MULTOS Providing Appropriate Trust For IoT Devices

December 2016
Paul Wilson
Commercial Manager
Representing the MULTOS Consortium

MULTOS - Trusted Worldwide Technology

850+ Million Devices

45 Countries

1000s Issuers

Smart Card Common Criteria Security Certification													
EAL 1	1+	EAL 2	2+	EAL 3	3+	EAL 4	4+	EAL 5	5+	EAL 6	6+	EAL 7	7+

Majority of Smart Card Implementations

1st - 2013 MULTOS

ESTADOS UNIDOS MEXICANOS
LICENCIA PARA CONDUCIR
011E130140

GOBIERNO DEL ESTADO DE TABASCO

TABASCO

ARACELI GRACIELA
VILLAVICENCIO GARCIA

R.F.C. o CURP VIGA781113MFJA0109
Nacionalidad MEXICANA
Sexo FEMENINO
Oficina que Expide VILLAHERMOSA
Fecha de Expedición 06/SEP/2007
Fecha de Vencimiento 06/SEP/2009
Usa Lentes NO

SERVICIO PARTICULAR
VEHICULOS HASTA
UNA TONELADA

AUTOMOVILISTA

ABnote Since 1795
UnionPay 银联 中国银联 China Unionpay
consult hyperion securing tomorrow's transactions
cpi card group Solutions For Your Success

CRYPTOMAThIC
CTS CALIBER Matches your future
DNP The Dai Nippon Printing Group
DeltaCrypt Technologies Inc.

DISCOVER
ECOSCARD
Entrust Datacard
EuroSmartict

FIS
fiserv.
gemalto security to be free
Giesecke & Devrient Creating Confidence.

HITACHI Inspire the Next
infineon
mastercard

multos international
newtech
oberthur TECHNOLOGIES THE M COMPANY
paySmart

Smart Energy Networks
ST life.augmented
TechTrex Inc.
THALES e-Security

TOSHIBA Leading Innovation
TSYS
UBIVELOX

MULTOS tm

IoT Security Foundation WE'RE CONNECTED

Connectivity Breeding Security Issues

Product recalls
(Connected vehicles)

Poor user experience
(Smart home devices)

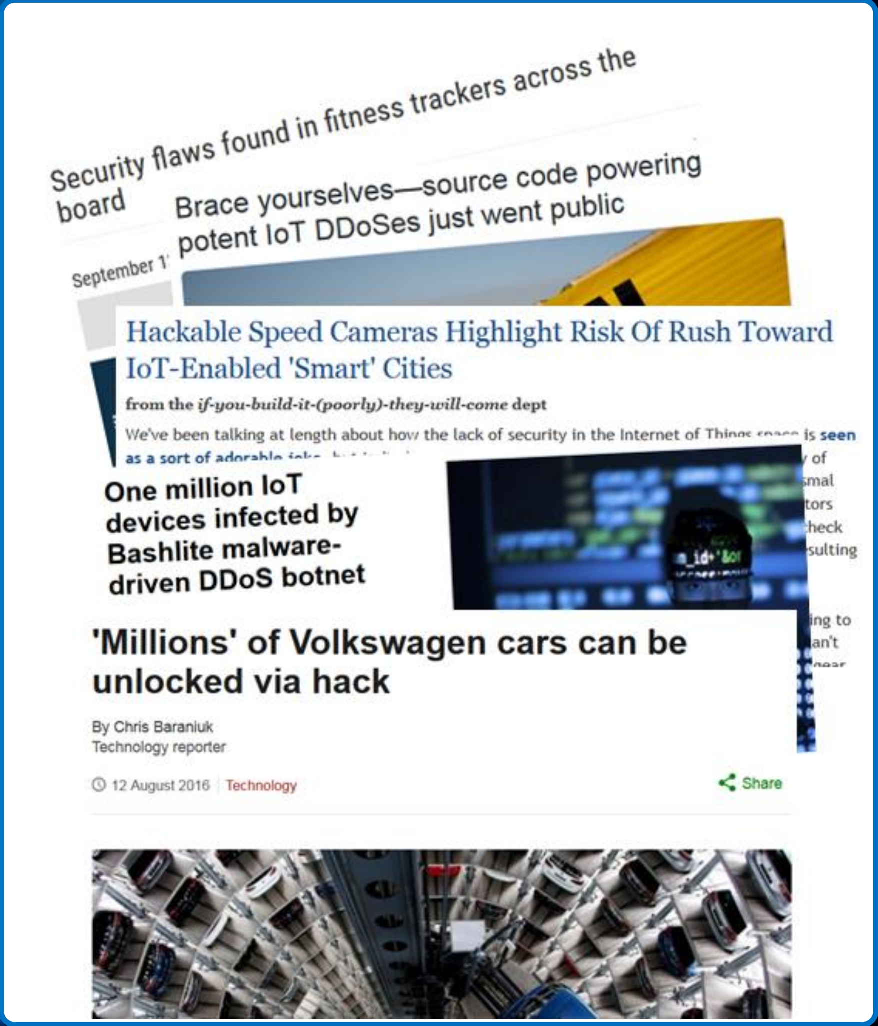
Industrial disruption
(Furnace control systems)

