

« IoT Made Easy » Webinars

Solutions From Sensors to Cloud

- 4 Sessions with end to end System approach

Session 1 (14 Sept, 2pm CET)

« Power Efficient Solutions for your IoT Applications »

Keywords : Low Power, Analog, Mixed Signals, Power Management, MCU

Session 2 (15 Sept, 2pm CET)

« Connectivity Made Easy and Scalable for your IoT Application »

Keywords : Wireless and how to comply to Regulations & Certification, Chip down or module, Wired Solutions and Ethernet, Security and Robustness

Session 3 (16 Sept, 2pm CET)

« Security Matters... and How it is now so Easy »

Keywords : EN 303-645 from ETSI, Secure Element, Keys and how to protect them, Pre-provisioning, easy on-boarding, MOQ

Session 4 (17 Sept, 2pm CET)

« Scale your Business : from Easy Prototyping to Production »

Keywords : Software Development Framework, Applications drivers, Turnkey Solutions and Reference Designs, Github



- 6 Local Experts from Microchip Europe

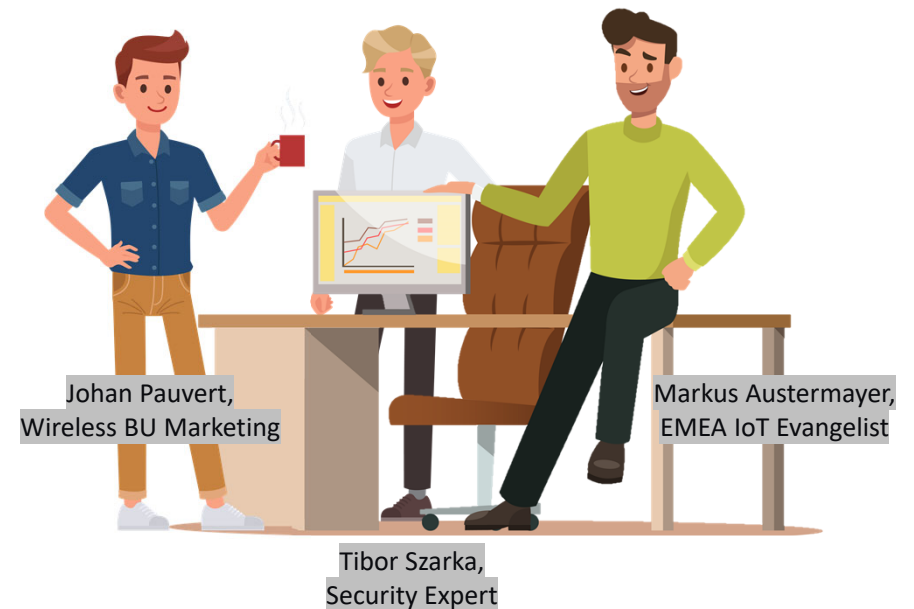


Johan (Connectivity) Tarek (MCU) Markus (IoT)
Miroslaw (Firmware) Tibor (Security) Thierry (Analog)

Contact details of our 6 experts will be available at the end of this presentation

IoT Made Easy – Session 3/4

Security Matters & How it is Now so Easy



Session 1 (14 Sept, 2pm CET) : « Power Efficient Solutions for your IoT Applications »
Session 2 (15 Sept, 2pm CET) : « Connectivity Made Easy and Scalable for your IoT Application »
Session 3 (16 Sept, 2pm CET) : « Security Matters... and How it is Now so Easy »
Session 4 (17 Sept, 2pm CET) : « Scale your Business : from Easy Prototyping to Fast Time to Market »

The Challenge We Will Resolve Today

How to Overcome Complexity of Security

- **How to build a secure Low Power IoT sensor?**
 - Regulations and requirements?
 - What threats and enemies are out there?
 - Are all IoT cloud providers using the same methodology?
 - How to deal with security software complexity?
 - What keys do I need? Unique keys per device?
 - Where can I store device keys? Are they safe?
 - Do I need a secure factory to produce a secured device?
 - How do I respect the low power budget I have?
- **Don't worry, we've got you covered with this session!**



Why Security for IoT?

Save Costs, Reduce Risk, Increase Revenue



Preserve brand quality



Safety, Liability and Regulation



Revenue stream protection



Enable service revenue streams

IoT Security – Main Challenges

Seen from YOUR perspective

- Very large attack surface and widespread deployment
- Security for safety (especially for critical sectors)
- Interoperability, increased connectivity & cascading effects
- Security & privacy (by design) not a top priority
- Lack of expertise
- Applying security updates
- Lack of secure development practices
- Fragmentation of good practices & standards
- Unclear liabilities



European Standard

EN 303 645 is NOW Published!



