Identity-Driven Zero Trust: On-Prem MFA and PKI Integration

190
countries/nationalities which have had their citizen identities verified

24M+
SWIFT messages encrypted and secured daily

100M+
protected workforce and consumer identities

20B
payment cards issued

690K
websites secured globally

95%
of IT professionals say Entrust is highly respected

10B
ID cards activated for students, employees, and citizens

Søren Christiansen

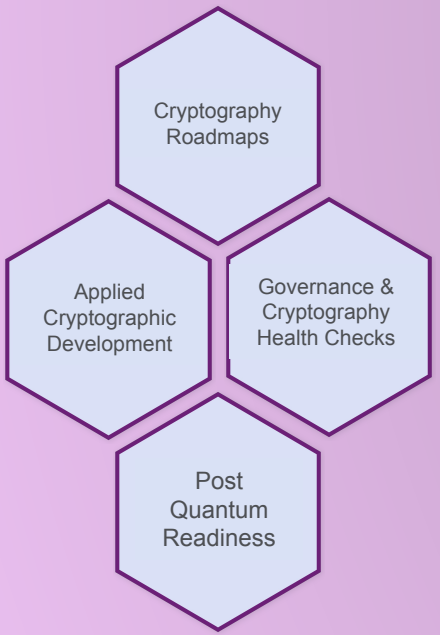
Sr. Security Architect

ENTRUST

Agenda

1. **Entrust - What do we do?**
2. **Attack Surfaces – Traditional vs Hybrid**
3. **Entrust Zero Trust Identity-Centric security**

ENTRUST


Cryptography Roadmaps
Applied Cryptographic Development
Governance & Cryptography Health Checks
Post Quantum Readiness


PKI for Machines and People
Custom Solutions
Digital/Code Signing & Time Stamping
Crypto Discovery, Control & Automation
Trust Anchors
IDV CIAM
Digital onboarding
Identity & Smart Credentials
Key/Secrets Management
Hardware Key protection
Blockchain & MPC security
Instant & Bureau Card & Passport Issuance
Digital Payment Cards
Data Encryption Services
Cloud compliance & control

ENTRUST

What is Zero Trust ?

Never Trust, Always Verify

- Verify Explicitly
- Least Privilege
- Assume Breach

ENTRUST

ENTRUST ZERO TRUST IDENTITY-CENTRIC SECURITY

Secure Identity

Enable high assurance and phishing resistant identities to ensure verified and authorized access to resources

IAM IDV PKI

Secure Connections

Establish end-to-end encryption for secure access and communications across devices, networks, and cloud

