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.

-

- **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

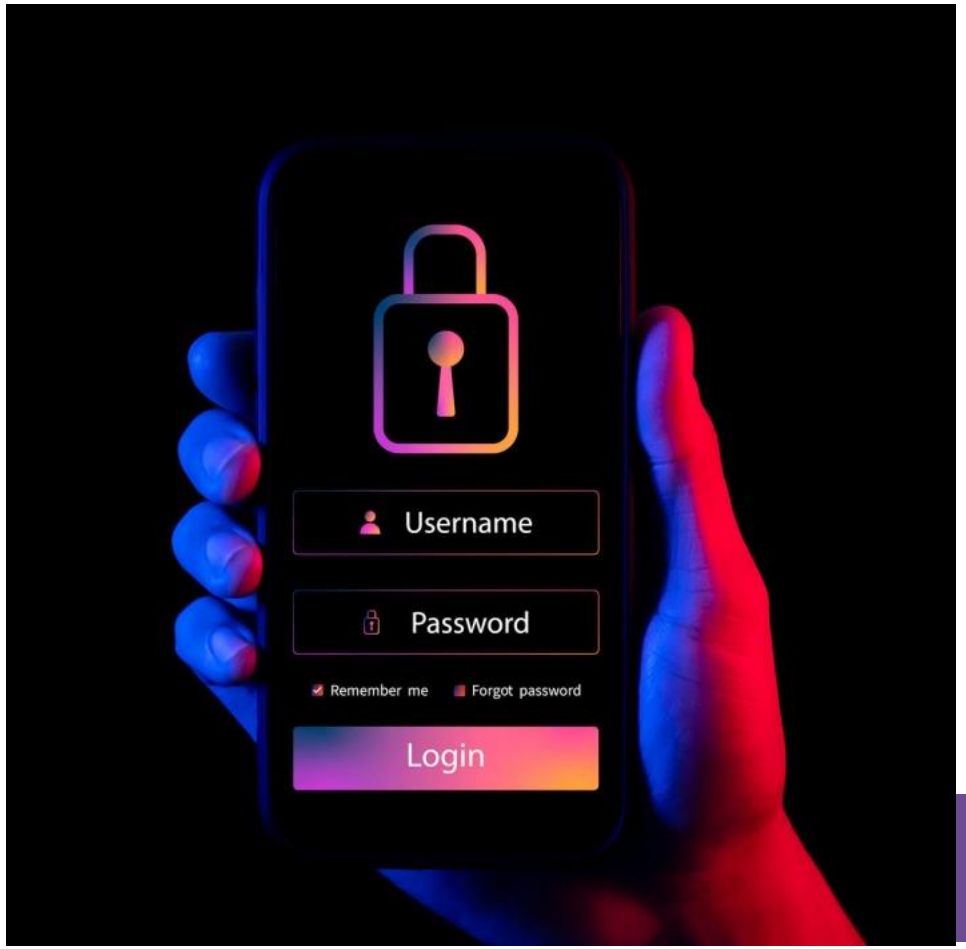
'Show me every certificate connected to this DB2 subsystem, when it expires, and who owns the renewal.'

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

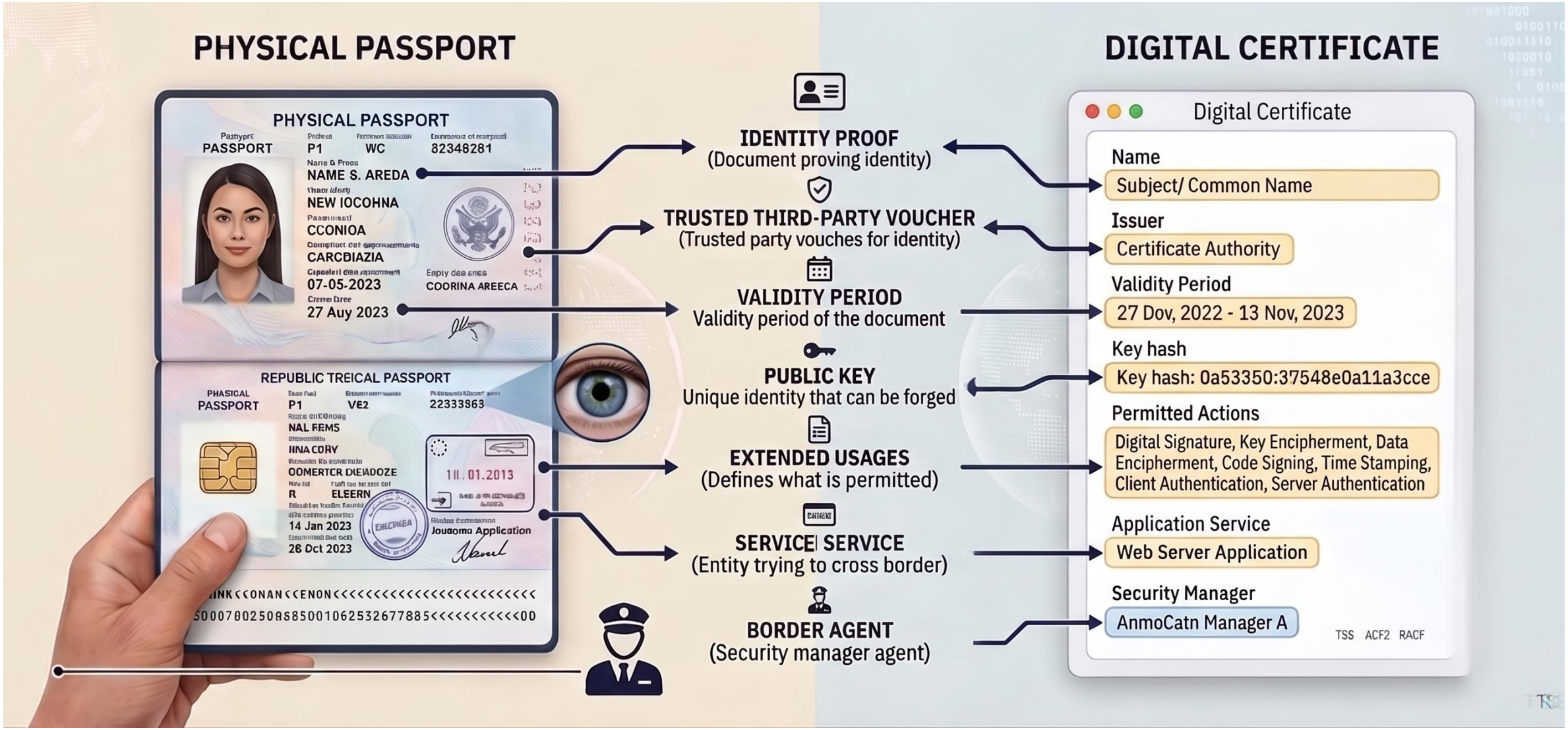
Non-Repudiation: Proof of integrity and origin of data

Trust: Establishes trust between parties in online interactions

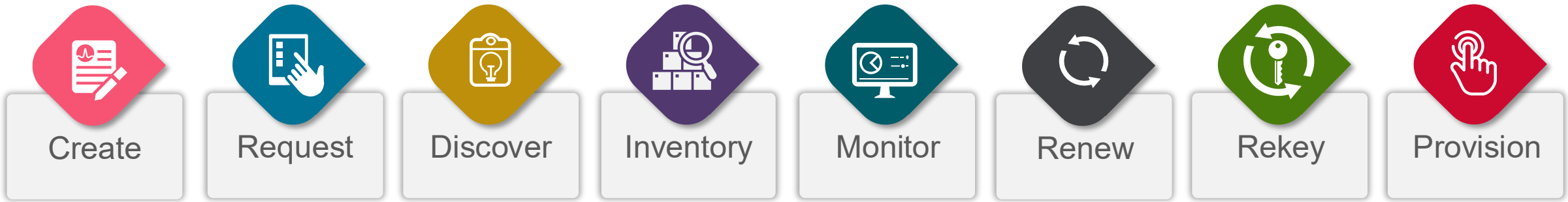
A **digital certificate** is a file that contains a **public key** and is tied to a **private key** that is kept secret.

