Entrust DataCard

Securing Digital Transactions and Identities

Presenter : Debs F Debs
VP Professional Services Amercias

Entrust Datacard™

AGENDA

- About Entrust DataCard
- Digital Transactions
- Role of PKI in securing Digital Transactions
- PKI Integrations
- PKI and Internet of Things (IoT)
- Crypto Summary.

Entrust DataCard Overview

Entrust Datacard™

Entrust Datacard

SOLUTION AREAS

- Financial Instant Issuance
- Authentication
- Bureau Services
- PKI
- Basic Access Control
- SSL Certificates

Entrust Datacard

Digital Transactions

Entrust Datacard™

DIGITAL TRANSACTIONS

We transact daily when we generate , post, search and retrieve data

- Website, and Forms (Gov employee, ministries, public, partners)
- Emails, Files (classified content, judicial , PII, etc..)
- Sensitive changes(Changes to our system, processes, IT & security notifications)
- Financial data and transactions
- Access to Resources (Sharepoint, VPN, Wirelss,building access, record access...)

VALUE OF TRANSACTED DATA

The value of transacted data is not just monetary!!

- Advantage
- Access to personal records, espionage
- May be used to breach
- Ransom
- Reputation and brand tarnish
- Other

ATTACK VECTORS

Attack vectors vary depending on how the transactions are carried

- Masquerading
- Fishing and spearfishing
- Un-protected websites (non SSL enabled, DNS poisoning)
- Malware (downloaded, or installed, Key loggers, Scripts part of forms, Adobe, non signed drivers, applications, etc...)
- Password-less & Password only access to resources (Wireless, VPN)
- Un-authorized devices (BYOD, Laptops, tablets) gaining access

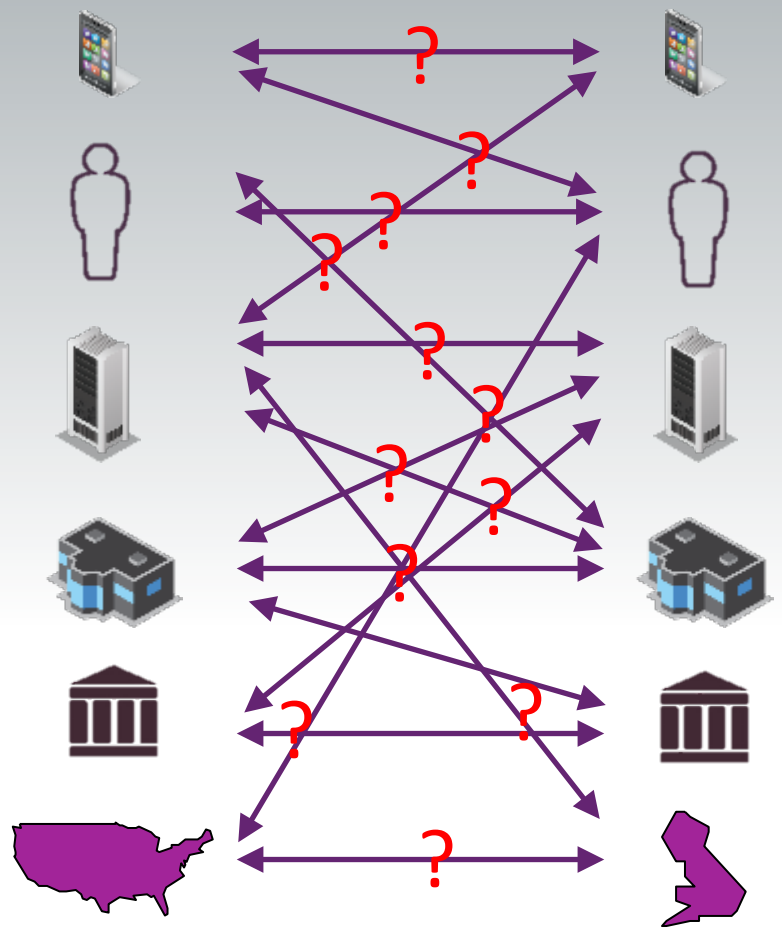
Many forms to list, however all of the attacks are after your Identity.

Once the identity is stolen, data follow.

