



# Mastering Digital Certificates: The Keys for Creating a Streamlined Experience

Kranthi Kumar Vemula

Product Owner

Cybersecurity & Compliance

**Broadcom**



# Disclaimer

- Certain information in this presentation may outline Broadcom's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of Broadcom or its licensees under any existing or future license agreement or services agreement relating to any Broadcom software product; or (ii) amend any product documentation or specifications for any Broadcom software product. This presentation is based on current information and resource allocations as of September 10, 2024, and is **subject to change or withdrawal by Broadcom at any time without notice. The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion.**
- Notwithstanding anything in this presentation to the contrary, upon the general availability of any future Broadcom product release referenced in this presentation, Broadcom may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to Broadcom maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.
- Broadcom may use any feedback provided by you related to a Broadcom product or this presentation for any Broadcom business purposes (including but not limited to, preparation, reproduction, and distribution of derivative works based upon such feedback), without any obligation to you including consent or payment.
- Copyright © 2024 Broadcom. All rights reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom.
- **THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY.** Broadcom assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Broadcom be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if Broadcom is expressly advised in advance of the possibility of such damages.





What if the DBA on call  
gets an alert at 2 AM that

**DB2 connections are refused**  
by all remote clients?

DB2 is up, the LPAR is healthy, and the CPU usage is low. But all Java applications connecting via JDBC is failing with a **'Connection Refused'** error. **The culprit?**





Your auditor in your next audit asks you

**'Show me every certificate connected to this DB2 subsystem, when it expires, and who owns the renewal.'**

PCI-DSS, HIPAA, and EU DORA now have 'Certificate' language. Your next auditor will speak it fluently.

**Will you?**



# What is a Digital Certificate?



# 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:** Proof of integrity and origin of data

---

**Trust:** Establishes trust between parties in online interactions

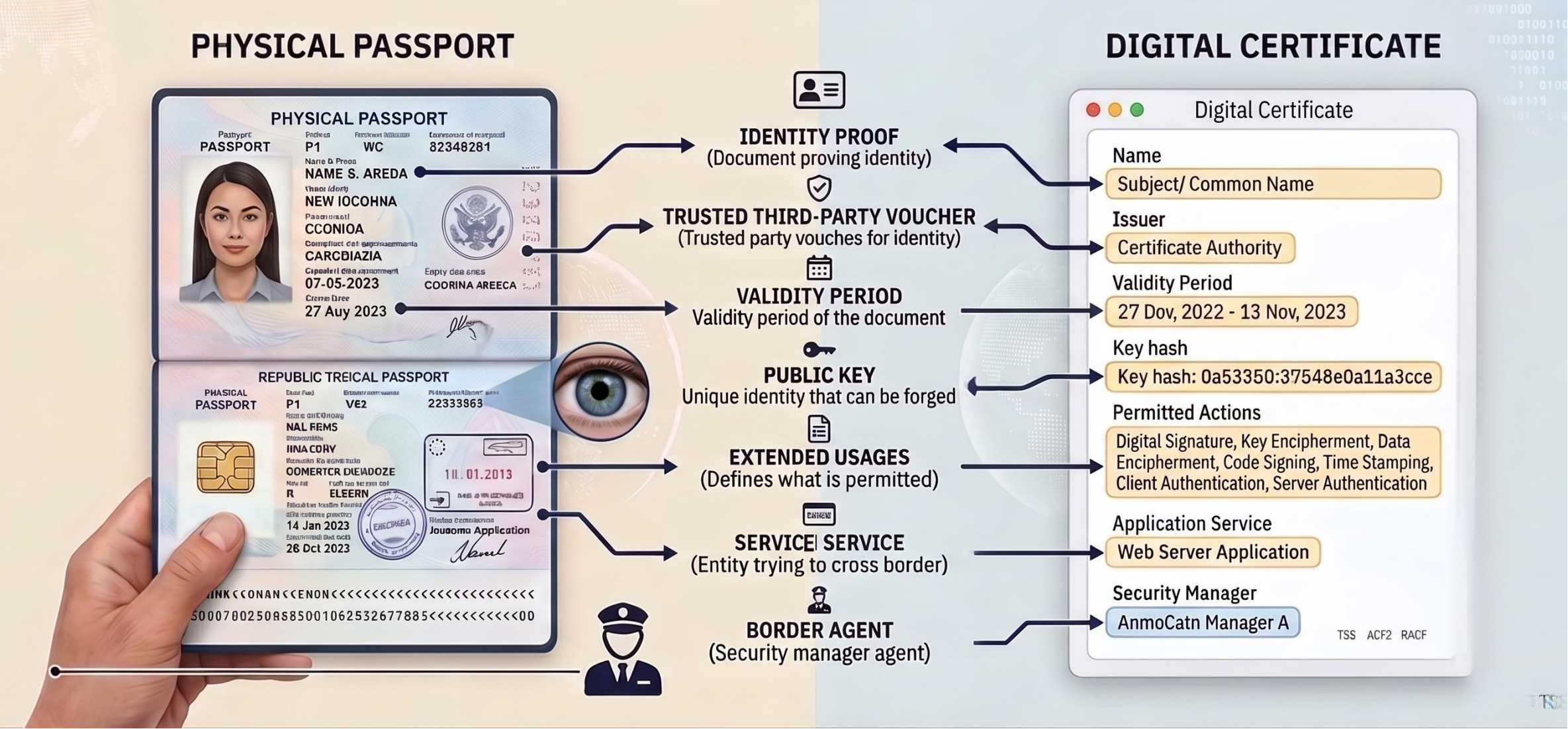
---

A **digital certificate** is a file that contains a **public key** and is tied to a **private key** that is kept secret.

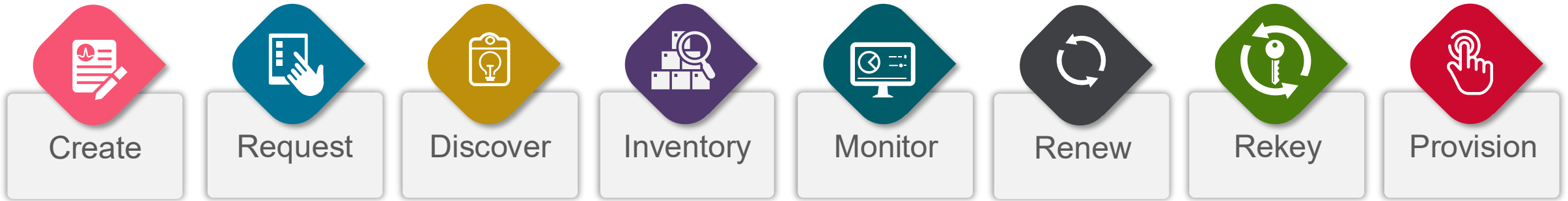
Our customers have **100 – 1,000+ certs per mainframe**. A single error can cause an outage.



# Digital Certificate and Passport - An Analogy



# Digital Certificate and its eight essential phases





How many  
Certificates  
do you think are  
stored on your laptop?

**Any Guesses?**

# Digital Certificates have a massive impact on organizations

**114K+**

Avg. internal certificates managed

The scale of digital certificates is massive.