ETSI EN 303 645 V2.1.1 (2020-06)



CYBER;
Cyber Security for Consumer Internet of Things:
Baseline Requirements

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

The screenshot shows the ETSI website's news section. The main headline is "ETSI releases world-leading Consumer IoT Security standard". Below the headline is a navigation bar with links: "News and social wall", "News and Press Releases", "News", "Press Releases", "Magazine", "Blogs", and "Press contact". The article text begins with "ETSI RELEASES WORLD-LEADING CONSUMER IOT SECURITY STANDARD" and "Sophia Antipolis, 30 June 2020". The main body of the article states: "The ETSI Technical Committee on Cybersecurity (TC CYBER) today unveils ETSI EN 303 645, a standard for cybersecurity in the Internet of Things that establishes a security baseline for internet-connected consumer products and provides a basis for future IoT certification schemes. Based on the ETSI specification TS 103 645, EN 303 645 went through National Standards Organization comments and voting, engaging even more stakeholders in its development and ultimately strengthening the resulting standard. The EN is a result of collaboration and expertise from industry, academics and government." It continues: "As more devices in the home connect to the internet, the cybersecurity of the Internet of Things (IoT) has become a growing concern. The EN is designed to prevent large-scale, prevalent attacks against smart devices that cybersecurity experts see every day. Compliance with the standard will restrict the ability of attackers to control devices across the globe - known as botnets - to launch DDoS attacks, mine cryptocurrency and spy on users in their own homes. By preventing these attacks, the EN represents a huge uplift in baseline security and privacy." The article concludes with: "ETSI EN 303 645 specifies 13 provisions for the security of Internet-connected consumer devices and their associated services. IoT products in scope include connected children's toys and baby monitors, connected safety-relevant products such as smoke detectors and door locks, smart cameras, TVs and speakers, wearable health trackers, connected home automation and alarm systems, connected appliances (e.g. washing machines, fridges) and smart home assistants. The EN also includes 5 specific data protection provisions for consumer IoT."

<https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard#:~:text=The%20ETSI%20Technical%20Committee%20on,for%20future%20IoT%20certification%20schemes.>



Other Regulations and Specifications Available for Different Market Segments

Organizations | Students | About ISA | Feedback
Phone: (919) 549-8411

MEMBERSHIP TRAINING & CERTIFICATIONS STANDARDS & PUBLICATIONS CONFERENCES & EVENTS NEWS & PRESS RELEASES RESOURCES TECHNICAL TOPICS

Product Details

ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels

Item Details:
This part of the ISA-62443 series provides detailed technical control system requirements (SRS) associated with the security...

www.isa.org

www.iotsecurityfoundation.org/tag/iot-security-compliance-framework/

IoT Security Compliance Framework
Release 2 December 2018

PUBLICATIONS

NISTIR 8259A

IoT Device Cybersecurity Capability Core Baseline

Date Published: May 2020

Planning Note (7/14/2020):

NIST is developing a **federal profile of the Core Baseline** established in NISTIR 8259A ("Federal Profile") and *seeks feedback from all stakeholders* on this initial catalog of proposed IoT device cybersecurity capabilities and related non-technical capabilities. [Learn more in the FAQ.](#)

See the latest developments from the [NIST Cybersecurity for IoT Program](#).

<https://csrc.nist.gov/publications/detail/nistir/8259a/final>

UL 2900: A Cybersecurity aid for industry and regulators

A baseline of cybersecurity hygiene

UL 2900 establishes that manufacturers have characterized and documented the technologies used in their products that could constitute an "attack surface". It requires threat modeling based on intended use and relative exposure. The standard demonstrates the effective implementation of security controls protecting both sensitive data (e.g. PII, PHI) and also other assets such as command and control data. It provides objective evidence that software weaknesses, and vulnerabilities have been appropriately dispositioned and further verified via penetration testing and promotes defensive design (e.g. defense-in-depth, partitioning, etc).

UL 2900 generally helps ensure system robustness (e.g. fuzz testing / malformed input testing):

