Security & Connectivity in the Future of the Internet of Things

By Guillaume Crinon

Table of contents

ABOUT THE AUTHOR

Guillaume Crinon is the Global IoT Strategy Manager at Avnet, responsible for security and connectivity solutions. He has more than 20 years of experience in the semiconductor industry, mostly in radio-frequency circuit design, but also has extensive experience in metering, building/home automation and security systems. He joined Avnet in 2011. Guillaume graduated from SUPELEC in Paris (MSc in EE) and has co-authored 12 international patents in wireless systems, IC architectures and design to date.

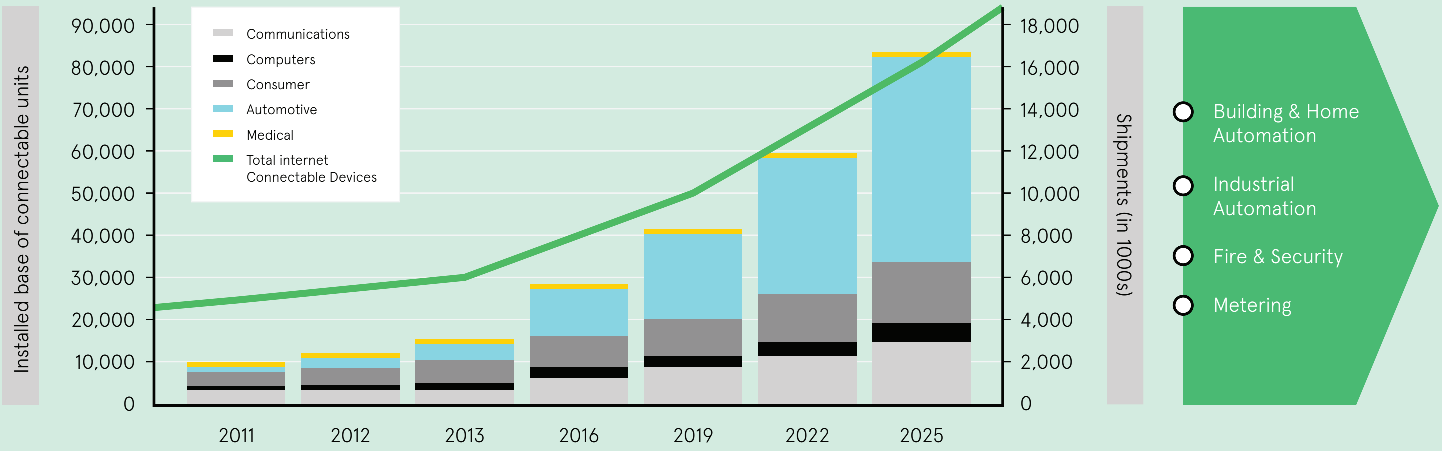
The future of IoT security & connectivity

THE INTERNET OF THINGS IS HERE. ARE YOU READY (AND SECURE)?

Ten years from now, it will be hard for us to remember a world where everything wasn't connected to the internet in a way or another. Even today, we don't really care to know which technology will be used; things will be simply either connected or will be a problem (and your kids, customers or business partners will chase you until you get everything connected back).

THIS IS WHAT YOU HAVE TO BALANCE WITH THE BIG BUSINESS OPPORTUNITY AROUND IoT.

Gartner says worldwide IoT security spending will reach $1.5 billion this year. That's no surprise, considering the global IoT market should be $3.9 trillion dollars by 2021, led by discrete manufacturing, transportation, logistics and utilities.



However, there is no one-size-fits-all technology to accomplish IoT security. A custom solution IoT also presents a number of big security challenges—all on faster timelines and with more data breaches than ever.

This is probably why a recent survey found that only 40% of service providers said they were preparing for a breach within the next two years. That means 6 out of every 10 providers aren't really preparing for a crack in the system. That same number, 40%, of IoT specialists, however, assume their service provider will never have a security breach.

Either we've got a big challenge, a big opportunity, or—as we'll argue, both. Plus, trillions in economic value.

TOTAL SPENDING ON ENDPOINTS & SERVICES WILL REACH

$3.9T IN 2021

-Gartner, Forecast: Internet of Things — Endpoints and Associated Services, Worldwide, 2017, 21 December 2017

$3.9-$11T

POTENTIAL ANNUAL IMPACT BY 2025
-McKinsey & Company

IoT starts with data. But setting up the right infrastructure to collect that data may require a myriad of specialists. How do you secure or update a non-standard device? Avoid wireless interference? Regulate sensors to control connectivity fees?