**53%**

still rely on manual process

**60%**

experienced exploits due to weak cryptography

Weak cryptography and possibility of exploits

**55%**

Struggle to keep up with the growing volume

**79%**

anticipate a spike in machine identities

Anticipated spike in the certificates' footprint

**~4 hrs**

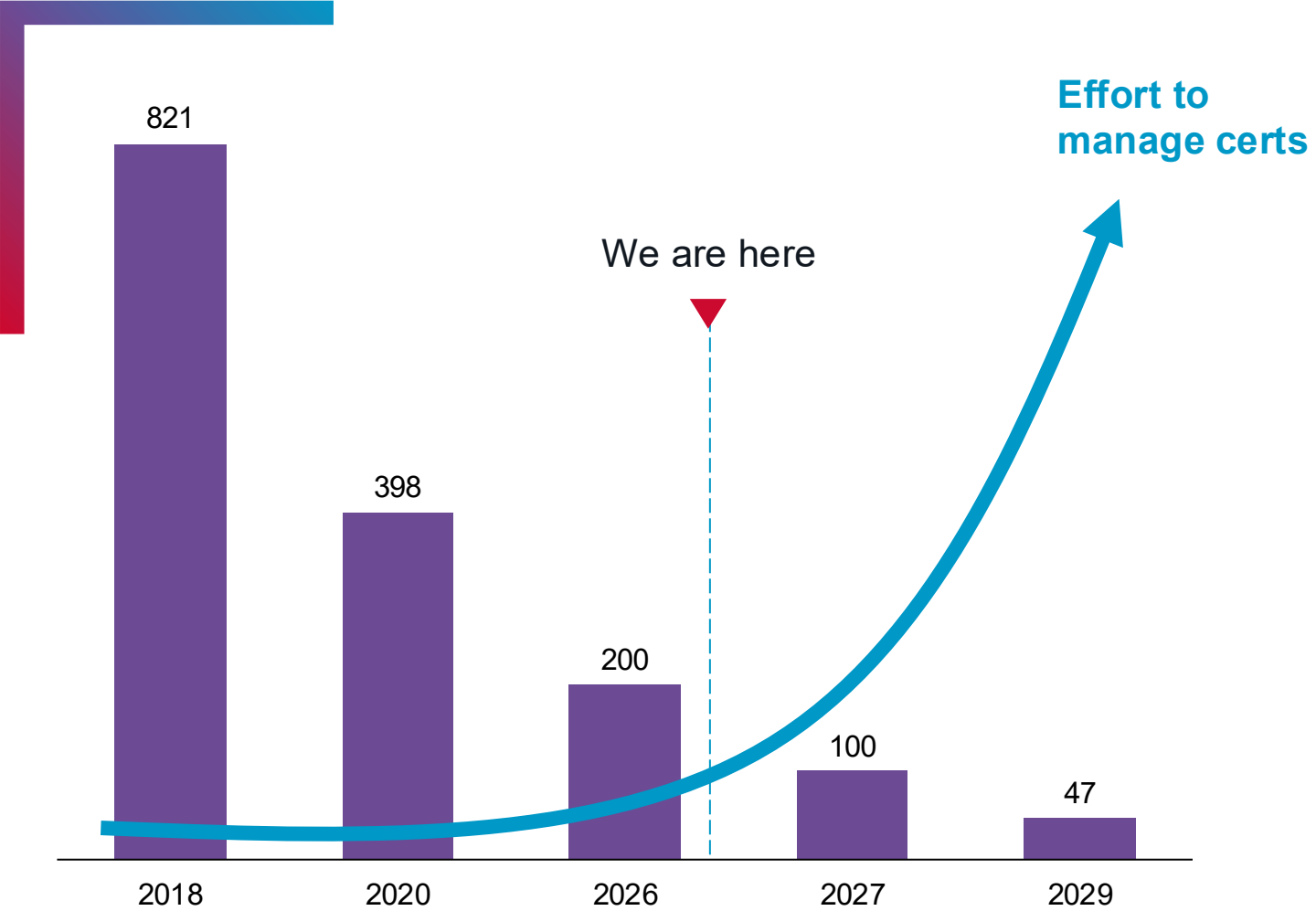
Avg. time it takes to identify, remediate and recover

Significant downtime resulting in substantial losses.

- Jan 2026 research by Poneman Institute & CyberArk based in insights from nearly **2,000 global IT and security practitioners**
- 2025 State of Machine Identity Security Report by CyberArk
- State of Machine Identity Management 2023 research by Ponemon Institute and Keyfactor



# Decreasing Certificate Lifespans are a Ticking Time Bomb



It's already  
**2x More**  
effort since  
March 2026

**8x**  
worse by 2029



# There are multiple reasons for decreasing certificate lifespans

Minimizing the  
“Window of Exposure”

Cryptographic Agility  
(Preparing for  
Quantum)

Forcing Automation  
(Eliminating Manual Error)

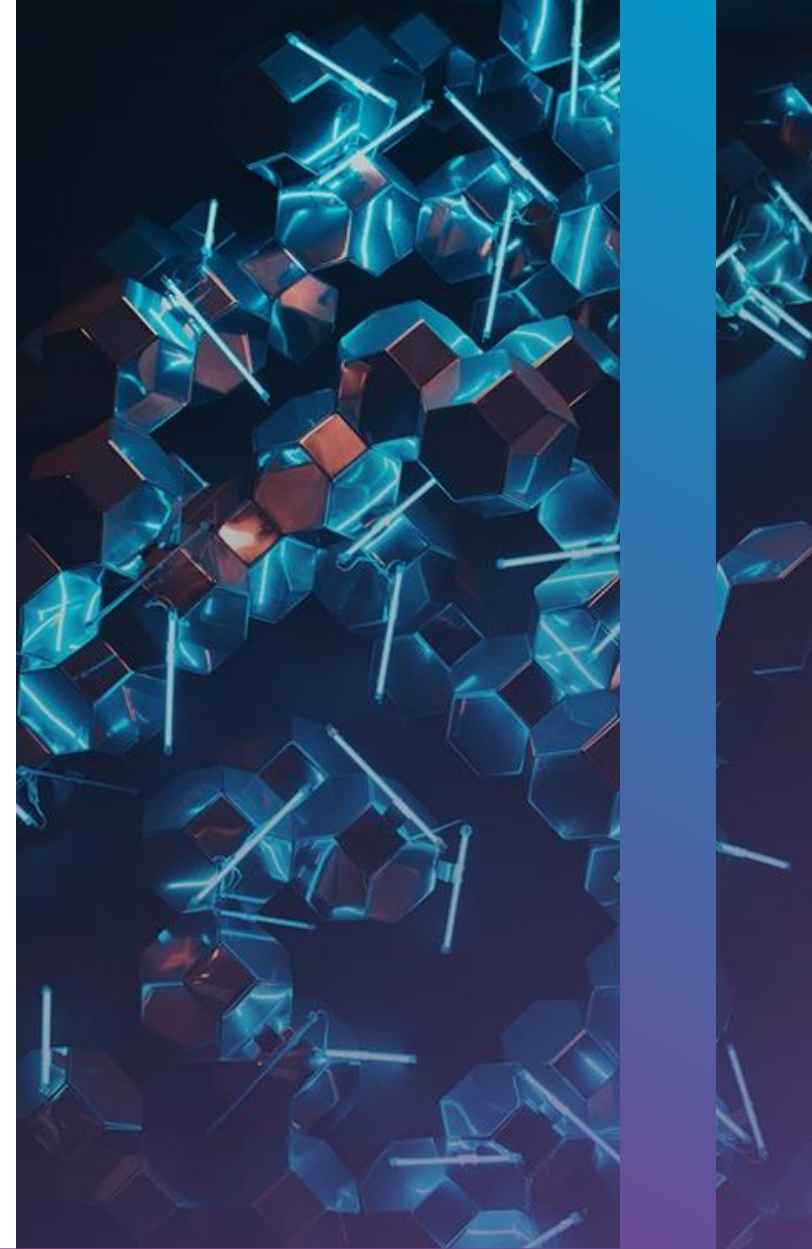
Strengthening Domain  
Validation

The goal isn't just **shorter dates**,  
the goal is to reach a point where **trust is verified in near real-time**,





# Certificates on Mainframe



# The Invisible Pulse: Certificates are playing a Critical Role on Mainframe

## Network Layer (AT-TLS)

**Server certificates** to secure DB2 DDF, FTP and TN3270 traffic

## Data at Rest (Tape/DASD Encryption)

**Personal Certificates** to sign and encrypt backup tapes

## Web Services (TLS 1.3)

**Client Certificates** for supporting REST APIs and modern UIs

## Software Integrity (SMP/E & GIMZIP)

**Code Signing Certificates** to verify PTFs are not tampered

## Establish Identity (Replacing passwords)

**User Certificates** are issued and mapped to a Mainframe ID enabling 'The password-less future'

And more..



