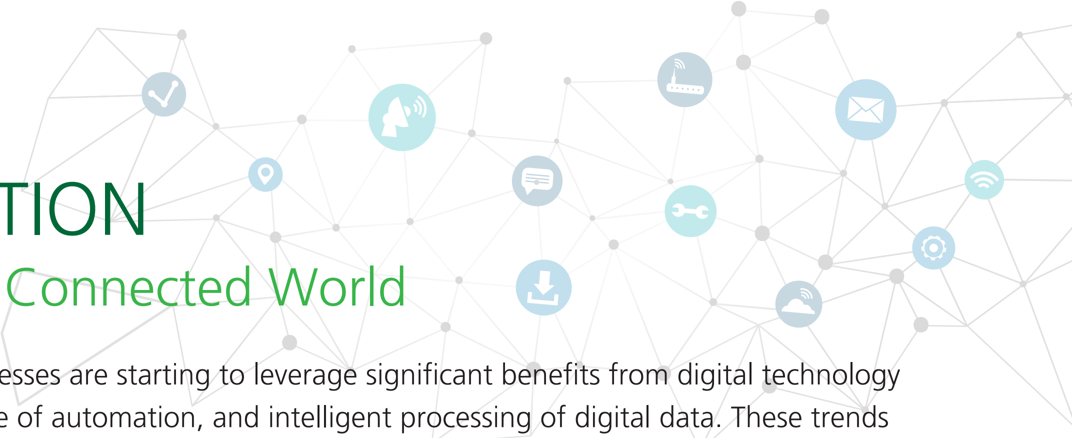
MULTOS tm

SECURITY FOR IoT WITH MULTOS TRUST ANCHOR

Internet of Things White Paper

www.multos.com

TABLE OF CONTENTS



INTRODUCTION

An Increasingly Connected World

Today, consumers and businesses are starting to leverage significant benefits from digital technology advancements, increased use of automation, and intelligent processing of digital data. These trends are often facilitated by devices and services becoming ever more interconnected. Common phrases for this evolving paradigm include; the second digital revolution, the fourth industrial revolution, and the Internet of Things (IoT).

> **“The installed base of IoT devices is forecast to rise from 27 Billion in 2017 to 73 Billion in 2025 [1].”**

Edge-based computing use cases for devices at the edge of networks are expected to be powerful catalysts for growth across the key vertical IoT markets such as; Industrial, Connected & Smart Home, Smart Cities, Medical IoT, and Personal IoT [1]. The International Data Corporation has forecast that IoT spending will reach $1.2 trillion in 2022 [2], so clearly there are great opportunities for IoT product and solution providers.

However, various reports have highlighted the need for a much stronger focus on security.

IoT devices attacked with more than **120,000 modifications of malware** in 1H 2018. 3 times the IoT malware seen in 2017.[3]
Kaspersky Lab

IoT attacks increased from about 6,000 in 2016 to 50,000 in 2017.
A 600% rise in just 1 year. [4]
Symantec

By 2020, it is estimated that 25% of cyberattacks will target IoT devices.[5]
Trustlook

Of course, the level of security required by IoT devices and their supporting solutions will vary depending on the specific functions they are performing, the criticality of the data they are managing, and the level of desire to prevent business and reputational impacts. Weak links in the solution chain can be exploited and may include; the software running on devices, hardware protection, sensitive data storage and communication, device identification, controlling system identification, remote system access and update processes, and initial provisioning security.

> **“Previously Gartner has predicted that worldwide IoT security spend will increase to $3.1B in 2021, attaining a 27.87% CAGR.[6]”**

By reviewing appropriate security measures and planning at design stage, businesses can prepare for the risks of today and the inevitable risks of tomorrow whilst capitalising on the potentially lucrative connected technology opportunities.

In this document, we will introduce you to the MULTOS technology platform which offers high security, ease and flexibility of provisioning that make it well suited to addressing the security challenges with widespread IoT solution deployment.

What is MULTOS and how can it be leveraged for Connected Devices?

Connected devices by their very nature introduce risk by potentially allowing remote intrusion to their own device or access to other connected devices and supporting systems. The devices often referred to as endpoints may have singular connections to a controlling system, or may have multiple connections in a wider more complex and perhaps dynamically evolving architecture.

Endpoint applications of course, vary in function but regardless, most require a number of sensitive processes to be protected including:

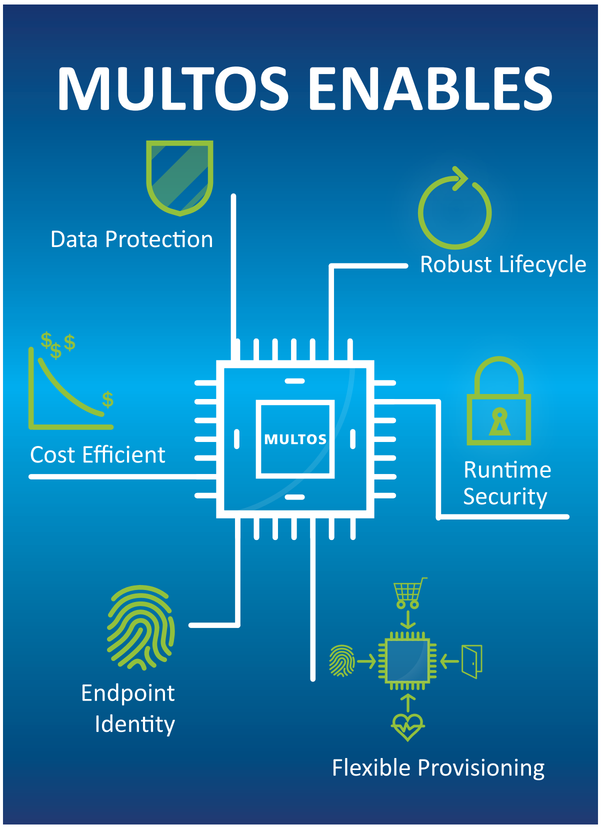
- Device software secured and protected from intrusion
- Endpoint device identity ensured with authentication mechanisms to facilitate operation
- Data stored and transmitted with adequate safeguards
- Controlled and flexible provisioning
- Lifecycle management

