MULTOS
20 YEARS OF SECURITY AND INNOVATION

DIGITAL SECURITY INSIGHTS

Concise news, information and know-how from the MULTOS Consortium

Issue 3, 2017

Trustech 2017

TRUSTECH
PAY | IDENTIFY | CONNECT & SECURE

The MULTOS Consortium once again attended Trustech at Cannes (28th – 30th November). Over 11,000 participants from 125 countries attended, including 43 startups and FinTech companies and 300 exhibitors and sponsors, of which 130 were new to the event. The prominent MULTOS stand was located upstairs in the Lerin's area – the booth number was very easy to remember, ***007***, (where Paul did his best impersonation of the Daniel Craig era James Bond).

This year we celebrated the double milestones of ***20 years of MULTOS*** and the ***1 billionth device*** shipment.

On the demo desk, Chris showcased the latest use-cases for MULTOS technology, including an interesting smart solar panel with Trusted Renewable – which won ***first prize*** in the Sesame Awards in the IoT category! We also demonstrated how easy it is to provision MULTOS devices that would be well-suited to wearables and other payment tokenization services. We also enjoyed a celebratory drink (or two) over lunchtime snacks where we played our 20th Anniversary video featuring prominent figures from the world of payments and ID; and other characters that would not look out of place as villains in a Bond movie (one of the installments from the 1970s). It was great to see some old friends and plenty of new faces at Trustech this year. Wishing everyone a safe and happy holiday season.

Consortium News

New Members

DIGISEQ universal SMARTCARDS allpay·cards

Since the previous issue, the MULTOS Consortium welcomed three new members to the family. The Consortium growth reflects increasing interest in the deployment of MULTOS for innovative secure device and payment methods as well as continued strong demand in traditional markets. You can read more about all our members and their MULTOS offerings in our **Product Directory**.

New Promotional Materials

The consortium has also produced a number of new joint promotional collaterals with members ABCorp, Trusted Renewables Ltd, DigiSEq, Universal Smartcards and allpay cards.

We have released a new flyer called "**Design-In MULTOS**" that summarises the key benefits of including MULTOS in the design of a new breed of smart, secure connected devices.

And we are very pleased to launch a brand new short animation that explains the MULTOS benefits for all kinds of secure devices, offering:

- Endpoint identity
- Runtime security
- Data protection
- Robust lifecycle
- Cost efficiency

To watch, please visit our **YouTube channel.**

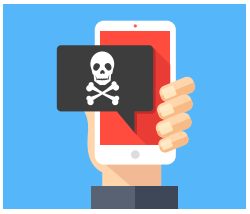
INSIDE:

Fast News

ATM Malware

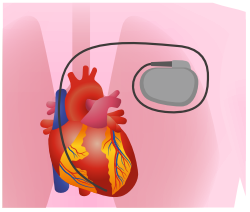
A recent **white paper** from Trend Micro discusses the different types of ATM malware seen around the world. As discussed in the paper, ATM attacks are moving beyond physical interventions, such as skimmers, and into networks. Many ATMs run unsupported version of Microsoft Windows. As with many security breaches, attacks often start with introducing malware via phishing e-mails.

More Mobile Mayhem



Last time we highlighted a report summarising threat data for mobile devices. This time we pick up on a specific and particularly nasty threat currently targeting Android devices. Google Play automatically screens apps for threats but new malware dubbed ExpensiveWall bypasses these checks through obfuscation techniques, making the 'bad' code impossible to detect statically. **Read more**

Pacemaker Vulnerabilities



Ars Technica UK reports on fundamental vulnerabilities in many radio controlled heart pacemakers. Chief amongst the vulnerabilities is the ability for programming devices to be able to change pacemaker settings without requiring authentication. Programming devices are freely and cheaply available.

The Rise of Thingbots

Unprotected IoT devices are becoming the weapon of choice for botnet-building attackers, according to a recent report from **F5 Labs**. Their popularity arises from being easily hacked and literally "free" for the taking. Often based on small but powerful microcontrollers running a rich operating system, they make ideal platforms for launching DDOS attacks and can be easily accessed using unprotected Telnet connections.