# Transport Layer Security (TLS) Certificates Critical to today's Mainframe

## **TLS Certificates are used for:**

- HTTPS
- REST API
- VPNs
- Email servers
- Cloud services
- IoT devices
- Database connections
- Microservices

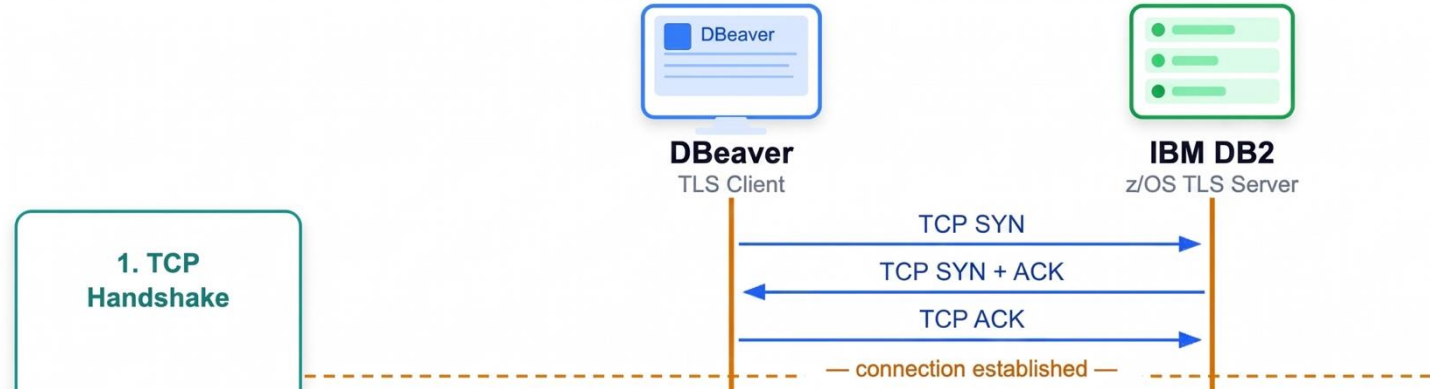
**In Broadcom Mainframe products, TLS Certificates are used in more than 20 products, and the list is ever increasing.**

### **Data Management**

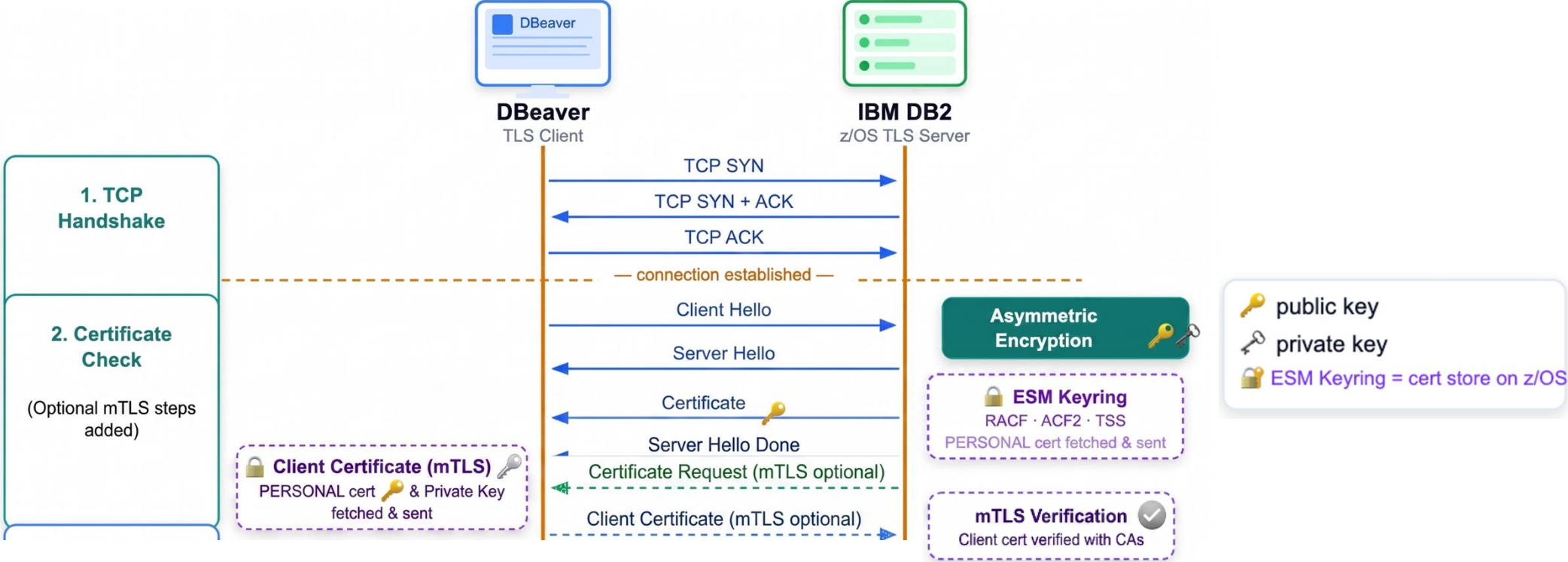
- Datacom
- Db2 Tools
- IDMS
- CenterStage for Database Management



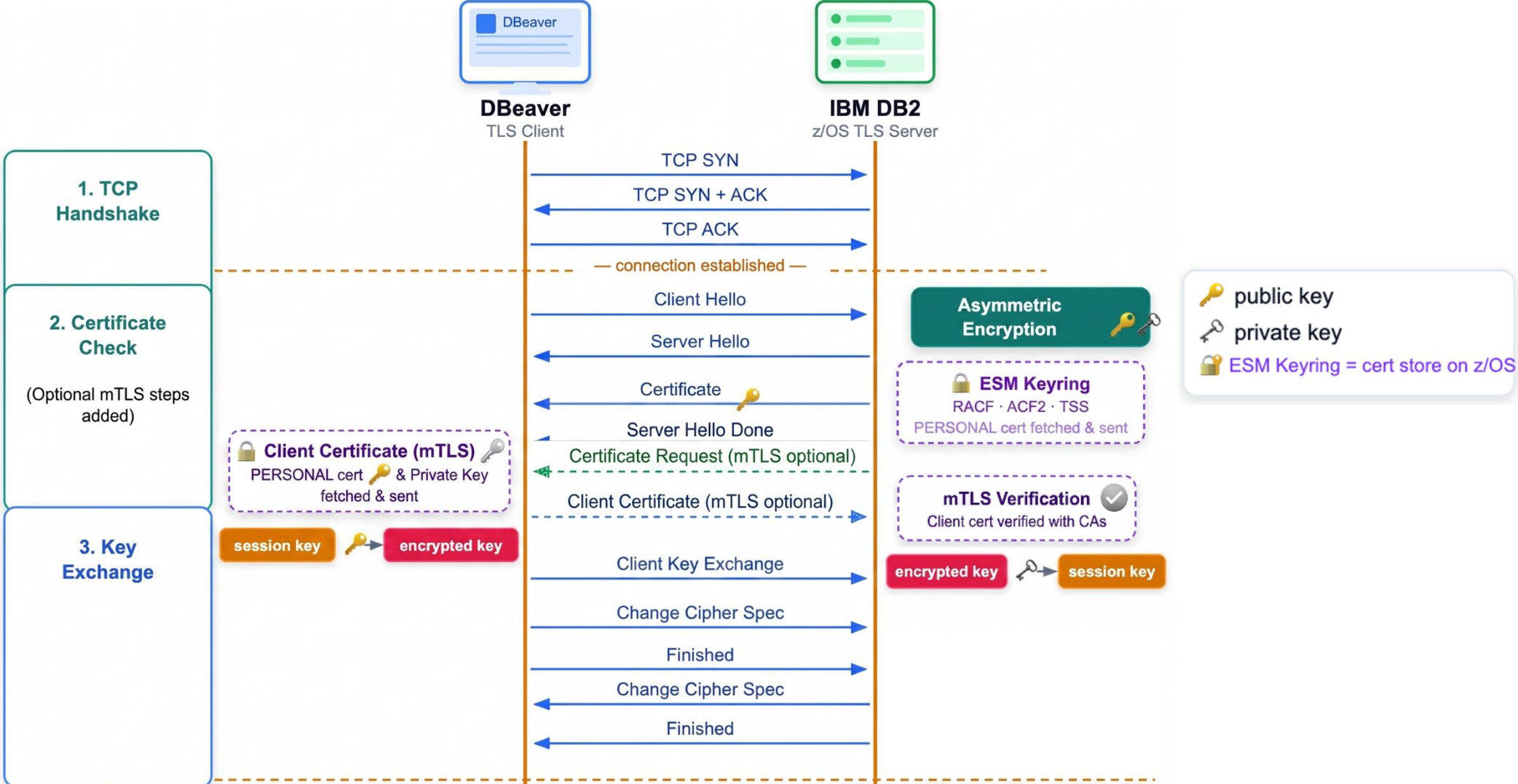
# TLS Handshake – Various phases and steps involved