Some endpoints may also require or benefit from:

- Flexible remote interactions - to update or modify behaviour, for monitoring and management.
- Cost efficiencies - for scaling, issuance, updating, and decommissioning.

Through the implementation of Public Key Infrastructure (PKI), MULTOS technology can provide connected devices with an appropriate **"Hardware Root of Trust"** and cost effective mechanisms to address all such requirements. MULTOS utilises PKI at its core to secure endpoint connected devices. Solution and service providers can leverage MULTOS Trust Anchors, comprising embedded integrated circuits with the loaded MULTOS Operating System, which provides an ultra-secure execution environment for numerous applications, protecting the device from malware and other digital attacks. Critical data transmission can also be secured to and from the device.

MULTOS Trust Anchors are supported by cryptographic services via hosted or licensed MULTOS Certificate Authority platforms, facilitating full end-to-end protection.



MULTOS OVERVIEW

More than 20 Years of Security and Innovation

1 BILLION+
DEVICES
3,500+
BUSINESSES
50
COUNTRIES
20 MULTOS
YEARS OF
SECURITY AND
INNOVATION

MULTOS was designed to address the need for a secure, efficient, and common standard to provision smart cards such as those used in payment "Chip and PIN" cards, and government issued citizen identity cards. The MULTOS platform ensures these cards are operated during their lifespan with a high degree of robust protection against fraudsters.

The secure and flexible MULTOS features, along with its industry-leading reputation have allowed the technology to also become widely used in numerous security applications, such as Identity, Access Control, Authentication and Government Programs, in addition to secure EMV and contactless payment devices. Implemented worldwide in mass volume, the MULTOS design has met and surpassed its initial brief.

MULTOS is the only secure OS platform to achieve the highest level of security evaluation possible - Common Criteria EAL 7 which is an Information Technology Security Evaluation measurement of smart cards and other secure devices.

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+

Most Smart Card Implementations

MULTOS

Enabling this achievement are the security features and processes built into the specifications that essentially provide the two core benefits of:

- **A highly secure smart device operating system** to ensure reliable and robust functioning.
- **A managed provisioning** and **lifecycle process** to ensure full issuer control with flexible third party interaction options.

DEVICE SOFTWARE SECURITY

One significant area of risk in connected devices is the firmware and software operating systems and applications. Once embedded code and applications become corrupted or infected with malware, serious issues can arise.

Infected devices may cease to function as designed causing end user frustration or additional business management effort. Knock on effects such as incorrect data captured from the endpoint may infect or invalidate data stored centrally. As many devices require some form of sensitive data to be stored at the endpoint such as authentication keys, fraudsters have a clear target for their malicious endeavors. Likewise, attackers may target the downloading of software stored on the device and threaten the device provider's intellectual property.

The very nature of connected devices lends itself to cost effective remote software updates to patch weaknesses or address incorrect functioning, but that operation assumes the device will still interact with remote controlling systems as expected once the device becomes infected with malware, which of course, may not be the case and may lead to unexpected replacement costs and engineer visits. Fraudsters and hackers are likely to target these areas of risk.

Another area of concern is the lack of regulatory environment mandated by governments or industry that can include things such as the right security and functionality that all these connected devices must achieve.

Common Risks

- Incorrect functioning
- False data generation
- Secret credential exposure
- Remote update failure
- Code extraction

This leaves the device designer to make the judgement and that can be problematic. What may seem to be a good decision at first, such as using a chip with some so-called 'secure software' platform, may not end up being the right choice. Most chip companies are not experts in or have a long track record in developing the s/w operating platform that is required for a properly secure, flexible and open environment.

