-ACF-CERT') -
 LABEL(TOMCAT CA CERT)
* GENCERT Personal Certificate *
GENCERT CEMETOM.srvcert SIGNWITH(CERTAUTH.TOMCAT) -
 SUBJSDN(CN='TOMCAT-SERVER-ACF-CERT') LABEL(TOMUSER CERT) -
 ALTNAME(DOMAIN=SYSTEST.NYC.CORPACOM.NET)
* CHKCERT CHAIN *
CHKCERT CEMETOM.srvcert CHAIN
* CREATE Keyring *
SET PROFILE(USER) DIVISION(KEYRING)
INSERT CEMETOM.RING RINGNAME(TOMCAT)
* CONNECT CA Certificate *
CONNECT CERTDATA(CERTAUTH.TOMCAT) KEYRING(CEMETOM.RING)
* CONNECT Personal Certificate *
CONNECT CERTDATA(CEMETOM.srvcert) KEYRING(CEMETOM.RING) -
 USAGE(PERSONAL) DEFAULT
* LIST KEYRING *
LIST CEMETOM.RING
* EXPORT CA Certificate for deployment *
EXPORT CERTAUTH.TOMCAT DSN('SECMF.CERTAUTH.TOMCAT.EXPORT') FORMAT(CERTB64)
```

Broadcom Education Offerings

Digital Certificates All Roles Learning Path

06SEC001LP

- Digital Certificates Overview 100
- Client Server Certificate Configuration and Authentication 200
- Keyring and Certificates Security 200
- Debugging - SSL Keyring/Certificate Problems 200
- Internal Certificate Authority 200
- External Certificate Authority 200
- SMP/E Internet Service Retrieval Configuration 200

Understanding a few key Certificate concepts can reduce confusion

- **Internal/Self-Signed:** You sign it with your own key (Usually a test system)
  - In some instances, you act as your own CA (challenge with browser)
- **CA (external) Signed*:** Certificate Authority signs
  - Resolves public key distribution and ensures trust
- **Keyring:** Certificate storage and sharing within the ESM
  - Connecting keyrings = sharing
- **CSR:** Certificate Signing Request: a temp certificate sent to the CA for external signing with all the details needed to get an external certificate signed

Avoid these Common Certificate Creation Challenges

- **Common Name** (aka Subject CN):
  - Not a URL, it should be your server host name (www.example.com or test.example.com)
  - The CN in the certificate MUST match the host name you wish to protect, or it will fail
- **Subject Alternative Name:**
  - This is where you put in the IP address as well as the CN
- **Key Usage:**
  - HANDSHAKE is needed for TLS Certificates. CERTSIGN is reserved for certs used to sign other certificates such as ROOT CA.
- **Missing Intermediate Certificates:**
  - Be sure to add all certificates in the chain to the ESM. CA's provide certificates individually so be sure to download all. Best bet: Always choose a package for download
- **KEYRING:**
  - Ensure that KEYRINGS containing all the certificates needed by applications are connected. Connecting a KEYRING allows access to those certificates and keys.

Many Mainframe solutions require certs to encrypt communications

If you see a padlock symbol, a digital cert is encrypting web communications (TLS encryption)

Some of the Broadcom Solutions needing Certificates

AIOps
- CA-7
- ESP
- JCLCheck
- MICS
- MOI
- NetMaster
- OPS/MVS
- SYSVIEW
- Topology
- WatchTower (Alert Insights)
- WatchTower (Data Insights)
- Watchtower (Metric Catalog)

Security
- Compliance Event Manager
- Security Insights

DM
- Datacom
- Db2 Tools
- IDMS

DevOps
- Endevor
- File Master Plus
- InterTest
- MAT
- SymDump
- Test4z

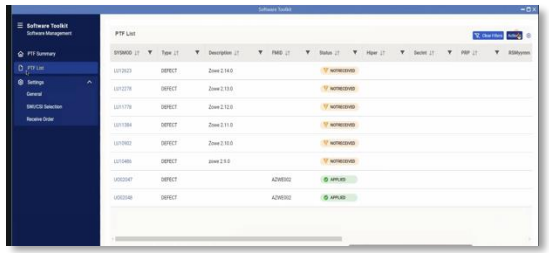
Foundation & Open
- API State Monitor

Not just for Zowe APIs, but also anything with web UI (Tomcat)

Broadcom is simplifying certificates creation as solutions utilize more certificates

- Broadcom provides zOSMF Workflows and Packages for simpler Product Install/Configuration.
- We now offer simple creation and configuration of Zowe and Broadcom Product Digital Certificates to the zOSMF experience

Project
Certificate Toolkit Plug in for zOS



zOSMF Plug-in that will automatically build digital certificates required for Broadcom Product install to reduce errors and speed deployments and upgrades of Broadcom solutions.