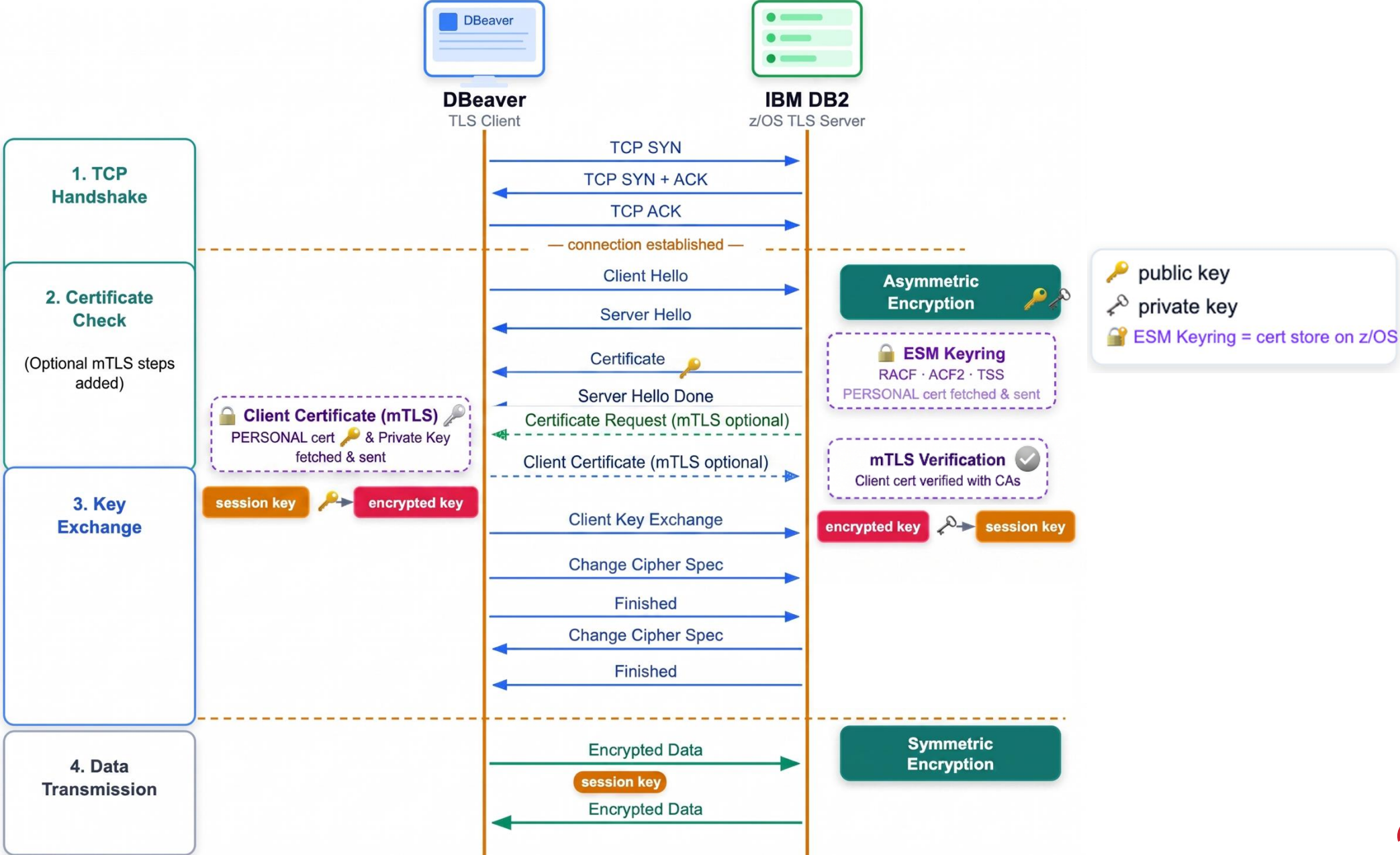
# TLS Handshake – Various phases and steps involved



# TLS Handshake – Various phases and steps involved

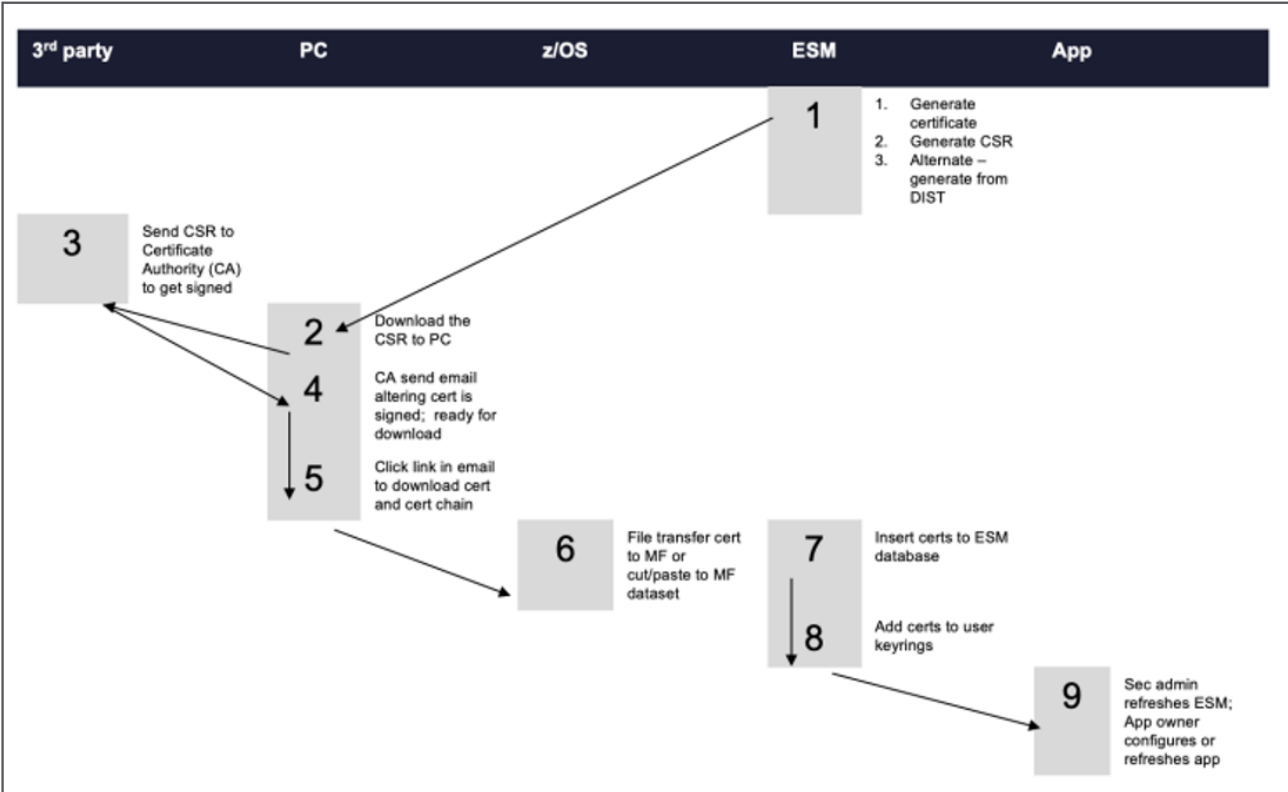


# TLS Handshake – Various phases and steps involved



# Current Mainframe Certificate Management Processes are Manual

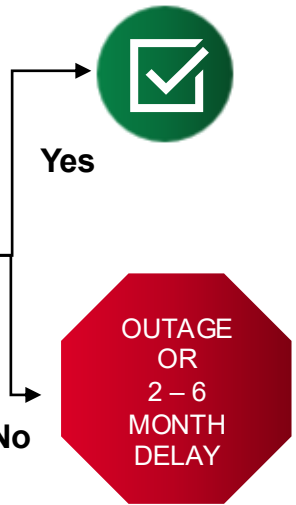
Today's Mainframe Certificate Creation Process



Real and Opportunity Cost:  
1-4 FTEs for certs

Long, error prone journey  
3 steps + (Wait Time) + 4 steps

Does it work?