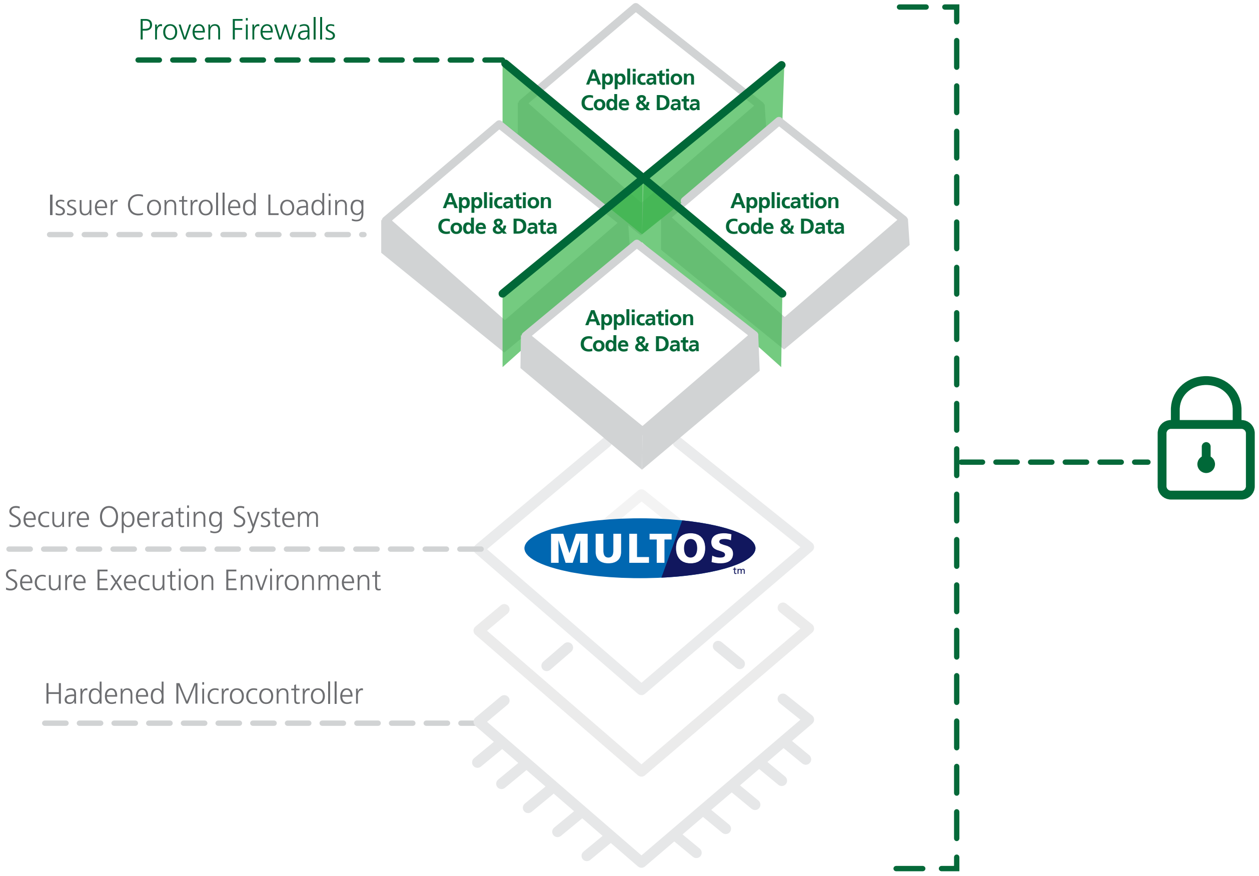
So what countermeasures can be employed to address under-protected software?

All such issues may be prevented by using a combination of hardware and software from organisations that have a track record of developing secure solutions – real security.

A hardened chip or co-processor with associated secure functions such as power scrambling, internal data encryption, and advanced error detection is a fundamental starting point. This approach of designing a device with core hardware and software countermeasures and utilizing specific cryptographic functions to protect operations has been the bedrock for the micro-processor industry for over 20 years, and is considered critical to thwart cyber-attacks and prevent loss of confidence in the technology.

MULTOS technology is the dedicated secure software environment implemented on hardened processors and undergoes a security evaluation. To further boost the protection, the addition of a Secure Execution Environment (SEE) is built into the operating system. The SEE acts as an on-device policing agent, ensuring strict application and associated data segregation.

The mechanism was designed to support the multi-application capability leveraged by some MULTOS implementation clients.



ENDPOINT DEVICE IDENTITY AND AUTHENTICATION

For many connected devices, it can be critical to ensure the device has a unique identity within the network it is interacting with. If a device is unable to maintain its intended identity, any data provided by it to a central system may not be considered trustworthy or valid. Through provisioning faults or intended attacks, device ID duplications are a system risk which at best can lead to confusion and service disruption, but in more severe cases can lead to fraudulent behaviour. Clearly a strong identity should be a fundamental cornerstone of a connected device to prevent.

Good IT security practice suggests that specific processes should be applied to address this risk. One such option is to personalise the endpoint with a specific identification serial number, another is to add a robust unique cryptographic identity – something which is already built into the MULTOS technology platform and has been utilised by over a billion devices. A unique chip identifier is generated during the manufacturing process for MULTOS and is injected into the device to ensure a cryptographic binding of each chip to a specific owner.

Public key cryptography is a proven mechanism to ensure flexible IT architecture endpoint identities and has been used as the foundational security for functions ranging from IT networks, to banking platforms.

MULTOS uses this process where asymmetric key pairs (matched sets containing a public and a private key) are generated and loaded into the secure chip to provide the endpoint with a strong personalised identity. The MULTOS Carrier Device (MCD) ID number is linked with a specific device issuer ID number and the PKI key set to form the robust unique identity. The latest MULTOS specifications support strong PKI cryptographic algorithms with extended key lengths.

Common Risks

- Unidentified entity
- Device duplication
- ID impersonation
- Central data corruption

A second option to address the risk of a weak endpoint identity is to enforce strong mutual authentication between the device and its interacting devices and systems. The supported asymmetric and symmetric cryptographic functions within a hardened processor can be used by the applications to ensure robust mutual authenticity when appropriate.