Increasing Security Concerns

1/10 adequately secured
(IOActive)

52% lacking security focus
(Capgemini)

50% unable to address threats
(Gartner)



Security flaws found in fitness trackers across the board

September 1

Brace yourselves—source code powering potent IoT DDoSes just went public

Hackable Speed Cameras Highlight Risk Of Rush Toward IoT-Enabled 'Smart' Cities

from the *if-you-build-it-(poorly)-they-will-come* dept

We've been talking at length about how the lack of security in the Internet of Things [illegible] is seen as a sort of [illegible]

One million IoT devices infected by Bashlite malware-driven DDoS botnet

'Millions' of Volkswagen cars can be unlocked via hack

By Chris Baraniuk
Technology reporter

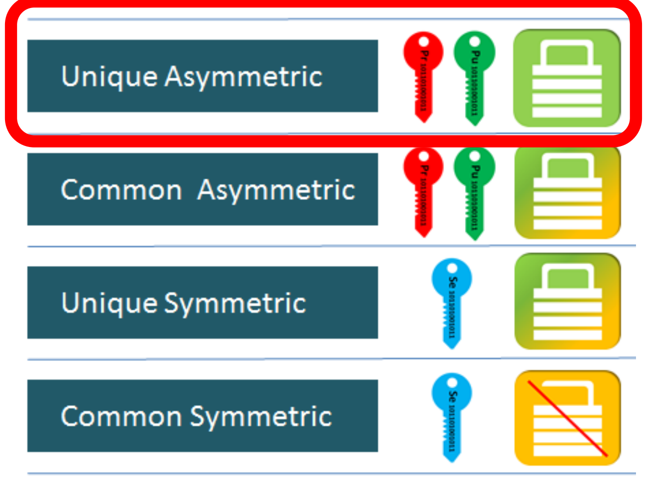
12 August 2016 | Technology

Share

Secure the Runtime

Derived from the GSMA Critical Recommendations IoT Security Guidelines Endpoint Ecosystem Version 1.0 08 February 2016

Runtime Protection



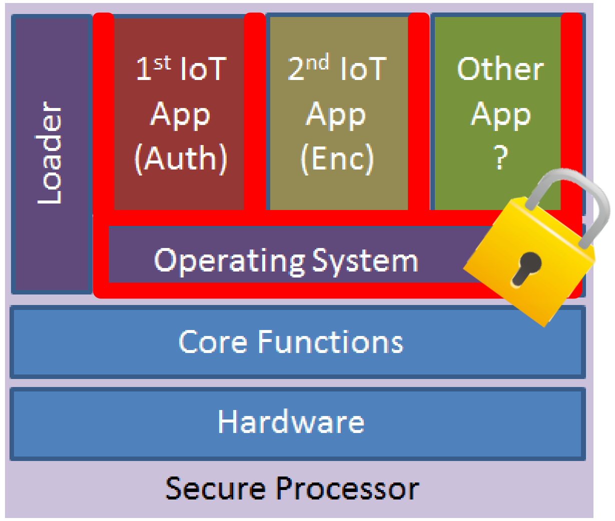
At Risk Software

- Incorrect functioning
- False data generation
- Credential Leakage
- Remote update / reset failure
- Code extraction

Runtime Protection

- Bootstrap processor
- Only run verified s/w
- Protect critical credentials
- Runtime segregation and access with SEE (Secure Execution Environment)

- Hardware Countermeasures
- Software Countermeasures



Ensure Endpoint Identity

Derived from the GSMA Critical Recommendations IoT Security Guidelines Endpoint Ecosystem Version 1.0 08 February 2016		Mutual Authentication	Endpoint Personalisation
Unique Asymmetric	Pr Pu	🔒	🔒
Common Asymmetric	Pr Pu	🔒	🔒
Unique Symmetric	Se	🔒	🔒
Common Symmetric	Se	✗	🔒

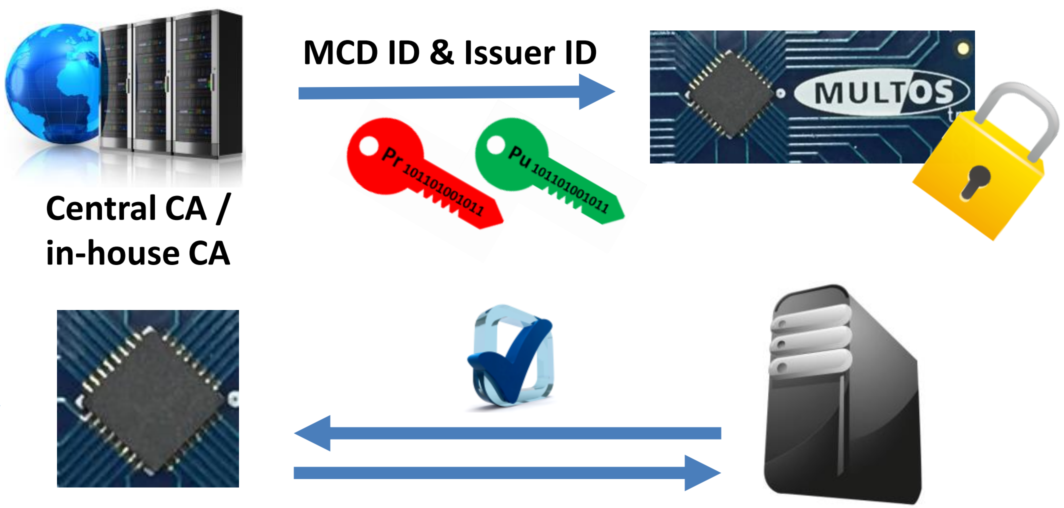
Weak Identity

- Unidentified entity
- Device duplication / confusion
- ID impersonation
- Central data corruption
- Genuine entity impact