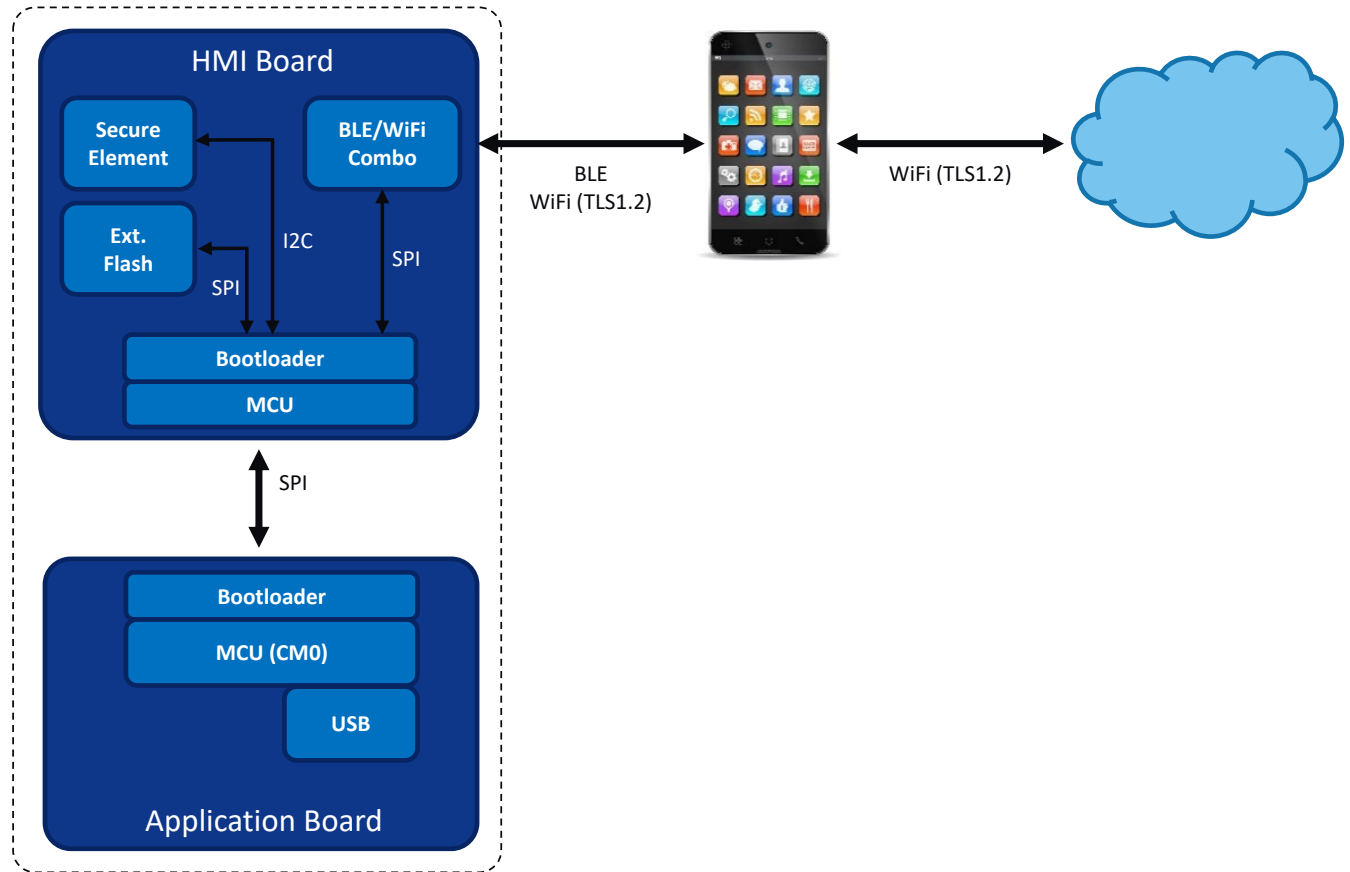
- Monitoring for security events
- Logging of security events
- Managing security logs
- Updating software to address safety, essential performance, and security issues
- Handling failures in the software update process (e.g. roll-back)
- Component purchasing controls
- Management of sensitive data
- Remote product management
- Decommissioning (e.g. purging of PII / PHI)

