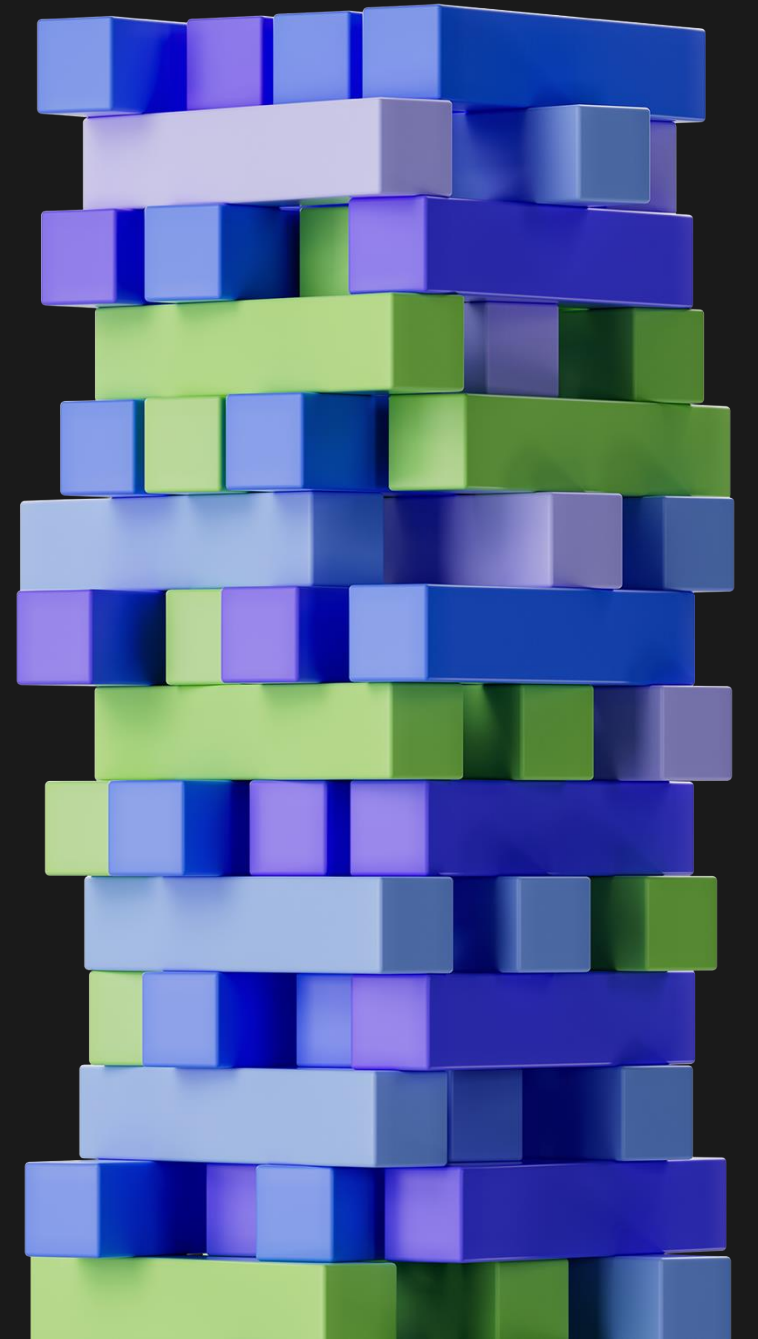


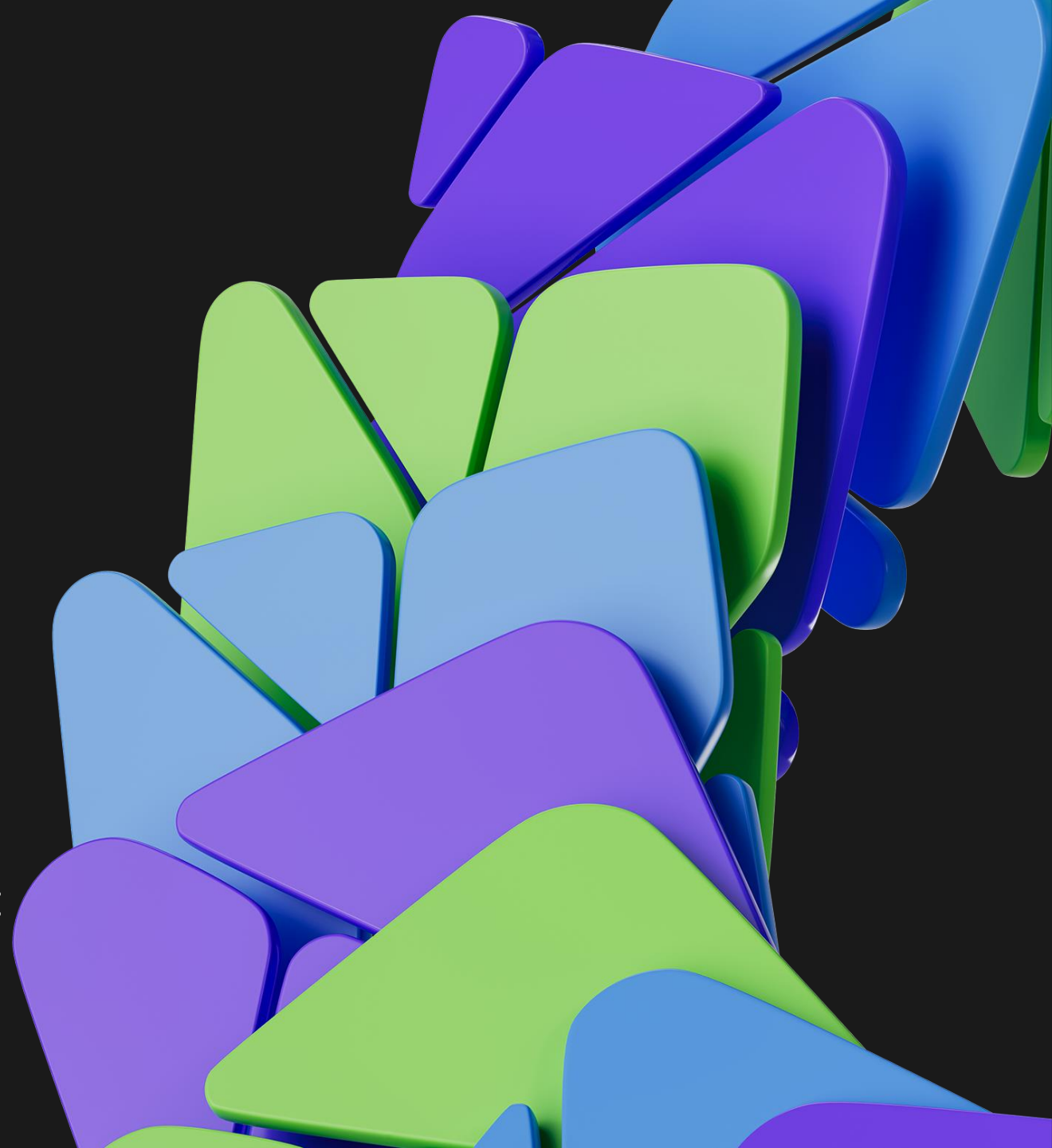
KEYFACTOR



KEYFACTOR


Winter 2024 Product Briefing Europe

Keyfactor Product Management and Product
Marketing



Agenda

- Introduction, Regulations, and High-Level Roadmap
- Insiders Update
- Bouncy Castle and PQC
- EJBCA 9.1 and Hardware Appliance
- SignServer 7.1 and Signum Improvements
- What's New in Command 24.4
- Customer Interview with Mihkel Tammsalu of SK ID Solutions

The background features a series of overlapping, wavy lines in shades of blue and green, creating a sense of depth and movement. The lines are most prominent on the right side of the slide, where they curve and flow downwards. The left side of the slide is a solid black area containing the text.