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

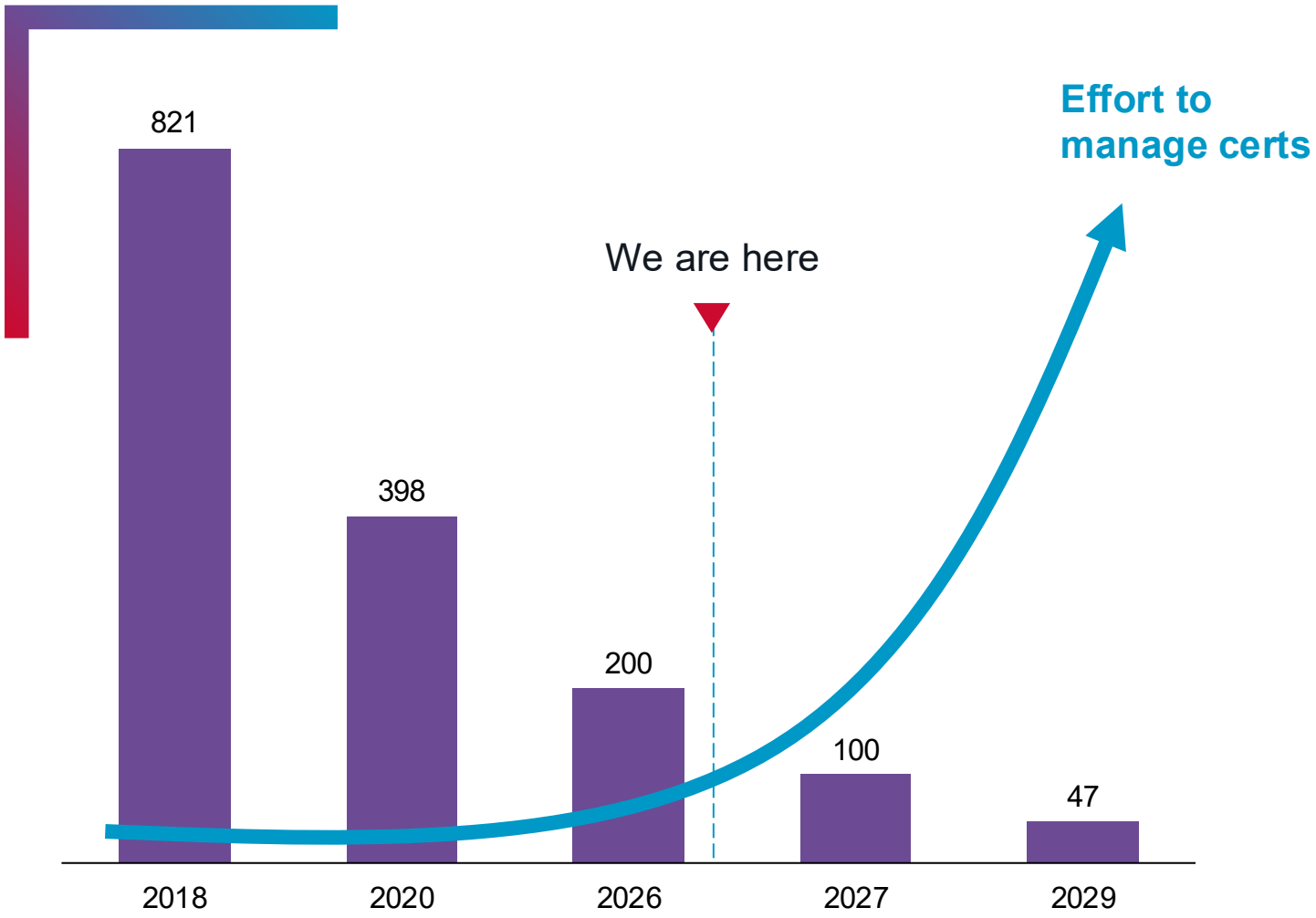
~4 hrs

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)

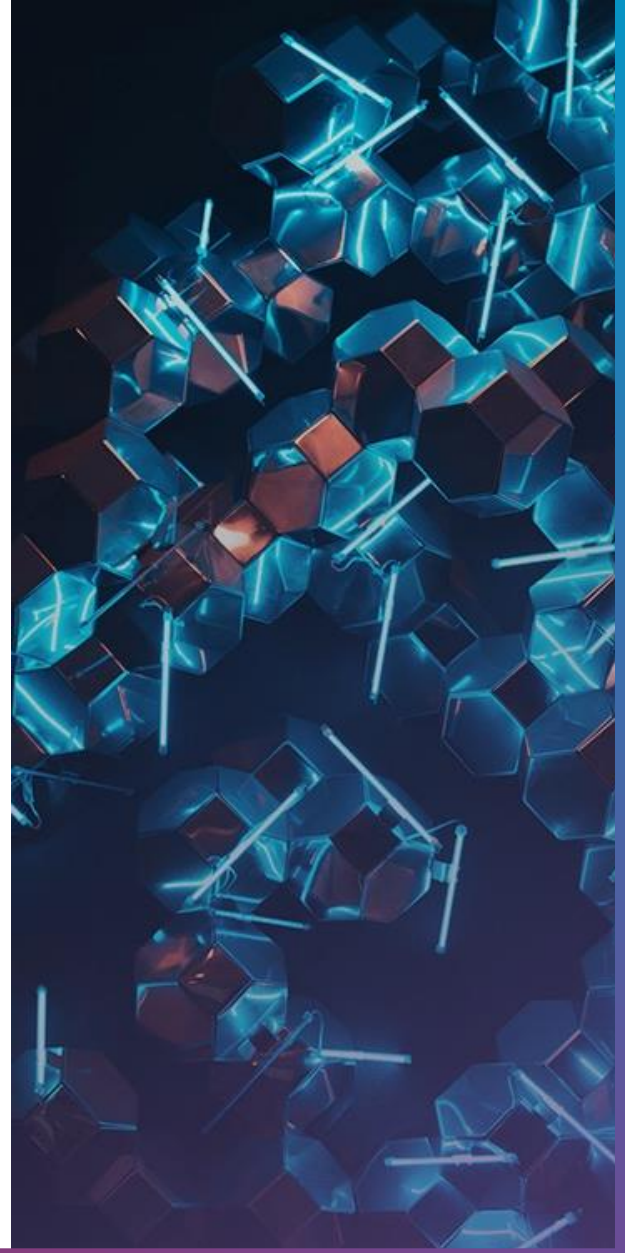
Forcing Automation (Eliminating Manual Error)

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**,

BROADCOM®
MAINFRAME SOFTWARE

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:

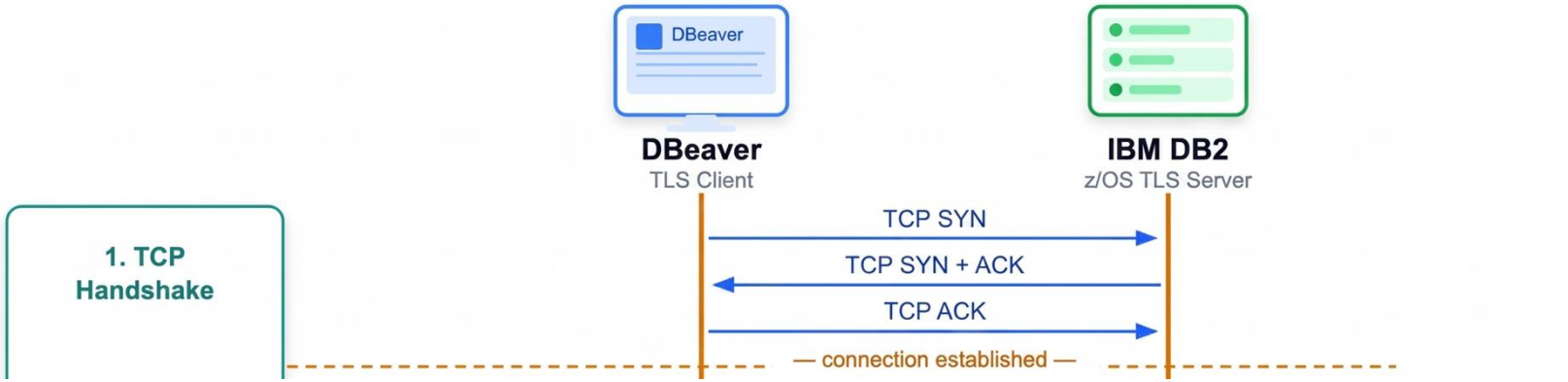
- HTTPS
- REST API
- VPNs
- Email servers
- Cloud services
- IoT devices
- Database connections
- Microservices