# What we have heard from customers

- Digital Certificates are complex on any platform, on Mainframe even more so.
  - Complex and unfamiliar commands
  - Confusing terms
  - Requires actions outside Mainframe
  - Often part of internal process but not integrated, or possible to integrate

*“No tools available for Mainframe certificates”*

*“We have to build and maintain our own scripts for certificates”*

*“Its full-time work just to identify and track mainframe certificates”*

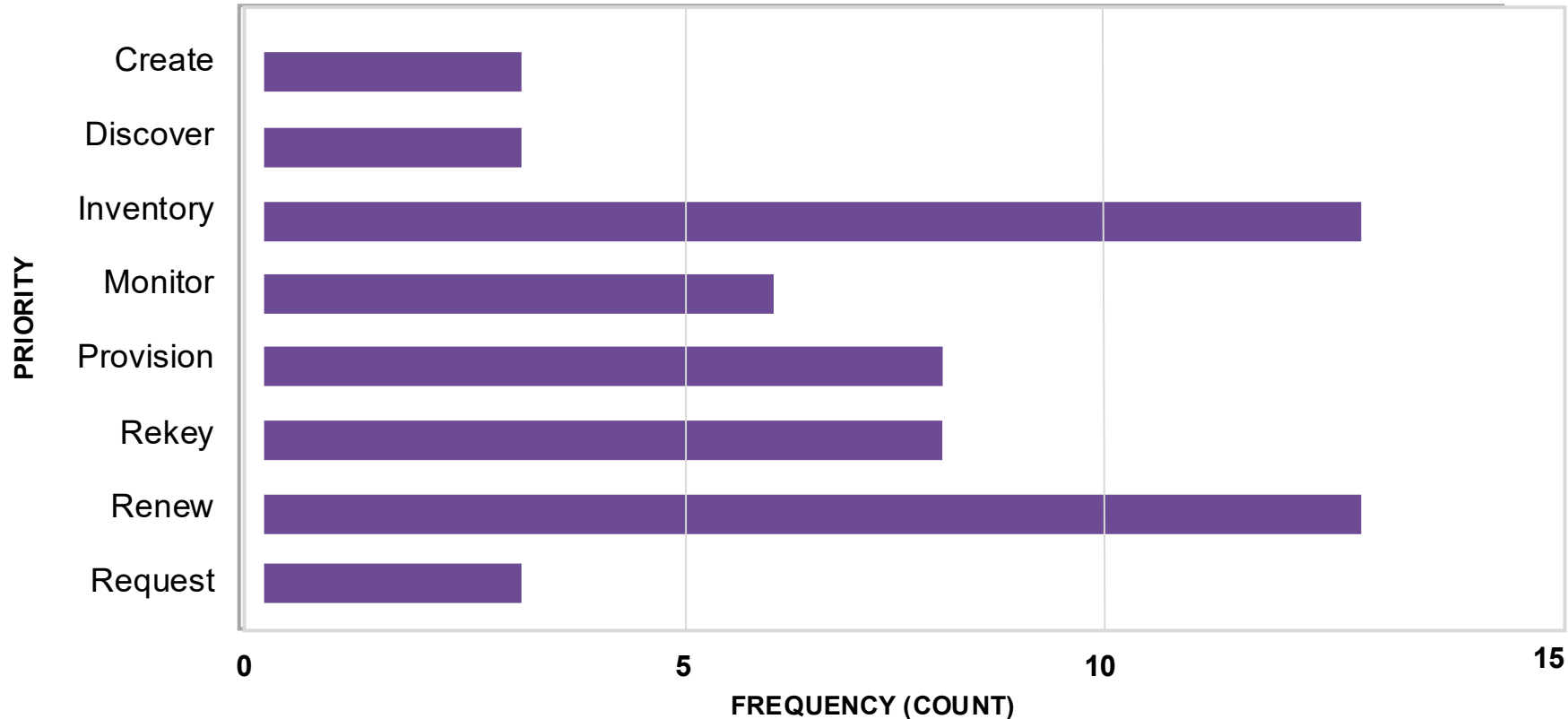
## Our Goal:

Enable system wide certificate lifecycle management and automate digital certificate creation and renewal on the Mainframe.



# Certificate Inventory & Renewal are Top of Mind for Customers

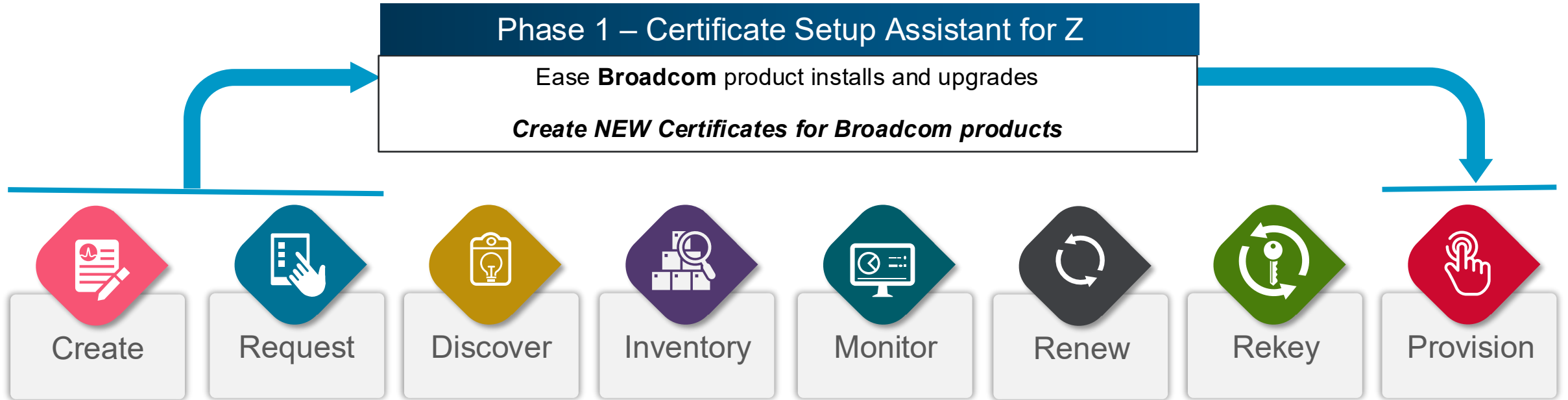
## Frequency of Top Three Cert Management Priorities



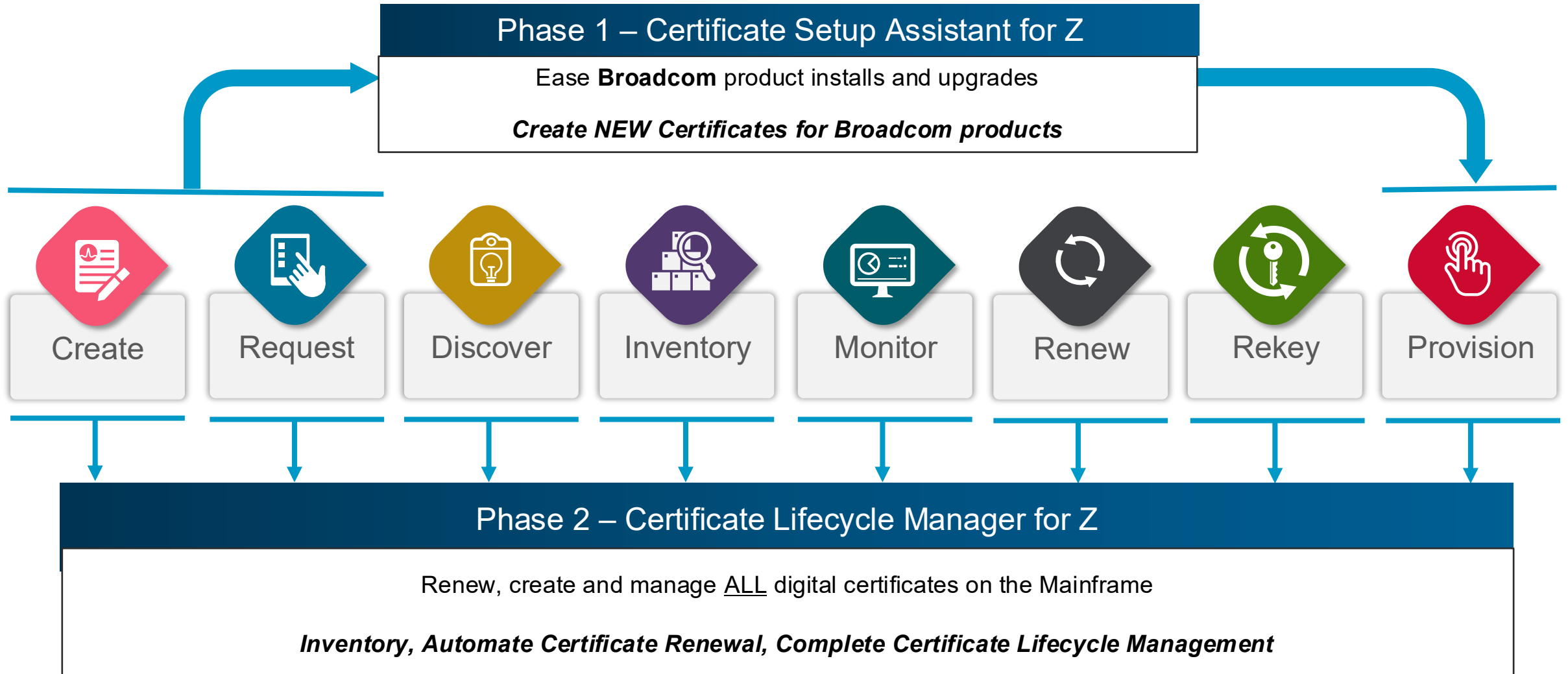
**Do they align with your priorities? Thoughts?**