Introduction, Regulations, and High-Level Roadmap

Admir Abdurahmanovic, SVP Strategy

Mark Thompson, SVP of Product Management

KEYFACTOR

Let's talk about

What's changing in the regulatory landscape?

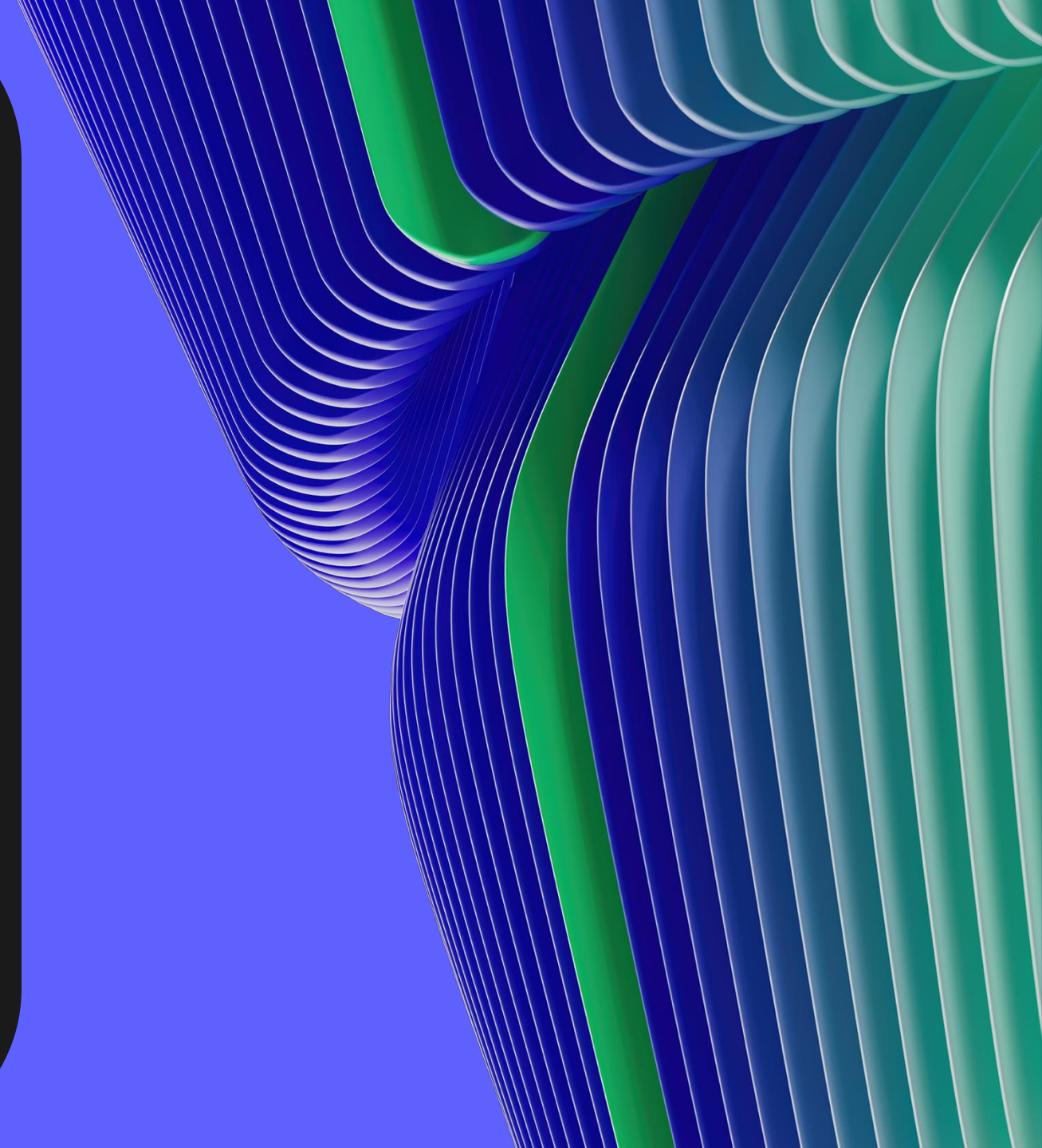
NIS2 | Critical Infrastructure

DORA | Financial Sector

Insiders Update

Ryan Sanders, Sr. Director of Product and Customer
Marketing

KEYFACTOR





Keyfactor Insider Program

Get insider access to the latest updates, events, exclusive content, and opportunities to engage with industry peers.

Benefits:



Be the First to Know



Insider Tips & Training



Access Insider Opportunities

✓ Insider Newsletter

Monthly updates on product releases, relevant content, and events.

✓ Release Notifications

Timely alerts on software and feature releases relevant to you.

✓ Content & Feedback

Participate in surveys and get early access to exclusive content.

✓ Unique Experiences

Invitations to exclusive events and speaking opportunities.

✓ Roadmap Sessions

Virtual session with product owners.



KEYFACTOR
connect
Frankfurt



25+

Peers from
leading German
manufacturers
and enterprises






30+

Peers from leading UK enterprises and government agencies

KEYFACTOR *Tech Days*

 *Hotel Fountainsbleu Miami Beach*

 *March 4-5, 2025*



KEYFACTOR

connect

Tech Days Edition

Learn

Engage,

Connect

Gain insights and best practices

Hear from Zoom, GRENKE, ServiceNow, Royal Caribbean, and other customer speakers.

Dig deep and ask questions

Get in-depth insights into the roadmap and ask questions directly from our product teams.

Connect with your peers

Network with peers and Keyfactor end-users in at social events and in roundtables.



Need a few more reasons to attend?

- Earn up to 12+ CPE credits
- Hands-on experiences & interactive workshops and demos
- Sharpen your expertise in PQC, PKI, compliance, and product security
- Hear from industry leaders, including Gary Foote, CIO at Haas Formula 1 Team plus Executives from Zoom, DocuSign, ServiceNow, M&T Bank, Gallagher, Santander Bank, and more!

Register by **December 20** for just **\$399**

Poll #2

Are you planning to attend our customer conference Keyfactor Tech Days March 4-5, 2025 in Miami, Florida?