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

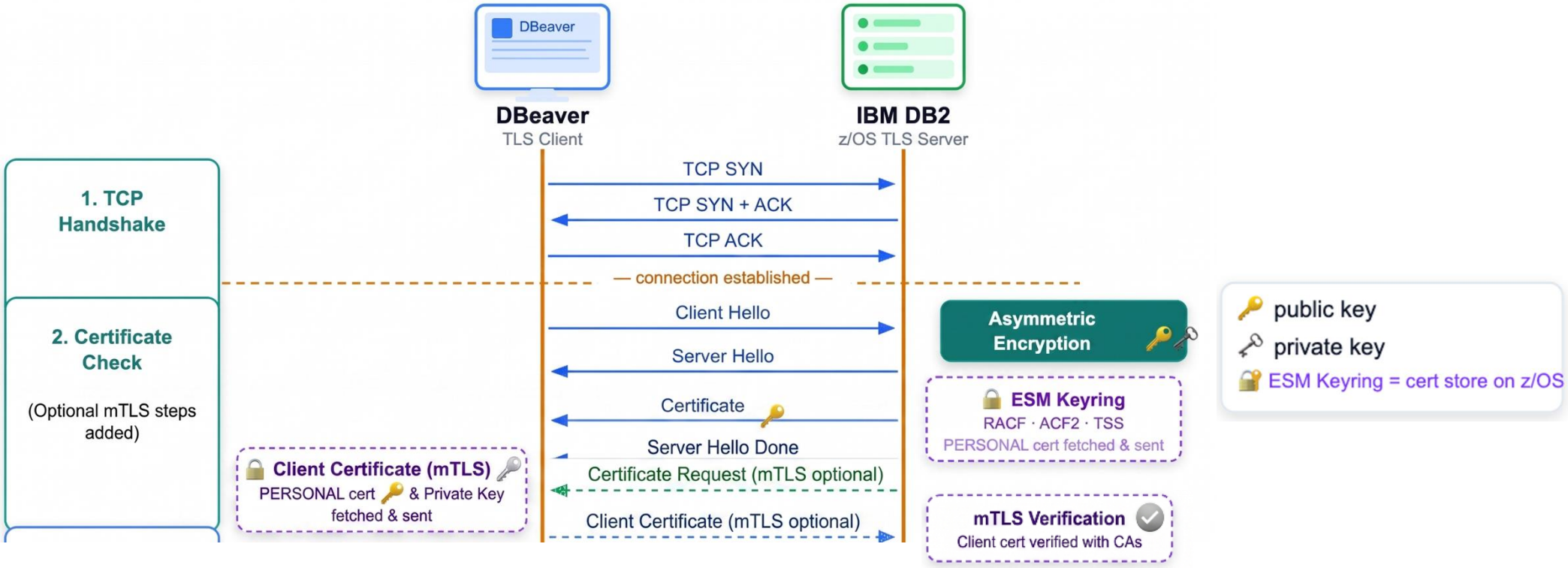
Data Management

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

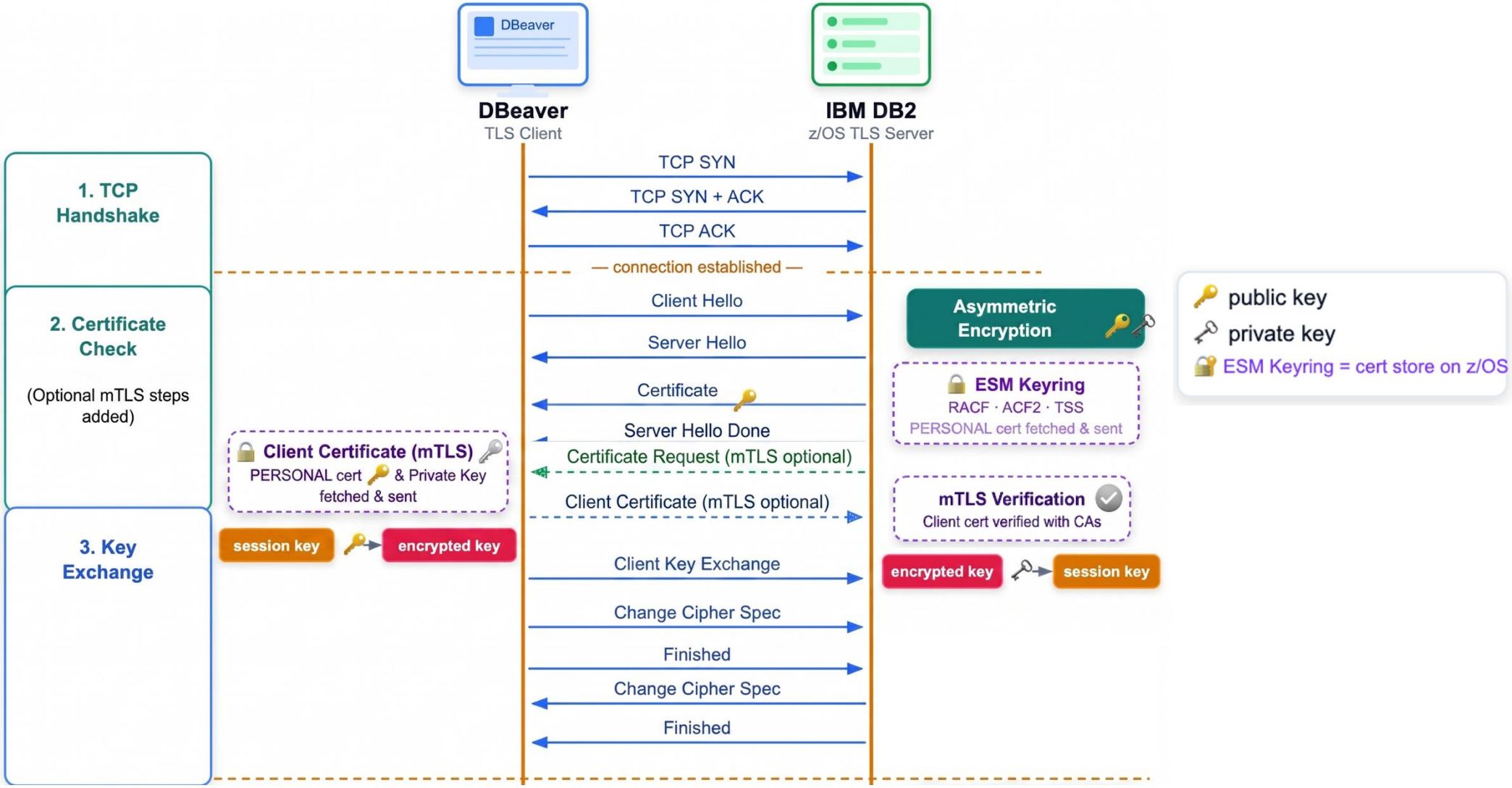
TLS Handshake – Various phases and steps involved