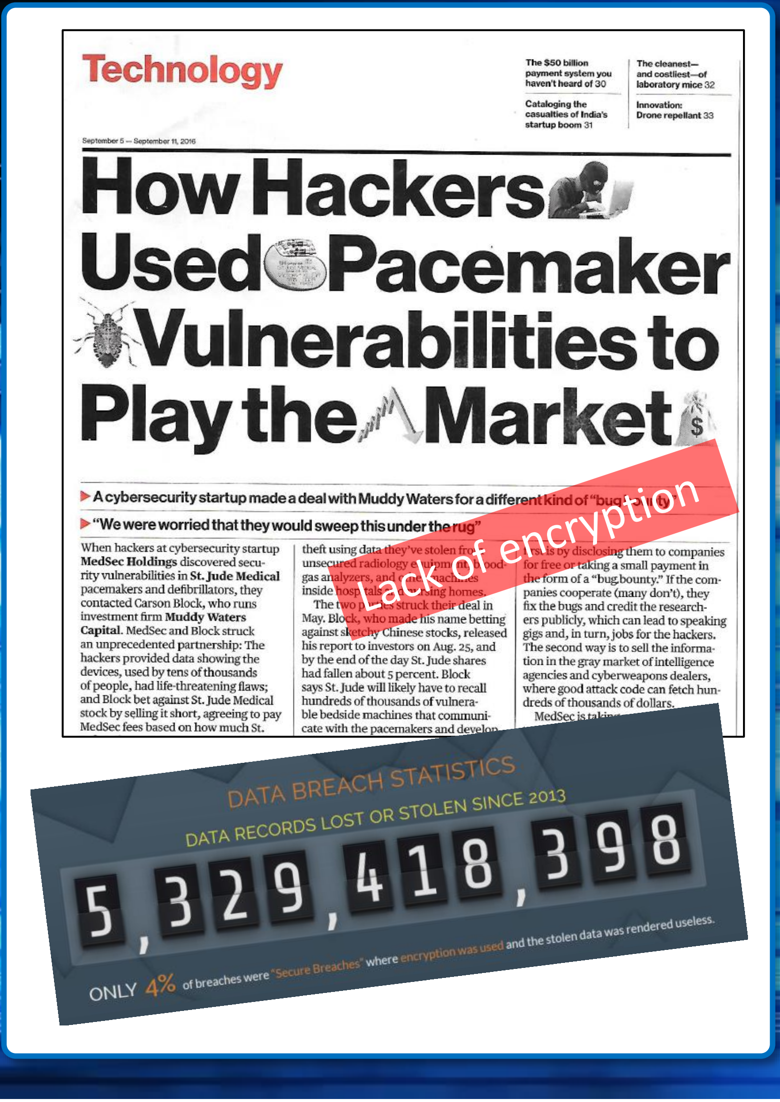
Identity Protection

Personalise the endpoint
- Cryptographically unique

Authenticate the entity
- Mutual authentication policy



Secure the Data



Technology

The $50 billion payment system you haven't heard of 30

The cleanest—and costliest—of laboratory mice 32

Cataloging the casualties of India's startup boom 31

Innovation: Drone repellant 33

September 5 — September 11, 2016

How Hackers Used Pacemaker Vulnerabilities to Play the Market

- A cybersecurity startup made a deal with Muddy Waters for a different kind of "bug bounty"
- "We were worried that they would sweep this under the rug"

When hackers at cybersecurity startup **MedSec Holdings** discovered security vulnerabilities in **St. Jude Medical** pacemakers and defibrillators, they contacted Carson Block, who runs investment firm **Muddy Waters Capital**. MedSec and Block struck an unprecedented partnership: The hackers provided data showing the devices, used by tens of thousands of people, had life-threatening flaws; and Block bet against St. Jude Medical stock by selling it short, agreeing to pay MedSec fees based on how much St.

theft using data they've stolen from unsecured radiology equipment, blood-gas analyzers, and other machines inside hospitals and nursing homes.

The two parties struck their deal in May. Block, who made his name betting against sketchy Chinese stocks, released his report to investors on Aug. 25, and by the end of the day St. Jude shares had fallen about 5 percent. Block says St. Jude will likely have to recall hundreds of thousands of vulnerable bedside machines that communicate with the pacemakers and develop

first is by disclosing them to companies for free or taking a small payment in the form of a "bug bounty." If the companies cooperate (many don't), they fix the bugs and credit the researchers publicly, which can lead to speaking gigs and, in turn, jobs for the hackers. The second way is to sell the information in the gray market of intelligence agencies and cyberweapons dealers, where good attack code can fetch hundreds of thousands of dollars.