IoT Security Foundation

IoT Security Foundation

The IoT Security Foundation (IoTSF) is one of a small number of international bodies looking at how to make the Internet of Things as safe as possible. Founded in 2015 after a summit of modern-day experts at the iconic Bletchley Park, England, its mission is to promote knowledge and clear best practice.

"Our mission is to help secure the Internet of Things, in order to aid its adoption and maximise its benefits. To do this we will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems.

Make it safe to connect"

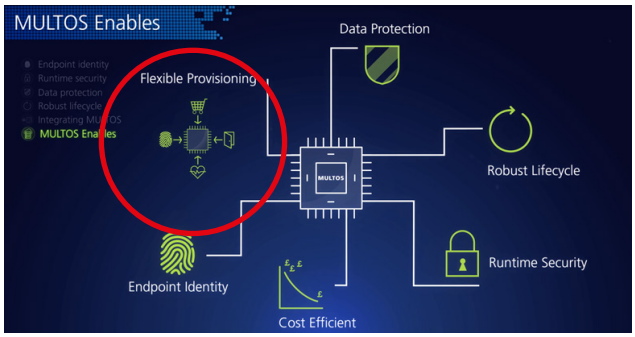
Unlike other consortia working in the IoT domain, the IoTSF does not promote any particular technology or solution set. Instead, it highlights through its best practice guides what needs to be achieved for security, rather than how. Much of what they recommend is common to those working in the smart card industry and importantly the IoTSF recognises that IoT Security is NOT the same as general I.T. security.

Technology Briefing – Exploding a MULTOS Myth

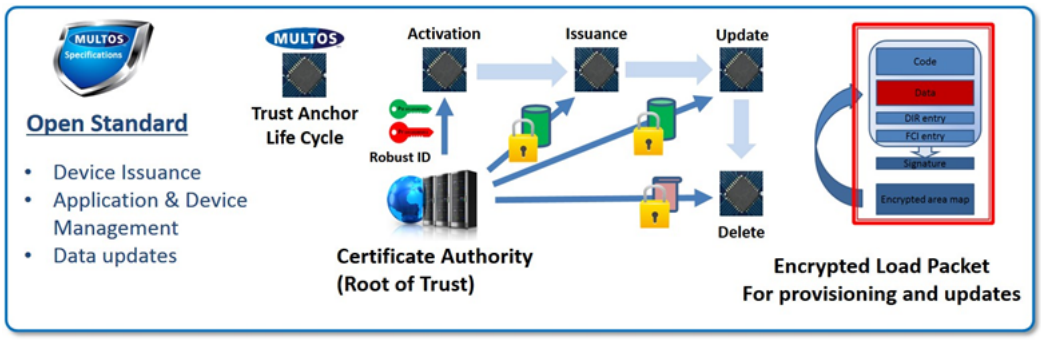
You may have heard that MULTOS is difficult to personalise.

MULTOS personalisation is issuer (or bureau) centric, and was explicitly designed that way from the very beginning of its life some 20 years ago, and now successfully deployed over 1 billion times. Some organisations, however, may portray the bureau-centric processes of MULTOS as complex and therefore difficult to personalise. The truth is in fact completely different. Indeed MULTOS offers process options for the bureau, as we shall see below, to serve the varying needs of all kinds of personalisation bureau operations of all sizes and skill levels. Read on to get a short guide to how MULTOS devices are personalised. For those that have known MULTOS for some time, you might be interested to take a look to discover a few new features available in recent releases of the platform.

So let's talk about this concept of "Flexible Provisioning" for the MULTOS secure platform.



MULTOS is unique in that it does not require any pre-personalisation stage prior to shipment, allowing for generic 'vanilla' devices to be deployed to any bureau ready for any issuer customer. The whole lifecycle is protected by the strong key processes of MULTOS that are built-into the operating system on each chip.



There are 3 basic steps for provisioning a MULTOS device, and even these can now even be combined and performed during a single step interaction with the chip. Let's take a look at those key steps and highlight the options available.

1. Enablement

You can think about this step as ***device activation***. Prior to this, the MULTOS device will not execute any application and it can be associated to any issuer owner. The enablement step provides the cryptographic lock between each unique MULTOS device and the issuer and opens the chip to accept authorised applications to be loaded.