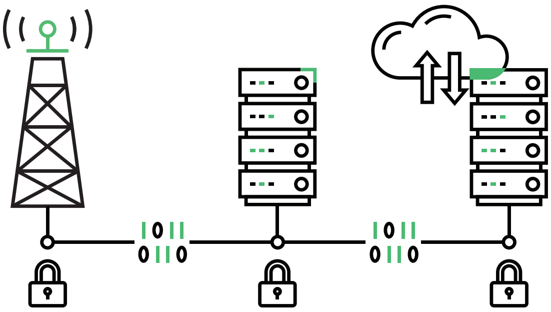
That leads right into the connection: it could be public cellular, which involves data plans and extra taxes on your network, or it could be your own private infrastructure, which you'll need to maintain to keep connections running 24/7. It could even be a hybrid managed private network involving servicing fees as well. Bottom line: internet connectivity never comes for free, but it is a necessary evil.

All that is just for collecting the data.
Then you've got to aggregate, store and analyze it.

But deploying an IoT solution isn't like putting a product on a shelf. It needs regular maintenance and security updates as good IoT solutions can flex with business needs and security challenges. A safe protocol today might get hacked tomorrow. A field of sensors could be compromised or marked end of life six months after you deploy them globally. You need to be ready to act right away with an update plan and a clear understanding of exactly which vendor is responsible for doing it.

FEELING SECURE ABOUT YOUR IOT SECURITY YET?

Above, we've posed a lot of questions. Now, we'll walk you through how to get the answers.



THE RIGHT INFRASTRUCTURE FOR YOUR BUSINESS

Public Cellular Data
Involves data plans and extra taxes on your network

Private Infrastructure
Requires maintenance to keep connections running 24/7

Private Network
Hybrid managed networks incur service fees as well

Custom comes with a competitive edge–and security challenge

We talked about this before: there's no one-size-fits-all IoT solution because every industry, vertical and business is different.

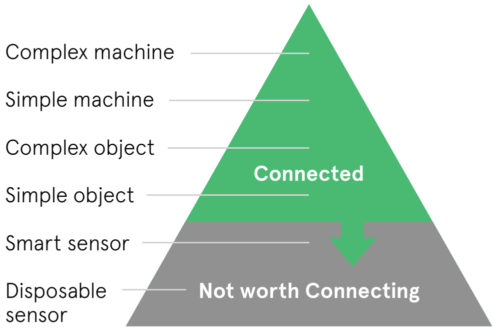
Whether you have an in-house team or are exporting the building of infrastructure to a trusted partner, make sure the team is asking the right questions when it comes to implementing and deploying IoT solutions.

Ask yourself questions like: What does it need to return in order to afford its cost? What's possible in the roadmap? What do you have that's ready for an IoT deployment in-house? Then lay over each connection possibility and security protocol.

There is no one-size-fits-all technology to connect objects, machines, sensors, devices and appliances to the internet. In an ideal world we would empower every single sensor with unlimited energy and unlimited wireless broadband IPv6 access to the internet.

However, in the real world, wireless connectivity has a cost in terms of radio spectrum, energy and hardware. This cost needs to be weighed in the financial equation of the application and service being deployed, where total cost of ownership (TCO) and return on investment (ROI) dictate.

Much like connecting people was once a luxury for the rich that's now become a mature business across a number of verticals, connecting things will soon move from luxury to necessity as the expanding market pushes down the cost of IoT deployments.



TOTAL COST OF OWNERSHIP OF THE CONNECTED "THING"

DEPENDING ON COST AND POWER CONSTRAINTS ON A CASE-BY-CASE BASIS, ONLY A SELECTION OF CONNECTIVITY TECHNOLOGIES MAY APPLY:

- **Low-cost body accessories** can count on a close-by Bluetooth-capable smartphone to play the role of the internet gateway. That way, these devices can run on small button-cell batteries for months or years.
- **Mains-powered home automation devices and machines** such as kitchen appliances, voice assistants and heaters can count on the home WiFi network bridging to a DSL or fiber box.
- **Battery-powered home appliances** such as smoke detectors, thermostats and pet trackers will require the deployment of a low-power local area network based upon Zigbee, Thread, LoRaWAN or a proprietary protocol.
- **Always-on vending machines or display panels** can afford 2G/3G/4G cellular connectivity.
- **Battery-powered smart meters or environmental sensors** may take advantage of a cellular LPWAN like SIGFOX, public LoRaWAN and Cat-NB1 (NB-IoT) when available.
- For **industrial assets sitting in very complex radio environments** where cellular coverage is harsh, such as factories, you will need to install a self-managed or external vendor-managed NaaS (N-as-a-Service) LoRaWAN network that is able to extract signals from behind thick reinforced concrete walls and floors.

Your solution's point person should then perform a readiness assessment, evaluating cost, value, ROI and even a pilot test to get the right buy-in.

An in-house build allows for an IoT solution that's fully customized to your use case. Need a specific protocol to help your sensors pick up information, communicate it to the cloud and then deliver it to a custom app adapted for iOS and Android? An-in house build from an in-house team is in lock step with your internal business goals, customizing your build accordingly.