1. Yes
2. No
3. Undecided

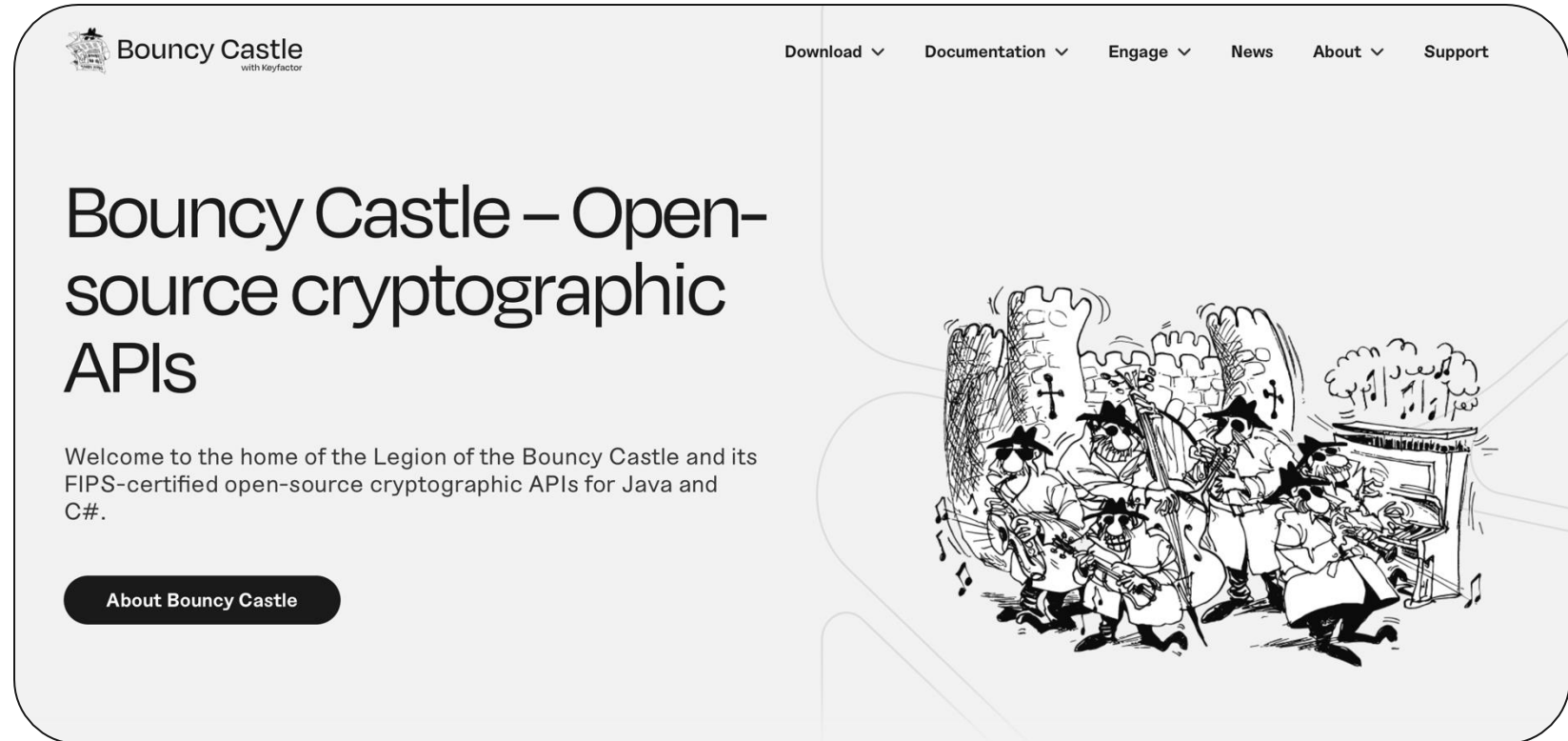
Bouncy Castle and PQC

Mark Thompson, SVP of Product Management

KEYFACTOR

About Bouncy Castle

- Open-source cryptographic APIs for Java and C#
- Offering solutions for 20+ years for:
 - FIPS certifications
 - LTS releases
 - Quantum-ready support
- Free to use, with support contracts available



The screenshot shows the Bouncy Castle website homepage. At the top left is the logo "Bouncy Castle with Keyfactor". To the right is a navigation menu with links: "Download", "Documentation", "Engage", "News", "About", and "Support". The main heading is "Bouncy Castle – Open-source cryptographic APIs". Below this is a welcome message: "Welcome to the home of the Legion of the Bouncy Castle and its FIPS-certified open-source cryptographic APIs for Java and C#." A dark button labeled "About Bouncy Castle" is positioned below the text. On the right side of the page is a cartoon illustration of a castle with a cross on its tower, surrounded by a group of knights in medieval attire playing musical instruments like lutes and a keyboard.

More information at bouncycastle.org

PQC Algorithm Momentum: Releases

Java v1.79 contains full implementations of the new PQC algorithms

- ML-KEM
- ML-DSA
- SLH-DSA

Bouncy Castle C# .NET 2.5.0, also featuring the new PQC algorithm set is planned to be released soon.

- A working beta containing PQC support is already available.

October 31, 2024

December, 2024

Other Bouncy Castle PQC Updates

BC-FNA 2.0.0, the in-progress FIPS 140-3 module for C#, now has ML-KEM, ML-DSA, and SLH-DSA added to it as well and is currently going through final algorithm validation.

BC-FJA 2.2.0, the update to BC-FJA 2.0.0, our existing FIPS 140-3 Java certificate, is going through initial algorithm validation for the new PQC algorithm set as well.

PQC Algorithm Usage

Supporting PQC Algorithms in:

- CMS
- PKI
- TLS

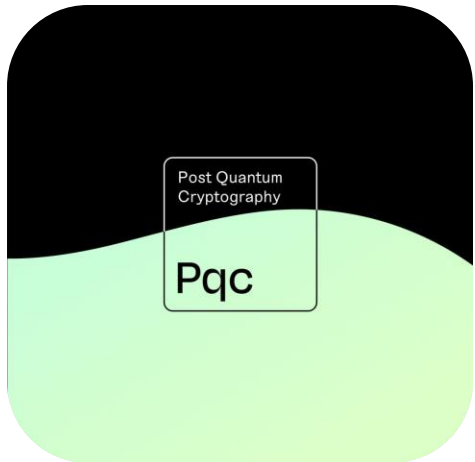
KEM Usage:

- Supporting RFC 9629, which enables:
 - Use of KEM algorithms in CMS
 - Enables the issuing of certificates for KEM keys via protocols such as CRMF

Initial work for this has already appeared in BC Java 1.79 (October), and should appear in BC C# .NET 2.5.0 as well

Evolution of Standards and Interop Testing:

- IETF hackathons
- X9 Accredited Standards Committee
- National Cybersecurity Center of Excellence (NCCoE)



EJBCA 9.1 and Next-Generation Hardware Appliance

Magnus Normark, Sr Product Manager

Lutz Stumpe, Senior Product Manager

KEYFACTOR

KEYFACTOR

EJBCA 9.1

Mark Thompson, SVP of
Product Management



What's in EJBCA 9.1

Available Now!