SSL CLM PKI

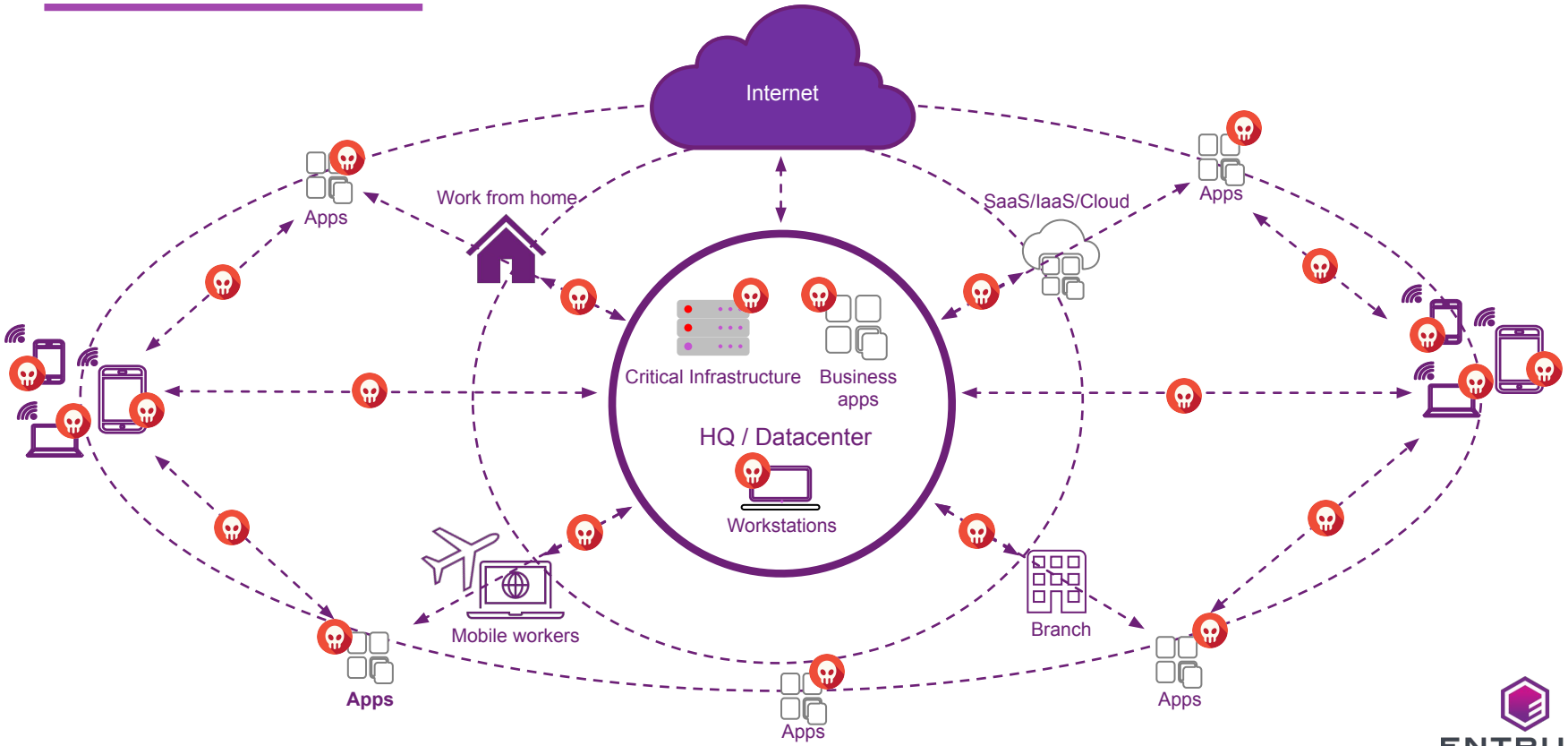
Secure Data

Secure the keys and secrets your organizations uses to protect sensitive data

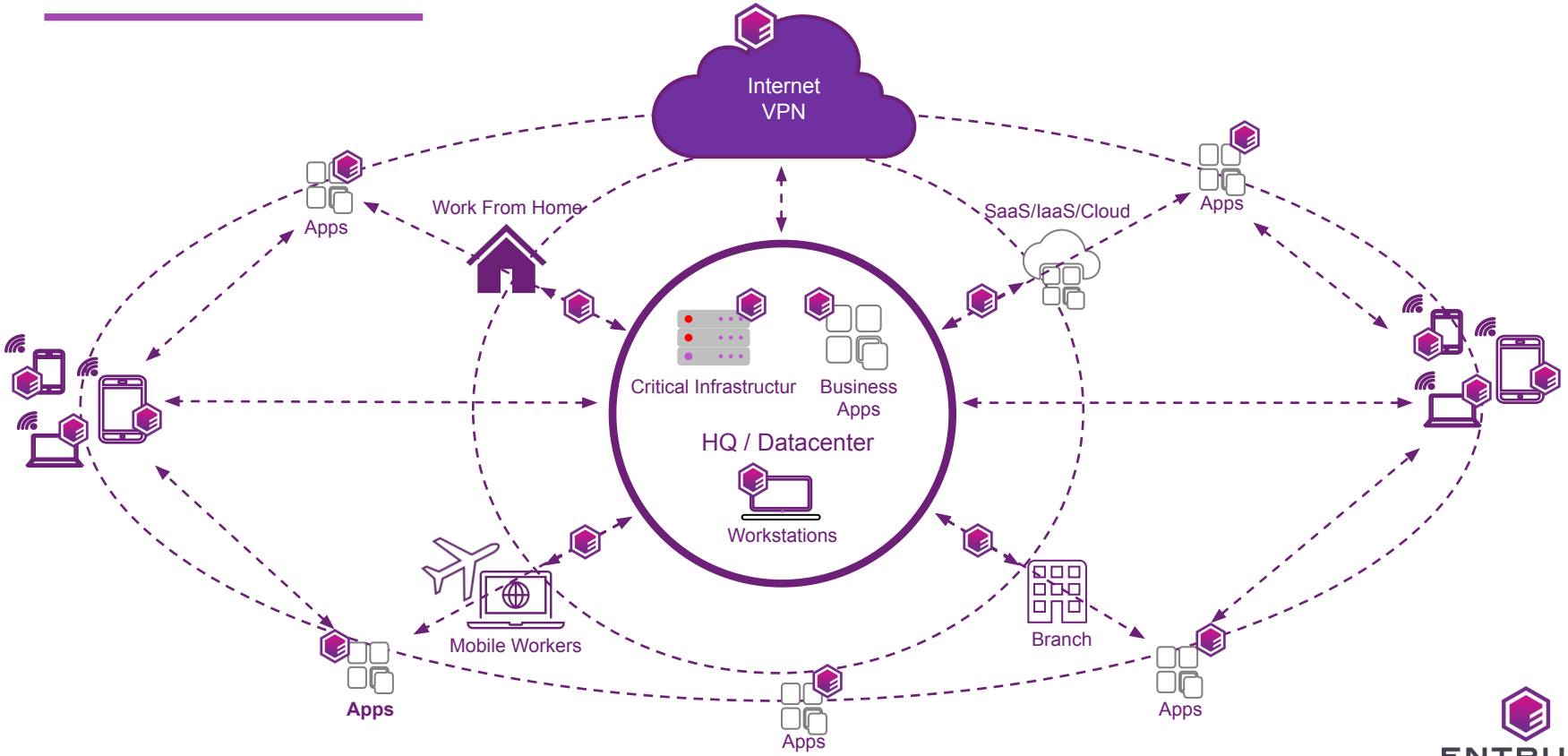
HSM Key Mgmt

ENTRUST

THE NEW ATTACK SURFACE



ENTRUST CAN SUPPORT YOU!



ENTRUST

IAM Trends

Workforce

2.7B email/password pairs exposed in Collection #1 breach highlights need for **Credential-based authentication**

Gartner predicts that 60% of large and global enterprises, and 90% of midsize enterprises, will implement **Passwordless** methods in more than 50% of use cases.

78% of IT security teams are looking to embrace **Zero Trust** network access in the future[2]

Consumer

85% of consumers wish there were more companies they could **Trust** with their data[3]

Compliance: PSD2 and strong customer authentication mandate across Europe, SAMA for Saudi Arabia, other jurisdictions to follow

73% customers: **Experience** important in purchasing decision with 43% willing to pay more for convenience[4]

[1] Ant Allan, Vice President Analyst, Gartner
[2] 2019 Zero Trust Adoption Report, Cybersecurity Insiders
[3] PwC Consumer Intelligence Series, 2020
[4] PwC Experience is Everything: Here is how to get it right

ENTRUST

Entrust Identity – Solution Portfolio

Entrust Identity for Workforce

Identity as a Service	High assurance credential-based authentication; SSO; passwordless login and SSO	Cloud
Identity Enterprise	High assurance credential-based authentication; physical smart card issuance; passwordless login	On-premises
Identity Essentials	Best-in-class MFA for Windows-based organizations; remote access protection (VPN clients, RDP)	On-premises