MedSec is taking

Lack of encryption

DATA BREACH STATISTICS

DATA RECORDS LOST OR STOLEN SINCE 2013

5,329,418,398

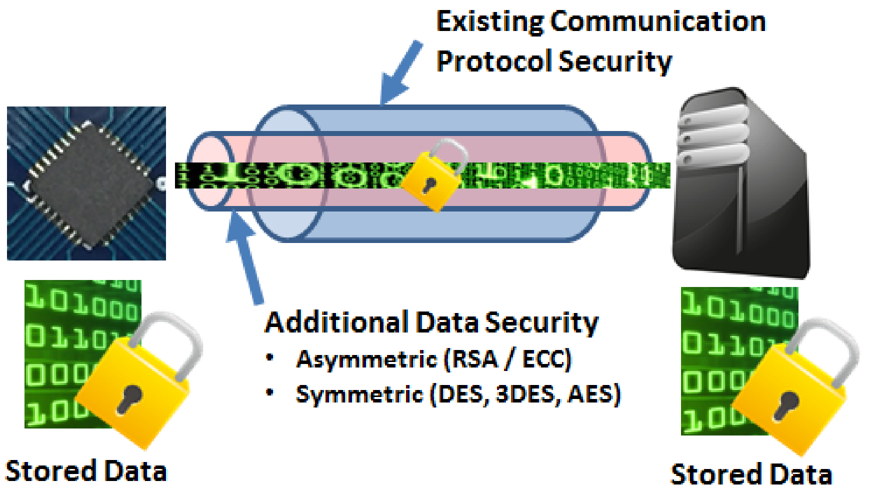
ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

Insecure Data

- Data theft / corruption / fraud
- Communication channel may be compromised
- Data stored may not be secured

Data Protection

- Encrypt sensitive / personal data at point of capture
- Store sensitive / personal data encrypted



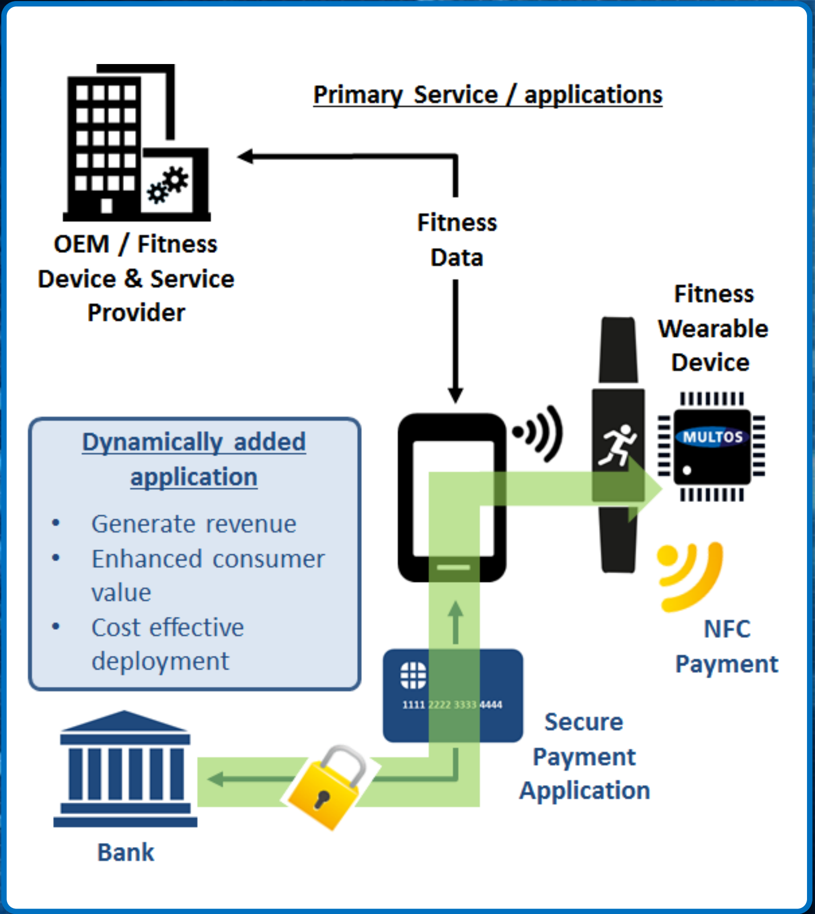
Existing Communication Protocol Security

Additional Data Security
- Asymmetric (RSA / ECC)
- Symmetric (DES, 3DES, AES)