# Broadcom is Developing an End-to-end Solution for Certificate Management – Phase 1

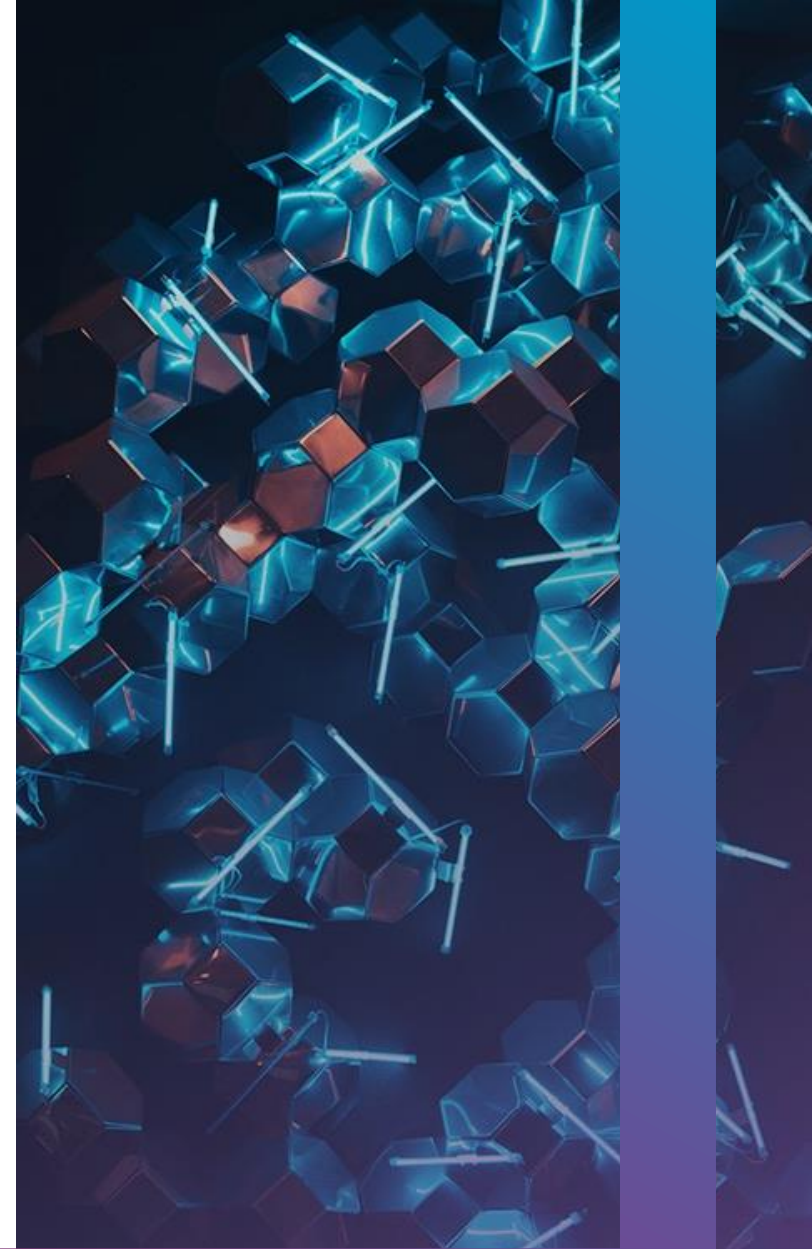


# Broadcom is Developing an End-to-end Solution for Certificate Management – Phase 2





# Certificate Setup Assistant for z (CSAz)



# CSAz marks the first milestone in our broader Certificate Lifecycle Management journey

- CSAz is a guided assistant in z/OSMF for Broadcom products and Zowe.
- Leverages product-specific guide files
- Helps admins generate
  - **Certificates**
  - **CSRs**
  - **Keyrings**
  - **Connections**
- Validated improvement over current “Manual Guide + JCL + ISPF” process.



# CSAz's Preconfigured Options Aid in Clarity

## Compliance Event Manager 7.0 Certificate and Keyring Setup (Dry Run)

Displayed Scope **PROD001** Apply

Overview Keyring TCEMRING **3 Certificate TCEMCERT** 4 CSR for TCEMCERT (optional) 5 Import signed TCEMCERT (optional) Final review

This step creates the THIS IS A TEST CERTIFICATE FOR CEM certificate.  
Do you want to Create New, Select Existing, or Import a Certificate?

Create  
 Select  
 Import

### Certificate Identification \*

Certificate Label

TCEMCERTLABEL

Owner / Type \*

acid

CERTAUTH

CERTSITE

Certificate name \*

TCEMCERT

### Subject (Issued To) \*

Common Name (CN) \*

COMPANY

Title (T) \*

CERTIFICATE

Organizational Unit (OU) \*

C

Organization (O) \*

C

Locality (L)

State or Province (SP)

Country (C)

Type the Country

### Alternative Names

Add Alternative Name

### Validity

Not Before

03/03/2026 12:24:56

Not After

03/03/2027 12:24:56

### Cryptographic Parameters

Key Algorithm \*

RSA

Key Size \*

4096

Key Usage

HANDSHAKE

DOCSIGN

CERTSIGN

DATAENCRYPT

Private Key Storage

Generate key pair using a cryptographic coprocessor and store in ICSF PKDS.

PKDS Label

### Signing

Create a Self-signed Certificate

Generate a Certificate Signing Request (CSR)

Sign with a Certificate Authority (CA)

### Generated Commands:

Generate Command

Close

Back

Next

- Broadcom Product teams create default recommendations for Certificate criteria
- Add site-specific criteria for quick certificate creation
- For many criteria, examples can be overridden with specific details if necessary
  - Required criteria will not be overridden, as may impact usefulness of resulting certificate.



# CSAz: Delivering on the Challenge

## Benefits

### Guided Assistance

For creating digital certificates required for Broadcom products and Zowe

### Built-in Configs

Broadcom Product recommended certificate and keyring configurations built-in

### Accelerated Deployment

Speeds up the deployment of Broadcom products and upgrades

### Reduces Rework

Reduce rework and improve clarity in digital certificate creation for Broadcom products and Zowe.