Public Key Infrastructure
Role
In securing the Digital World

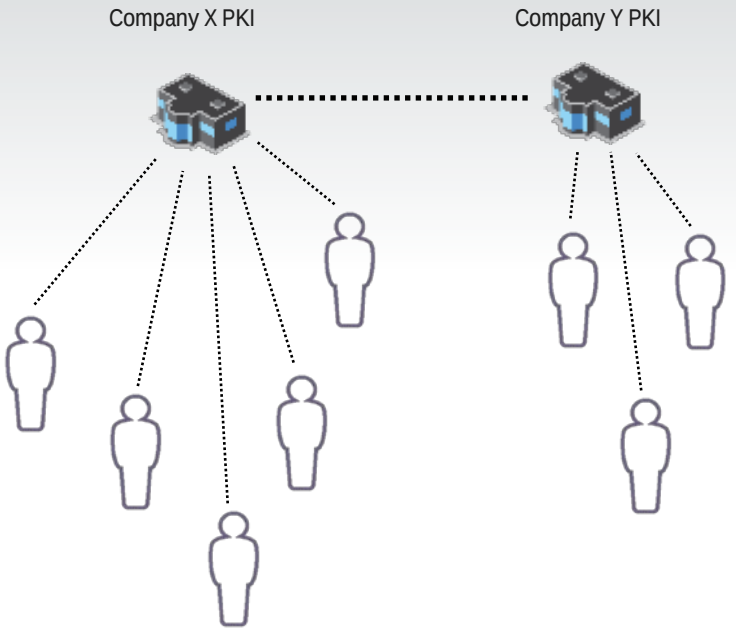
Entrust Datacard™

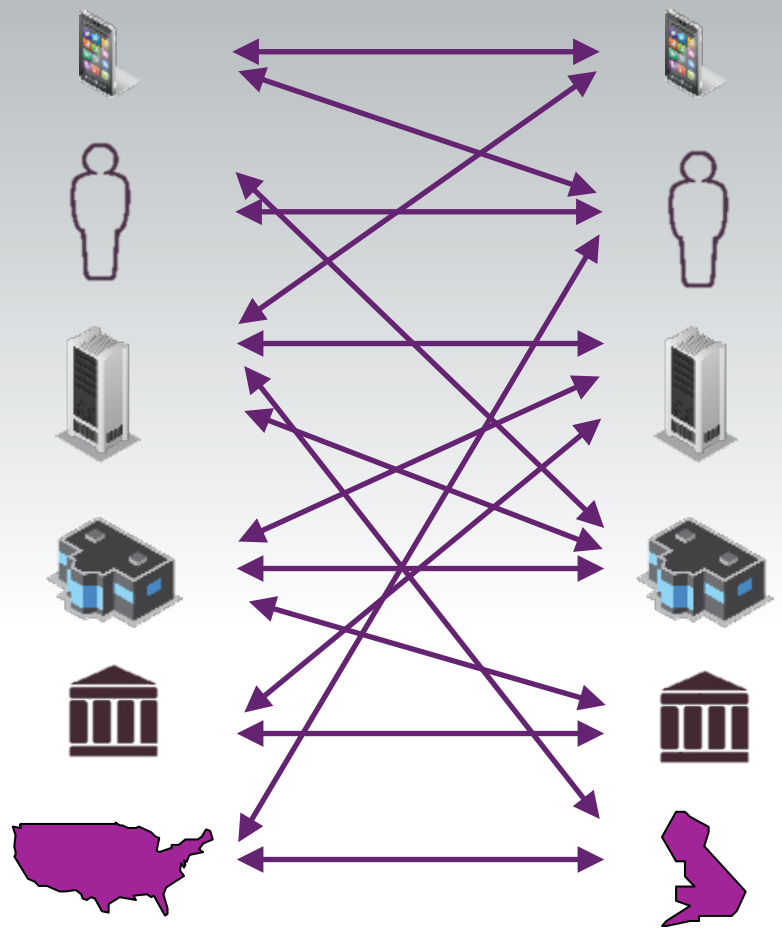
TRANSACTIONS – THINGS TO CONSIDER



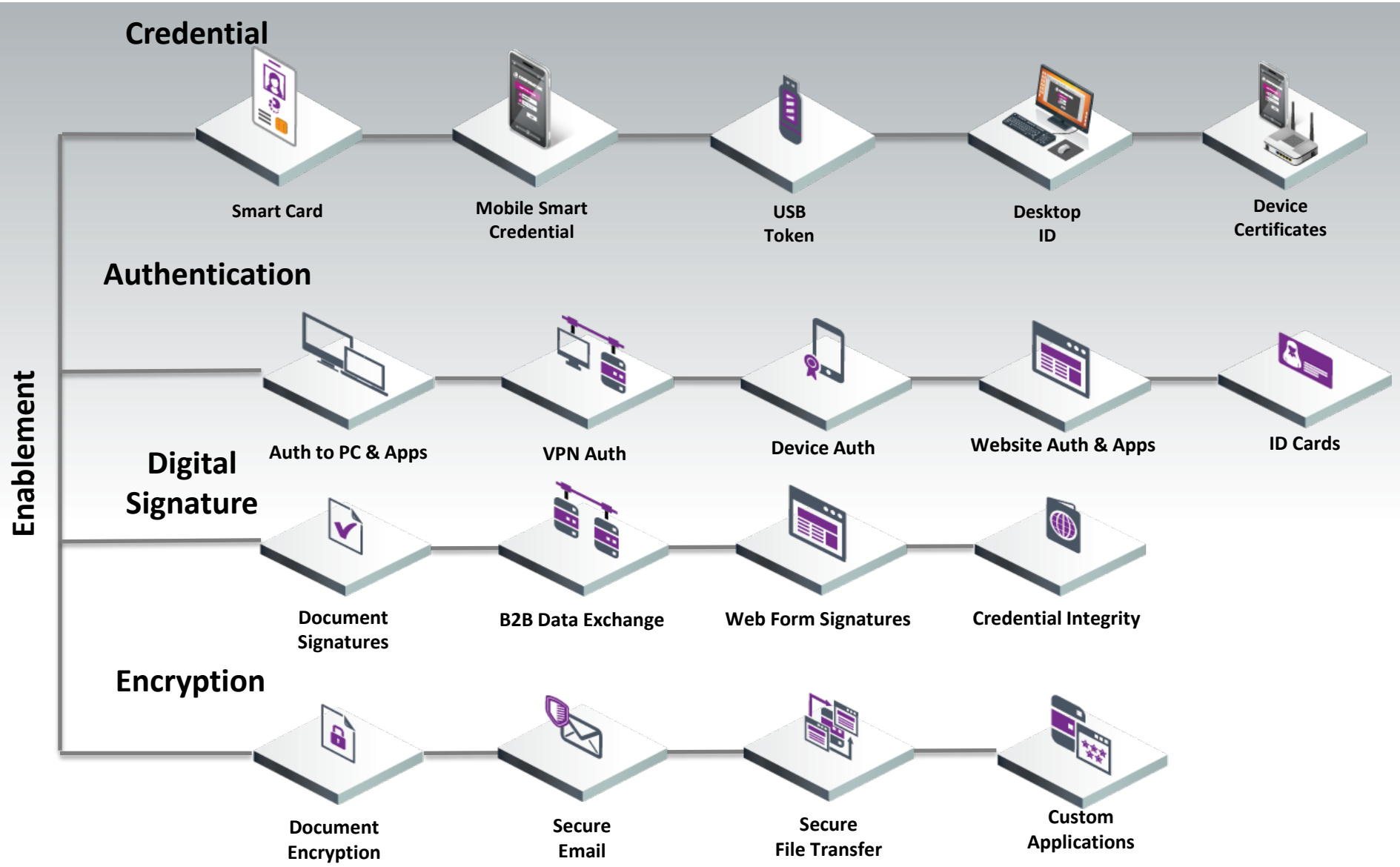
WHAT IS THE END GAME?

- Connect
  - Anyone or Anything ANYWHERE
- …and Trust
  - it is or they are who they say they are
- …and Enable to transact securely



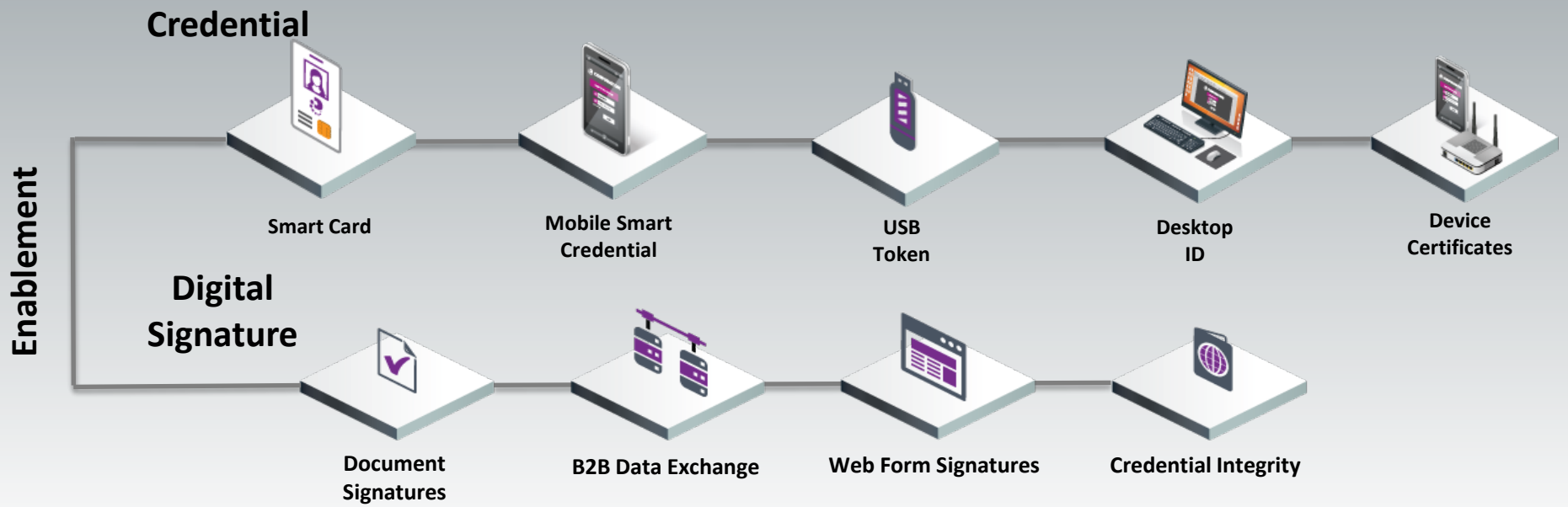


THE ACTUAL END GAME..