www.ul.com/offerings/cybersecurity-assurance-and-compliance



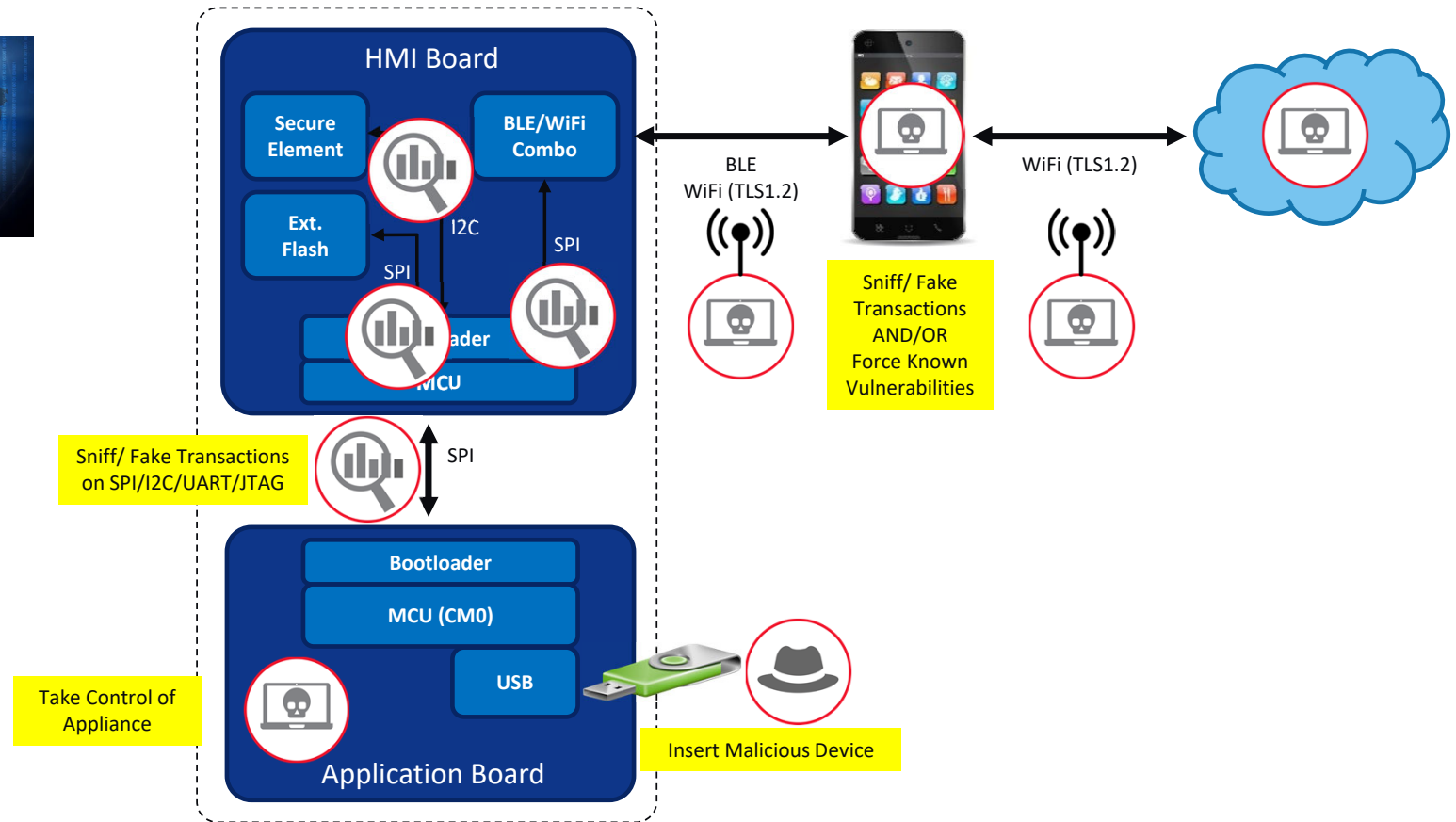
Real Life Use Case in Europe

Appliance with Multiple Boards & Connectivities



Real Life Use Case in Europe

Appliance with Multiple Boards & Connectivities



Real Life Use Case in Europe

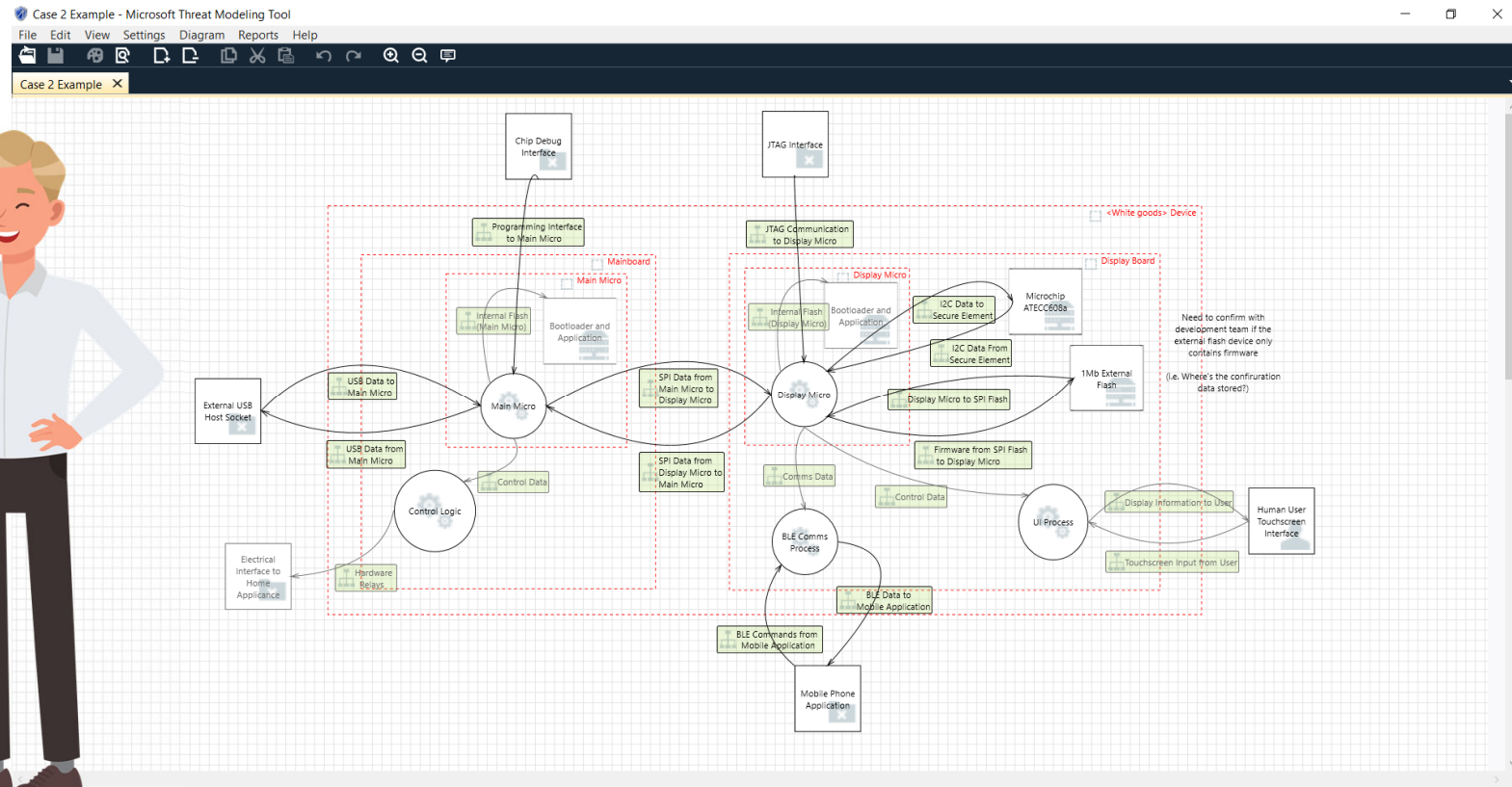
Appliance with Multiple Boards & Connectivities