Our Goal:

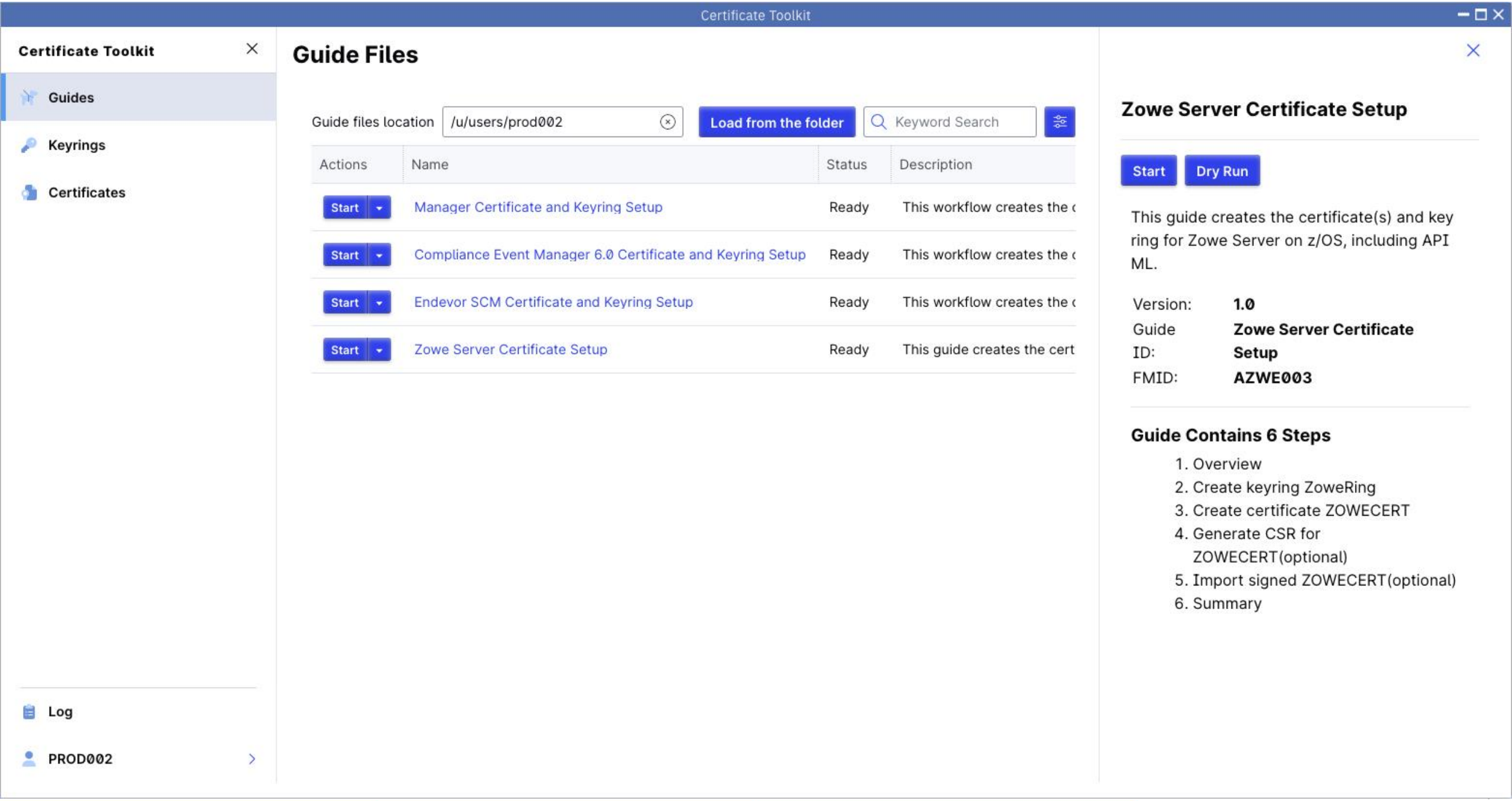
Ease product install and upgrades with pre-configured certificate creation tool for Zowe and Broadcom solutions

CERTIFICATE TOOLKIT PLUGIN FOR Z/OSMF DEMO

Project Certificate Toolkit

- Mission: To streamline certificate infrastructure creation for REST API enabled products and simplify its troubleshooting

- Available as Mainframe Essential component for all Broadcom customers


Certificate Toolkit
Certificate Toolkit
Guides
Keyrings
Certificates
Log
PROD002
Guide Files
Guide files location
/u/users/prod002
Load from the folder
Keyword Search
Actions
Name
Status
Description
Start
Manager Certificate and Keyring Setup
Ready
This workflow creates the
Start
Compliance Event Manager 6.0 Certificate and Keyring Setup
Ready
This workflow creates the
Start
Endevor SCM Certificate and Keyring Setup
Ready
This workflow creates the
Start
Zowe Server Certificate Setup
Ready
This guide creates the cert
Zowe Server Certificate Setup
Start
Dry Run
This guide creates the certificate(s) and key ring for Zowe Server on z/OS, including API ML.
Version: 1.0
Guide ID: Zowe Server Certificate Setup
FMID: AZWE003
Guide Contains 6 Steps
1. Overview
2. Create keyring ZoweRing
3. Create certificate ZOWECERT
4. Generate CSR for ZOWECERT(optional)
5. Import signed ZOWECERT(optional)
6. Summary

QUESTIONS?

Join a Mainframe Technical Exchange

SHARE
EDUCATE • NETWORK • INFLUENCE

Apr. 21-23, 2026	June 23-25, 2026	Oct. 20-22, 2026
European MTE Prague, Czech Republic	Virtual MTE Held Virtually	North American MTE Plano, TX

- Network with peers and Mainframe technical experts
- Participate in technical how-to sessions and hands-on workshops
- No registration fee!

Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation

THANK YOU