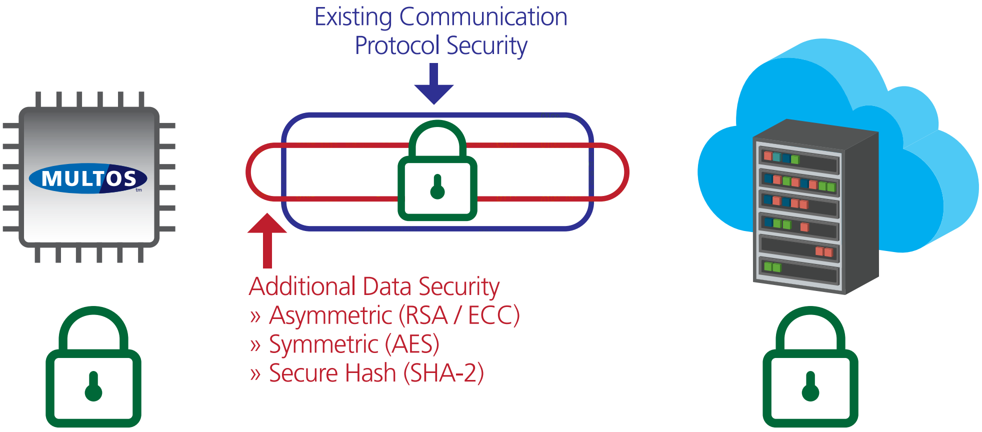
Lost, stolen, or corrupt data can have significant financial and reputational impacts for businesses. Data stored at endpoint devices, at central systems, and in transit within networks is potentially at risk. Communication protocols which are necessary to allow system interaction are not always as secure as they might be perceived, and if considered secure, all the security feature options within them may not have been implemented.

DATA SAFEGUARDS

Of course, not all data may need the same level of protection, and the application or service, be that medical, personal, financial, or operational will dictate the level of protection required. To protect businesses and consumers, how can a multi-layer approach be applied to ensure adequate protection of sensitive data?

Highly secure smart card chip technology has been developed, enhanced and deployed worldwide for over 20 years. Therefore, why not use the cryptographic features supported by smart card platforms such as those within MULTOS products to allow additional levels of protection for data in IoT solutions, thus boosting the protection provided by any existing communication protocols and security features.

IoT devices could benefit from the cryptographic features supported by MULTOS to allow additional levels of protection for the sensitive data.



Symmetric or Asymmetric cryptography features can be employed to encrypt any data at risk, such that the data will be of no use to any third party accessing the data without authorisation.

Risks include:

» Data theft / corruption / fraud
» Communication channels may be compromised
» Data stored may not be secure

PROVISIONING

Often the provisioning of the required application software and associated data in electronic devices is performed as part of the manufacturing process, sometimes within physically and logically secure environments. For some connected devices this may continue to be the applied process. However, the greater reliance on connectivity opens up more dynamic possibilities for provisioning. It may make sense for commercial or practical reasons to remotely provision a device, particularly if personalised information is required to be loaded on the device, certain desired business models may seek to have third party applications and data loaded on devices which are already in use with consumers or businesses, proxy devices may be employed to facilitate remote provisioning.

The mechanism of remote provisioning may need to consider:

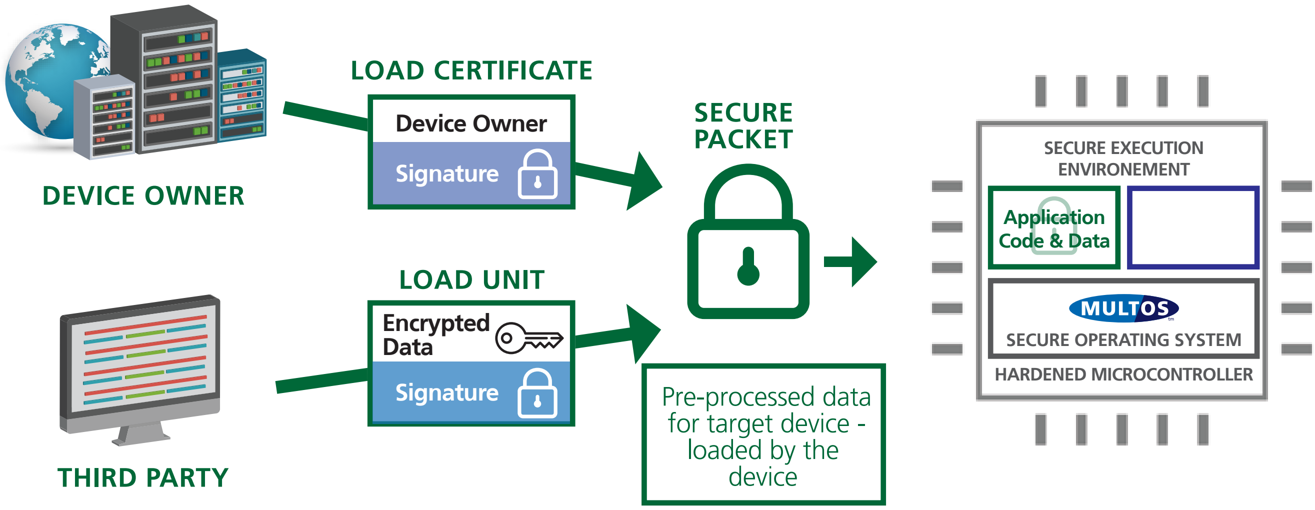
- Pre-provisioned / Post-provisioned
- Secure channel / Insecure channel
- Online / Offline
- Via proxy device
- Unreliable communications
- Data processing for scale

Device application and data provisioning requirements may vary depending on the service.