Microchip has the expertise, tools and products to make my application fully secure



Microchip's Security Expert



Importance of Keys in Security

Security: It's All About The Key

- **“A cryptosystem should be secure if everything about the system – except the key – is public knowledge”**
 - Kerckhoff's Principle



What a private key really looks like:

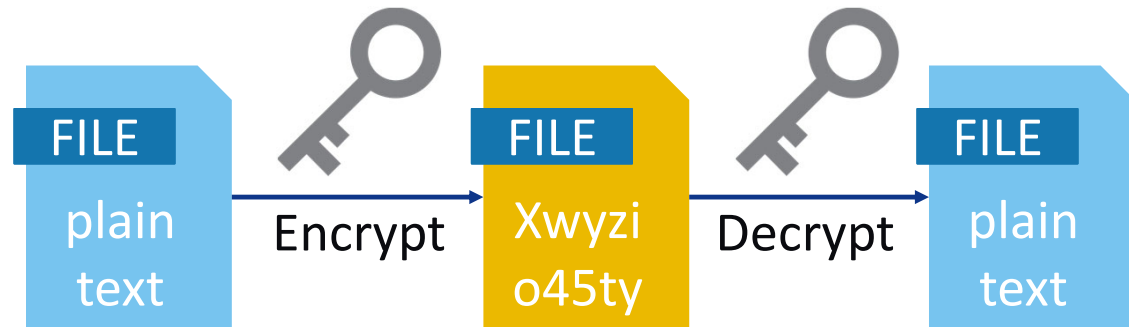
JVFDvdfvJvfdnjvjk543524cds9ics9cCDSCcs0dcw8eidpciswsn8934XSCDS

- **“The enemy knows the system”**
 - Claude Shannon
- **Why are the Keys important ?**
 - With the possession of the key, critical transactions can be impersonated



How to Look at Security

Don't Forget the Key!



- **FW/SW engineers (often the lead architects) focus on algorithms (the maths) forgetting the importance of keys (the secret)**
- **“I encrypted data with the key, so I am secure ... ”**
 - Yes but you need a key to encrypt
 - Is this key protected ?
- **Ok, I recognise the need to secure the key
But how do I implement that ?**

Security Solutions from Microchip

Full Portfolio of Secure Solutions for IoT

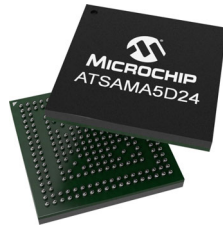
Hardware

Microcontrollers 32/16/8-bit



www.microchip.com/mcu

Microprocessors



www.microchip.com/mpu

Secure Elements Common Criteria (JIL) Rated HIGH



www.microchip.com/security

Wired & Wireless Solutions



www.microchip.com/wireless
www.microchip.com/ethernet

FPGA



www.microchip.com/fpgas-and-plds

Join Session 4 to learn how we make all of this super easy for you



Tarek, MCU BU Marketing and IoT Expert

Firmware



www.microchip.com/aws



www.microchip.com/azure



Google Cloud Platform
www.microchip.com/gcp



www.microchip.com/TrustGOLoRa



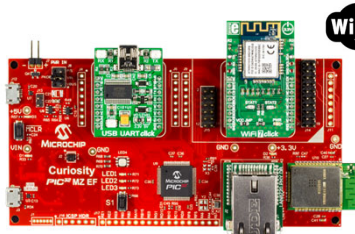
www.microchip.com/iot

Security Solutions from Microchip

A few Examples...

IoT Gateway

- Get started Now with DM320104-BNDL Board
www.microchip.com/DM320104-BNDL



Winc1500 Wifi Controller
www.microchip.com/winc1500

LAN8720A Ethernet PHY
www.microchip.com/lan8720a

PIC32MZ EF 32-bit MCU
www.microchip.com/pic32mzef

AWS IoT Cloud Authentication

- Get started Now with 32-bit MCU Wifi, embedding Trust&Go and enhanced security including WPA3

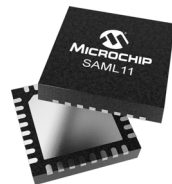


32-bit MCU Wifi with Trust&Go
Secure Element
www.microchip.com/wifi

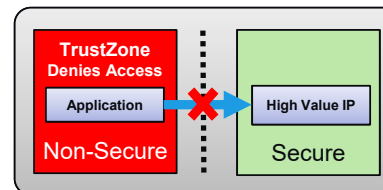
Ksz8091 Ethernet PHY
www.microchip.com/ksz8091

IP Protection & anti-cloning

- Get started Now with SAML11 family and Chip-Level Security plus arm® TrustZone® Technology



ATSAML11 32-bit MCU
www.microchip.com/saml11



Microchip's Unique Value Proposition

Provisioning IoT Devices...

- **Who generates the identity for your IoT product ?**

How can I keep the flexibility for the selection of the EMS and still guarantee that my product is secure ?