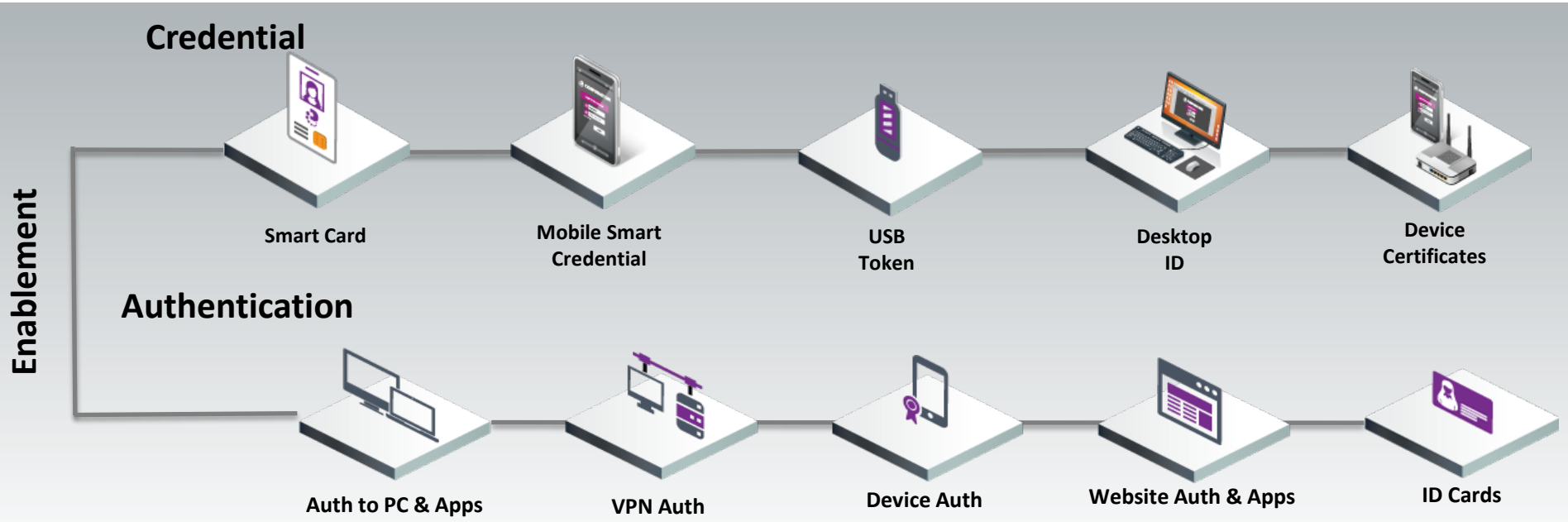
Entrust Datacard™

ENABLING PKI SIGNATURES



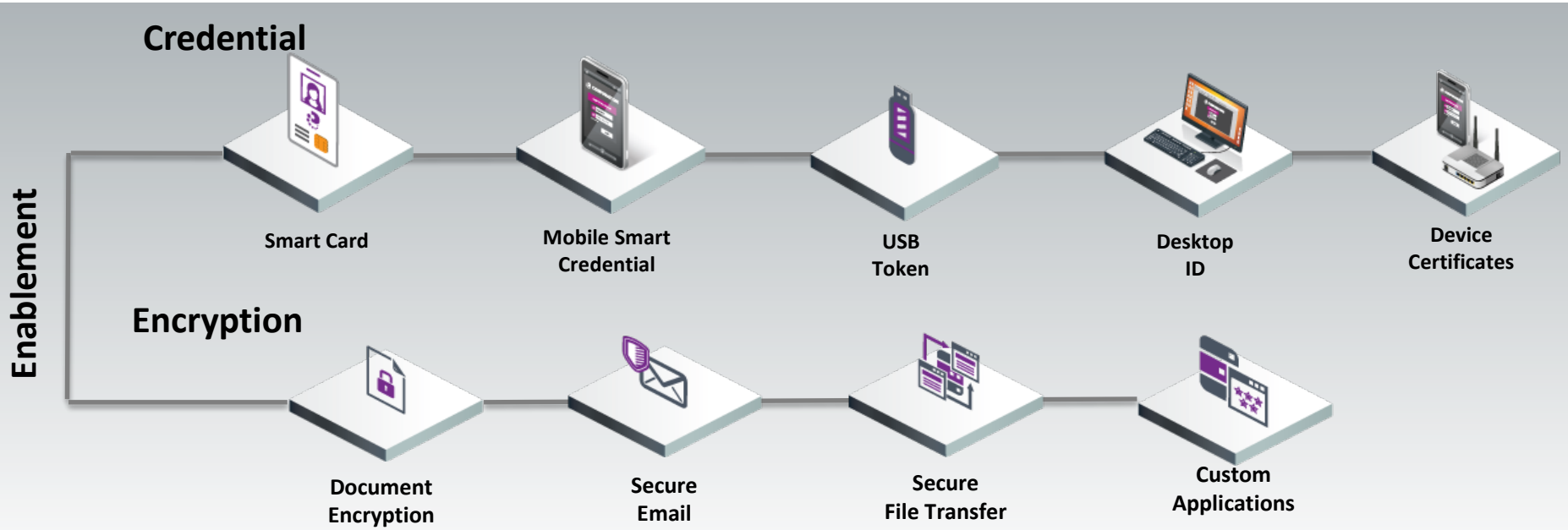
Document Signatures	B2B Data Exchange	Web Form Signatures	Credential Integrity
Leveraging built-in capability	Transaction integrity	Transparent	Signed data on RFID chip
Right-click files in folders	Standards compliant	Provable, signs & stores whole page	
Interoperable	Toolkits		
Inside the enterprise			

STRONG AUTHENTICATION



Auth to PC & Apps	VPN Auth	Device Auth	Website Auth & Apps	ID Cards
Windows Smart Card Login	IPsec VPN SSL VPN	Domain controller certificates for smart card login 802.1x Server Authentication Automated Teller Machines	SSL Server Certificates SSL EV SSL client certificates Enterprise portal authentication Consumer/Citizen Web Auth (+ Sign)	Citizen Identity Card Employee ID Physical & Logical Access

ENABLING PKI ENCRYPTION



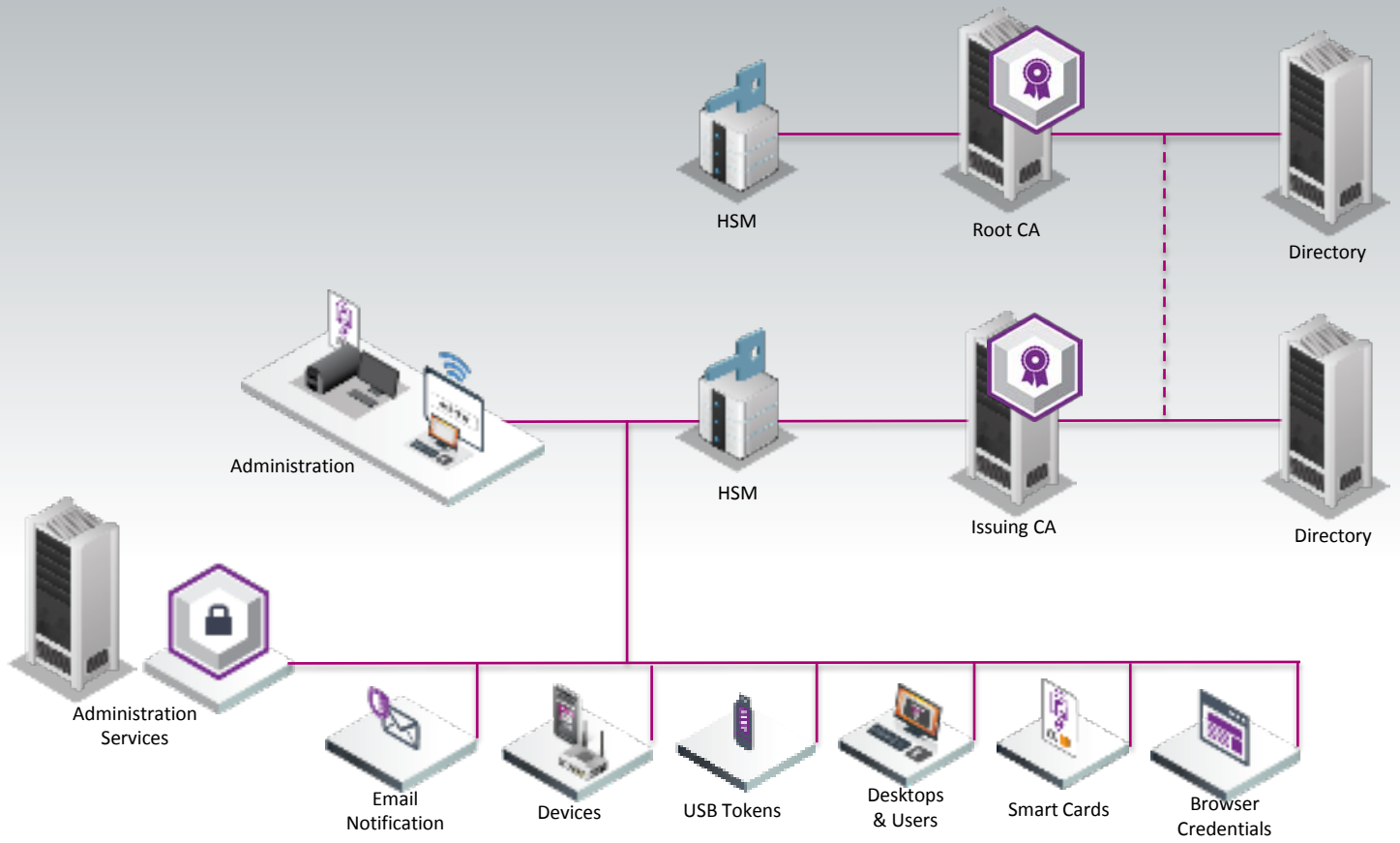
Document Encryption	Secure Email	Secure File Transfer	Custom Applications
Right-click files in folders	End to End Email	Packaged Tools	Standards compliant
Adobe Acrobat	Complementary to EMS	Custom Apps	Java or C++ Toolkits
Windows EFS		WebMethods	
		Tibco	
		Axway/Cyclone	
		Standards-based	