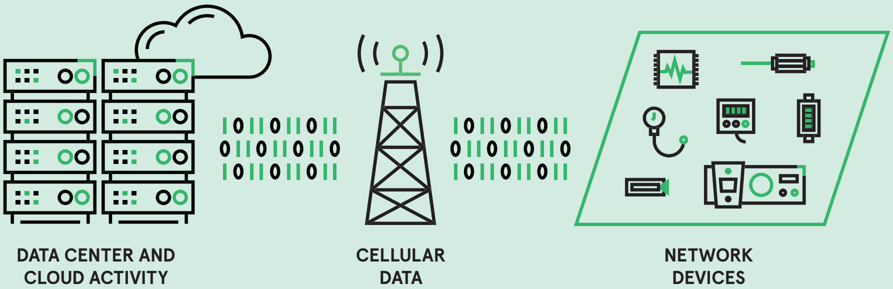
However, collective knowledge from a global network means someone in some corner of the world is keeping up with IoT deployments and solutions from competitors in your industry and innovative companies in others. This built-in competitive intelligence can help them vet your business case with an objective eye, run diagnostics to prove ROI early to top executives, recommend the best solutions during the development phase and ensure security and maintenance not only with an on-site deployment but also a lifecycle management engagement.

Either way, it's true that a fully customized in-house solution isn't vetted for quality and assurance the way something tried and true is. Check the validation of your assumptions in order to ensure customization doesn't leave you vulnerable to IoT security challenges you have yet to consider.

Connectivity and security and communications—oh my!

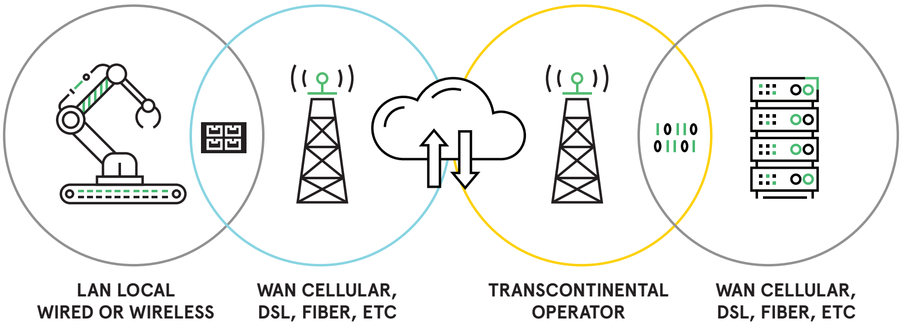
Once you get to actual development, you'll find that currently, in most cases, these devices never talk to one another.

M2M is a misleading acronym. For scalability reasons, in most commonly deploying IoT architectures, machines, appliances, devices, sensors do not directly talk to one another but report and pull data to and from more or less distant larger systems capable of analyzing and making decisions. This happens either on the edge of the cloud or in the cloud itself.



It is absolutely impossible to anticipate which route, network and backhaul will carry the data. We only know it will be multiple legs operated by as many providers with no guarantee of persistence: network routes are dynamic and the route from point A to point B can be different every day.

