black hat

EUROPE 2019

DECEMBER 2-5, 2019

EXCEL LONDON, UK

#BHEU @BLACK HAT EVENTS

Bring Your Own Token (BYOT)

To Replace the Traditional Smartcards for Strong Authentication & Signing

cisco | CRYPTO SERVICES

Eric Hampshire
Information Security Architect
Cisco Systems

Karthik Ramasamy
Information Security Architect
Cisco Systems

Agenda

- Smartcards – Introduction and Use Cases
- Smartcards at Cisco - Evolution Timeline
- Limitations with traditional smartcards
- Introducing Bring Your Own Token
- BYOT - Advantages, Limitations and Best Practices
- Key Takeaways
- Demo and Q&A

Smartcards – Introduction

BEHOLD! MY LATEST CREATION... THE SMART CARD!
WHAT IS IT?
WHEN A DUMB GUY DISAGREES WITH YOU, YOU PULL OUT THE SMART CARD. IT MEANS "I'M SMART. YOU'RE NOT. PLEASE BE QUIET NOW."
OH, GEE. THAT'S JUST SILLY. I MEAN—
SHHHHHHHHHH....

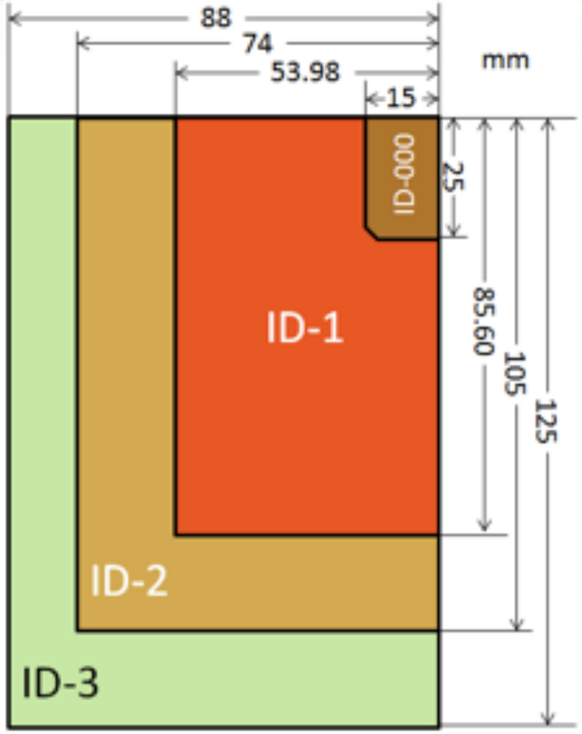
© Stephan Pastis/Dist. by UFS, Inc.

MY KOAN IS TO COMPREHEND THE SOUND OF ONE HAND CLAPPING.
MINE IS TO FIGURE OUT HOW THIS SMART CARD WORKS.
S. Harris

CartoonStock.com

Smartcards – Introduction

- Plastic card with an embedded integrated circuit chip
- Provides a tamper-resistant secure crypto processor and secure file system
- Different types (**contact/contactless**) and dimensions (**ID-000**, **ID-1**, etc.)
- ISO Standards define physical characteristics, electrical interface, transmission protocols, crypto mechanisms,
  - Contact: **ISO/IEC 7810** and **ISO/IEC 7816**
  - Contactless/proximity: **ISO/IEC 14443**
- The cryptographic key material and the digital certificates are securely generated/imported to the chip



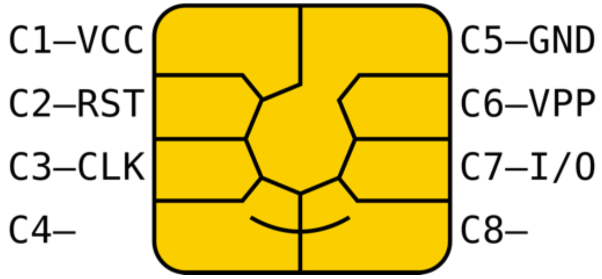
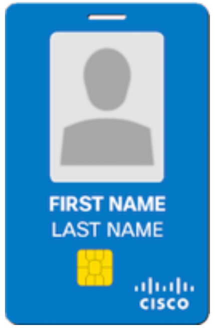


Image Source: Wikipedia

Smartcards – Use Cases

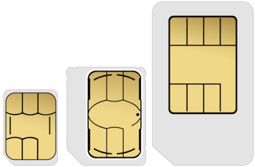


IT

- Strong Authentication (Smartcard Logon, TLS Client Authentication)
- Signing (Email, Document, Software)
- Encryption