The bureau can choose how device activation is done:

- Centralised key management with the MULTOS KMA
- Using Real-Time Enablement, by integrating the key management utility into the bureau to perform this step live, in real-time during personalisation
- Pre-enablement. Having the chips enabled and locked to the issuer/bureau prior to shipment from the MULTOS vendor

2. Application Data Preparation

A MULTOS application can be fully personalised prior to loading onto the target card/chip/device. That is a unique feature of MULTOS, but not the only way to manage applications. Application dataprep is supported by the major industry personalisation system software providers and is performed off-card, without holding up the perso system; including options to encrypt the application. This approach takes the 'secure packet' concept of getting a payment application to a device, rather than trying to rely on the inefficient 'secure channel' approach. This is also the most efficient way to manage provisioning of a payment application to the device already in the field (Instant issuance & post-issuance is all much easier to achieve with MULTOS).

3. Application Loading

This covers the very simple commands to load a MULTOS application during the personalisation stage (the application can be already personalised – by doing the dataprep component in the previous step– or it can be loaded blank). If you hate scripts and all the chopping and changing that is required to support other smartcard platforms, then MULTOS loading is the answer. But if you really love scripts and want to manage the ins-and-outs of CPS, then that is ***now an option***[1] with the range of new MULTOS devices that can support CPS methods of application data loading.

A note about Enablement

Enablement is best described as the activation of a MULTOS device, and not as onerous or inflexible as pre-personalisation. With Enablement, the need for HSMs, key custodians, key administration etc. is greatly reduced and therefore considerably minimising the risk of errors and wastage. The process cryptographically binds a card to an issuer and provides it with all the keys it requires making it ready to receive an application.

Other platforms require multiple keys and key exchanges to reach the same point, as well as multiple HSMs to ensure secure data communication.

[1]This is new, you may not have known this….but the newest MULTOS products can support CPS via an application plug-in

Technology Briefing - Continued

Real Time Enablement

Customers now have the choice of how to obtain the keys and certificates needed for loading each card; i) the traditional "batch mode" way using a central root of trust (the KMA) or with an in-house PC or ii) ***"Real Time Enablement[2]"*** by using an using an integrated HSM - giving radically improved (10x faster) throughput and optionally connected directly to the personalisation machines to generate the required data instantly, on demand, for just the cards being personalised.

A note about Scripting
Each new product or variation of other smartcard products often requires a new personalisation script, whereas MULTOS requires one basic standard personalisation script to be presented to the loading machine, irrespective of the application to be loaded and irrespective of the card/device manufacturer. MULTOS greatly increases the simplicity for the bureau, removing the need to manage expensive scripting changes and the risks associated with that.

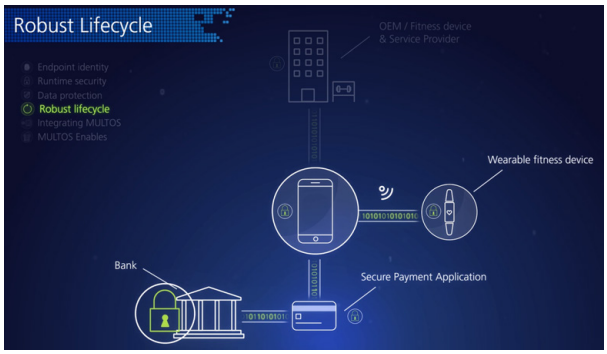
CPS and MULTOS - Common Personalisation

MULTOS has been doing a common personalisation method since it was devised some 20yrs ago. However, with all the various proprietary smartcard platforms and the multitude of JavaCard flavours, there was a need by the industry to develop a Common Perso Spec (CPS) for all those non-standard and non-interoperable devices. Unfortunately, there is a strong case in arguing that CPS is a misnomer with no real 'Common' part as such, since DGIs (Data Group Identifiers) are not common between applications, or even different implementations of the same application. That's why perso scripts are in constant need of updating, editing or developing on those perso systems inside the bureau. But with MULTOS, a single generic perso script is all you need regardless of application, supplier or profile setup. So MULTOS already achieves one part of what CPS is trying to achieve.