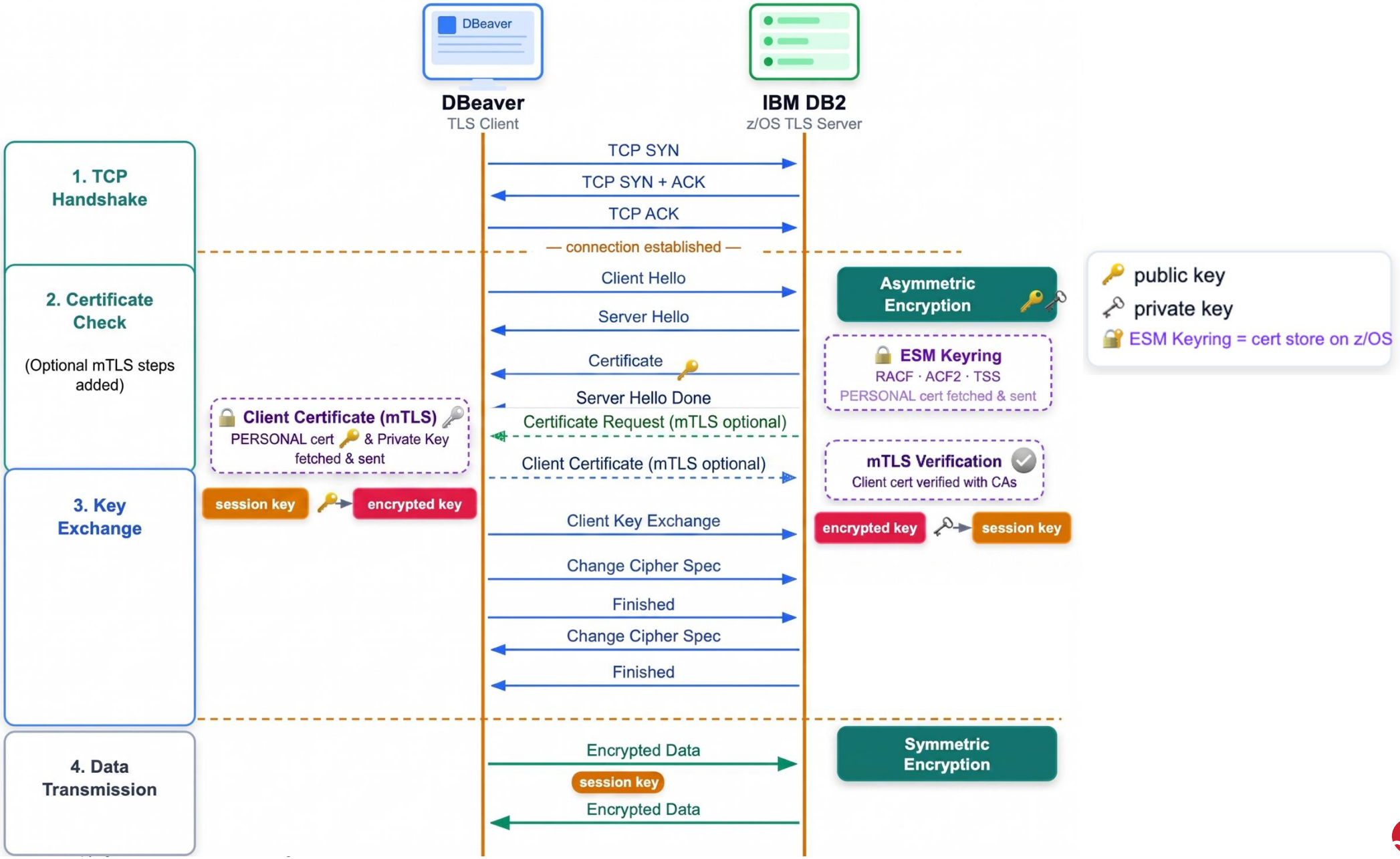
TLS Handshake – Various phases and steps involved



TLS Handshake – Various phases and steps involved

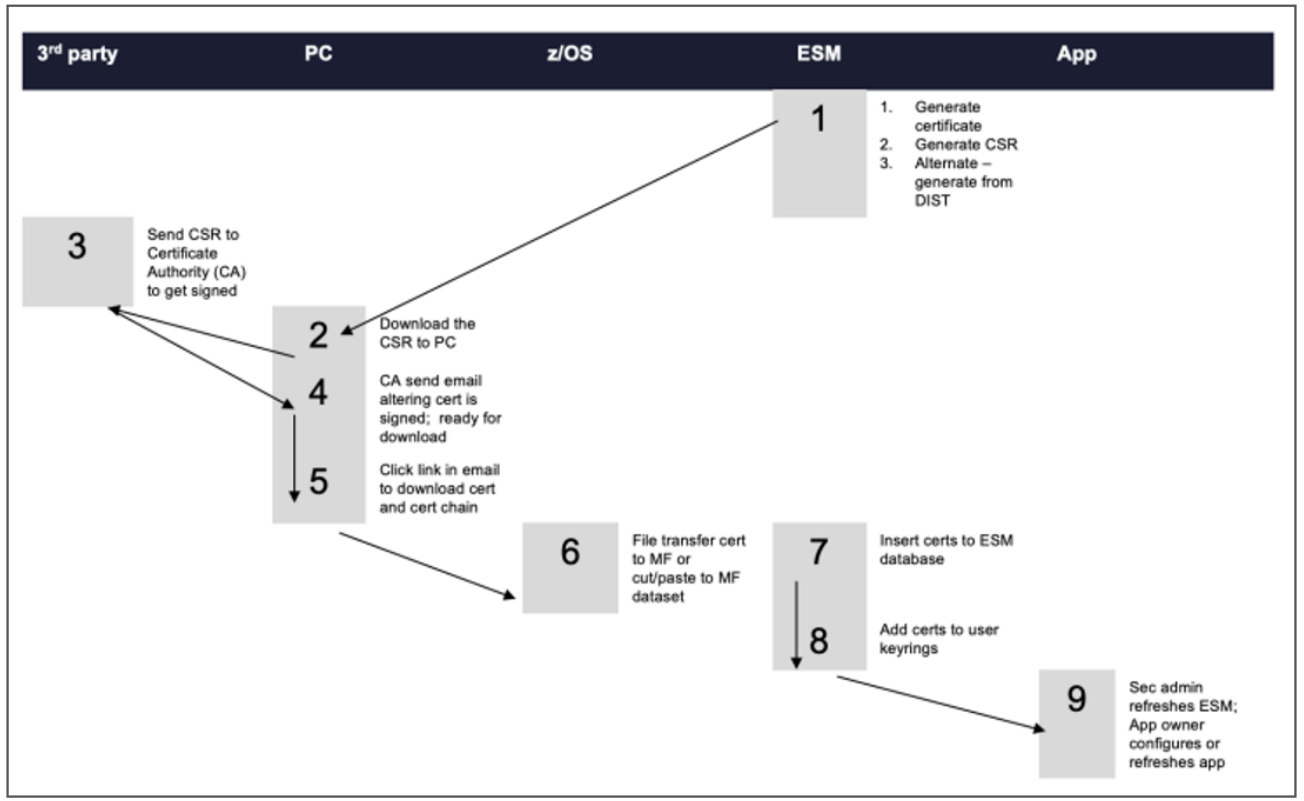


TLS Handshake – Various phases and steps involved



Current Mainframe Certificate Management Processes are Manual

Today's Mainframe Certificate Creation Process



Customer Impact

Real and Opportunity Cost: 1-4 FTEs for certs

Long, error prone journey

3 steps + (Wait Time) + 4 steps

Does it work?