Banking & Retail

- EMV Chip cards (Chip & PIN / Chip & Signature)



Mobile Communication

- Subscriber Identity Module (SIM)

CCID and PIV Standards

- **C**hip **C**ard **I**nterface **D**evice
  - USB standards work group, March 2001
  - Protocol and requirements for card reader using a standard USB interface
  - Latest Revision: 1.1 - April 2005.
- **P**ersonal **I**dentity **V**erification
  - FIPS 201 document by NIST in Feb 2005
  - Architecture and technical requirements for a common identification standard
  - Latest Revision: FIPS 201-2 - August 2013

Slot	Key Type	PIN Requirement
04	PIV Secure Messaging	Never
9A	**PIV Authentication**	**Once per session**
9B	PIV Card Application Administration	Never
9C	Digital Signature	Every use
9D	**Key Management**	**Once per session**
9E	Card Authentication	Never
82, 83, 84, 85, 86, 87, 88, 89, 8A, 8B, 8C, 8D, 8E, 8F, 90, 91, 92, 93, 94, 95	Retired Key Management	Once per session

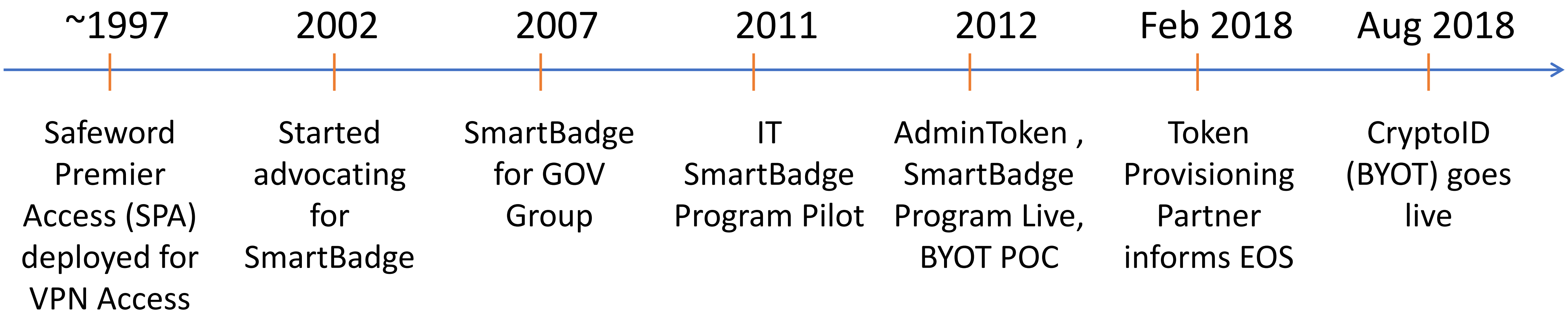
Traditional Usage at Large Enterprises

Hybrid cards that provides both the physical proximity card and logical smartcard functionalities (smart badge)

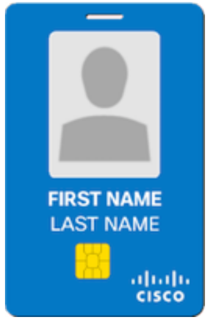
Single card for both facility access as well as strong authentication to IT servers/applications

Digital identity certificates are either provisioned on premise in the badging office using kiosks or using a 3rd party provisioning partners

Smartcards at Cisco – Timeline of Strong Authentication Solutions



~1997	2002	2007	2011	2012	Feb 2018	Aug 2018
Safeword Premier Access (SPA) deployed for VPN Access	Started advocating for SmartBadge	SmartBadge for GOV Group	IT SmartBadge Program Pilot	AdminToken , SmartBadge Program Live, BYOT POC	Token Provisioning Partner informs EOS	CryptoID (BYOT) goes live



Limitations with traditional smartcards

Provisioning Costs and Delays

- Need for Kiosks or 3rd party provisioning services
- Support for Remote workers

Support issues related to card readers

- Driver/middleware issues
- Dongles!