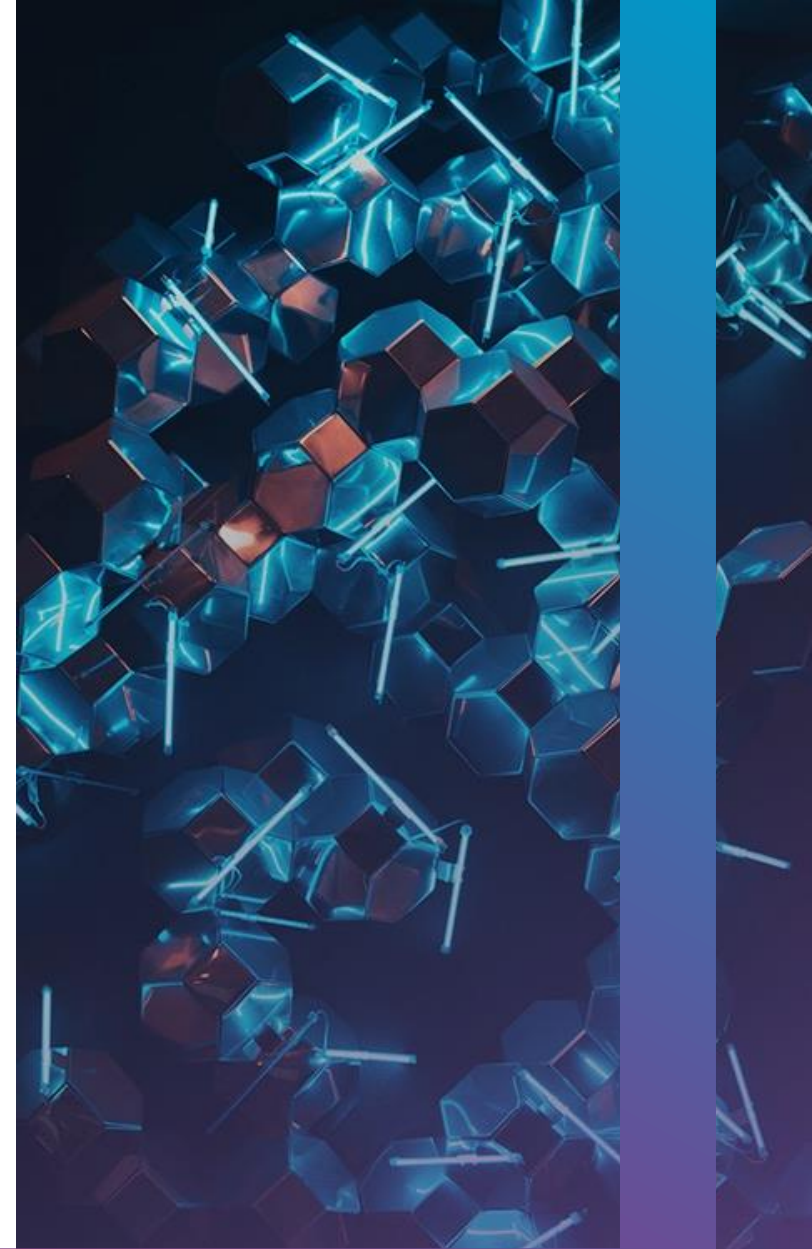
### Ease of Create and Config

Eases Zowe API ML digital certificate configuration and creation

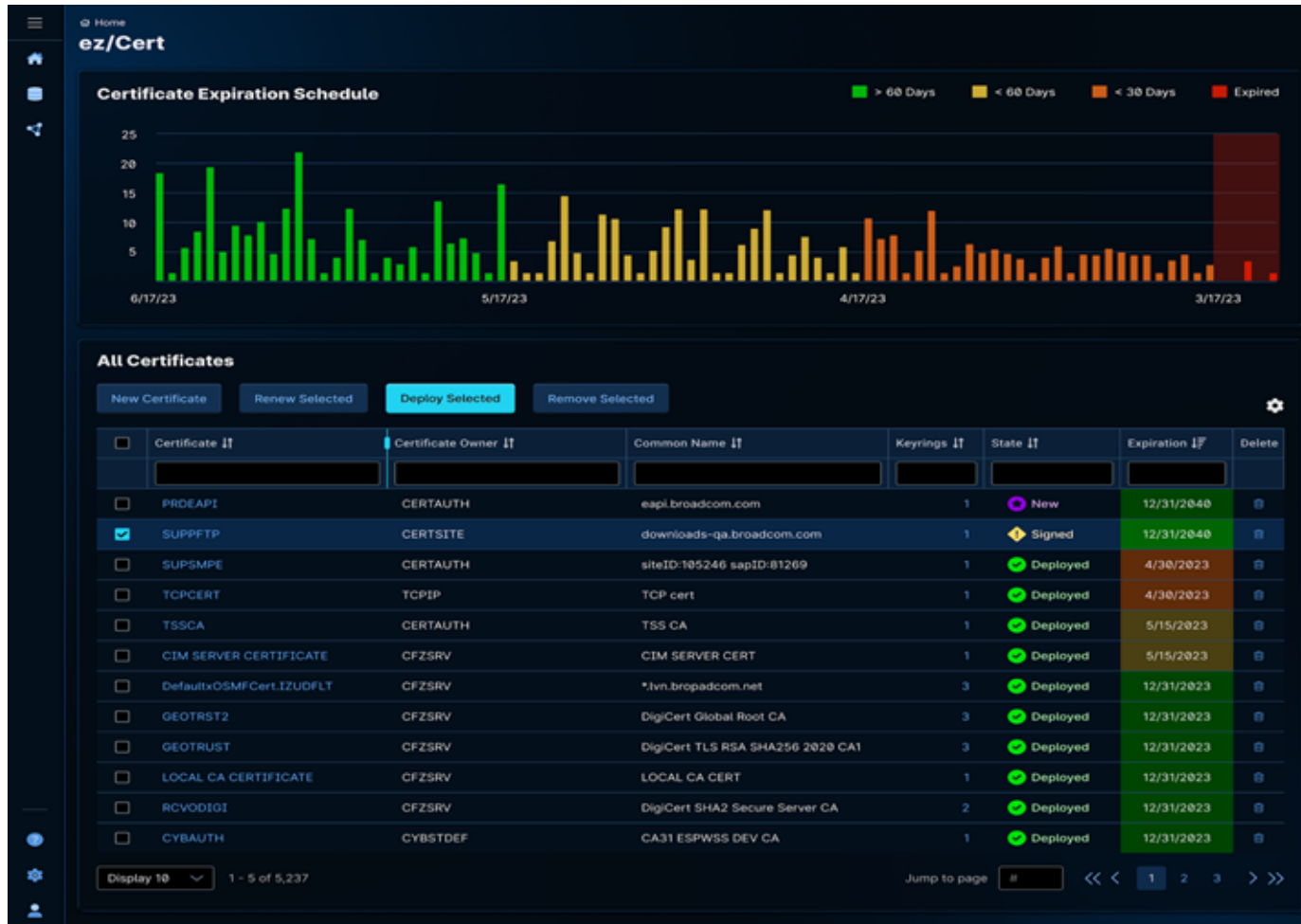




# Certificate Lifecycle Management for z (CLMz)



# CLMz aims to support full certificate lifecycle management, third party integrations and scheduling



- Full Lifecycle Support:
  - Inventory
  - Identification of expiring certificates and intermediates
  - Renewal
  - Rekey
  - Create new certificates and keyrings
  - Removal and Retirement of certificates
- Automated renewal and deployment:
  - Validation
  - Scheduling of deployments
  - Delegation to Line Of Business for deployment.
- Integration with Enterprise solutions and Service Desks to renew and leverage existing processes



# Flexible Architecture to Address Complex Customer Processes

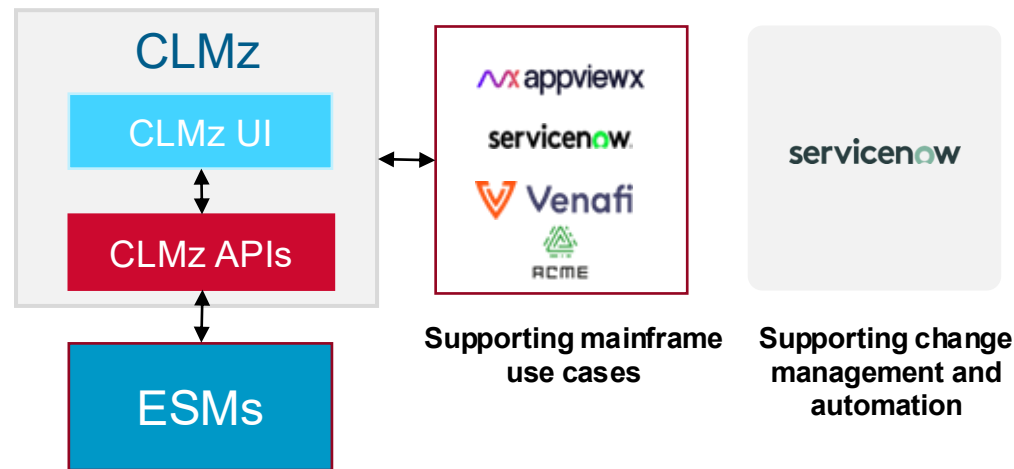
## End-End Solution

Program logic and Web UI showing lists of certificate, expiration, simple forms to renew and create certs, keyrings, CSRs. Delegate and schedule.