Yes

No

OUTAGE OR 2 – 6 MONTH DELAY

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

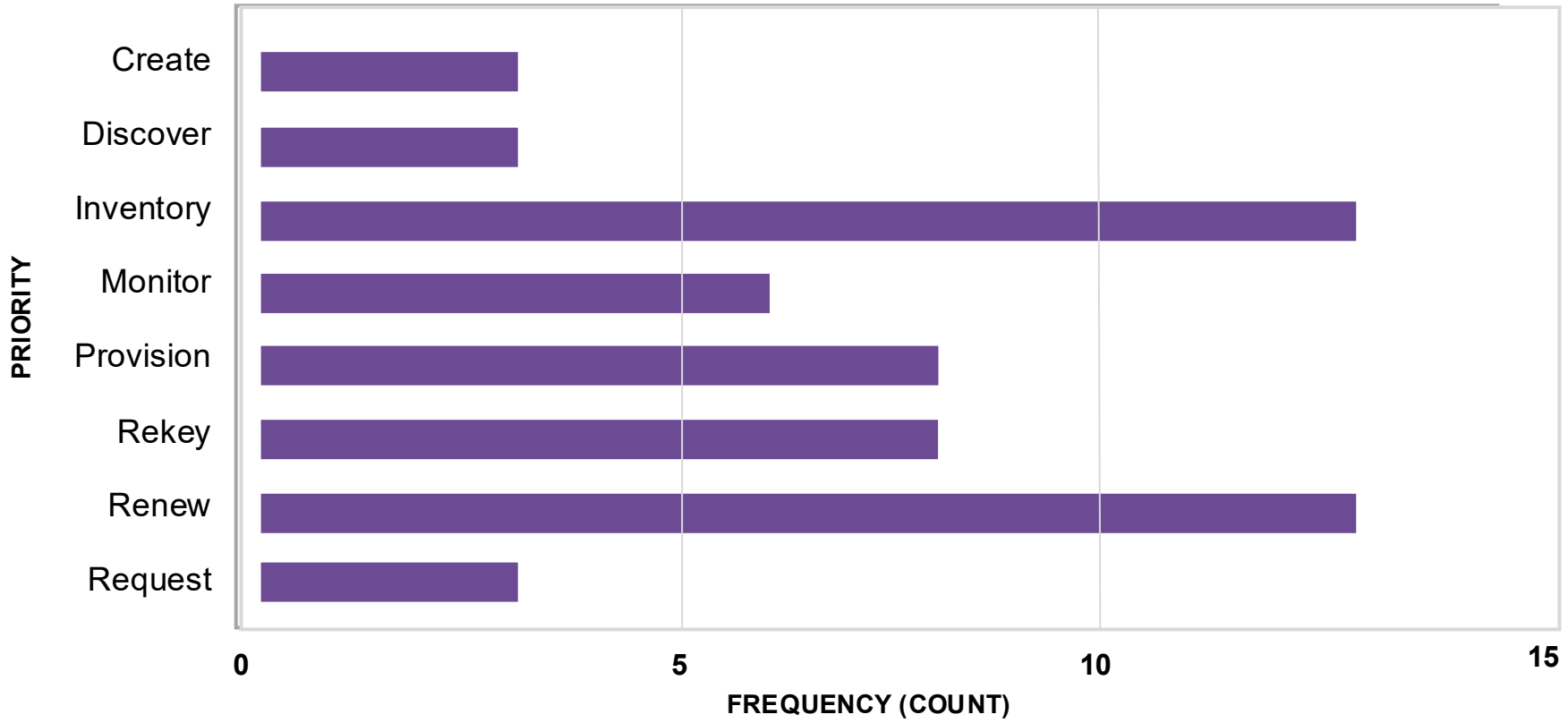
"No tools available for Mainframe certificates"
"We have to build and maintain our own scripts for certificates"
"Its full-time work just to identify and track mainframe certificates"

Our Goal:

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

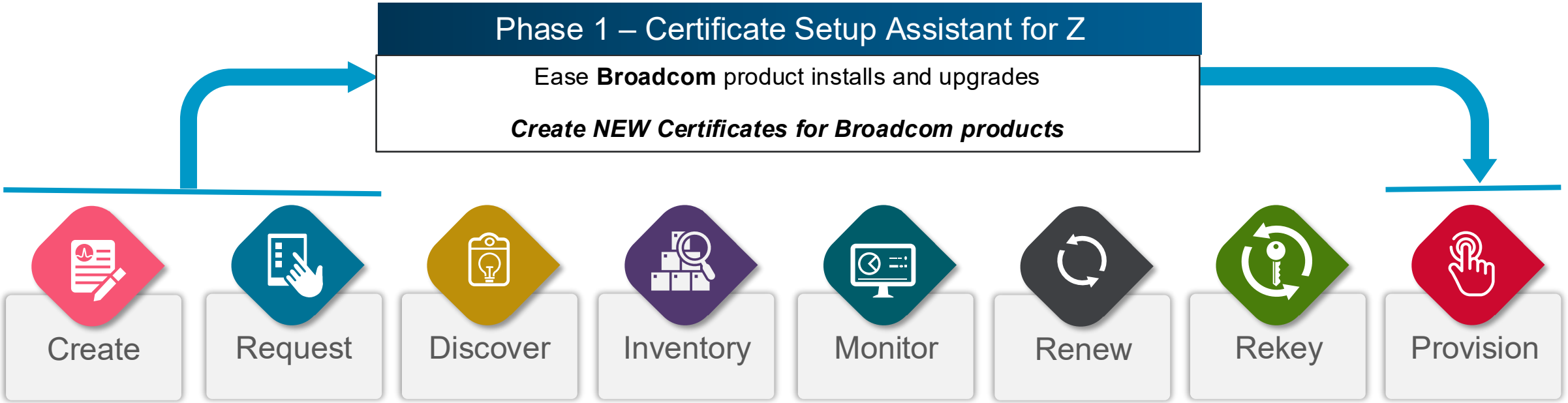
Certificate Inventory & Renewal are Top of Mind for Customers

Frequency of Top Three Cert Management Priorities

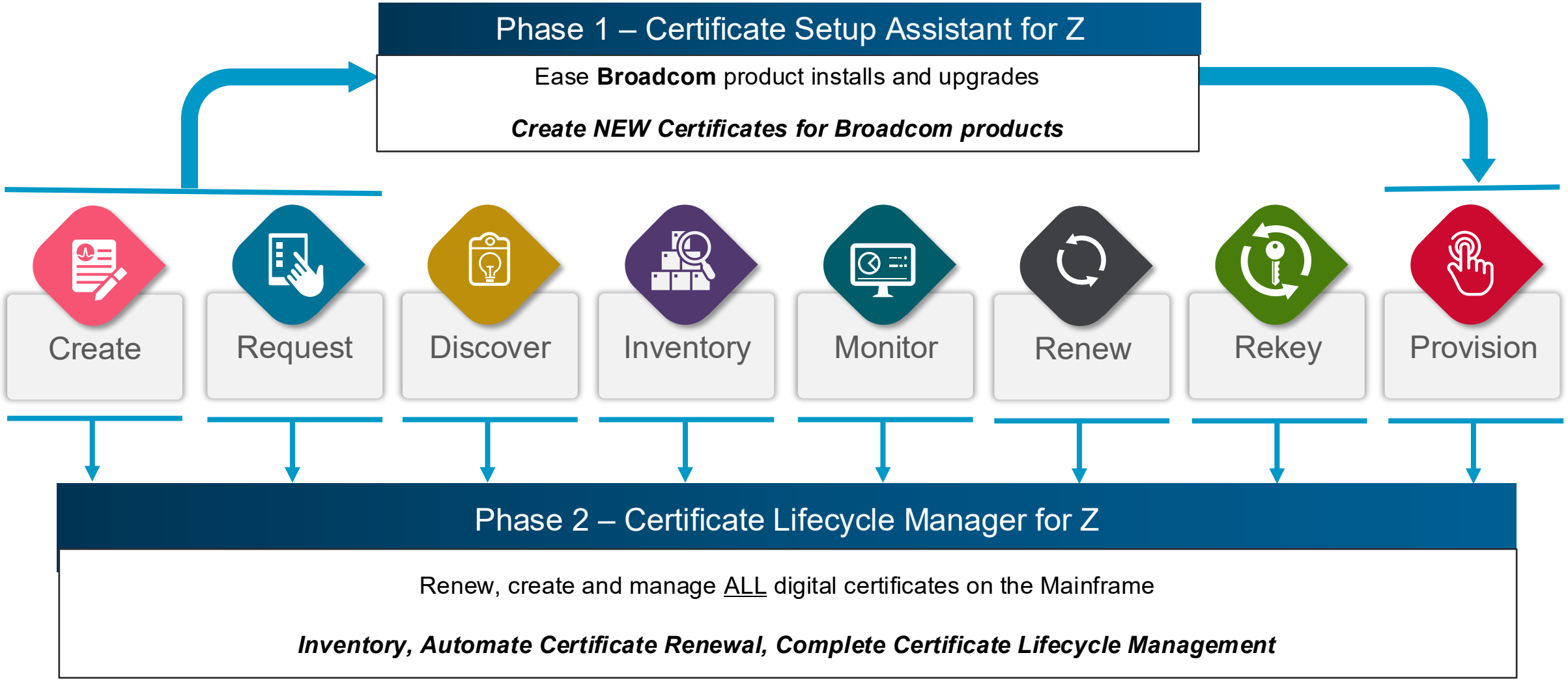


Do they align with your priorities? Thoughts?