All versions available for customer
download

Quantum-Safe PKI

- Issue certificates with NIST Approved PQC standards
- Hybrid and single algorithm certificates

Compliance & Protocols

- Matter Operational Certificates
- CAA for S/MIME certificates

Major Tech Upgrades

- WildFly 32+
- JBoss EAP 8
- Bouncy Castle 1.79
- Gradle

Other improvements

- Extended HSM support
- REST API Extensions

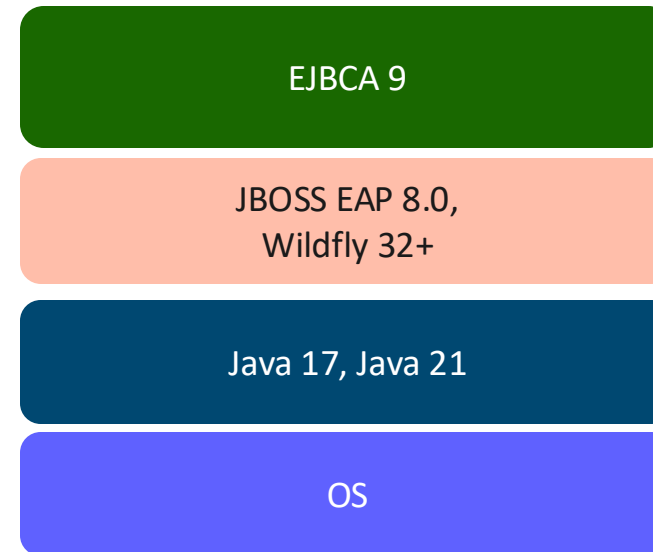
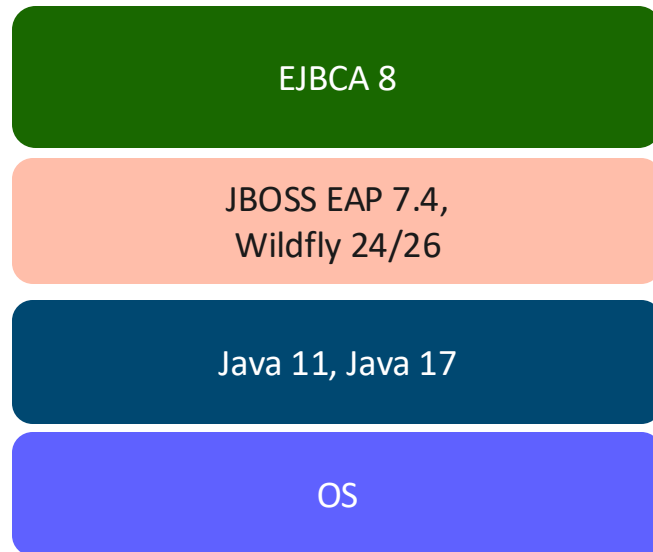
NIST Approved PQC Algorithms in EJBCA



Approved Algorihtm	Replaces Candidate Algorithm	EJBCA support
ML-DSA	Dilithium	EJBCA 9.1
ML-KEM	Kyber	EJBCA 9.1
SLH-DSA	SPHINCS+	Roadmap 2025

- NIST Approved PQC Algorithms currently supported with **Soft Crypto Tokens only**
- NIST Approved PQC Algorithms with HSM support in roadmap for 2025
 - PKCS11 draft standard with support for NIST approved PQC algorithms exists

EJBCA 8 vs EJBCA 9: Tech Stack Upgrade



KEYFACTOR

Next Generation Hardware Appliance

Lutz Stumpe, Senior Product Manager

Next-Gen Hardware Appliance

Built on 10 years of deployment experience



New Hardware Layout

1 HU half-length industrial-grade appliance

New Software Architecture

Flexible, container-based software under the hood

Whats Inside NX HW App

NX Hardware

- Intel XEON Silver 4410T
- 2TB SSD memory
- 64GB RAM
- Dual, field replaceable power supply

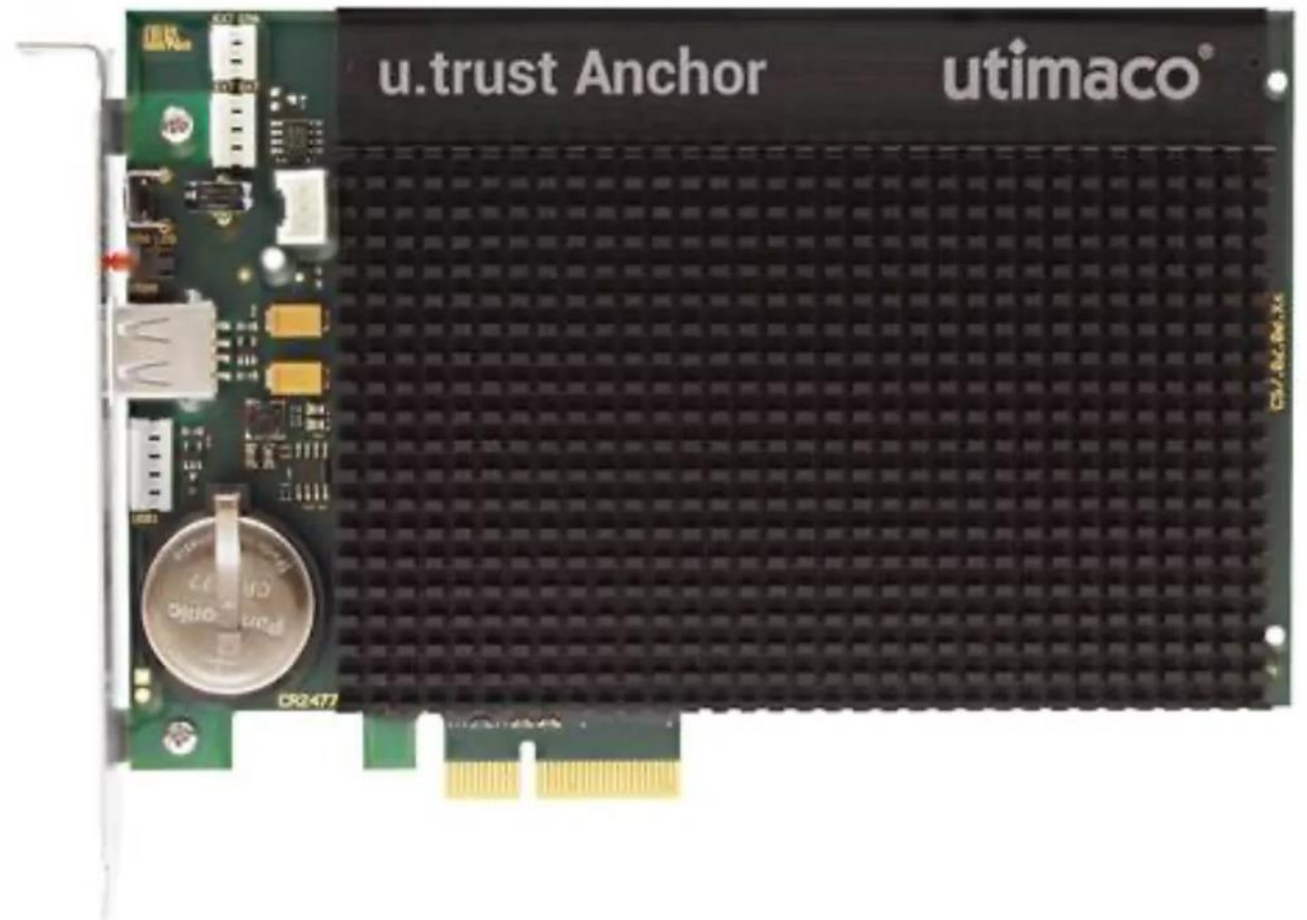
NX Software Stack

- Containerization
- Off-the-shelf Linux
- Off-the-shelf orchestration
- Inter-container REST based communication
- Side-car containers for managing container lifecycle
- [HSM agnostic](#)