Stored Data

Stored Data

Simple and Secure Provisioning



Primary Service / applications

OEM / Fitness Device & Service Provider

Fitness Data

Fitness Wearable Device

NFC Payment

Secure Payment Application

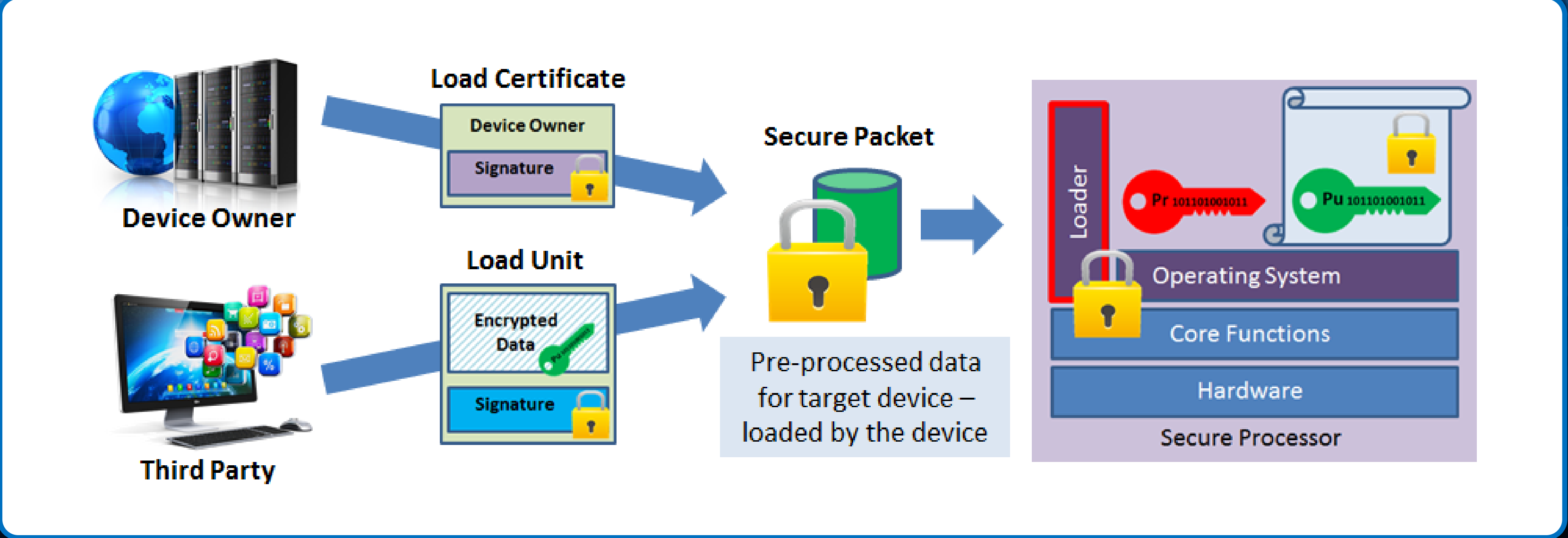
Bank

Dynamically added application

- Generate revenue
- Enhanced consumer value
- Cost effective deployment

Flexible Device Provisioning

- Pre-provisioned / post- provisioned
- Secure channel / insecure channel
- Online / offline
- Via proxy device
- Unreliable communications
- Data processing for scale



Device Owner

Third Party

Load Certificate

Device Owner

Signature

Load Unit

Encrypted Data

Signature

Secure Packet

Pre-processed data for target device – loaded by the device

Loader

Operating System

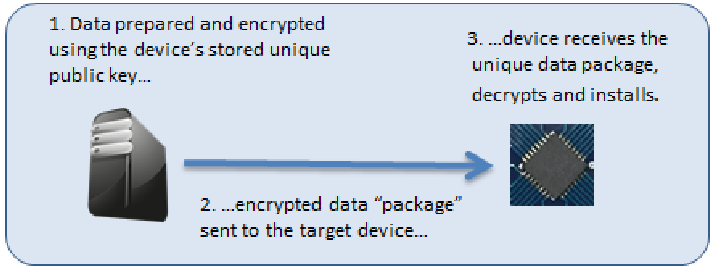
Core Functions

Hardware

Secure Processor

Enhance Provisioning Flexibility

Push - Known Public Key

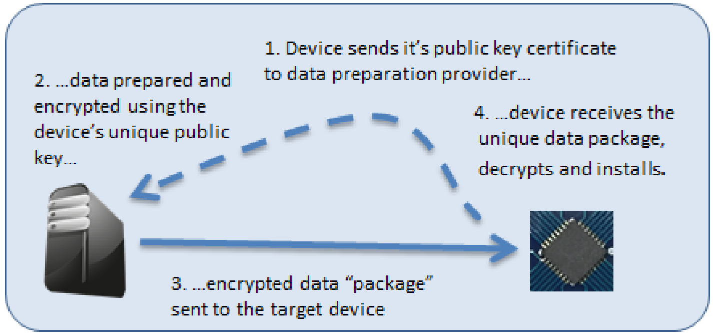


1. Data prepared and encrypted using the device's stored unique public key…

2. …encrypted data "package" sent to the target device…

3. …device receives the unique data package, decrypts and installs.