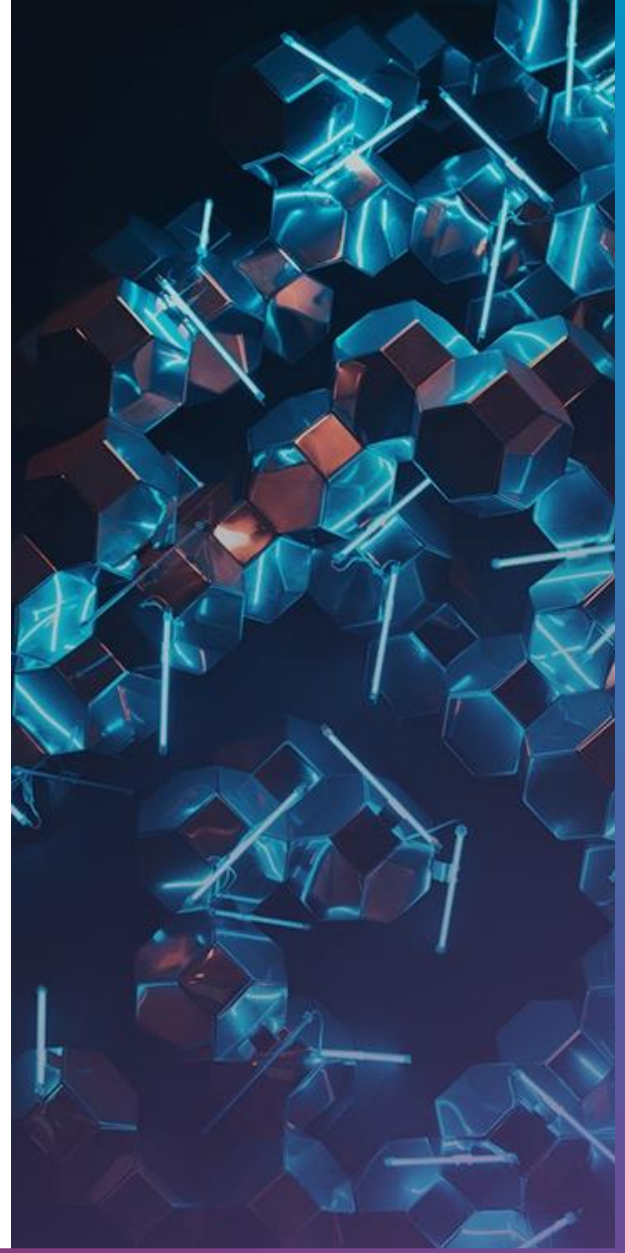
Broadcom is Developing an End-to-end Solution for Certificate Management – Phase 1



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



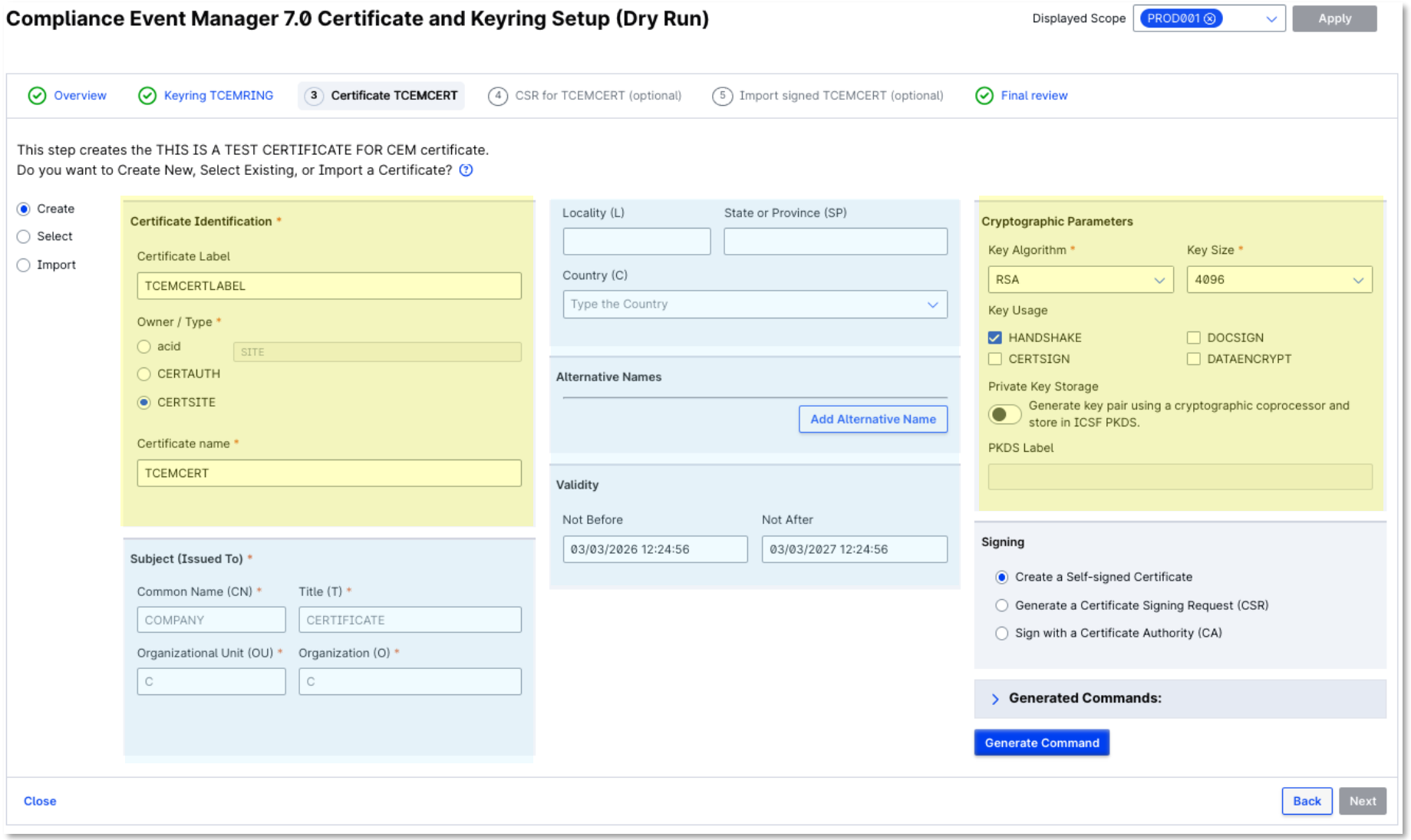
Certificate Setup Assistant for z (CSAz)