- **A smart wearable device** may need a payment application added after the device has been purchased by the consumer.
- **A smart meter** may need new keys and configuration data loading when a consumer changes utility provider.
- **A connected vehicle** may need a new insurance linked telematics application adding when the driver changes insurance provider.

Hence how can a secure and simple mechanism be provided to facilitate these in-field remote processes? Utilising a strong key management method can provide the necessary simplification and security required for a robust provisioning solution.

An option could be to utilise asymmetric cryptography as supported by MULTOS for managing the deployment of the device, and utilising either a secure packet or a secure channel to deploy the device content. The use of secure, encrypted load packets between the device and the host can further simplify and reduce key management.



The use of asymmetric cryptography easily allows the device to be managed by the device owner and the initial issuer, whilst third party businesses can load their content to the device assuming the owner has authorized the change. Any third party sensitive content can be encrypted such that the owner and any unauthorized entity would not have access. This versatile mechanism built into the MULTOS specifications could be an efficient solution for the likely complex business models of future connected devices and allow firms to deliver their services on already issued infrastructure, potentially reducing costs and speed to market.

LIFECYCLE MANAGEMENT

Full consideration of the lifecycle of any connected device should feature highly with solution providers. Some IoT devices, particularly the more industrial type, could be in use for many years and the cost to physically attend would be prohibitive and therefore most would benefit from a well-managed, flexible and controlled lifecycle. Even if some devices are intended to have shorter lifecycles, there are still good reasons to carefully control the lifecycle.

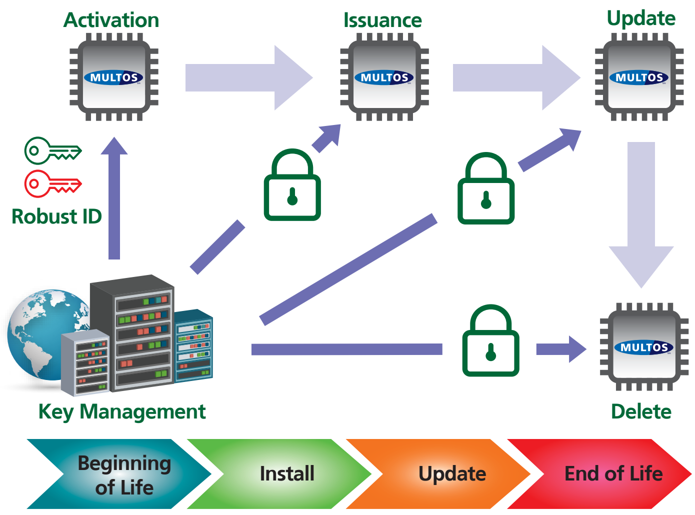
Many of these devices may contain sensitive business, personal, or financial data; or be related to infrastructure or other mission-critical applications, and it may not be desirable to leave this data within devices when no longer required. A device may need a number of remote functional updates to reconfigure or modify the service over time. Of course, security updates are a likely requirement as attacks evolve and improve over time.

What mechanism could deliver the required security and flexibility to support these needs?

The processes for this flexibility and control were built into the open MULTOS specifications many years ago which include;

- Initial activation where the device receives its robust cryptographic ID
- Application loading for issuance
- Subsequent updating as required
- Eventual application and associated data deletion at the end of life

MULTOS LIFECYCLE MANAGEMENT



Key Considerations:

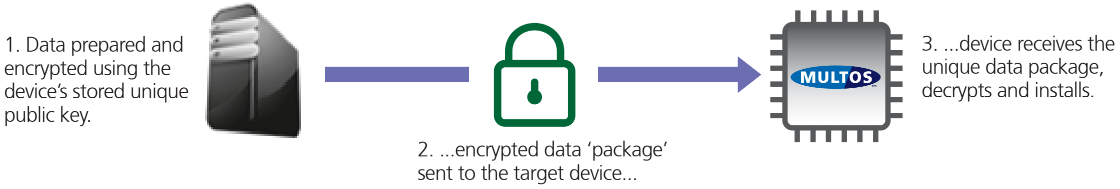
- Initial issuance / configuration
- Functional updates over time
- Security updates over time
- Additional service entity
- Change of service entity
- End of life management

FLEXIBLE REMOTE INTERACTIONS

Many businesses are developing or have already developed management systems to remotely service connected devices. These IoT device management platforms such as Amazon AWS IoT and Device Authority's KeyScaler, can perform a range of activities including; diagnostics, software updates, and lifecycle management to devices remotely. IoT device management software can be used in conjunction with other systems including IoT security software, IoT analytics and IoT platforms. As these connected device ecosystems merge and interact, what flexible processes could be implemented to leverage existing systems?

Asymmetric cryptography using the processes already supported by MULTOS technology can not only simplify the key management, but can also ensure a high degree of provisioning and device management flexibility. A device could be updated directly by a system that knows the endpoint and its PKI credentials. Alternatively if the system does not know the device credentials, the device can be requested to provide them, thus allowing third parties to modify the device content, assuming they have an agreement to do so with the device owner. This could be a very useful feature for systems updating endpoint devices that they do not own. Also a system could prepare the device updates offline, perhaps using a batch processing approach, allowing for later retrieval and updating by the device itself.