Handling of lost/misplaced cards

Issuing temporary/replacement smart cards

Handling certificate expiry/renewals

SNICKER
SNERK
EXCUSE ME. WHERE ARE YOUR DONGLES?
THANKS A LOT, APPLE.
ECTRONICS
Dist. by King Features Syndicate

Introducing Bring Your Own Token

Separate smartcard functions from the physical access card

Use USB Hardware Tokens that supports **PIV** and **CCID** standards

Enable Self-provisioning and management

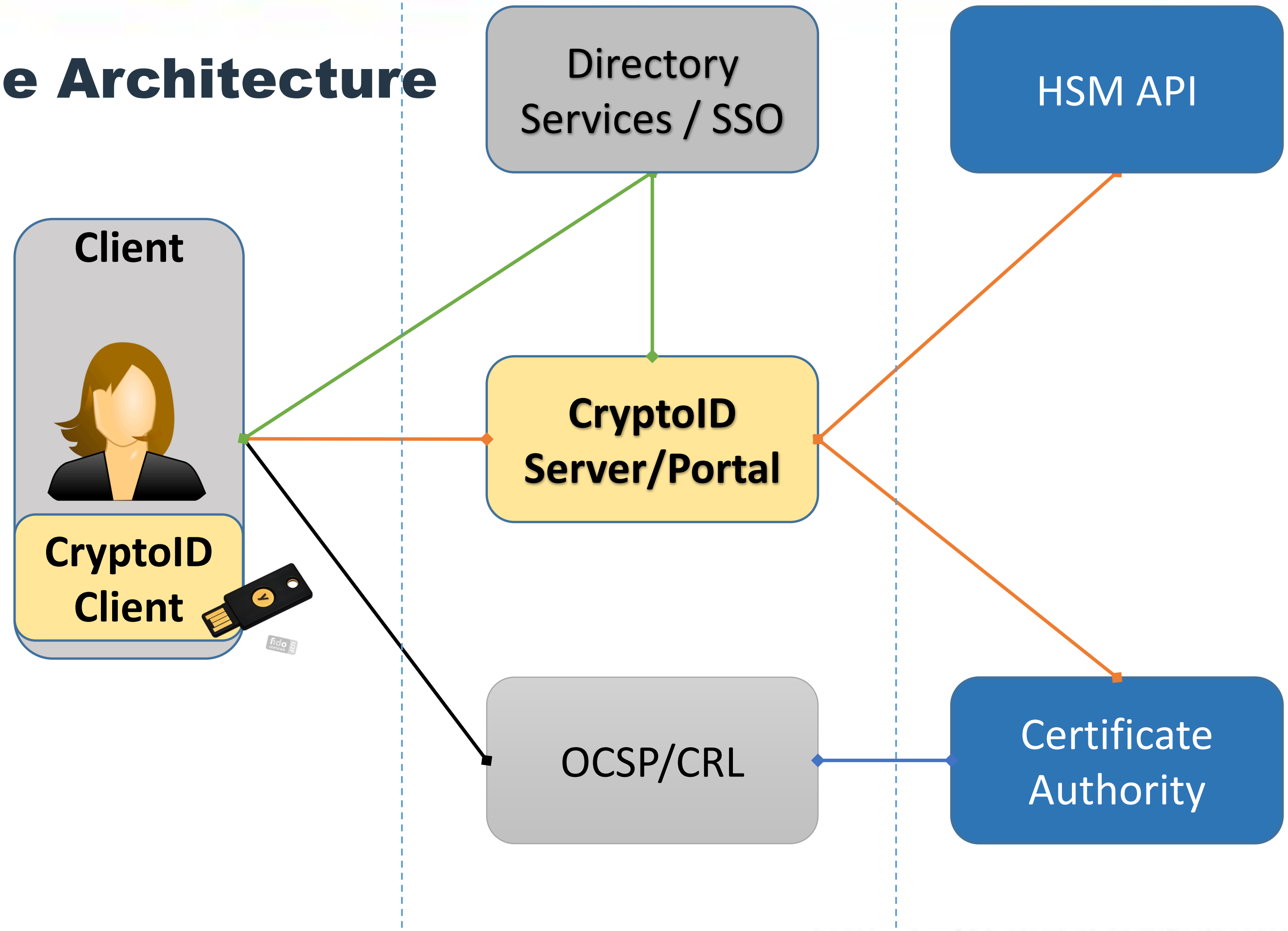
Token Selection Criteria

- Compliance with FIPS 201-2
  - Crypto Specs: NIST SP 800-78-4
    - RSA 2048 or better (PKCS #1 v1.5/PSS)
    - EC (Curve P-256 or P-384)
- Driver and application support
  - For commonly used OS
- Multi purpose tokens
  - Multi protocol support: PIV, OTP, FIDO2
- Security Updates
- Cost and Reliability