Utimaco U.Trust

- U.trust Se100
- U.trust Se 2k
- FIPS 140-2 Level 3
 - FIPS 140-3 pending



Thales Luna S790

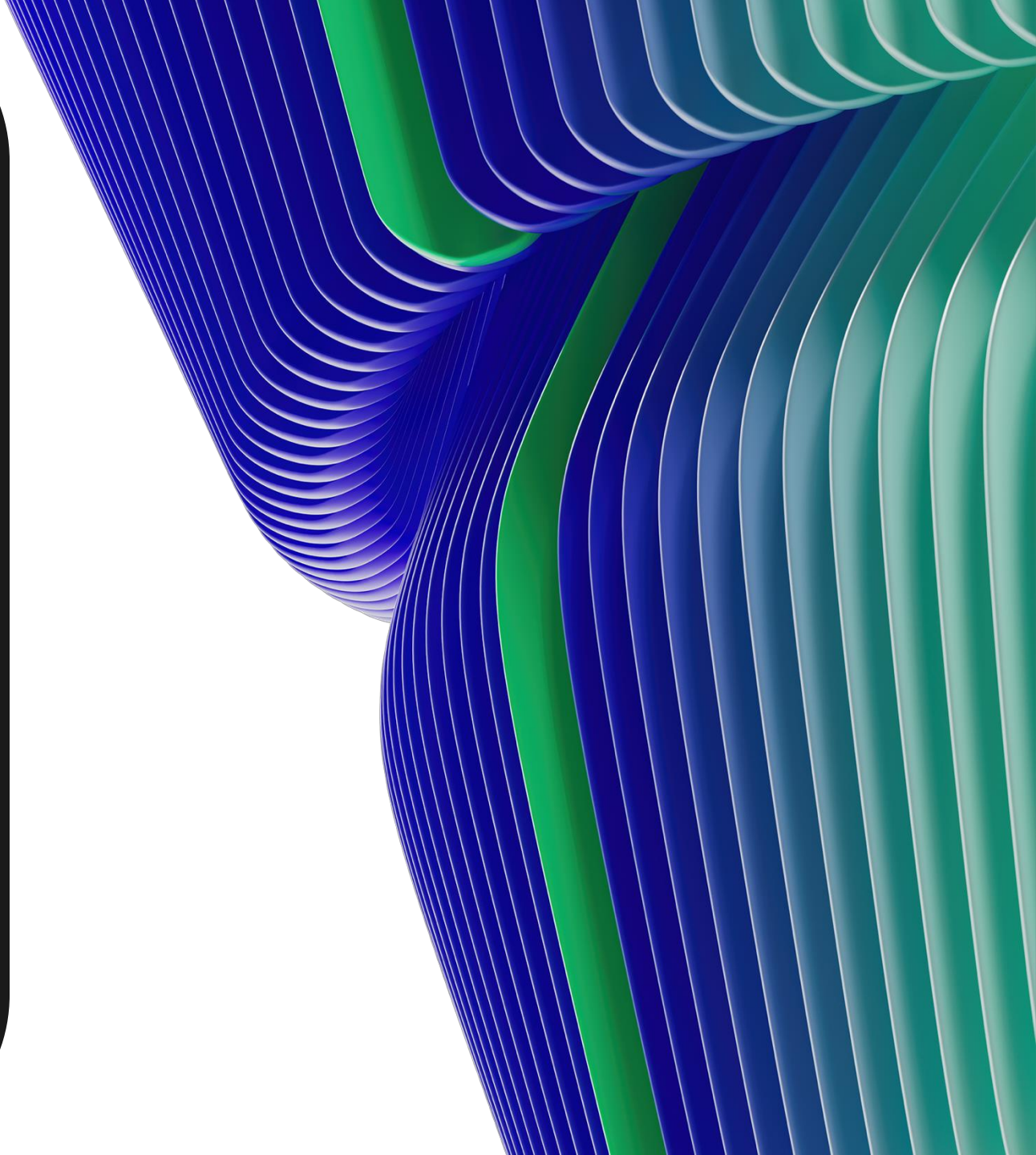
- PCIe card
- 1 Backup HSM
- 1 PED device
- 10 PED Keys
- 10 Partitions
- FIPS 140-2
- FIPS 140-3



SignServer 7.1 and Signum Improvements

Ben Dewberry, Product Manager Signing and Key
Management

KEYFACTOR



SignServer 7.1

Meet the new NIST PQ Algorithms Now Supported:

FIPs 204 | ML-DSA (previously Dilithium)

- Quantum Resistance but larger key sizes, is approved for generating digital signatures

FIPs 205 | SLH-DSA (previously SPHINCS+)

- Stateless hash-based, a NIST standard but not yet approved for creating digital signatures for NSS
- Larger signatures and slower compared to ML-DSA

More Info: [CNSA 2.0 FAQ \(April 2024\)](#)

SignServer 7.1

Deep Dive

Algorithm	Spec	Signature Size
ECDSA	P-256	72B
RSA	4096	512B
ML-DSA	44	2.4K
ML-DSA	65	3.2K
ML-DSA	87	4.5K
SLH-DSA	SHA2-128S	7.7K
SLH-DSA	SHA2-128F	17K

Strength Options

Simple: Optimized for small sigs but slower

Fast: Optimized for speed but larger sigs

ML-DSA-44/65/87
Strength

SLH-DSA-SHA2/SHAKE-128/192/256-f/s
Hash Algorithm Strength & 2 options

Marketplace Customer Portal Demo and Roadmap

Mike Bailey, Sr. Product Marketing Manager

KEYFACTOR

Keyfactor Customer Portal Intro

What is it?

- Revised customer portal
- Switch between deployments, even with different cloud providers

Who gets access to it?