However, recognising that some perso system vendors are slow to develop MULTOS application support, some bureau operations prefer to work with the cumbersome CPS methods, or some provisioning systems are still stuck in the past with old secure channel methods, MULTOS products have expanded perso support and now offer bolt-on modules that can support CPS-style application personalisation; including the restrictions and complications that come along with any CPS product. Interestingly, these products are the only ones on the market that can support a choice of either CPS-style perso or the more efficient and faster MULTOS perso methods.

Provisioning Choice

We like to show off the provisioning flexibility of MULTOS technology, utilising the various security concepts built into the platform architecture and the options on how to package and send an application to the device. Here below is just one example of how to easily deploy a payment application, using a mobile phone as the communication/reader device to provision a wearable with the personalised (tokenised if required) payment app. Just like the basic motto of the MULTOS platform - **simple, fast, secure.**



Conclusion

As you can see, MULTOS products are able to cover the needs of every issuer and bureau with a comprehensive range of options not matched by any other product in the market.

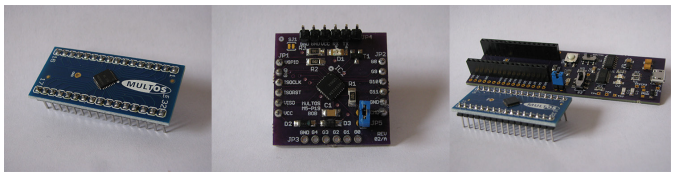
Tech Tip – MULTOS Trust Anchor Development Kit

The MULTOS Consortium will be launching a new development kit, based on an embedded version of MULTOS, during Q1 2018, aimed at making it easy to design-in MULTOS to secure a wide range of connected devices.

The kit will comprise three main components:-
i) A breakout board – the QFN32 packaged MULTOS chip is mounted on a 32 pin dual in-line board making it easy to use in breadboards for hardware development.

ii) An evaluation board – this board provides all the facilities needed to develop and load MULTOS applications. You simply plug in the breakout board, connect the evaluation board to your Windows PC (using the supplied micro-usb cable) and install the SDK. The evaluation board includes a 3.3V regulator for providing power via the USB connection or an external DC source, a push-switch, an LED, and headers for making external connections to the MULTOS chip (such as its smartcard pins, GPIO pins, serial ports, I2C interface etc).

iii) A "nano" board – this small board, about the size of a postage stamp, mounts the MULTOS chip and provides external connection points. Its purpose is to allow you to easily incorporate the MULTOS chip into existing bigger systems without having to design your own PCB. For example, it makes it very easy to house and connect a MULTOS chip within existing device cases like that of a Raspberry Pi.



[2]This is also new….in case you missed it, all MULTOS and MULTOS step-one products released since 2015 support live enablement at the point of personalisation, we call it "Real Time Enablement"

MULTOS Q&A

Question: Where can I find the keys needed for generating protected and confidential ALUs for live cards such as those supplied in the training kit (ML3-36K-R1)?

Answer: Four keys are needed. The Hash Modulus and TKCK public keys can be downloaded from the **StepXpress website**. For the training kit cards you need the file MC3-36K-R1.zip. The application signing key is generated and owned by entity doing the ALU generation, so that is either you or a trusted third party. The final key is the card's own public key which can be obtained from the card itself using MUtil (MKD_PKC button) or using the APDU 80100700C8.

Question: The command hterm -card is returning "Unknown card type". Why?

Answer: This happens if the card is enabled with live keys. hterm -card only recognises developer cards enabled with known test keys.

Digital Doodle

Prize Puzzle

Solution to last issue's puzzle:
The actor winning the Oscar is Tom Hanks (his name is hidden using the NATO phonetic alphabet). Congratulations to **Laurence Sterling** from Multos International who wins the US$100 prize.

This issue's puzzle:

George the gorilla has learned to communicate with the help of simple encoding machine. What is he trying to tell the zookeeper?

16/A/11/17/8/2
17/C/5/D 12/D
21/E/11/E/11/E/7.

Email your solution to dev.support@multos.com. Can anyone beat Laurence? The first correct answer **wins a US$100 Amazon voucher.**

Something to say? If you would like to contribute a short article or have a question you would like answered we'd like to hear from you. Please e-mail us on **info@multos.com.**