Push - Requested Public Key



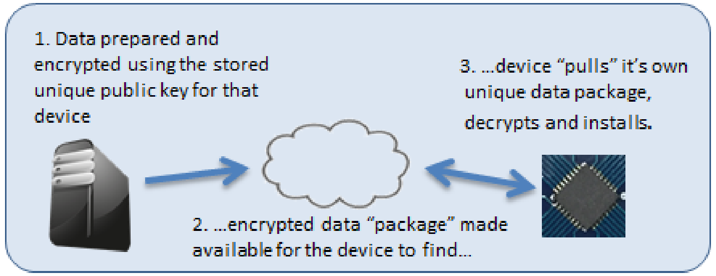
1. Device sends it's public key certificate to data preparation provider…

2. …data prepared and encrypted using the device's unique public key…

3. …encrypted data "package" sent to the target device

4. …device receives the unique data package, decrypts and installs.

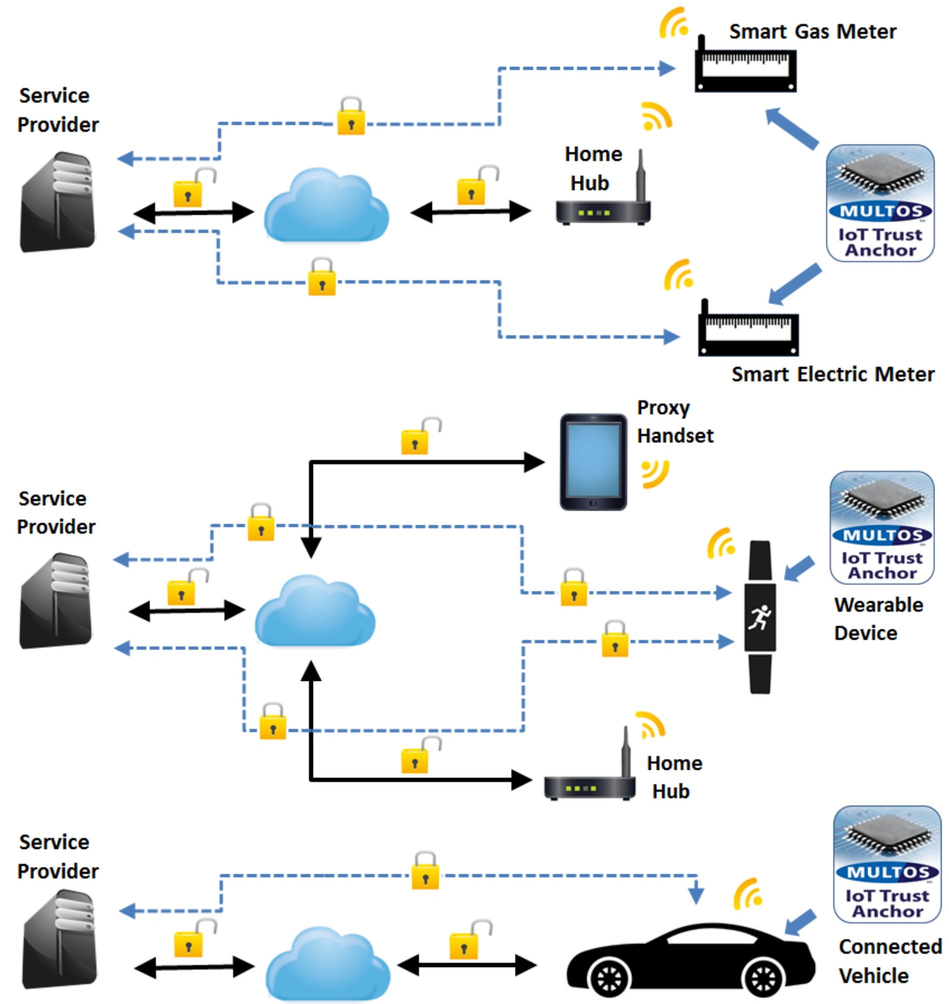
Pull – Known Public Key



1. Data prepared and encrypted using the stored unique public key for that device

2. …encrypted data "package" made available for the device to find…

3. …device "pulls" it's own unique data package, decrypts and installs.