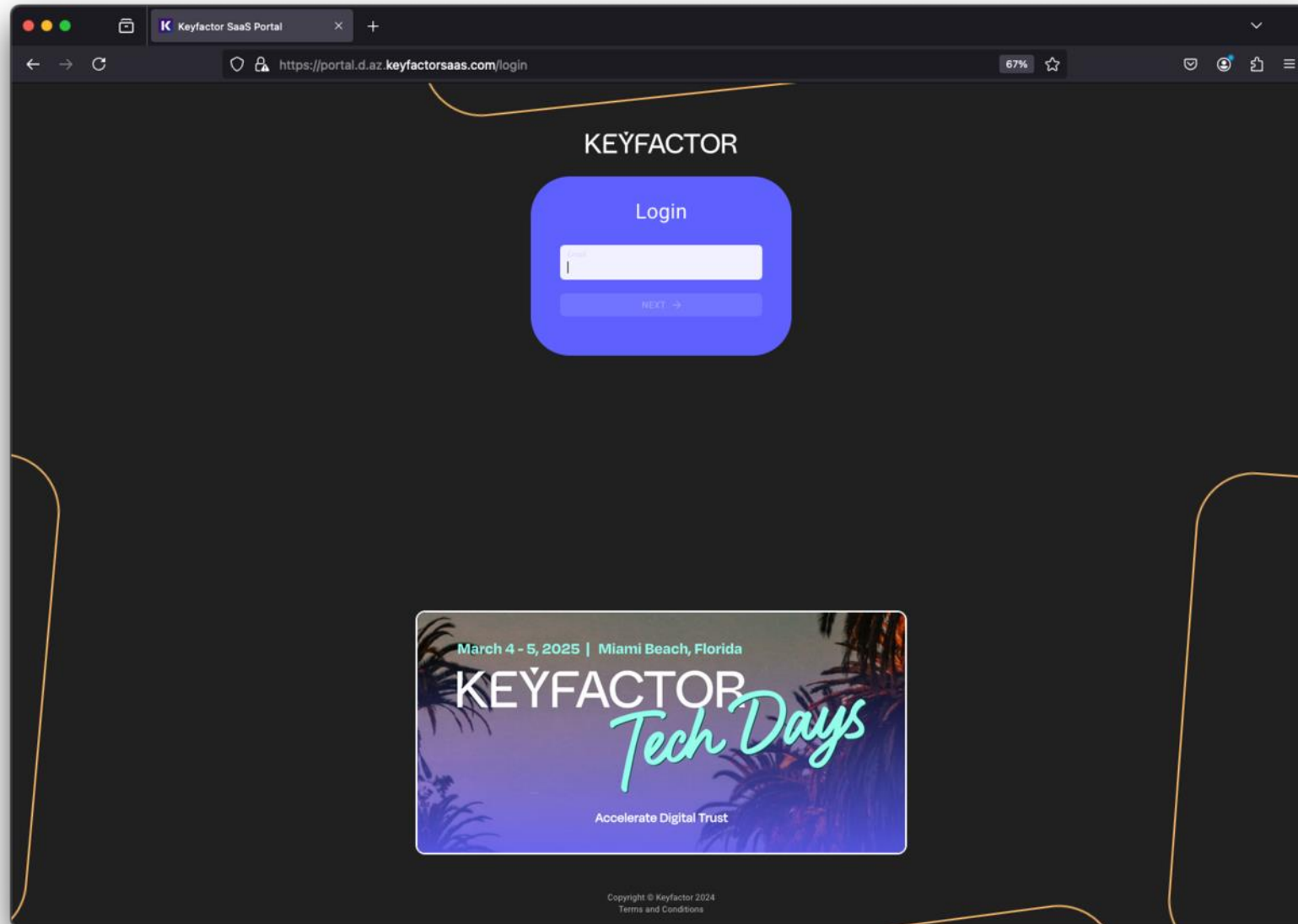
- **Now:** Azure users
- **December:** AWS users
 - Comms sent via email before the switch to the new portal

What else should I know?

- Existing customers will be migrated over with the same accounts
- SaaS production deployments will not be impacted
- Integrates with SSO solutions, with self-service SSO settings (Adaptive/Always)
- Entitlement data displayed at organization level for administrators

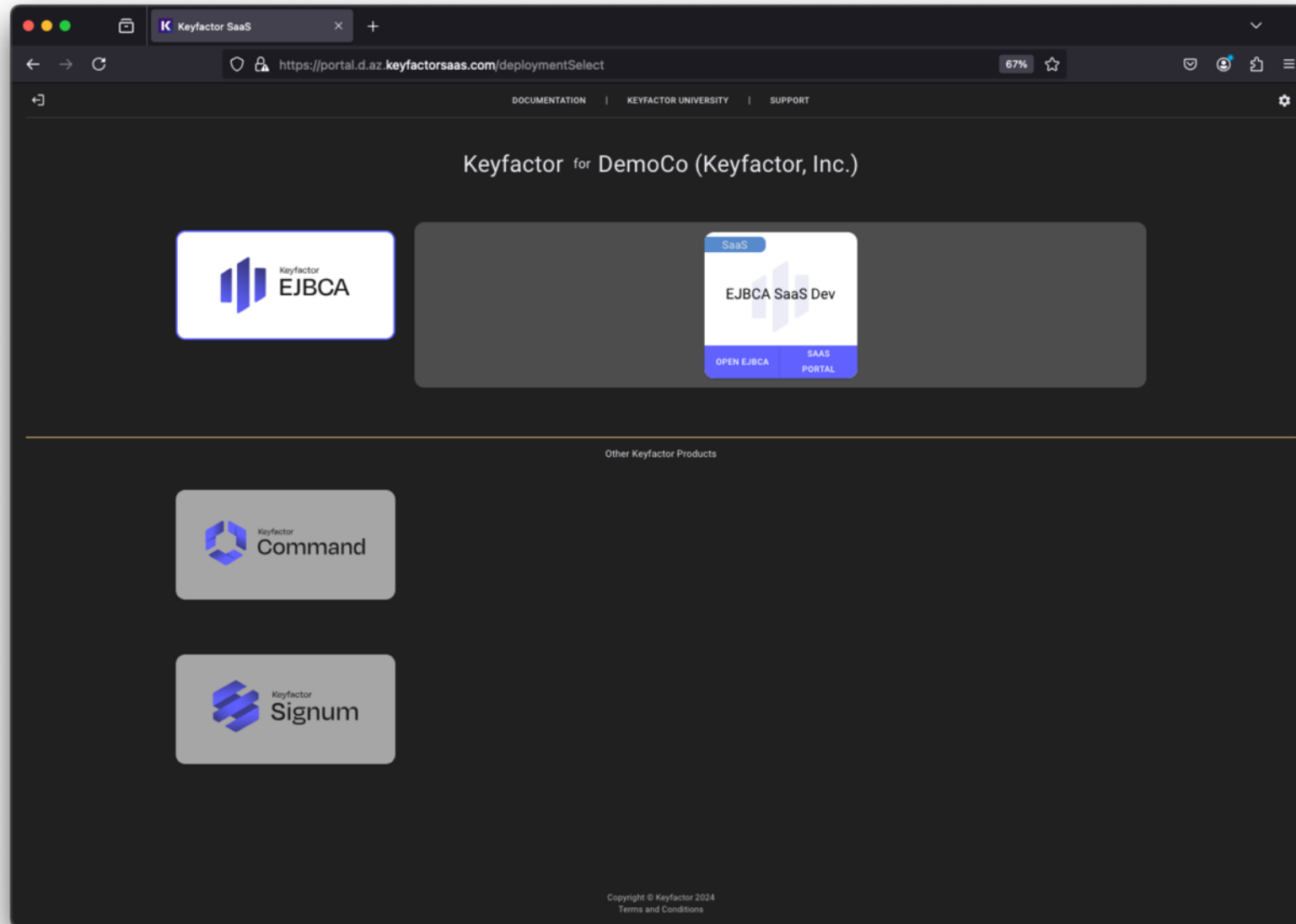
SaaS Portal - Login

AWS & Azure
SaaS
Customers
Only



SaaS Portal - Deployment Tiles

AWS & Azure
SaaS
Customers
Only



SaaS Portal - Additional Tiles

AWS & Azure
SaaS
Customers
Only

The screenshot shows a web browser window with the URL <https://portal.d.az.keyfactorsaas.com/deploymentSelect>. The page title is "Keyfactor for DemoCo (Keyfactor, Inc.)". The main content area features three product tiles: "Keyfactor EJBCA" (grey), "Keyfactor Command" (white), and "Keyfactor Signum" (grey). Below these is a section titled "Other Keyfactor Products" which highlights "Command SaaS Lite" in a white box. The "Command SaaS Lite" tile includes a description, three bullet points, and two buttons: "GO TO MARKETPLACE" and "CONTACT SALES".