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



- 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

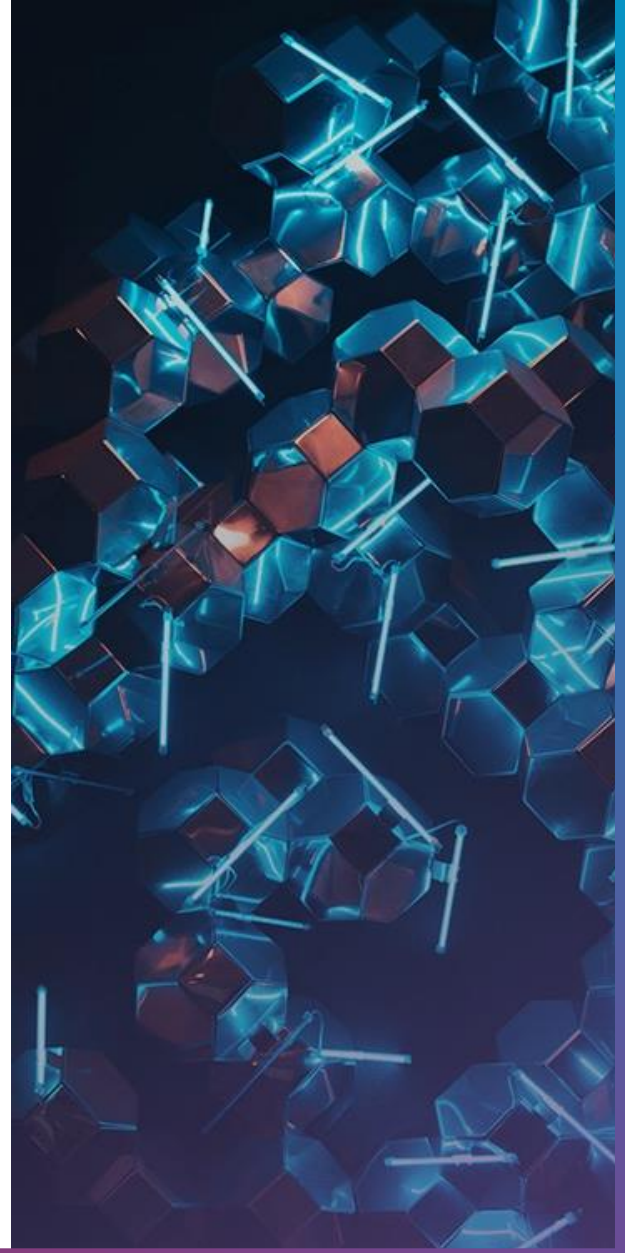
Reduces Rework

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

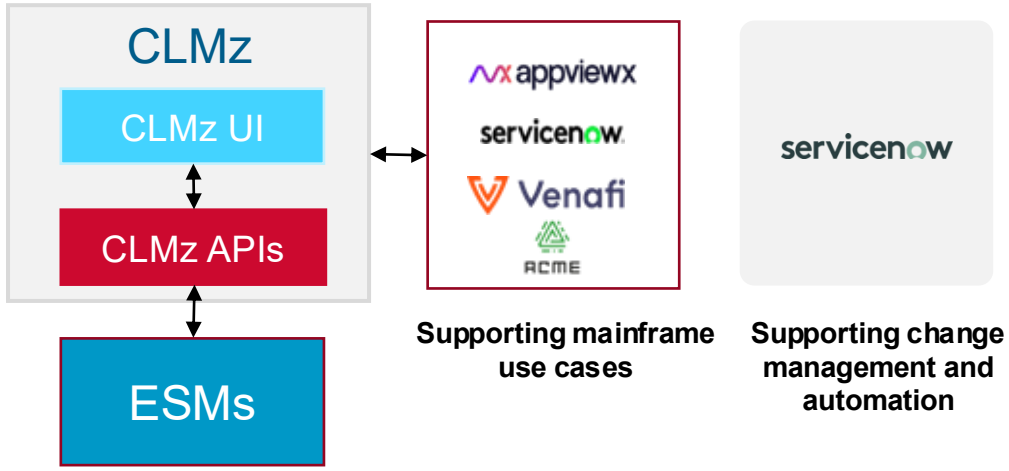
Flexible Architecture to Address Complex Customer Processes

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.



Supporting mainframe use cases

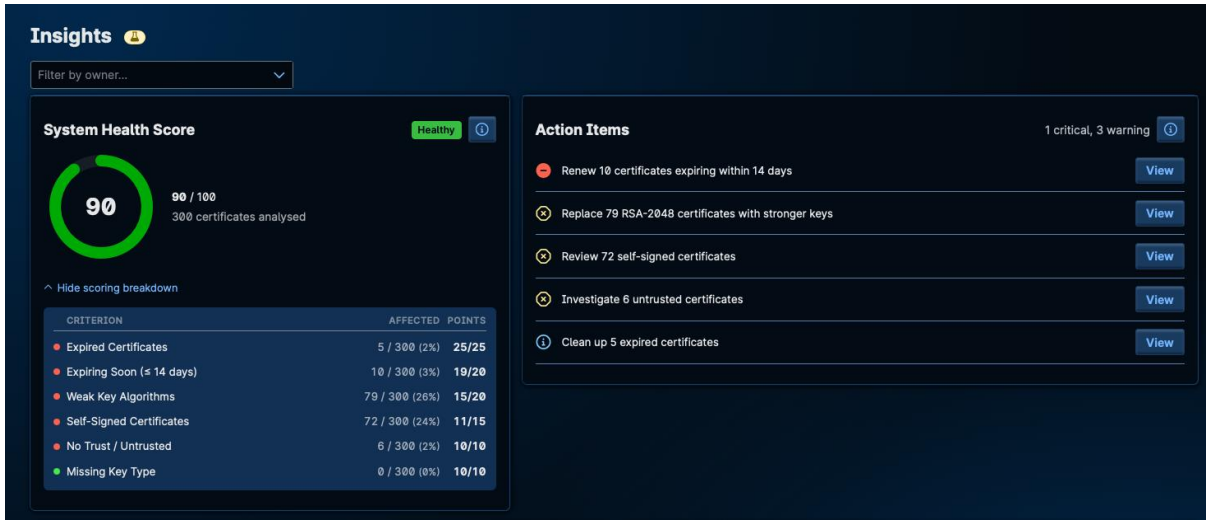
Supporting change management and automation