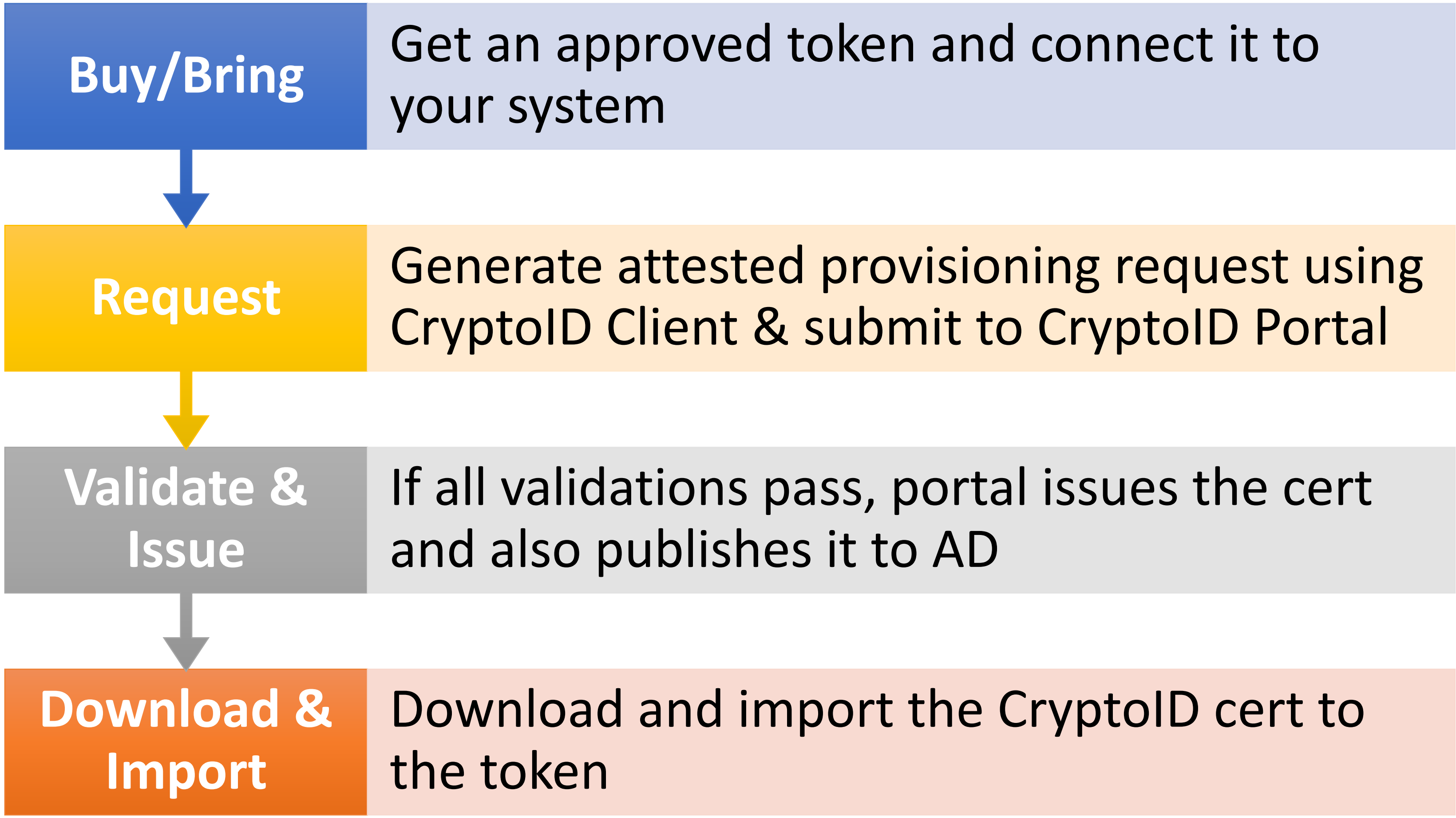
HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

CryptoID – BYOT Reference Architecture

- CryptoID Server (Portal)
- CryptoID Client Tool
- Other Existing IT/PKI Systems
  - LDAP/SSO
  - HSM API
  - Certificate Authority
  - CRL/OCSP Responders