Device Issuer (ROI) – Increase revenue from new services

Service Provider (Efficiency) – Leverage third party assets

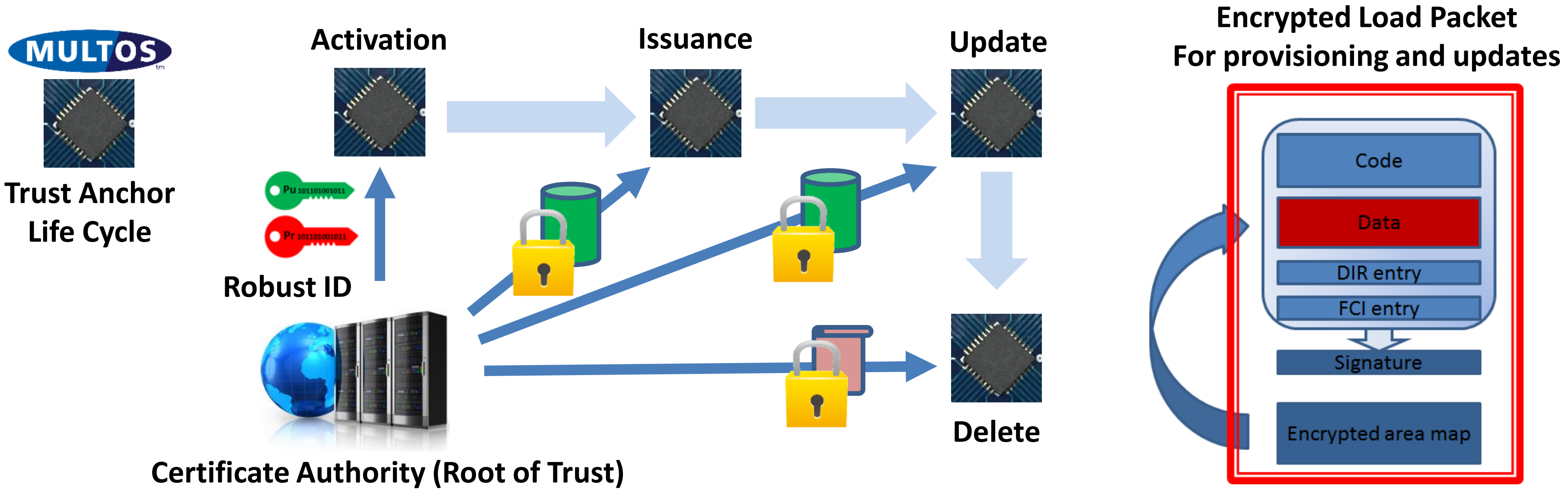
Support the Life Cycle

Device Life Cycle Requirements

- Initial issuance / configuration
- Functional updates over time
- Security updates over time
- Additional service entity
- Change of service entity
- End of Life management

Open Standard

- Device Issuance
- Application Loading
- Data updates
- Application Deleting



MULTOS

Trust Anchor
Life Cycle

Activation

Issuance

Update

Delete

Robust ID

Certificate Authority (Root of Trust)

Encrypted Load Packet
For provisioning and updates

Code

Data

DIR entry

FCI entry

Signature

Encrypted area map

Maximise Cost Efficiency

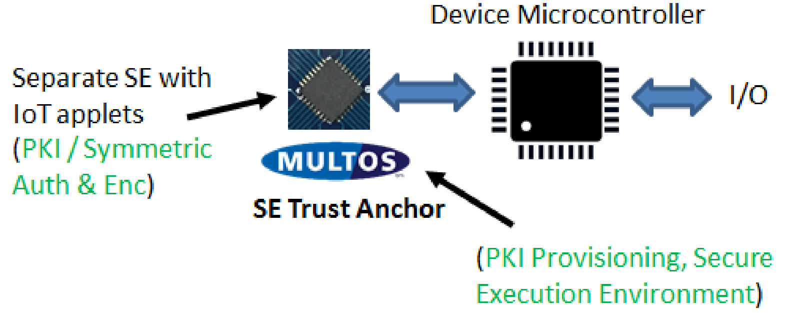
Derived from the GSMA
Critical Recommendations
IoT Security Guidelines
Endpoint Ecosystem
Version 1.0
08 February 2016

		Runtime Protection	Mutual Authentication	Endpoint Personalisation	Provisioning	Separation of Duties	Isolated Environments	
Unique Asymmetric	Pr Pu	🟩	🟩	🟩	🟩	🟩	🟩	← MULTOS
Common Asymmetric	Pr Pu	🟨	🟨	🟨	🟨	🟨	🟨	
Unique Symmetric	Se	🟨	🟨	🟨	🟨	☒	☒	
Common Symmetric	Se	☒	☒	🟨	🟨	☒	☒	

PKI Efficiencies

- PKI ID allows minimal key management
- No secure channel needed for device update
- Less complex & more flexible device management

Separate Co-processor



Separate SE with IoT applets (PKI / Symmetric Auth & Enc)

MULTOS

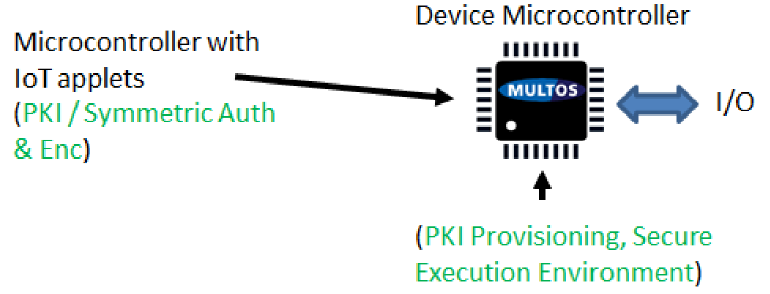
SE Trust Anchor

Device Microcontroller

I/O

(PKI Provisioning, Secure Execution Environment)

Integrated Microcontroller



Microcontroller with IoT applets (PKI / Symmetric Auth & Enc)