HOW IS IT DONE?

A digital certificate is an object that contains

- Holders Identity/Name
- Valid from to date
- Valid to date
- Issuer (Organization/Issuer Name)
- Public key used to communicate with you
- Private key the owner keeps to themselves

WHAT DOES A PKI LOOK LIKE



Entrust Datacard™

Using PKI

Entrust Datacard™

Uniqueness of PKI

Leverage Trusted Identities for Multiple Purposes

Authentication

Authenticity

Encryption

Secrecy & confidentiality

Digital Signatures

Accuracy & Integrity

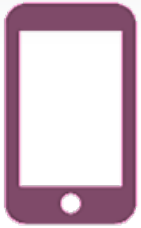
Entrust Datacard™

PKI End-Entities

Trusted Identities

People

Apps



Devices

Machines

Servers

Entrust Datacard™

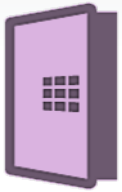
ENABLING TRANSACTIONS

Secure Transactions

Financial Transactions

Network Access

Border Crossing



Building Access

Infrastructure Control

Entrust Datacard™

ENTERPRISE APPLICATIONS

Enterprise Use Cases

Auth to PC & Apps

Secure Email

Network Auth

VPN Auth

Web Form Signatures

Entrust Datacard™

PKI FOR ENTERPRISE AND BEYOND

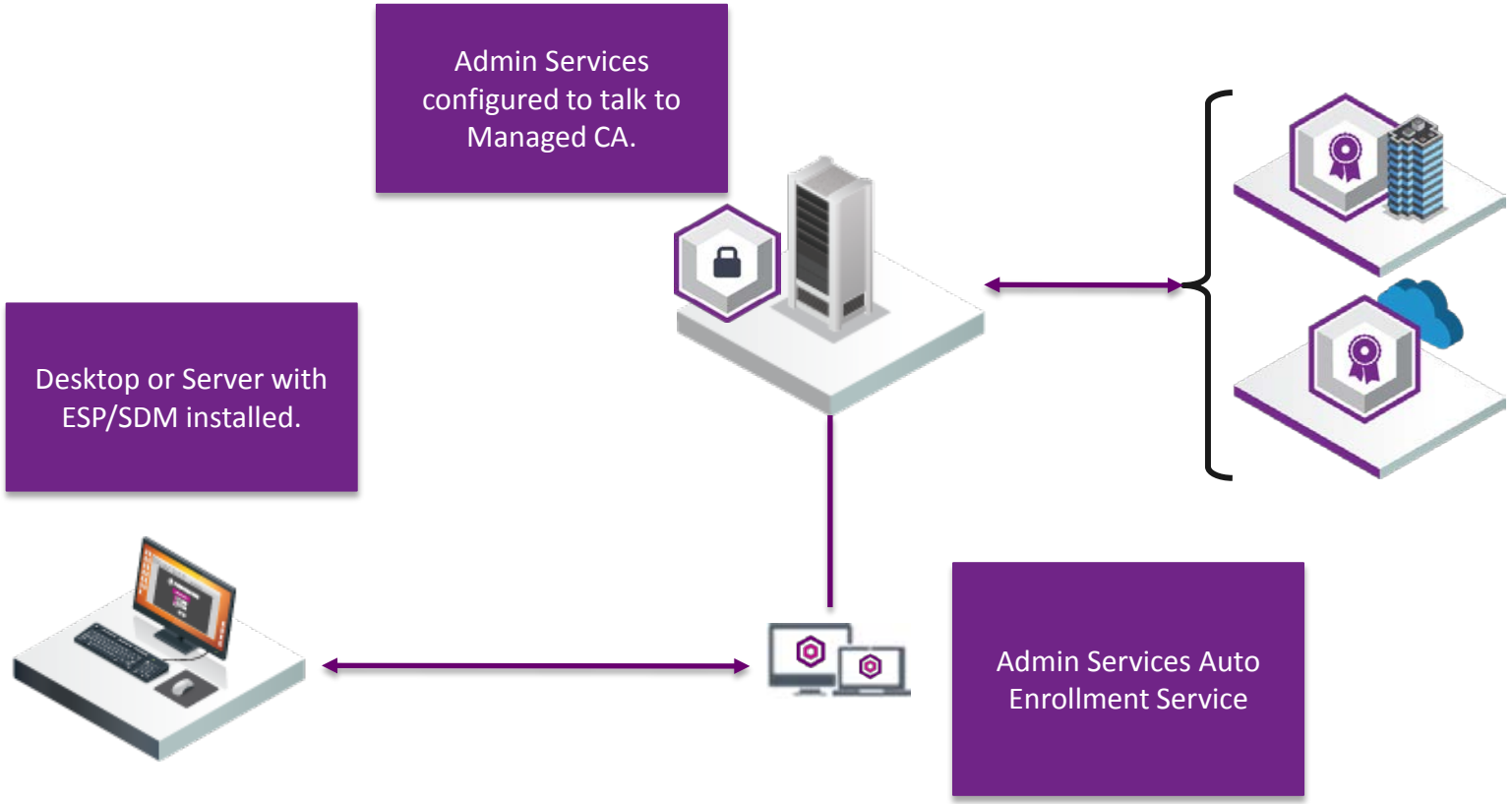
Entrust Datacard™

PKI Integrations

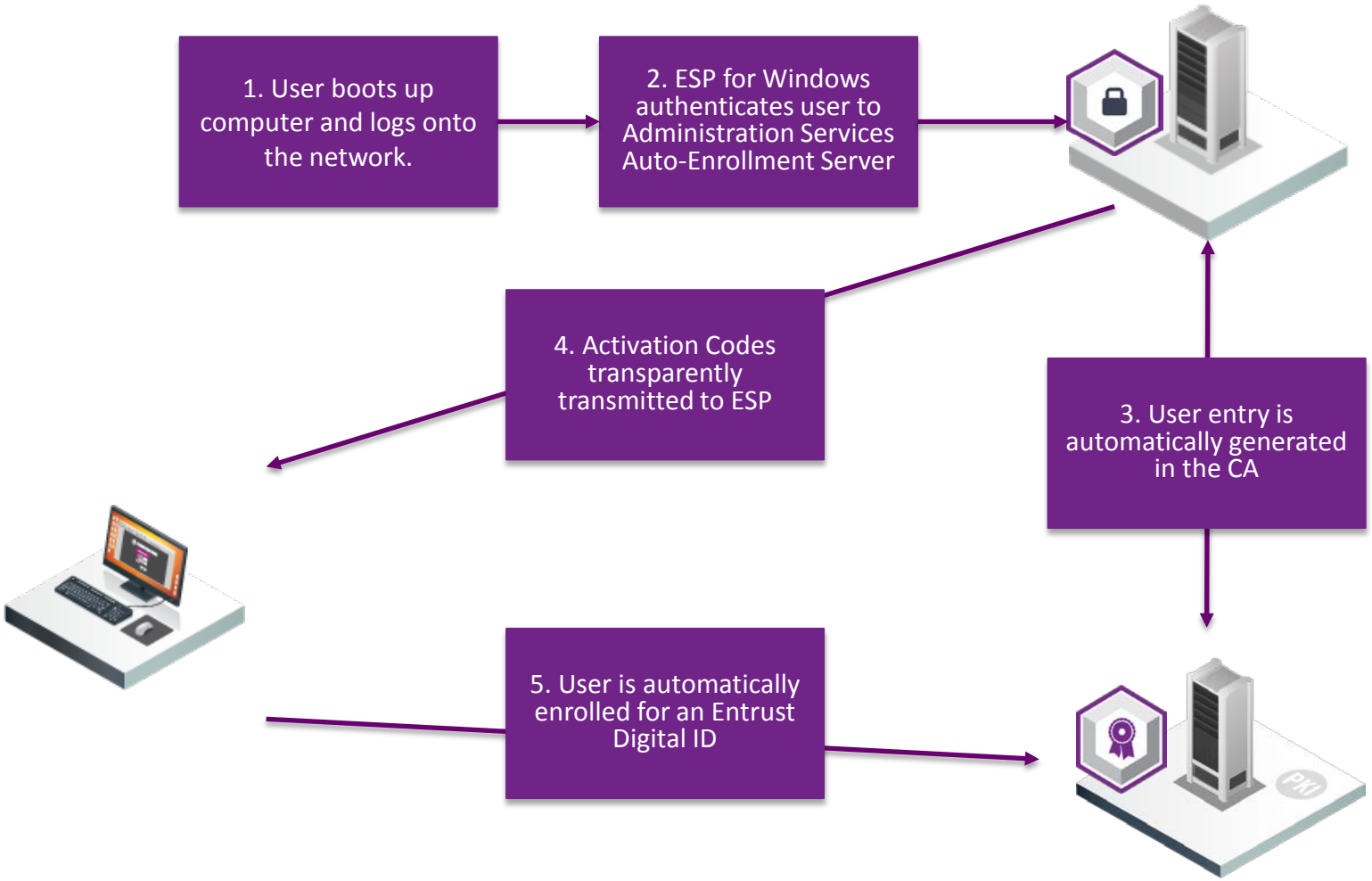
Entrust Datacard™

ENTELLIGENCE AUTO-ENROLLMENT

- Entrust Auto-Enrollment Service
  - Supports Auto-enrolment for:
    - Entrust Entelligence for Windows
    - Entrust Entelligence Secure Desktop for Mac (Coming in SDM 8.1 SP1)



ENTELLIGENCE AUTO-ENROLLMENT

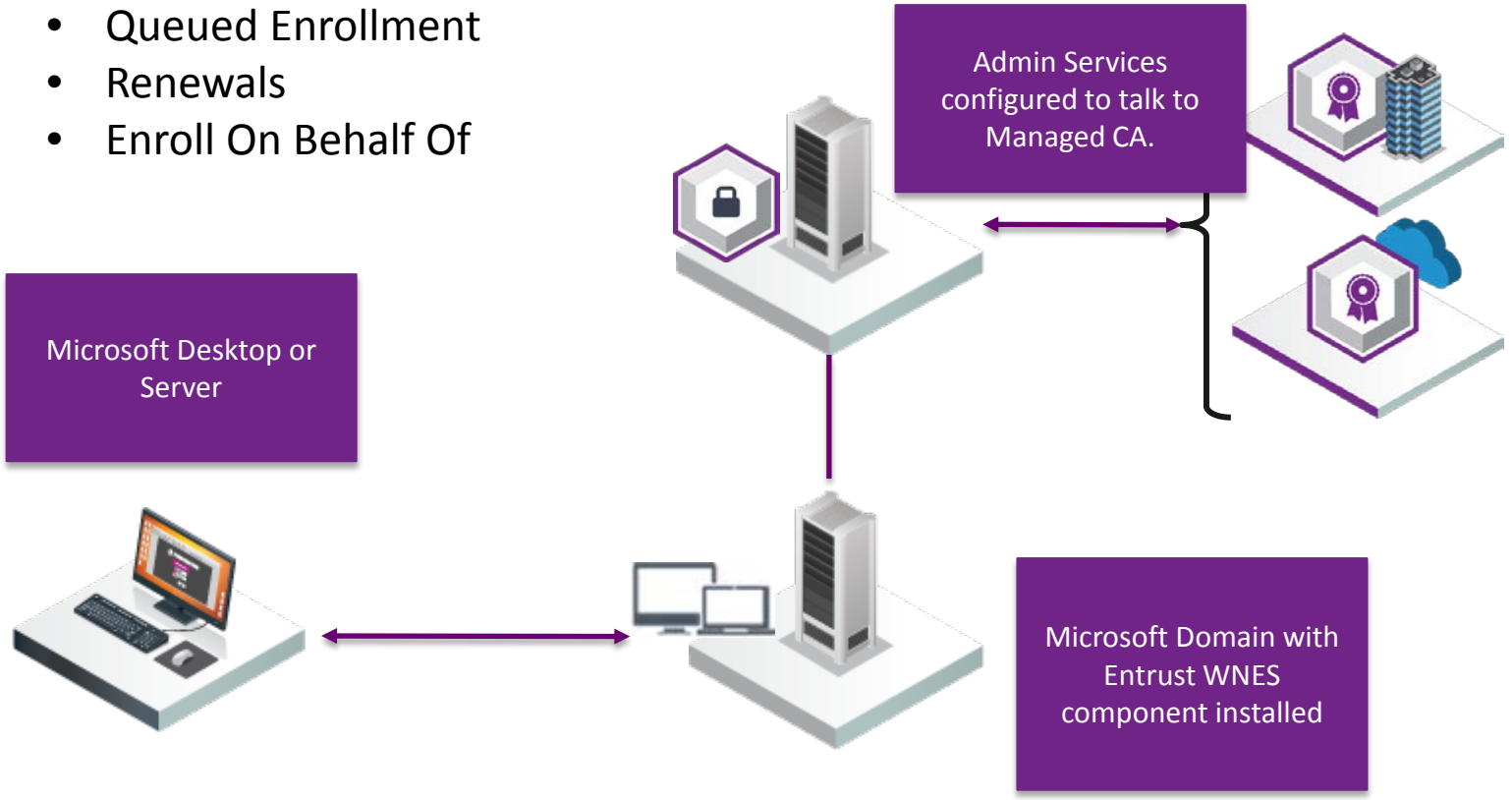


Users will be prompted to enter a PIN or password if the private keys are configured to be stored on smart cards/tokens or in an Entrust EPF file