Keyfactor for DemoCo (Keyfactor, Inc.)

Keyfactor EJBCA

Other Keyfactor Products

Command SaaS Lite

Keyfactor Command SaaS Lite helps teams maintain visibility and control of their expanding certificate needs. Without an accurate inventory, you're blind to certificates that may be vulnerable, nearing expiration, or don't comply with policy. Outages and audit failures caused by expired or weak certificates lead to expensive downtime and disruption.

- Faster Deployment:** Get up and running in minutes and use automated discovery to build a centralized inventory of public and private certificates in hours.
- Streamlined Management:** View all certificates from a centralized dashboard, drill into details, monitor status, and automate alerts to owners to prevent outages.
- Maintain Compliance:** Standardize enrollment & issuance of certificates and schedule reports to ace audits and keep stakeholders informed.

[GO TO MARKETPLACE](#) [CONTACT SALES](#)

Copyright © Keyfactor 2024
Terms and Conditions

SaaS Portal - Unified View

AWS & Azure
SaaS
Customers
Only

DOCUMENTATION | KEYFACTOR UNIVERSITY | SUPPORT

Keyfactor for DemoCo (US East Mfg)

Keyfactor Command

Keyfactor EJBCA

Keyfactor Signum

SaaS One to Start
OPEN COMMAND SAAS PORTAL CONFIGURE

SaaS Number Two For my org
CONFIGURE

SaaS Third test for DisOrg
CONFIGURE

CLaaS My CLaaS
LICENSE TOOLS

On-Prem My Command
LICENSE TOOLS

PKIaaS My PKIaaS
LICENSE TOOLS RESOURCES

SaaS Portal - Unified View

AWS & Azure
SaaS
Customers
Only

DOCUMENTATION | KEYFACTOR UNIVERSITY | SUPPORT

Keyfactor for DemoCo (US East Mfg)

Keyfactor Command

Keyfactor EJBCA

Keyfactor Signum

SaaS
Swedish Logic Puzzle Game You Want To Play
OPEN EJBCA | SAAS PORTAL

SaaS
Ejbca2, Brute
CONFIGURE

Cloud
My EJBCA Cloud
CLOUD RESOURCES

Hardware
My EJBCA Hardware Appliances
H/W RESOURCES

Software
My EJBCA Software Appliances
S/W RESOURCES

SaaS Portal - Unified View

AWS & Azure
SaaS
Customers
Only

The screenshot displays the Keyfactor SaaS Portal Unified View interface. At the top, there is a navigation bar with links for DOCUMENTATION, KEYFACTOR UNIVERSITY, and SUPPORT, along with a home icon and a settings gear icon. The main header reads "Keyfactor for DemoCo (US East Mfg)". Below this, three Keyfactor product tiles are visible: "Keyfactor Command", "Keyfactor EJBCA", and "Keyfactor Signum". The "Keyfactor Signum" tile is highlighted with a blue border. To the right, a "NewSigChartDev" tile is shown, featuring a "SaaS" label, the product name, and two buttons: "OPEN SIGNUM" and "SAAS PORTAL".

SaaS Portal - Unified View

AWS & Azure
SaaS
Customers
Only

The screenshot shows a dark-themed SaaS portal interface. At the top, it displays the organization name 'US East Mfg' with an edit icon. Below this are two menu items: 'User Management' and 'Authentication Settings', both with dropdown arrows. The main section is titled 'My Organization's Subscriptions' and contains a table with the following data:

Products for	Start Date	Expiration Date	Size	Quantity
Keyfactor Command Elite HA Multi-Region Environment	2022-03-31	2024-08-31	Enterprise Geo-Redundant	1
Gold Support	2022-03-31	2024-08-31	-	1
Keyfactor Command Mid-Enterprise CLaaS Environment	2022-03-31	2024-08-31	Mid-Enterprise	1
EJBCA SaaS Small with AWS HSM	2022-06-23	2024-09-29	Small	1
Azure EJBCA SaaS Extra Large with HSM	2022-09-30	2024-09-29	-	1
Signum	2023-07-12	2024-07-11	-	1

At the bottom of the page, there is a copyright notice: 'Copyright © Keyfactor 2024 Terms and Conditions'.

What's New in Command 24.4

Sami Van Vilet, Principal Product Manager

KEYFACTOR



Keyfactor

Command

Command in 2024

Workflows

- Certificate enters/leaves certificate store container
- Post-operation workflow steps
- Workflow disabling and version reverting
- Alerts can use workflows
- Set metadata workflow step
- External validation data in workflow data bucket

Certificate owner role

To make user management and certificate ownership even easier to manage, it can be set automatically or manually.

Multi-IdP support

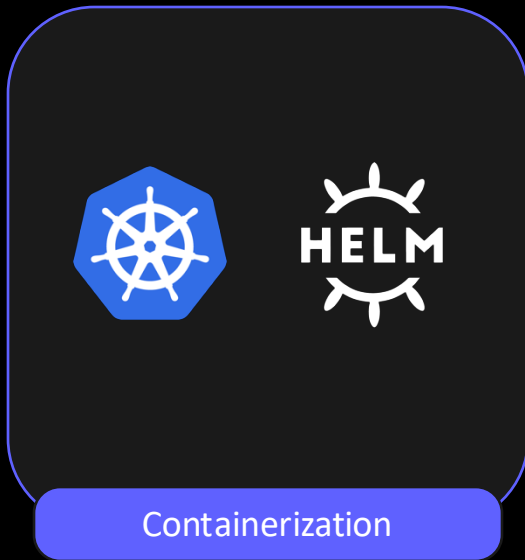
Enables support for multiple identity providers, such as Azure AD, Auth0, Okta, etc.

Other enhancements

- Orchestrator job history retention limit
- SSL/TLS scanning performance improvements
- Renewed certificate report
- Sync with EIBCA for PQ certificates

Coming Soon

Command 24.4



Containerization

A new container-based architecture for scalability, portability, and easy installation