Device Microcontroller

MULTOS

I/O

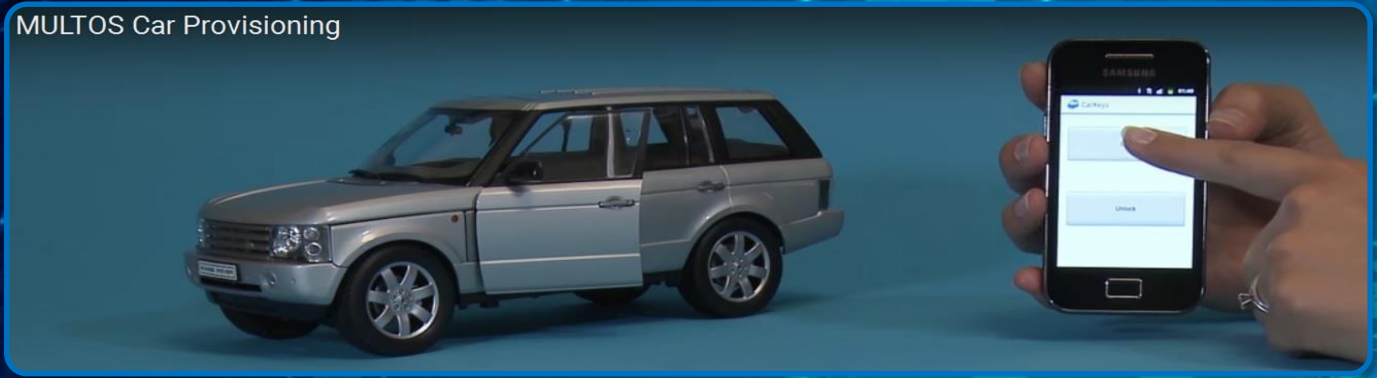
(PKI Provisioning, Secure Execution Environment)

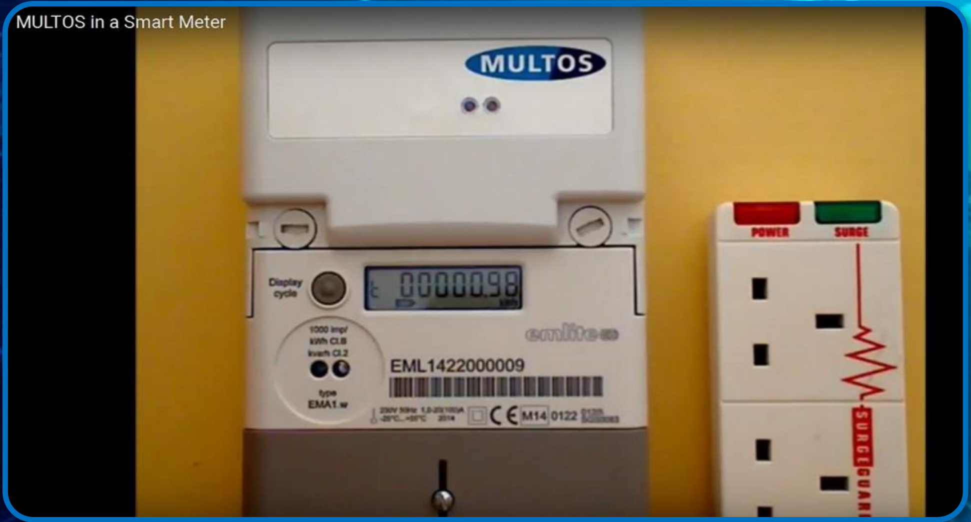
MULTOS tm

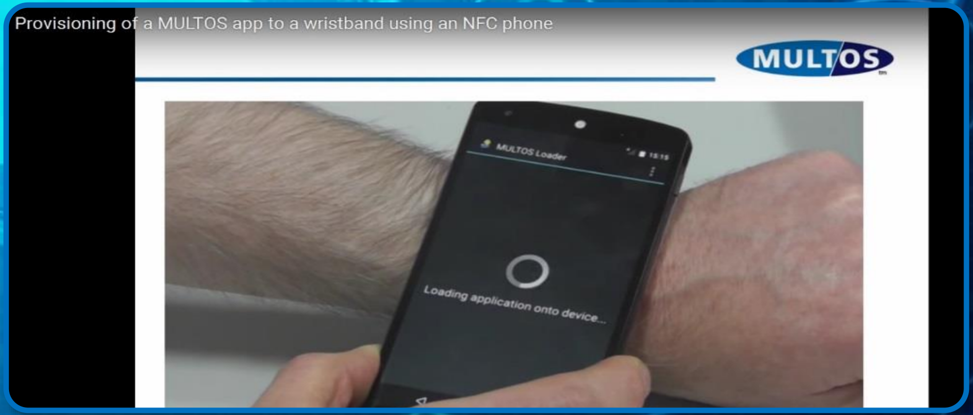
IoT Security Foundation

WE'RE CONNECTED

MULTOS IoT in Action


MULTOS Car Provisioning


MULTOS in a Smart Meter


Provisioning of a MULTOS app to a wristband using an NFC phone

www.multos.com / www.youtube.com

Demo components

Security and Flexibility designed in

- Secure the Runtime
- Ensure Endpoint Identity
- Secure the Data
- Simple & Secure Provisioning
- Enhance Provisioning Flexibility
- Support the Life Cycle
- Maximise Cost Efficiency

www.multos.com

paul.Wilson@multos.com

pr@multos.com

MULTOS tm

IOT Security Foundation WE'RE CONNECTED