PUSH - KNOWN PUBLIC KEY UPDATING

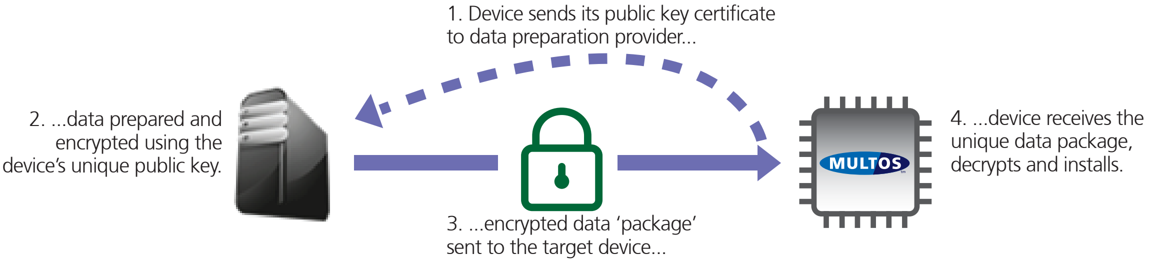


1. Data prepared and encrypted using the device's stored unique public key.

2. ...encrypted data 'package' sent to the target device...

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

PUSH - REQUESTED PUBLIC KEY UPDATING



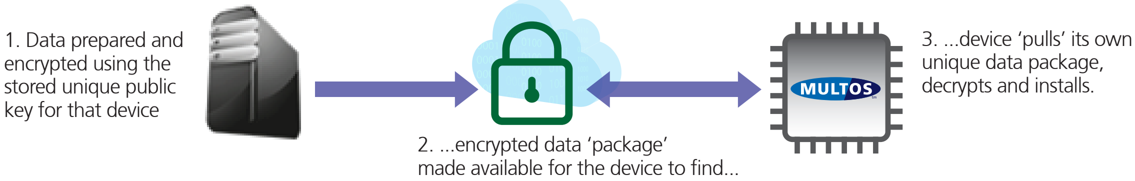
1. Device sends its public key certificate to data preparation provider...

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 UPDATING



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' its own unique data package, decrypts and installs.

Having this level of flexibility built into a system can help to future proof the solution by allowing for future new features and business models, and may ultimately improve the commercial monetization of the service.

COST EFFICIENCIES

Securing endpoints is fundamental, but allowing for cost efficient scaling is also important if large numbers of devices are required to be added to the connected device network. The cost of the devices and the overall system is often critical for business viability, and in some cases security may be sacrificed to reduce costs.

Each business must decide their own level of acceptable risk regarding any security verses cost trade-offs. In the digital technology industries few would argue that security is not a concern in the increasingly connected world, and systems not already targeted by hackers and fraudsters today may well become attractive targets in the future. So clearly some security is desirable, but is it possible to provide adequate security without significant additional cost?

By utilising PKI technology, it could well be possible to comprehensively address security concerns whilst minimizing costs. Derived from the GSMA IoT endpoint security guidelines[7], the diagram below highlights asymmetric security with personalised keys, which is supported by MULTOS, as the most secure approach to protect connected devices and the most likely to remain secure for the long life spans of IoT devices.

		Runtime Protection	Mutual Authentication	Endpoint Personalisation	Communication Privacy	Separation of Duties	Isolated Environment
Unique Asymmetric	🔑🔑	🟩	🟩	🟩	🟩	🟩	🟩
Common Asymmetric	🔑🔑	🟧	🟧	🟧	🟧	🟧	🟧
Unique Symmetric	🔑	🟧	🟧	🟧	🟧	🟥	🟥
Common Symmetric	🔑	🟥	🟥	🟧	🟧	🟥	🟥

MULTOS

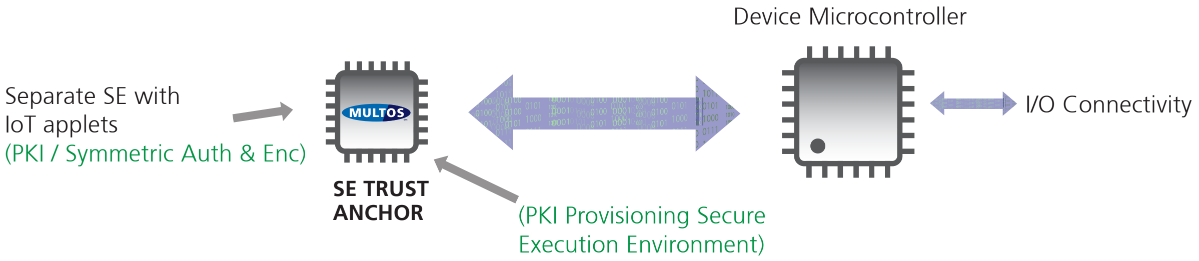
PKI Efficiencies

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

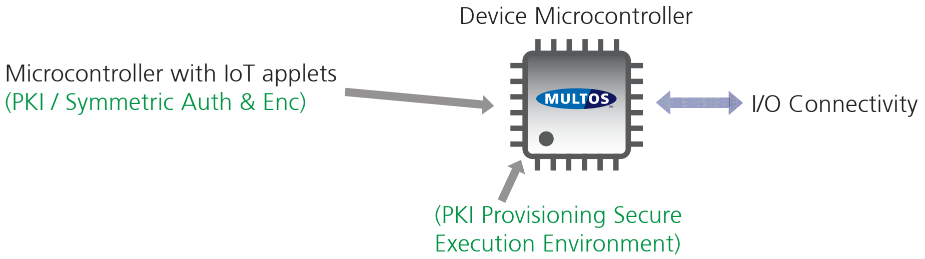
By using asymmetric cryptography, cost efficiencies could be realised, including:

- Not having to exchange symmetric keys with third parties which could reduce key management efforts and subsequent costs.
- Pre-generated application updates can be prepared offline facilitating lower cost batch data processing avoiding the need for reliable real-time connectivity.
- A device can directly present its public key certificate to ecosystem entities, thus potentially simplifying device management and reducing system complexity while enhancing flexibility.