Entrust Identity for Consumer/Citizen

Identity as a Service	Secure portals; MFA; adaptive step-up authentication; identity proofing	Cloud
Identity Enterprise	Secure portals; MFA; adaptive step-up authentication	On-premises

ENTRUST

Entrust Identity Enterprise

IAM/CIAM

Identity Enterprise at a glance

- Entrust Identity Enterprise is a server-based software product that authenticates, controls access and manages users and their authentication data
  - “**On Prem”** Identity Solution
  - Launched in Nov. 2004. Current Release 13.0.
  - Strong MFA suite of authenticators and features
  - Support for PIV, Citizen Smart Credentials Issuance and Encoding
  - Support for Federation/SSO with Federation Module

Identity Enterprise at a glance

Mobile SDK & API for CIAM

Identity Enterprise uses the Entrust Identity mobile SDK so you can embed IAM directly into your applications and brand as your own if desired. Use our Mobile Smart Credential SDK to develop your own passwordless and document signing applications.

Secure portals

Secure access to customer and partner portals.

Secure access to cloud applications

Deploy Identity Enterprise's Federation Module for federated and SSO applications, including Office 365 using SAML.

Smart Card

Instant Encoding and Issuing of Smart Cards from Entrust Card Printers

IDENTITY ENTERPRISE ROADMAP PLAN HIGHLIGHTS (CALENDAR YEAR)

	2024	2025	2026	2027/2028
Compliance Standards	• FIDO Registration & Authentication • mDL ISO 18013-5	• WCAG 2.2/2.1 US Rehab Section 508 Accessibility • IPv6 support	• WCAG 3.0 US Rehab Section 508 Accessibility • mDL ISO 18013-5, 23200 • OID4VC (for Verifiable Creds Issuance and Presentation)	• NIST PQC Cypher • OIDC support • REST APIs • W3C Decentralized Identities
Threat, Risk and Fraud Prevention	Support TLS 1.3	End to end encryption mechanism of application layer payload prior to TLS encoding	Integration with Entrust IDV for support of biometric authentication	• Support of Biometric Verified Credentials Authentication • PQC readiness (PIV creds, performance, PQC ready ECA & HSM integration)
Citizen Smart Credentials Issuance			Integration with Citizen ID Orchestration Solution Framework for issuance of (mDL, National ID)	Health, DTC ICAO Type II & III digital mobile credentials issuance and verification
Product usage experience	• Print Module displacement – Admin Smart Credentials Encoding (ACE) and wipe-out from smart cards. • Smart credential encoding on HID Crescendo Smart card in support of PIV logical access and PACS LF physical access	• Update UI for SSM and Web admin portal accessibility capabilities (WCAG 2.2/2.1 “AA” and “A”) • PIV encoding on HID C4000 cards • ECC encoding in Gemalto PIV 3 cards	• Update UI for SSM and Web admin portal accessibility capabilities (WCAG 3.0 “AA” and “A”) • Integration with Entrust PKIaaS	Support of Flexible Low Code/No code journeys via Entrust Workflow Studio framework integration: -Onboarding and authentication flows -Drag and drop flow configs
Secured and Flexible Authentication	Support of FIDO2 Authenticators – Device Bound and Sync'ed passkeys -Registration flow. -FIDO authentication SSM login, Web App login, DCP login (2FA)	• Enhanced push authentication with “**mutual verification**” • Identity Mobile configuration changes through IDE Policy updates synchronized with (pushed to) existing user MST app.	• Step up Authentication for user profile changes • Support 3rd party OTP soft-token apps (e.g. MSFT Authenticator OTP) • Support FIDO authenticator attestation	Federation Module 13.0: • Rebranding • Updated framework (CXF) and OS platform • FIDO authentication for SSO • OIDC support

ENTRUST

Authenticators

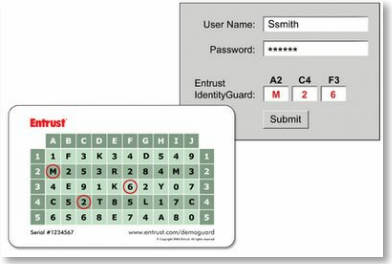
Some sample of authenticators.