WINDOWS NATIVE ENROLLMENT

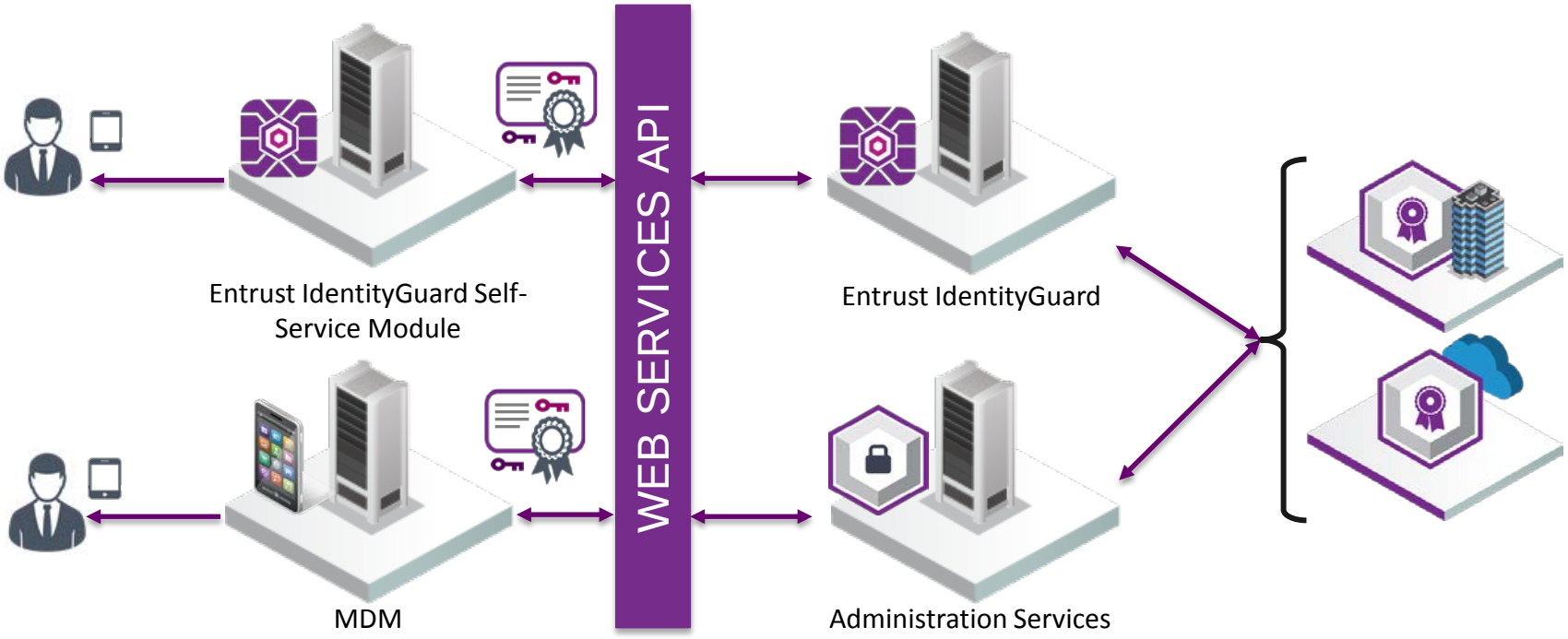
- Entrust Windows Network Enrollment Service
  - Provides client-less PKI enrolment for the Windows OS
  - Single Admin Services install can support multiple WNES / AD Domains

- Supports
  - Self-Enrollment
  - Queued Enrollment
  - Renewals
  - Enroll On Behalf Of
- Self Enrollment with Key Archive
- Enroll On Behalf Of with key archive



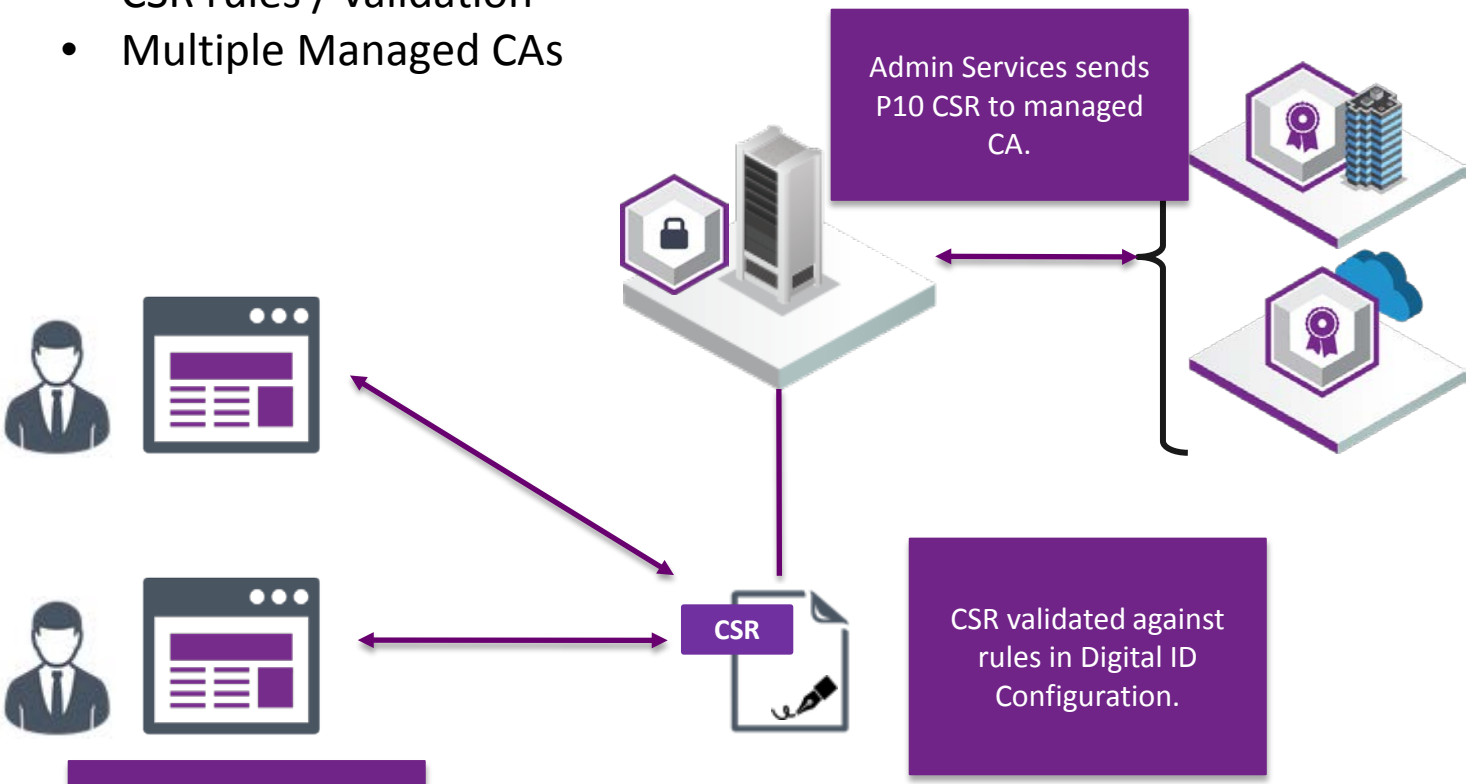
MDM INTEGRATION

- Allows MDMs to issue Entrust digital IDs to mobile devices
  - Unified WS Interface to both IDG and Admin Services
- IdentityGuard SSM has native capability to enroll Mobile Devices for certificates without MDM