Further cost efficiencies could be realised at the endpoint device via the configuration approach adopted. A separate secure element co-processor could be used by the main processor to handle specific security related functions. This architecture may be easier to implement for some designs as it may be less disruptive to an existing IoT product configuration.



Alternatively, the MULTOS security could be implemented within the main microcontroller. This could present a more cost efficient overall architecture with a lower bill of materials.



The specific configuration option selected should consider a number of factors including:

- **Product availability** – ensuring that the required secure element or integrated microcontroller can be supplied to meet the project requirements and scaling forecast demands.
- **Time-to-market** – reviewing any associated development efforts required to integrate the security options considered within the overall device design.
- **Cost** – ensuring an adequate level of security protection is included within the design based on the assessed risk of attack impacts and potential consequences.

SUMMARY

With the significant opportunities connected devices can offer businesses and consumers, and the evident increasing risks derived from the digital inter-connections, it is clear that security should be seriously considered within an overall system design. The level of acceptable security should be based on; costs, time-to-market, reputational and financial risks from cyber-attacks, business and consumer privacy, protection, safety, and potential evolutions required of a system or device over time.

Attackers targeting software is a common risk within IT and may increase as more devices are inter-connected. The MULTOS technology with hardware and software countermeasures and a long and successful history in the secure smart card industry does offer suitable protection for under-protected devices.

Endpoint Identity. Ensuring endpoint devices are identified as **unique** within their network and operate with adequate mutual authentication is an obvious design focus to avoid functional issues and potential fraud. With MULTOS authentication features, a robust unique cryptographic identity can be easily enforced.

Protecting data within systems may be critical. Different applications and data elements may require different levels of protection based on their sensitivity and type of use such as; medical, personal, financial, and operational. Hackers may target sensitive data to either commit fraudulent activities or damage business reputations. Trusted security features from the smart card industry as supported by MULTOS can further enhance any security provided by existing connectivity protocols. A sound "belt and braces" approach is recommended to ensure protection over time and the solution longevity.

Provisioning. The process to load applications and data within connected devices either initially or when in use should warrant some careful consideration of the current needs of potential future business opportunities. Some markets have requirements for this flexibility. MULTOS provisioning is ideally suited to provide a simple and secure mechanism to meet these requirements.

Robust Lifecyle. Device life spans may cover many years. Implementing a controlled whole lifecycle approach can not only protect the devices and solutions but can also ensure they remain flexible and versatile. The proven robust MULTOS lifecycle process can offer such security and flexibility.

Managing connected devices can often be most efficiently achieved via remote systems. Such device management systems may need to not only manage or interact with their own devices, but may also need to control applications and data on third party owned devices. MULTOS technology offers flexible options to facilitate these processes.

The implementation of PKI cryptography to enhance security and flexibility can help derive a number of total system **cost efficiencies.** Overall key management may be simplified reducing the effort, update processing may be managed in cost effective offline batches, and device management complexity may be reduced. MULTOS can fully support these potential system optimizations.

The **MULTOS Trust Anchors** using robust hardware Root of Trust mechanisms are very well suited to deliver exceptional levels of control, security, flexibility, and business efficiencies to the developing industry of connected devices.

REFERENCES

REAL WORLD SECURITY THREATS

- IoT security: What we can learn from recent threats – Jan 2020, IoTnow
- Smart, or Not So Smart? What the Ring Hacks Tell Us About the Future of IoT – Feb 2020, SecurityWeek
- Cyber threats to IoT in 2020 – Nov 2019, techradar
- 10 IoT Security Incidents That Make You Feel Less Secure – Jan 2020, CISO MAG
- Smart camera and baby monitor warning given by UK's cyber-defender – Mar 2020, BBC
- IoT: Always On, but Unsecured – Mar 2020, Payments Journal
- UK IoT security regulation encourages consumers to be more aware – Sept 2019, IoTnow
- Enterprise IoT and data breaches: what you need to know – Jun 2019, Information Age
- Enterprises are leaving IoT devices vulnerable to cybersecurity threats, finds nCipher Security – Oct 2019, IoTnow
- Future cities under risk of cyberattacks due to insufficient security investment, ABI Research warns – Aug 2019, IoTnews
- UK seeks to secure smart home gadgets – Oct 2018, BBC
- Top 10 Biggest IoT Security Issues – May 2019, intellectsoft
- Philips Hue vulnerability lets hacker controls bulbs, could escalate to network – Feb 2020, 9TO5Mac