Think out of the box, my friend Johan : simply go with Microchip pre-provisioned devices!
Check Session 2 for 2 great examples, smart connected and secure.



www.microchip.com/sam-r34-r35



www.microchip.com/wifi

- **Provisioned devices are easier to use and...**

- More efficient: You save money from an efficient production flow
- Minimize risk: You control overbuilds
- More secure: Your IoT product enjoys a world class level of embedded security

Microchip Unique Value Proposition

Provisioning IoT Devices : The Solution - Trust Platform



Pre-configured		YES	YES	NO
Pre-provisioned		YES	YES (flexible)	NO
MOQ	Low MOQ flow	10 units	2 000 units	4 000 units
	High Volume flow*	30 000 units	30 000 units	30 000 units
Development time		Lowest	Lower	Custom
Complexity		Lowest	Lower	Custom
Secure key Storage		JIL High	JIL High	JIL High
Devices		ATECC608	ATECC608 ATSHA204A (w/o RBH) – Q4/2020	ATECC608 ATSHA204A (w/o RBH) – Q3/2020

1

3

2

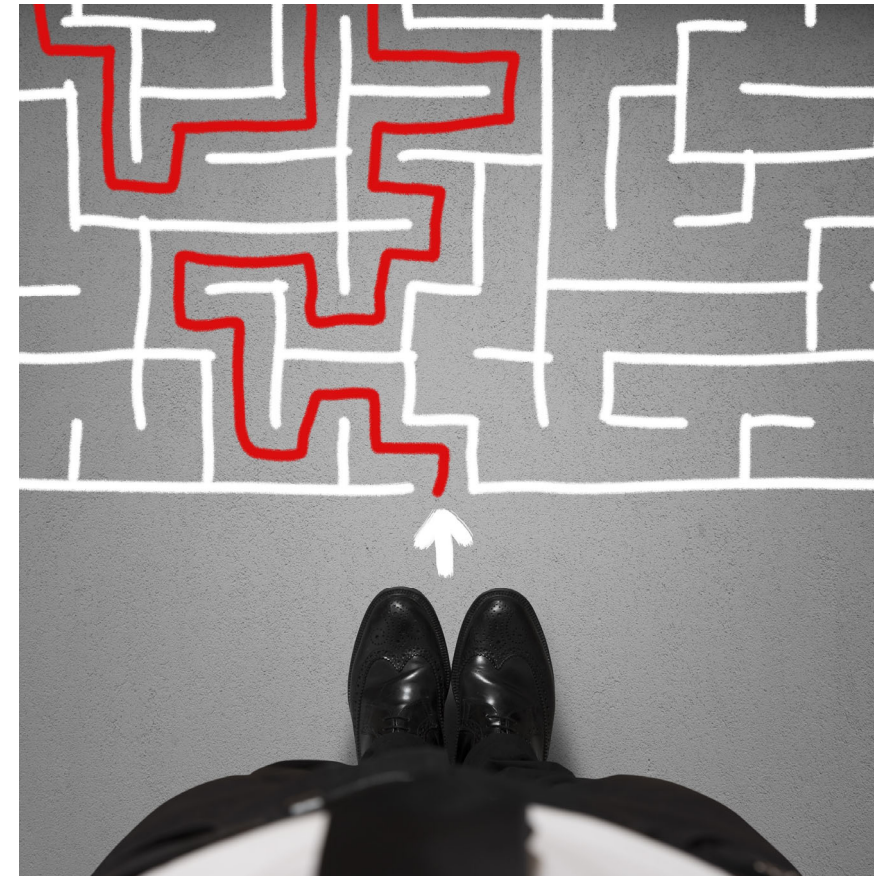
* MOQ depending on Package / Silicon – showing here the lowest MOQ through the whole product portfolio – **Minimum Annual Business of 100ku**

What about Power Efficiency ?

How to Optimize Power Consumption for my Device ?



- **Use Elliptic Curve Cryptography (ECC)**
 - Smaller key size than RSA for the same security bit level
- **Crypto-Hardware acceleration reduce code size**
- **Use crypto-companion to off load main MCU**
 - Reduce firmware validation time during boot and updates
 - Reduce TLS communication setup time
 - Dedicate your MCU core to the application logic
- **Crypto-Hardware acceleration save time and power!**



What about Power Efficiency ?