BYOT – CryptoID Provisioning Workflow



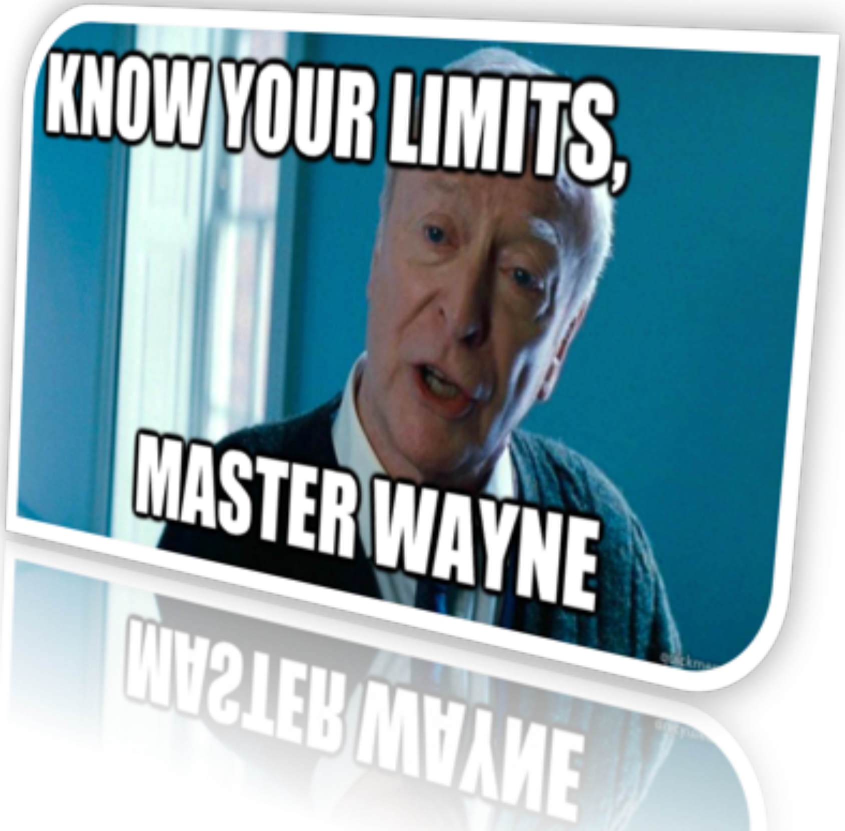
Buy/Bring	Get an approved token and connect it to your system
Request	Generate attested provisioning request using CryptoID Client & submit to CryptoID Portal
Validate & Issue	If all validations pass, portal issues the cert and also publishes it to AD
Download & Import	Download and import the CryptoID cert to the token

Advantages/ROI of CryptoID

- No external vendors in the provisioning process. No vendor lock-in for tokens.
- Reduced cost and support overhead. ~ $350K per year cost savings to Cisco
- Enhanced security – Easy to keep up with the security fixes in new models/firmware
- No complex integrations with the PAC systems
- Token consolidation – Multiple Protocols on Single Token : PIV/OTP/FIDO/U2F

Limitations of CryptoID

- Need for thorough evaluation before approving new token models
- Need to keep up with the security advisories of all supported tokens/models
- Users might not report lost tokens immediately
- PIN Lockouts – need to reset the token if the user forgets both PIN and PUK



Best practices and recommendations

- Get your **PKI** and **AD** guys involved
- Control what token **models, firmware** versions are allowed
- Monitor **Security Advisories** of the supported tokens
- Define and enforce the allowed **crypto**
- Control and manage the **PIN policies**
- Automated **revocation** for **terminated** employees
- Ensure the tokens provide **attestation** capability
- Consider **Key Escrow** for **S/MIME** Certificates

Black Hat Sound Bytes (Key Takeaways)

- Mandate hardware token-based authentication for critical/sensitive services
- Avoid dependencies on third parties to provision these tokens
  - Enable BYOT with self-provisioning and management
- Make your solution token vendor independent
  - Support more than 1 token vendor, but not too many!
  - Have a token evaluation checklist and selection criteria
- Are you hardware security token vendor?
  - Please include attestation features!
- Opportunity for enhancing PIV/CCID Standards
  - Include BYOT specific requirements such as attestation

Demo

Demo

- Token Provisioning
- Smartcard Authentication Using Token Certificate
- TLS Certificate Authentication Using Token Certificate
- SSH Authentication
- SMIME

Thank you!

@erichampshire

@karthikramasamy

black hat®

EUROPE 2019

DECEMBER 2-5, 2019

EXCEL LONDON, UK

#BHEU @BLACK HAT EVENTS