Mobile App (iOS / Android)

- Run on user mobile devices
- OTP
- Push Authentication
- Transaction verification & approval
- Virtual Smart Card (Smart Credential)

Hardware Token

- OTP (OT/AT/CR)
- Easy to use
- Battery last ~ 5 years



Grid Card

- Physical card or eCard
- Easy to use
- Good for location ban / not able to use electronic device (Manufacturing, Secure Location)

Identity Enterprise - Credential Management System (CMS)

Primary Issuance PIV Credential

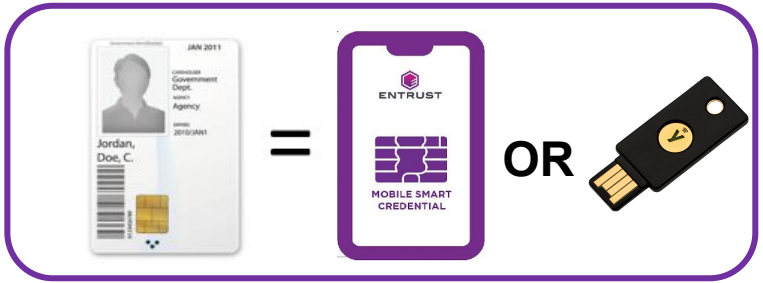
Entrust Mobile App
(iOS / Android)

Physical Smart Credential

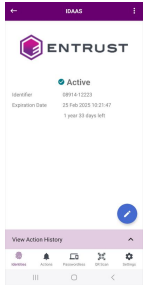
- PIV Credential
- Signing
- Encryption

Derived PIV Credential

New credential (a digital certificate) stored on a mobile device or YubiKey that is derived from the trust of a valid Personal Identity Verification (PIV) card.



Phishing Resistant Credentials



Entrust Mobile App
(iOS / Android)

- Run on user mobile devices
- OTP
- Push Authentication with Mutual Challenge
- Transaction verification & approval
- Virtual Smart Card (Smart Credential)

FIDO 2.0 / Passkeys

FIDO Authentication utilizes asymmetric cryptographic key pairs (with the private key stored on the user's device and the public key stored on the application server), which is proven to be resistant to threats of phishing, credential stuffing and other remote attacks.

Physical Smart Credential

- PIV Credential
- Login Windows/RDP
- Signing
- Encryption

Not all MFA authenticators offer the same level of protection from cyberattacks. Passwordless MFA authenticators from Entrust, such as high assurance PKI-based mobile smart credentials, FIDO2 keys, and passkeys offer phishing-resistant MFA options for greater security.