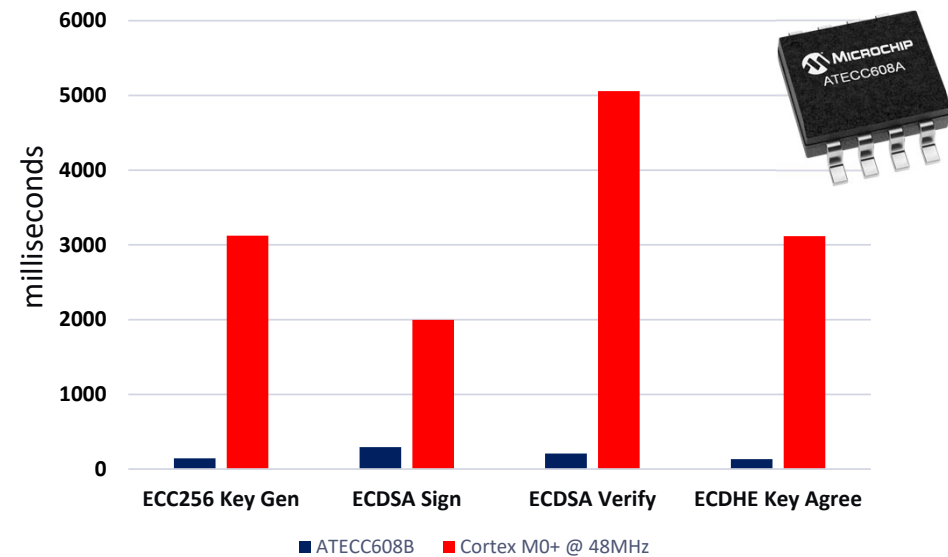
Efficiency Proven !



	Cortex M0+ 32-bit MCU @48MHz	Cortex M0+ 32-bit MCU @48MHz plus ATECC608B Secure Element
TLS connection setup time [ms]	3000 - 5000	less than 500
Firmware signature validation [ms]	5000	210

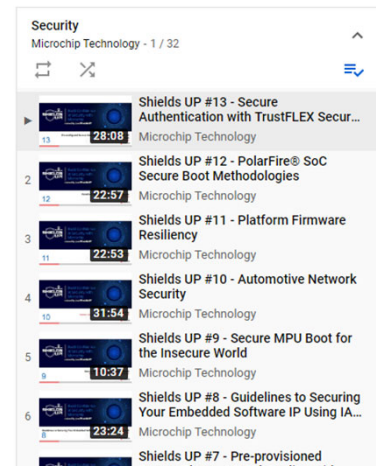
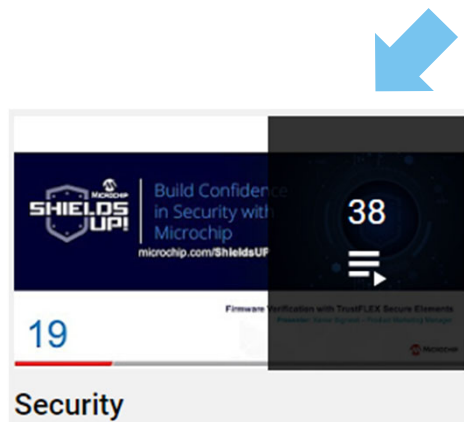
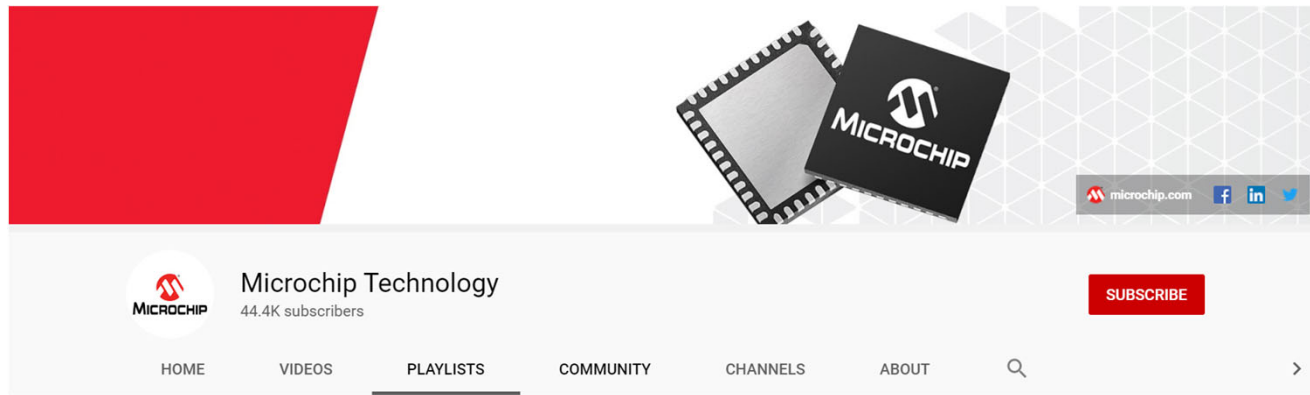
- Spend less resources and power to build secure system
- Sleep current down to 30nA!
- “2 Chip Hardened Solutions” from Slide 14 is then not only more secure but is also more power efficient and offers greater performance

Idle Power Supply Current	I _{IDLE}	—	800	—	μA	When device is in idle mode, V _{SDA} and V _{SCL} < 0.4V or > V _{CC} - 0.4
Sleep Current	I _{SLEEP}	—	30	150	nA	When device is in sleep mode, V _{CC} ≤ 3.6V, V _{SDA} and V _{SCL} < 0.4V or > V _{CC} - 0.4, T _A ≤ 55°C
		—	—	2	μA	When device is in sleep mode. Over full V _{CC} and temperature range.