FOOTNOTES

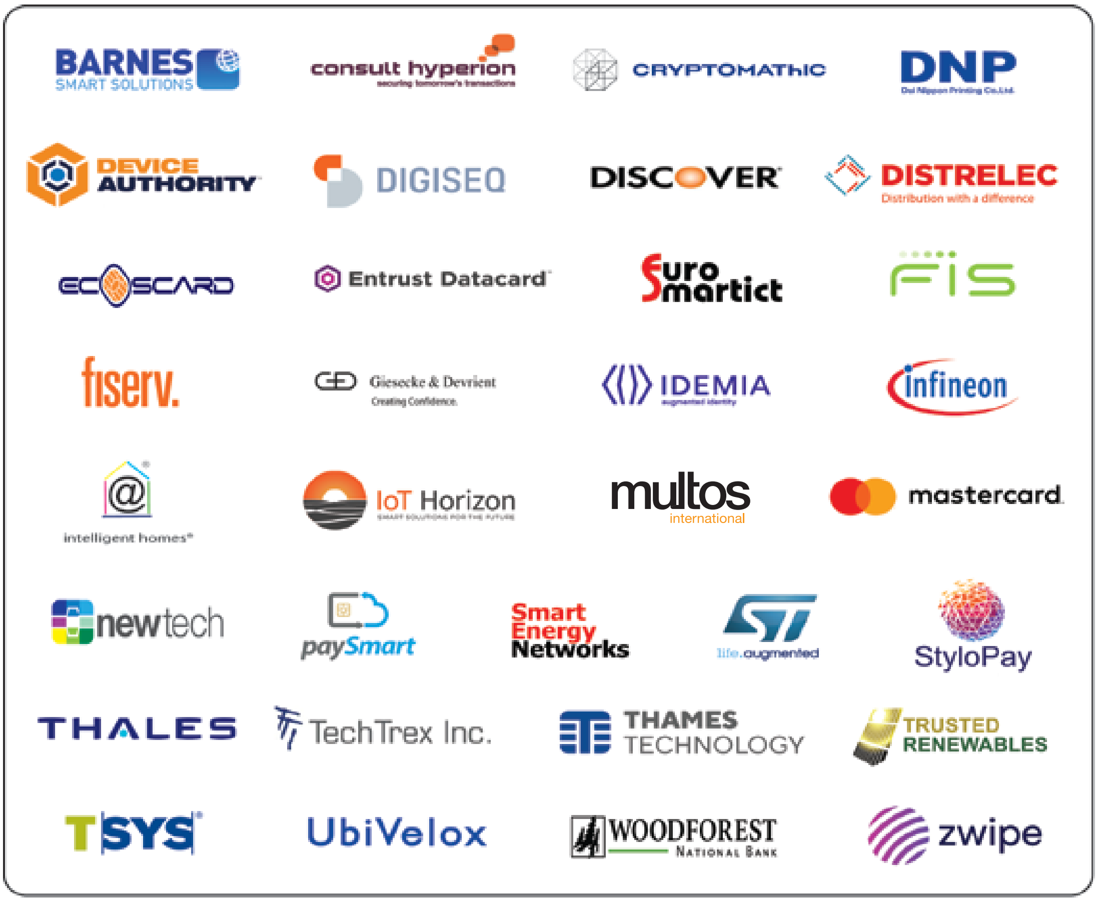
REF	SOURCE
[1]	IHS Markit 2018 Top Transformative Technology Trends.pdf https://cdn.ihs.com/www/pdf/IHS-Markit-2018-Top-Transformative-Technology-Trends.pdf
[2]	IDC Forecasts Worldwide Technology Spending on the Internet of Things to Reach $1.2 Trillion in 2022 https://www.idc.com/getdoc.jsp?containerId=prUS44596319
[3]	New IoT-malware grew three-fold in H1 2018 https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018
[4]	As IoT attacks increase 600% in one year, businesses need to up their security https://www.techrepublic.com/article/as-iot-attacks-increase-600-in-one-year-businesses-need-to-up-their-security/
[5]	IOT SECURITY:A COMING CRISIS? https://newblogtrustlook.files.wordpress.com/2017/09/iot-security-survey-infographic-2017.pdf
[6]	2018 Roundup Of Internet Of Things Forecasts And Market Estimates https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates
[7]	GSMA - IoT Security GuIdelIneS for endpoint ecosystems, Version 2.0, 31 October 2017 https://www.gsma.com/iot/wp-content/uploads/2017/10/CLP.13-v2.0.pdf

APPENDICES

The MULTOS CONSORTIUM

There are multiple stakeholders in the open MULTOS technology today. Thousands of card issuers such as banks and governments utilise the technology to issue in mass volumes to end users. Some businesses have extended their interest in the technology by becoming a member of the MULTOS Consortium which allows them to leverage the technology benefits for their own commercial gains.

CONSORTIUM MEMBERS



The Consortium is a diverse mix of respected global businesses and IT security businesses providing MULTOS related deliverables such as; secure chip supply, operating system supply, application supply and development, data processing for issuance services and post issuance interactions, personalization solutions and component provision, secure key management services and solutions, application and transaction processing, consultancy and training, and business development.

Today, the ever expanding smart card industry and new smart device applications such as the IoT are attracting new members to the Consortium and driving future MULTOS evolution.

> **“The Consortium is a diverse mix of respected global businesses and IT security businesses providing MULTOS related deliverables.”**

ABOUT MULTOS

MULTOS is a robust, industry-backed technology for smart devices, delivering high security, simplicity and flexibility to a variety of consumer and business IoT and connected devices. MULTOS has been at the heart of the secure token industry for 20 years, with over 1 billion secure MULTOS smart cards and devices shipped. A wide range of digital security applications including EMV payment, contactless payment, authentication, digital identity, biometrics, loyalty and mass-transit ticketing, and connected smart devices may be implemented and co-reside using a MULTOS powered chip.

MULTOS

multos.com