## APIs for existing workflows

Provide programmatic access to ESMs (RACF, ACF2, TSS) for Certificate automation and supporting use cases like Create, update, delete certs, keyrings, CSRs.



## Integrations

Integration with Enterprise Cert Management tools (Venafi, Keyfactor etc.).

Integration with Certificate Authorities (Digicert, LetsEncrypt, etc.) through ACME protocol



# Additional 'Insights' and 'Reporting' concepts we are exploring

### Insights

Filter by owner...

#### System Health Score

**90** / 100  
300 certificates analysed

Healthy

Hide scoring breakdown

CRITERION	AFFECTED	POINTS
Expired Certificates	5 / 300 (2%)	25/25
Expiring Soon (≤ 14 days)	10 / 300 (3%)	19/20
Weak Key Algorithms	79 / 300 (26%)	15/20
Self-Signed Certificates	72 / 300 (24%)	11/15
No Trust / Untrusted	6 / 300 (2%)	10/10
Missing Key Type	0 / 300 (0%)	10/10

#### Action Items

1 critical, 3 warning

- Renew 10 certificates expiring within 14 days [View](#)
- Replace 79 RSA-2048 certificates with stronger keys [View](#)
- Review 72 self-signed certificates [View](#)
- Investigate 6 untrusted certificates [View](#)
- Clean up 5 expired certificates [View](#)

#### Key Algorithm Distribution

5 algorithms across 300 certs

#### Trust Model Distribution

72 self-signed of 300 certs

#### PQC Readiness Score

**15** / 100  
300 certificates analysed  
CNFA 2.0: 56 months remaining

Not Started

Show breakdown

Show migration roadmap

#### Weekly Renewal Calendar

195 certs expiring in next 60 days

### Reports

Expiring Certificates | Inventory Summary | **Keyring Health** | Audit Trail

- 2 Empty Key Rings
- 1 All Certs Expired
- 25 Expiring ≤ 30d

28 issues found [Export](#)

Severity	Key Ring Name	Owner	Certs	Issue	Days to Expiry
CRITICAL	Audit Keyring	Amanda White	11	Soonest certificate expires in 1 day	1d
CRITICAL	Code Signing Keyring	Michael Chen	12	Soonest certificate expires in -5 days	5d overdue
CRITICAL	Emergency Renewal Keyring	Amanda White	9	Soonest certificate expires in 1 day	1d
CRITICAL	Expired Services Keyring	Robert Taylor	5	All certificates expired — broken configuration	30d overdue
CRITICAL	IoT Devices Keyring	James Brown	10	Soonest certificate expires in 7 days	7d
CRITICAL	Legacy Systems Keyring	Robert Taylor	10	Soonest certificate expires in 14 days	14d
CRITICAL	Monitoring Keyring	Lisa Wang	14	Soonest certificate expires in -21 days	21d overdue

### Audit Readiness

**Executive Summary** [Print / Export PDF](#)

- 84** Health Score
- 300** Total Certificates
- 33** Expired
- 61** Expiring ≤ 14d
- 79** Weak Keys
- 72** Self-Signed

**Top Action Items**

- Renew or remove 33 expired certificates
- Schedule renewal for 61 certificates expiring within 14 days
- Rotate 79 certificates with weak key algorithms to ECDSA or RSA 3072+

**65** Compliance Score

- 186** Weak Key Type
- 72** Self-Signed Certificate
- 0** Orphan Certificate
- 0** Expired but Deployed

258 findings [Export](#)

Severity	Finding	Certificate	Owner	Detail
WARNING	Weak Key Type	PROXY Server #2	Donna Hill	Key type "ECDSA P-256" is below recommended strength — review recommended
WARNING	Weak Key Type	Staging - Search #3	Maria Hernandez	Key type "ECDSA P-256" is below recommended strength — review recommended

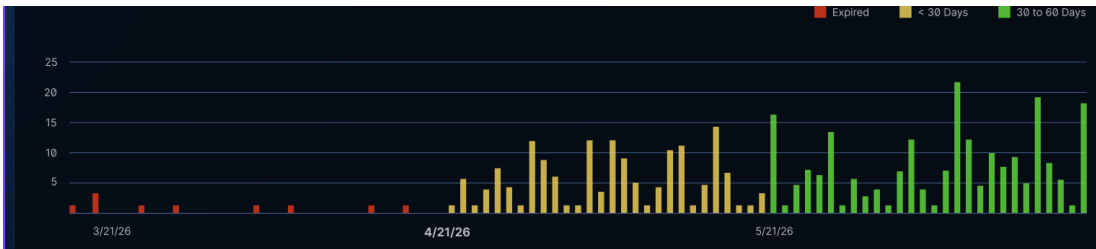


# Post-Quantum Cryptographic (PQC) Readiness

The ultimate 'North Star' of our CLMz solution

Certificate Label: \*.google.com | Certificate Owner: CERTAUTH

Trust Status: ✓ Trust | Crypto Strength: ⚠️ Deprecated | Expiration: ✓ 2026/05/24 | Renewal Status: 🕒 Scheduled | Renewal State: Ready



All Certificates

Certificate Label	Certificate Owner	Subject	Issuer	Trust Status	Crypto Strength	Expiration	Renewal Status	Renewal State
Data Engineering #13903	AB123456	eapi.broadcom.com	WR2	✓ Trust	✓ Compliant	2026/04/24	Manual	Ready
Internal Tools #13908	AB123456	downloads-ga.broadcom.com	WR2	✓ Trust	✓ Compliant	2026/05/24	Scheduled	Ready
Platform Engineering #13909	AB123456	siteID:105246 sapID:81269	WR2	✓ Trust	✓ Compliant	2026/04/24	Running	Get
TEST Server #13905	AB123456	TCP cert	WR2	✓ Trust	⚠️ Deprecated	2026/04/24	Manual	Deploy
Hoool API Gateway #13924	AB123456	TSS CA	WR2	✓ Trust	✓ Compliant	2026/04/24	Running	Verify
Compliance Certificate #13925	AB123456	CIM SERVER CERT	WR2	✓ Trust	⚠️ Deprecated	2026/04/24	Error	Get
K&S Server #13939	AB123456	*.lvn.broadcom.net	WRS	✓ Trust	✓ Compliant	2026/05/24	Scheduled	Ready
STATUS Server #13945	AB123456	DigiCert Global Root CA	WR2	✓ Hi-Trust	✓ Compliant	2026/05/24	Scheduled	Ready
IT Security Certificate #13957	AB123456	DigiCert TLS RSA SHA256 2020 CA1	WR2	⚠️ No Trust	⚠️ Forbidden	2026/04/24	Not Defined	Not Defined
Production - CI/CD #14043	AB123456	LOCAL CA CERT	WR2	✓ Trust	✓ Compliant	2026/03/24	Retired	Retired

**PQC Readiness Score** Not Started

**15** / 100  
300 certificates analysed  
CNSA 2.0: 55 months remaining

Hide breakdown

TIER	COUNT
Quantum-Safe	0 (0%)
Quantum-Ready	0 (0%)
Vulnerable	300 (100%)
Unknown	0 (0%)

CRITERION	%	POINTS
Quantum-Safe Certificates	0%	0/40
Quantum-Ready (Hybrid)	0%	0/20
Vulnerable Key Algorithms	100%	0/25
Vulnerable Signature Algorithms	0%	15/15

Hide migration roadmap

Timeline: Today, 2027 Interim CNSA, 2029 CRQC, 2030 CNSA 2.0

Enable 'Quantum Proof' Signing

Defeating 'Harvest Now, Decrypt Later' (HN DL)

Achieving required Crypto Agility

Achieving 'Quantum Leap' in Compliance



# Thank You!

---

Let's Keep  
the Dialogue  
Going.



KranthiKumar.Vemula  
@Broadcom.com



[https://www.linkedin.com  
/in/KranthiVemula/](https://www.linkedin.com/in/KranthiVemula/)