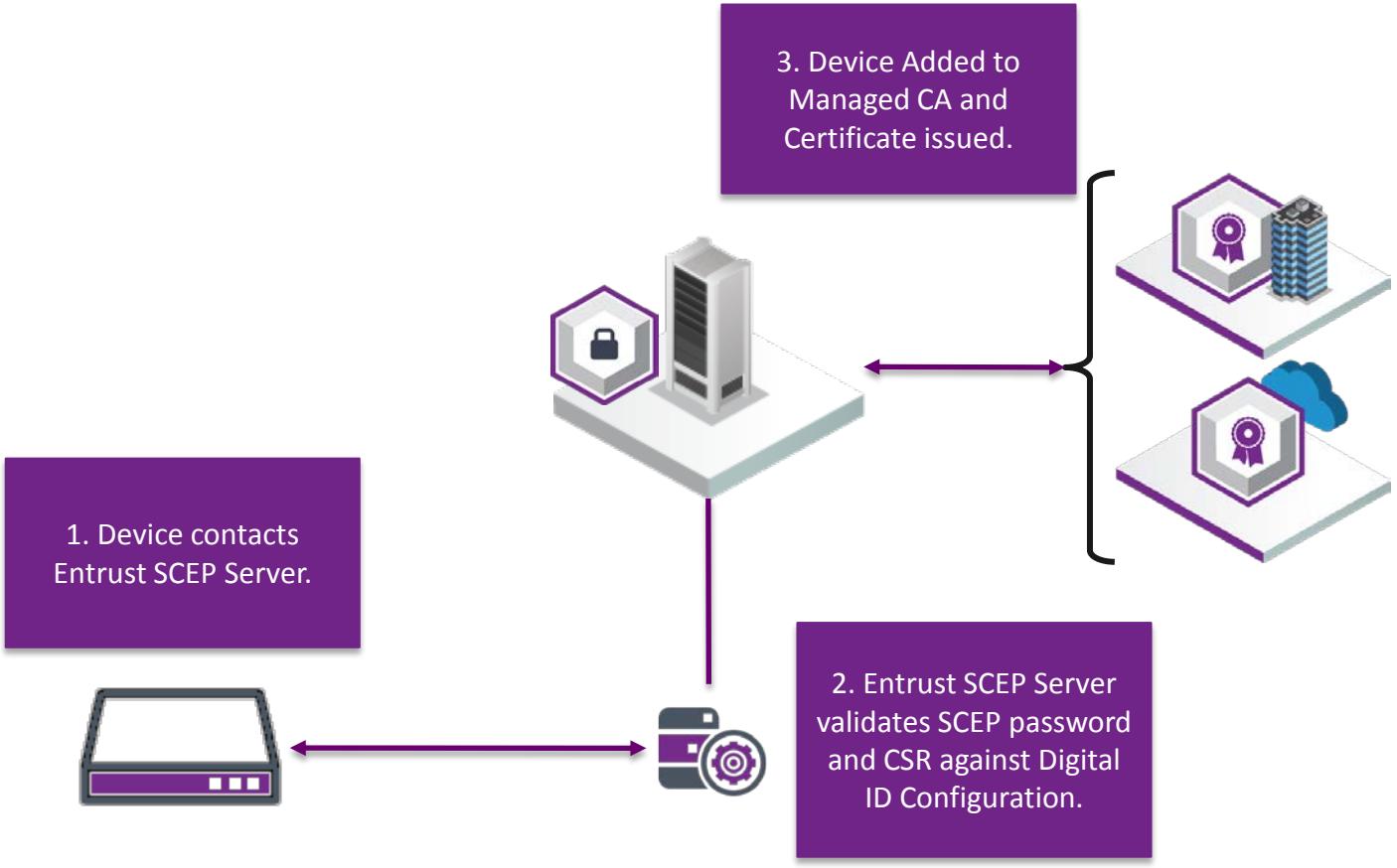
CSR ENROLLMENT

- Web Application for summation and approval of PKCS#10 CSR
- Supports
  - Client Auth / AD auth of submitters and approvers
  - Queued Operations
  - CSR rules / validation
  - Multiple Managed CAs



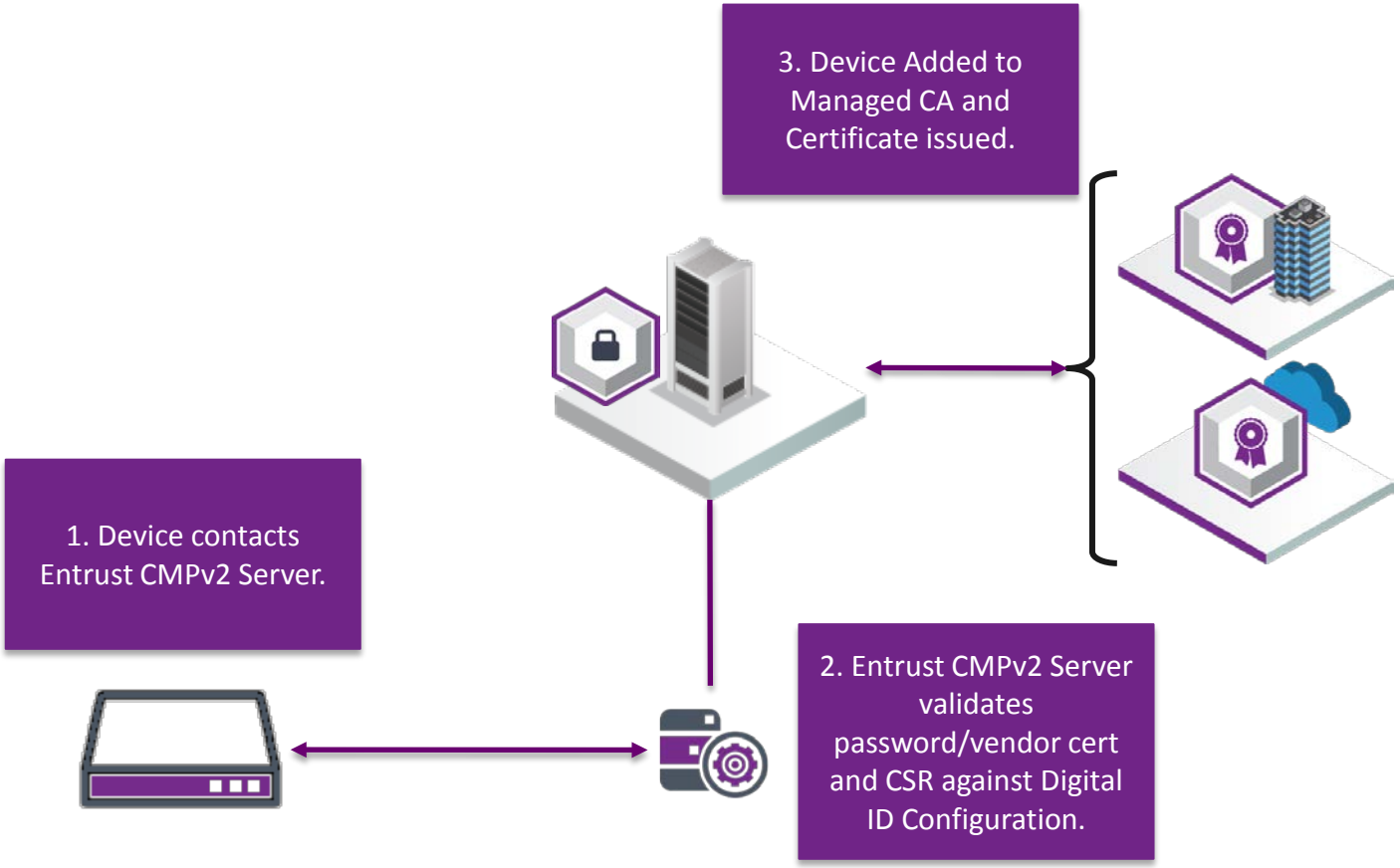
SCEP ENROLLMENT

- Entrust SCEP Implementation offers RSA and ECC enrollment
- Static SCEP Password defined for enrollment / renewal operations