Hybrid & PQC support

Ability to inventory and generate hybrid and PQC certificates



Support for local secrets

Users can now manage locally stored secrets from a PAM provider in the UI



DB upgrade tool

Users can ensure the database upgrade is successful before re-installing Command

Poll #3

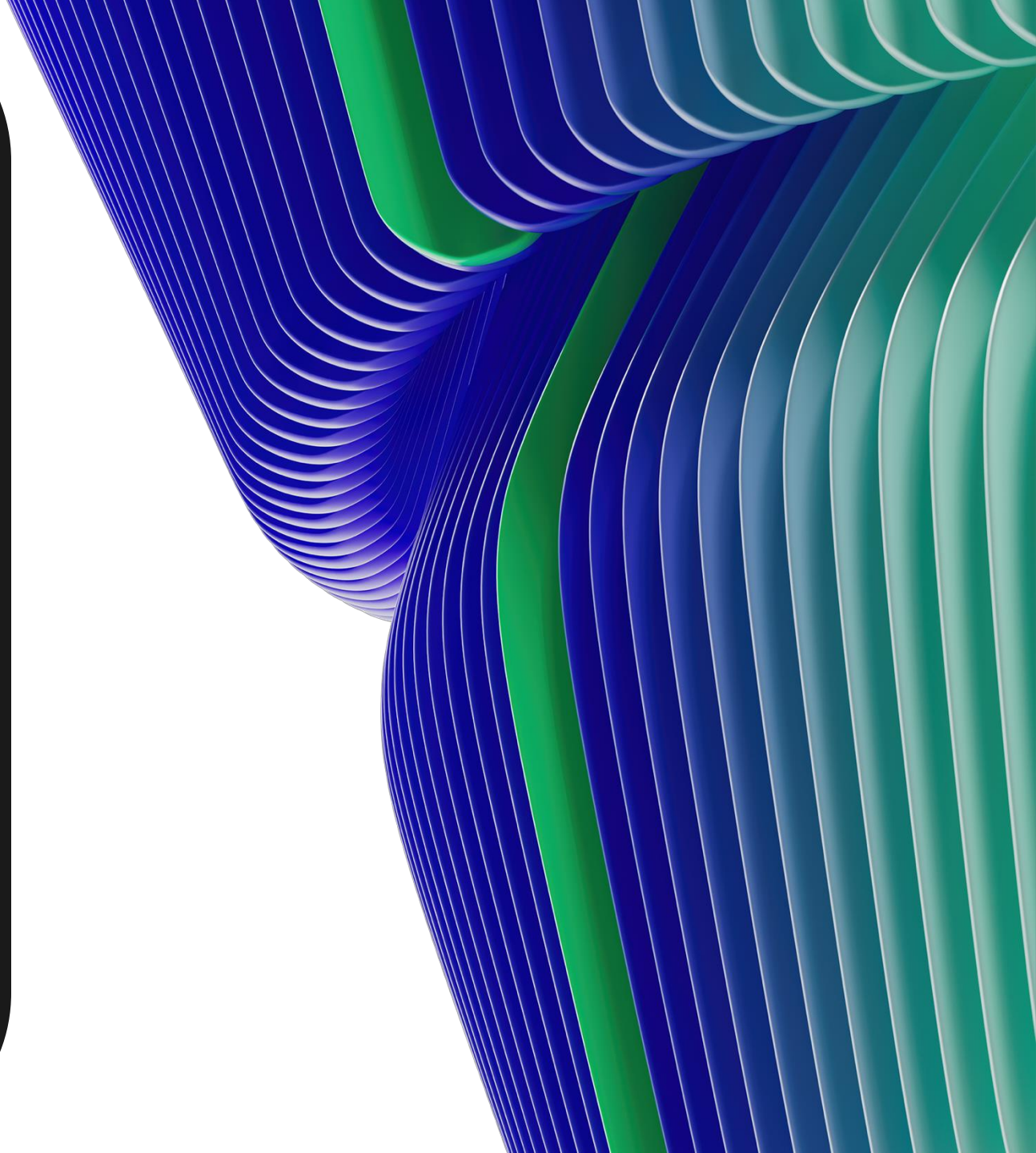
Which Keyfactor solution that you don't currently use would you like to learn more about?

1. EJBCA PKI platform
2. Command certificate lifecycle automation
3. SignServer or Signum signing
4. Bouncy Castle cryptographic APIs
5. PKI as a Service

Customer Interview with Mihkel Tammsalu of SK ID Solutions



KEYFACTOR



About SK ID Solutions

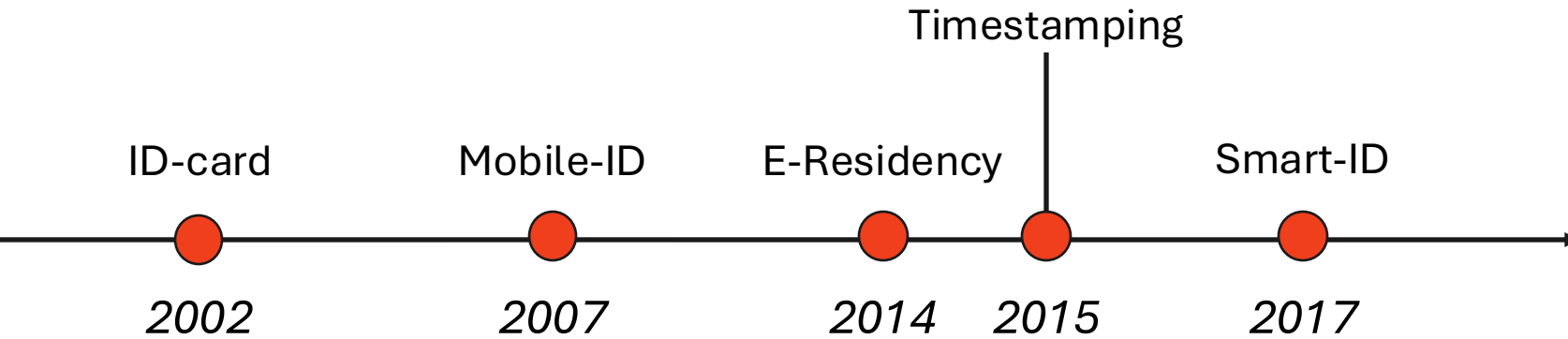
Key Highlights:

- Qualified Trust Service Provider in EU
 - Offices in EE, LV, LT
- Certified under eIDAS
- Included in EU Trusted List

Background

- Privately-held company founded in 2001
- Runs core infrastructure for Estonian National eID

SK ID SOLUTIONS Services Evolution



2.5B
Transactions per
year

Core Competencies

- E-identity solutions
- Strong customer authentication
- Legally binding e-signatures
- Biometric onboarding solutions
- Remote onboarding

KEY FACTOR

SK ID SOLUTIONS PKI Pain Points

- Previous CA product line EOL, used for ~10 years
- Changing architecture:
 - CA and OCSP under the same product
 - Infrastructure harmonization
 - More modular services

KEYFACTOR



Regulations and Requirements

- X.509 (ITU-T Recommendation)
- RFC
- eIDAS driver ETSI standards
- CA/Browser Forum (optional)
- CC EAL4+ certification
- Interoperability with FIPS, NIST domain

SK ID SOLUTIONS Migration Experience

20M

Active certificates (+
non-active)

5

Different
business services

- Service RA data
 - Oracle to Postgre
 - New service components
- Root PKI hierarchy



Advice for a Move to a New CA Platform

- Start early!
- Assess your needs – what kind of services you have or will have
 - Pricing model, support plan(s)
- Do requirements evaluation
 - Mandatory, optional, nice to have
- Have 2-3 vendors/platforms to consider
 - Talk to them
 - Test product technically – key requirements especially!

KEYFACTOR

Open Q&A

Ask us anything

Hunger Relief, One Review at a Time

The logo for KEYFACTOR, featuring the word "KEYFACTOR" in white, uppercase, sans-serif font on a solid blue rectangular background.

Exciting opportunity to make a difference

Keyfactor is partnering with G2 and World Central Kitchen to raise \$1000 for to feed those affected by crisis



Submit a Review

Your review of Keyfactor EJBCA/Command on G2 will help your peers choose the right solution



Support a great cause

Each review you submit unlocks a \$10 donation to World Central Kitchen, which provides meals to communities affected by crises around the world

KEYFACTOR

Thank you!

- Give us your feedback!
- Check out the attachments
- Register for the Insider Program
- Reach out to your CSM