For the Curious Ones... and Geeks Like Me

Microchip YouTube Channel



Firmware Verification with TrustFLEX Secure Elements

Presenter: Xavier Bignalet – Product Marketing Manager



Conclusion

Security is Complex... but Microchip has the Solutions made Easy for you

- Security has a real value for all stakeholders, including for your end customers
- You must act NOW, as IoT regulation is NOW in place in Europe
- Microchip offers a comprehensive variety of solutions for IoT Security. With full System Approach
- Security does not conflict with Power Efficiency
- Last but not least, our Microchip Security Experts are available to support you. And we are Local !



Do You Want To Become An IoT Expert?

We've got you covered !

- **Design Check : Online Design Review Services**

- Wireless, Ethernet LAN, PoE, MPU...
- www.microchip.com/design-check-services



- **Microchip IoT Landing Page**

- www.microchip.com/iot



- **Github**

- <https://github.com/MicrochipTech>



- **Microchip YouTube Channel**

- www.youtube.com/user/MicrochipTechnology

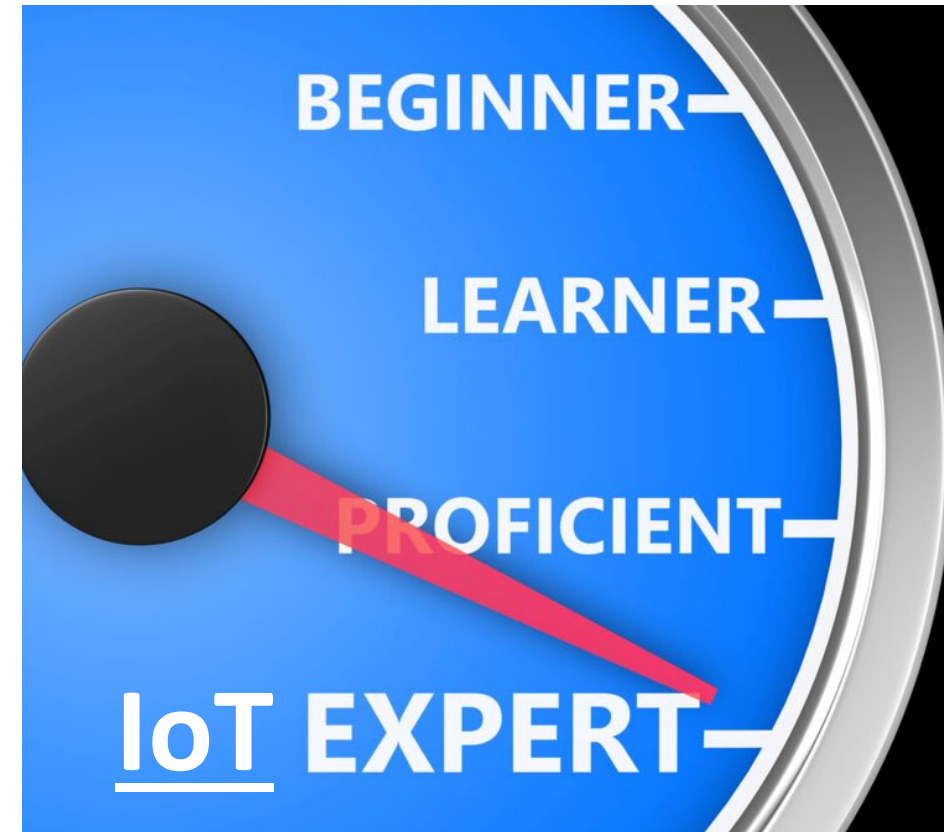


- **Design Partner:**

- <https://get.microchipdirect.com/design-partner-ecosystem/>



- **And your friendly and Local Microchip team !**



Let's Go For Q&A

Ask our Experts Now !



Johan Pauvert

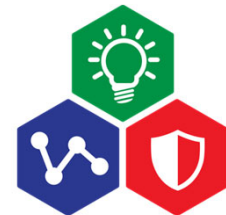
Wireless BU Marketing and IoT Geek
johan.pauvert@microchip.com
www.microchip.com/wireless
www.microchip.com/ethernet

Markus Austermayer

EMEA IoT Evangelist
markus.austermayer@microchip.com
www.microchip.com/iot

Tibor Szarka

Embedded Solutions Engineer in Security
tibor.szarka@microchip.com
www.microchip.com/security



SMART | CONNECTED | SECURE

Join Us Tomorrow for Our Next Webinar

Our Technical Experts Are Here For You



Markus Austermayer (Germany)

EMEA IoT Evangelist and your host for these 4 sessions

markus.austermayer@microchip.com

www.microchip.com/iot



Tibor Szarka (Slovak Republic)

Embedded Solutions Engineer and Expert in Security

tibor.szarka@microchip.com

www.microchip.com/security



Johan Pauvert (France)

Wireless BU Marketing and IoT Geek

johan.pauvert@microchip.com

www.microchip.com/wireless

www.microchip.com/ethernet



Thierry Riffart (France)

EMEA Analog Expert

thierry.riffart@microchip.com

www.microchip.com/analog



Miroslaw Dybizbanski (Poland)

Embedded Solutions Engineer and Low Power Expert

miroslaw.dybizbanski@microchip.com

www.microchip.com/iot



Tarek Alchaer (Slovak Republic)

MCU BU Marketing and IoT Expert

johan.pauvert@microchip.com

www.microchip.com/mcu