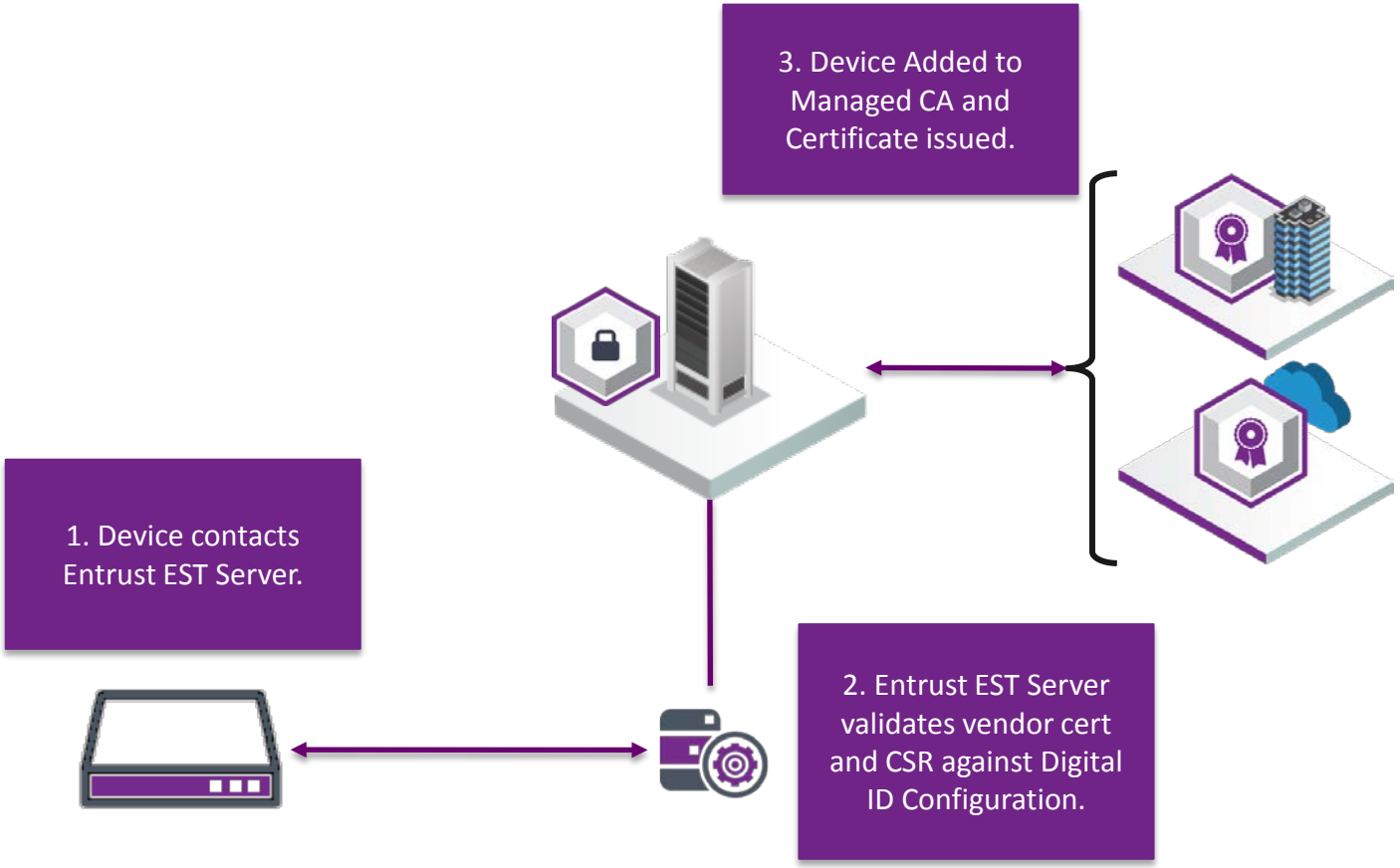
CMPV2 ENROLLMENT

- Entrust CMPv2 Implementation offers RSA and ECC enrollment
- Static Password or Vendor Certificate authentication enrollment / renewal operations
- IP Address or DNS whitelist validation



EST ENROLLMENT

- Entrust EST Implementation offers RSA and ECC enrollment
- Vendor Certificate authentication enrollment / renewal operations



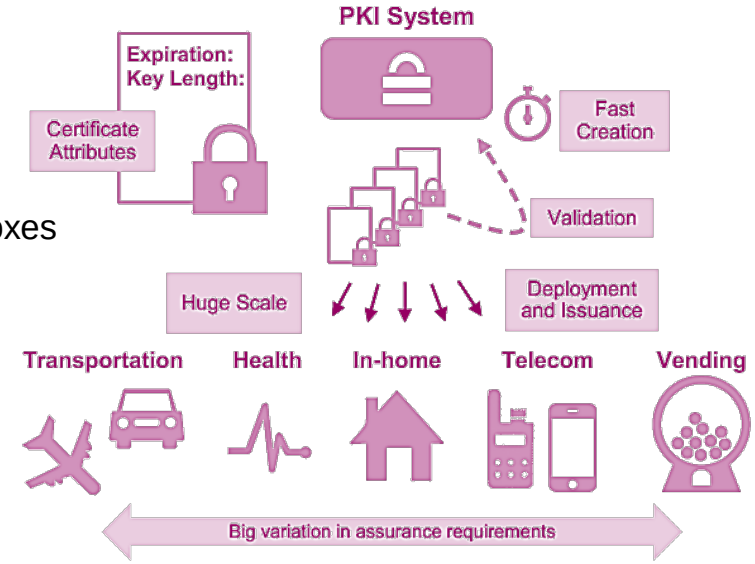
PKI
And
Internet of Things (IoT)

Entrust Datacard™

PKI MARKET TRENDS

- Internet of things
  - Wearables
  - Smart Traffic Systems
  - Automotive
  - Appliances
  - Smart Meters
  - Audio Visual Set-top Boxes
  - Vending machines
  - Toys

"Forecast: The Internet of Things, Worldwide, 2013" - Gartner



Source: Gartner (March 2014)

The installed base of "things," excluding PCs, tablets and smartphones, will grow to 26 billion units in 2020, which is almost 30-fold increase from 0.9 billion units in 2009

- IoT Challenges
  - Speed
  - Scale
  - Device heterogeneity, issuance and attributes
  - Assurance requirements and transaction types:
  - Closed usage model
  - Revocation and validation
  - Life cycle and renewal

Entrust Datacard

Latest Crypto

Entrust Datacard™

Summary

- RSA, ECC are still the crypto of choice
- Winternitz One Time Signagture (WOTS), Merklee Hash Tree(MHT), Extended Merklee Signature Scheme(XMSS)
- Quantum computers
  - Not just massively-parallel classical computers
- Large-scale quantum computers are coming
- This will result in the need for new cipher suites
  - But, not for several years
  - 2025 minus the algorithm security lifetime
- It can take several years to roll out a new cipher suite
  - Even if the new cipher suite has similar characteristics to those of the old one
- How long will it take if the new cipher suite has different characteristics? Such as:-
  - Upper limit on the number of signatures per key
  - The need to maintain state
- Not too early to be thinking about this

BIBLIOGRAPHY

Quantum computers:

"The quest for the quantum computer", Julian Brown, Touchstone, 2001

"Quantum Computing Lecture Notes", Ronald de Wolf, 2011, http://homepages.cwi.nl/~rdewolf/qcnotes.pdf

Post-Quantum Cryptography:

"NSA Suite B Cryptography", NSA, 2015-08-19, https://www.nsa.gov/ia/programs/suiteb_cryptography/

Commercial National Security Algorithm Suite and Quantum Computing, NSA, Jan 2016, https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/assets/public/upload/Commercial-National-Security-Algorithm-CNSA-Suite-Factsheet.pdf&WpKes=aF6woL7fQp3dJirQ4SVyNDqjbSJ9a88xZcnLAL

"A riddle wrapped in an enigma", Koblitz, Menezes, 2015-12-03, http://eprint.iacr.org/2015/1018.pdf

"Post-Quantum Cryptography for Long-Term Security", PQCrypto, September 2015, http://pqcrypto.eu.org/docs/initial-recommendations.pdf

Hash-based signatures:

"Hash based signatures", Imperial Violet, 18 Jul 2013, https://www.imperialviolet.org/2013/07/18/hashsig.html

XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions, Buchmann et al, November 2011, https://eprint.iacr.org/2011/484.pdf

XMSS: Extended Hash-Based Signatures draft-irtf-cfrg-xmss-hash-based-signatures-03, Huelsing et al, Feb 2016, https://www.ietf.org/id/draft-irtf-cfrg-xmss-hash-based-signatures-03.pdf

Lattice-based cryptography:

"Lattice-based Cryptography", Daniele Micciancio, Oded Regev, July 22, 2008, http://www.cims.nyu.edu/~regev/papers/pqc.pdf

Code-based cryptography:

"McBits: fast constant-time code-based cryptography", Bernstein et al, 2013, http://binary.cr.yp.to/mcbits-20130616.pdf

Wikipedia article on McEliece Cryptosystem

Questions?

Entrust Datacard™