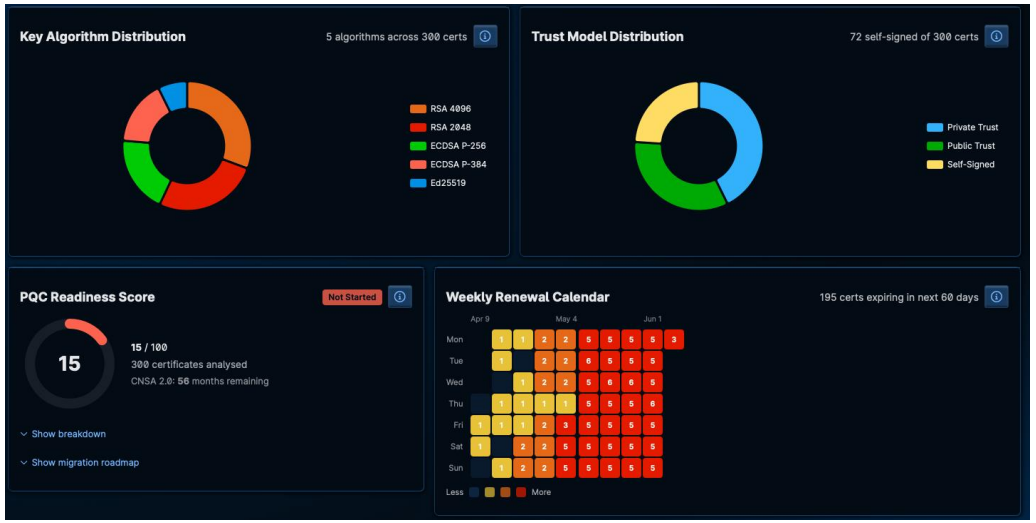
Integrations

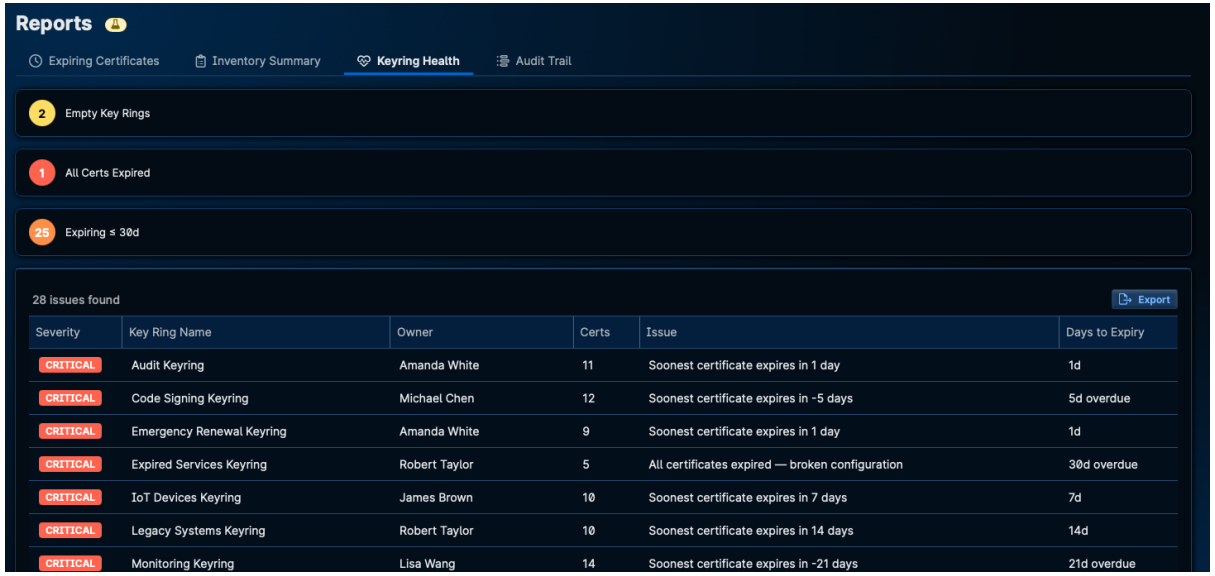
Integration with Enterprise Cert Management tools (Venafi, Keyfactor etc.).

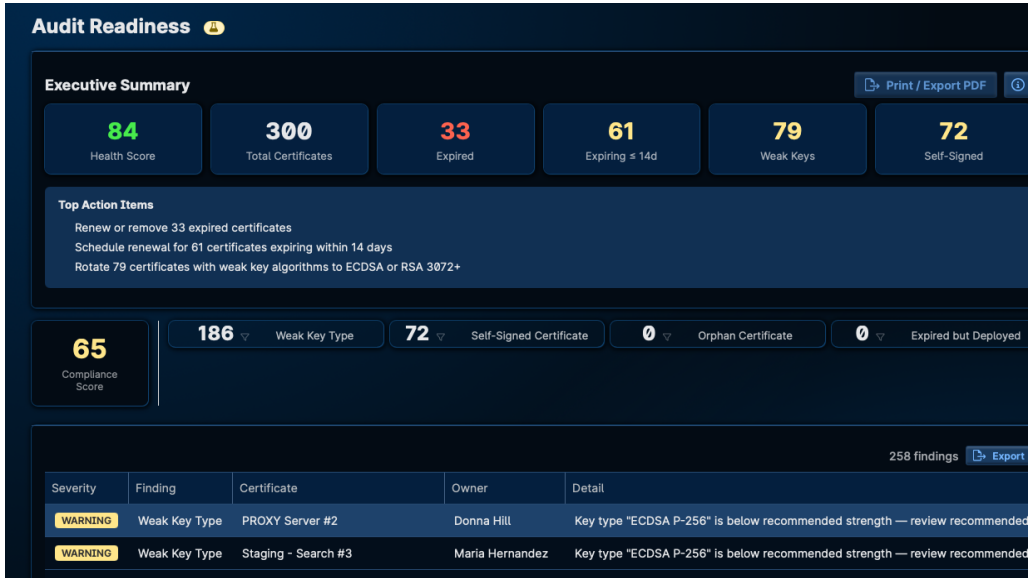
Integration with Certificate Authorities (Digicert, LetsEncrypt, etc.) through ACME protocol

Additional ‘Insights’ and ‘Reporting’ concepts we are exploring



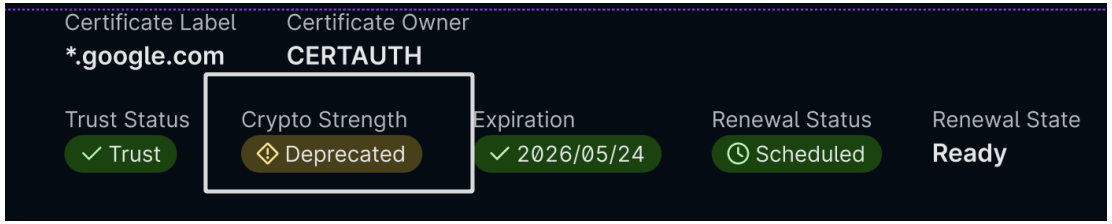


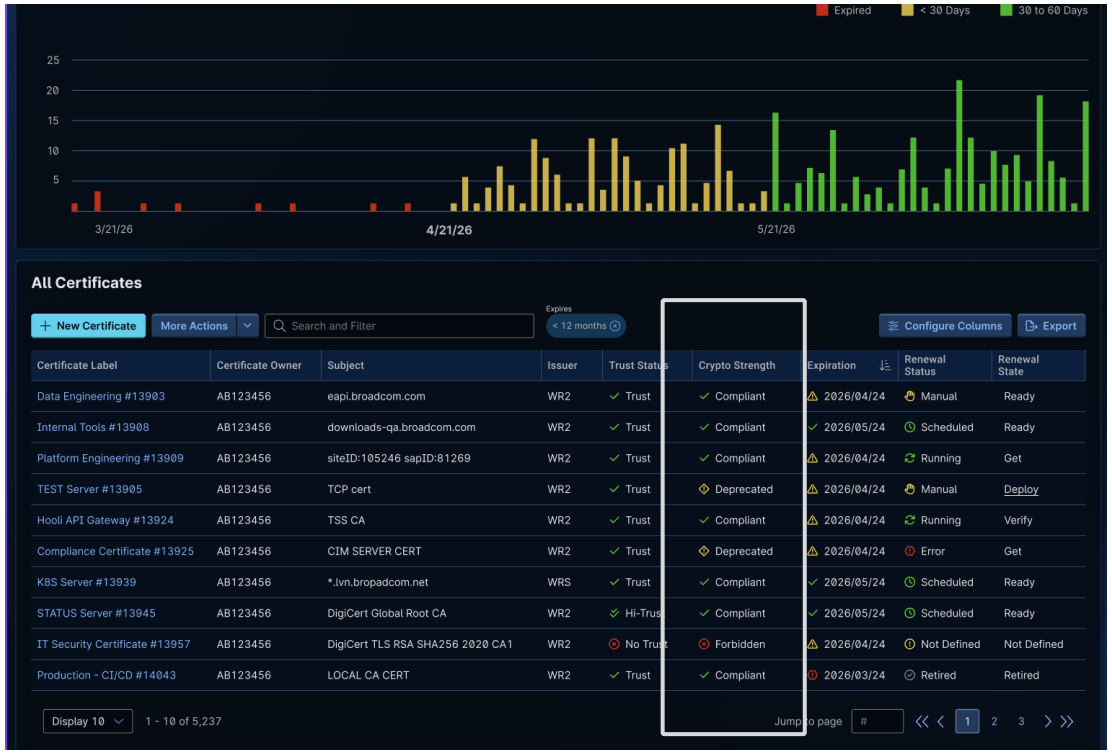




Post-Quantum Cryptographic (PQC) Readiness

The ultimate '**North Star**' of our CLMz solution





Enable 'Quantum Proof' Signing

Defeating 'Harvest Now, Decrypt Later' (HNDL)

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/