Use Cases

Defense: KIOSK Smart Card Solutions

- Identity Enterprise
- Card Readers
- Card Printers for images

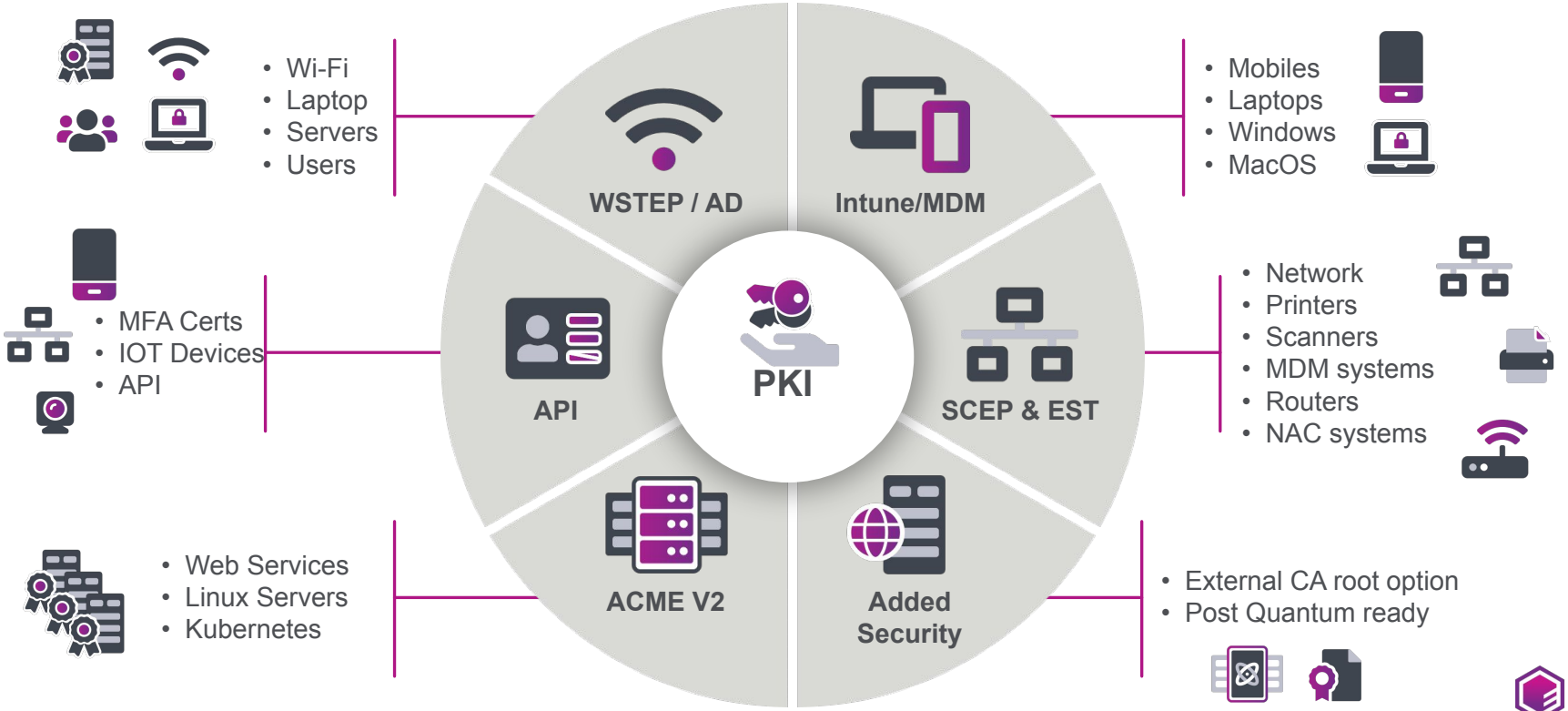
Financial: Customer logon and Transaction Verification

- Identity Enterprise
- Mobile SDK
- API integration from Banking Websites

Government workforce: Common use case like VPN, Windows Desktop Logon, O365 login, SAML application, Employee Badges, Self Service Portals

Entrust References

BETTER SECURITY AND USER EXPERIENCE – AUTOMATION INCLUDED



ENTRUST

KEY TAKE AWAYS

Secure Identity

Enable high assurance and phishing resistant identities to ensure verified and authorized access to resources

IAM IDV PKI

Secure Connections

Establish end-to-end encryption for secure access and communications across devices, networks, and cloud

SSL CLM PKI

Secure Data

Secure the keys and secrets your organizations uses to protect sensitive data

HSM Key Mgmt

ENTRUST

Thank You!

Thomas Damsgaard/ Thomas.Damsgaard@entrust.com

Søren Christiansen/ soren.christiansen@entrust.com