What do Blockchain, IoT, cloud and the new payment vectors mean for your security?

Giles Townley
UK Sales Director
Utimaco

utimaco®

Agenda

- Security Fundamentals
- Blockchain
- IoT
- Cloud
- New Payments vectors
- Security Fundamentals revisited

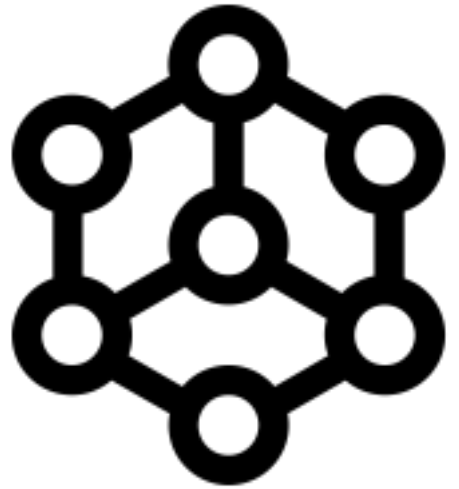
Security Fundamentals

- Identity – issuance, authentication, management, revocation
- Access Control – use identity to manage access to applications
- Encryption – data can only be accessed by permitted user

- Cryptography works – algorithms remain unbroken and mathematically powerful

- Cryptographic keys must be protected in order to secure the applications, data and identities with which they are associated
- Protected keys have the potential to be securely rolled into new key lengths and algorithms

Blockchain characteristics



- Non-repudiable chain of events (transaction or even “coin”)
- Public and private variants
- Decentralised ledgers and approvals (nodes)
- Open-source crypto-based technology

- **Challenges**
- End-point (node) vulnerability – access control and key theft

Authentication

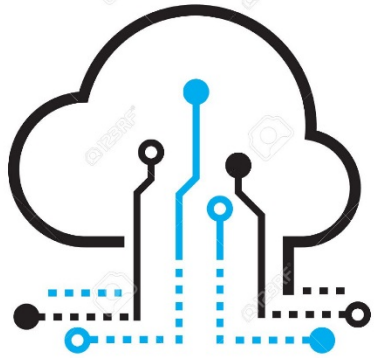
Conditional Access

Database Encryption

PKI

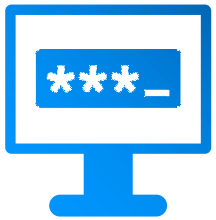
IoT characteristics

- What is the IoT?
- Huge number of end-points
- Necessity for trust relationships for connectivity
- Connectivity required
- Data sharing



- **Challenges**
- Legacy infrastructure
- High risk (physical and personal)
- Security of end-points and data

Authentication



Conditional Access

Database Encryption

PKI

Cloud characteristics

- Off-premise storage and usage of applications, data and transactions

- **Challenges**
- Security of access
- Security of data
- Availability vs security
- Geo-location

Authentication

Conditional Access

Database Encryption

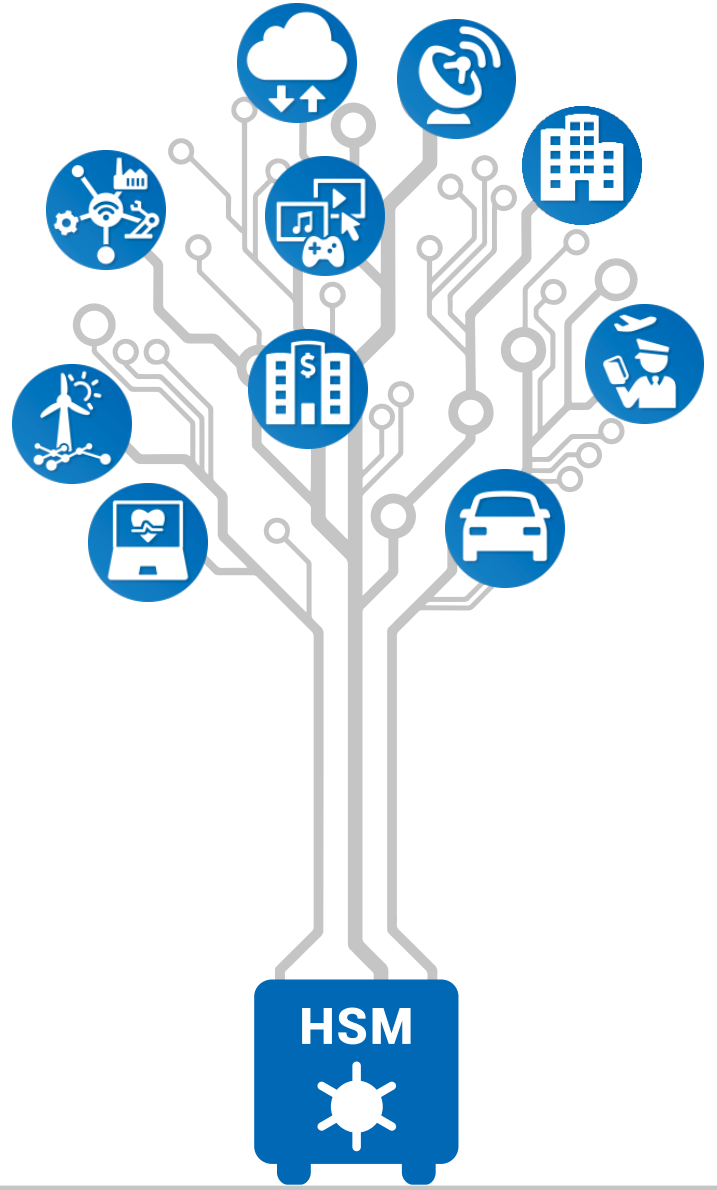
PKI

New Payments Vectors characteristics

- New payments solutions using multiple and new vectors – wearables, smartphones, embedded chips

- **Challenges**
- Compliance with PCI-DSS
- Secure identity issuance and management
- Secure transaction processing
- New/revised algorithms needing secure execution

And many other technology use cases



Security Fundamentals revisited

- Identity – issuance, authentication, management, revocation
- Access Control – use identity to manage access to applications
- Encryption – data can only be accessed by permitted user

- Cryptography works – algorithms remain unbroken and mathematically powerful

- Cryptographic keys must be protected in order to secure the applications, data and identities with which they are associated
- Protected keys have the potential to be securely rolled into new key lengths and algorithms

Questions?

Giles Townley

UK Sales Director

Utimaco

Giles.Townley@utimaco.com