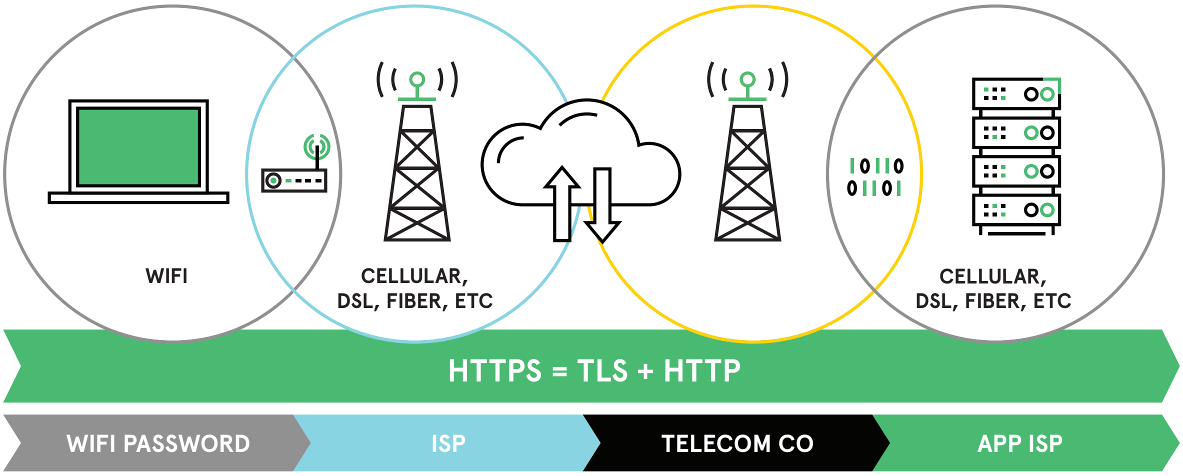
TYPICAL CONNECTION OF IoT DEVICE - IT IS A MULTI-NETWORK EFFORT



LAN LOCAL WIRED OR WIRELESS
WAN CELLULAR, DSL, FIBER, ETC
TRANSCONTINENTAL OPERATOR
WAN CELLULAR, DSL, FIBER, ETC

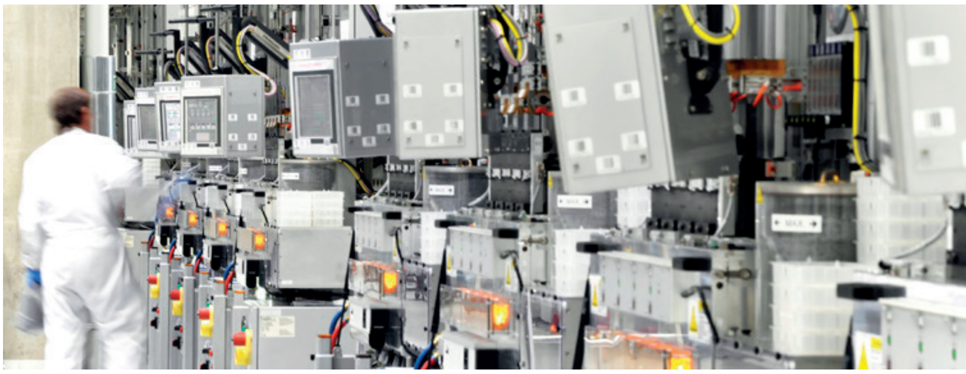
As a consequence, network security is insufficient as it only takes care of securing traffic on a leg-by-leg basis. As internet users, we know this very well: when accessing the web from public WiFi, our web browsers make sure we have an HTTPS/FTTPS connection to the URL we are visiting. Otherwise, we get a red flag in our URL bar.

WHEN USING THE INTERNET FROM YOUR COMPUTER/TABLET/SMARTPHONE, DO YOU HTTP ANYMORE?

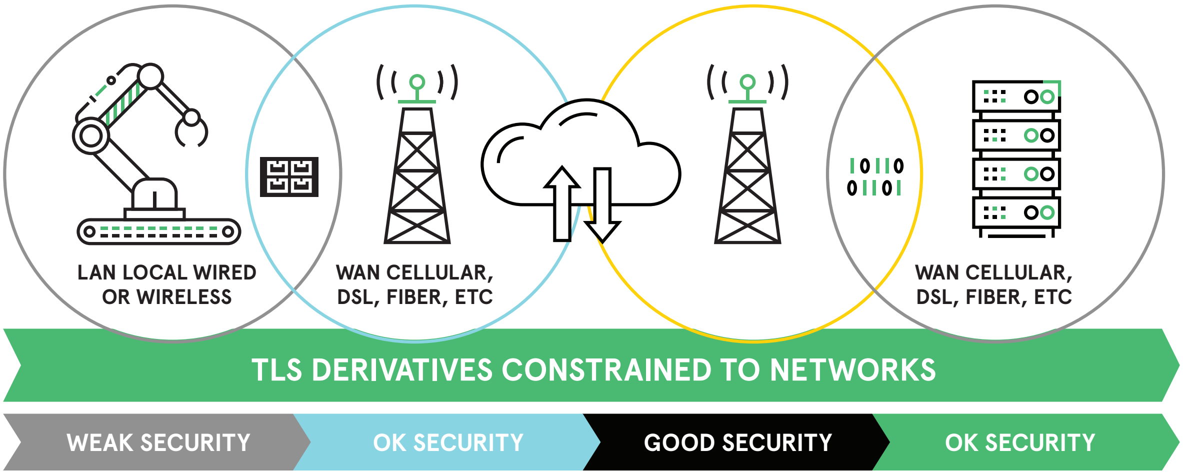


Exactly like HTTPS, we need an extra layer of end-to-end security between the connected device and the data repository above every network security so that we do not have to care and trust which network is carrying what.

Transport Layer Security (TLS) and derivatives are the best protocols to achieve this—it can be applied to HTTP, FTTP, MQTT and turns them into HTTPS, FTTPS, and MQTTS respectively, exactly what we need in the complicated security world of IoT.



CONNECTING MACHINES SHOULD NOT BE DIFFERENT. REMEMBER: EVERYTHING IS A COMPUTER.


LAN LOCAL WIRED OR WIRELESS
WAN CELLULAR, DSL, FIBER, ETC
WAN CELLULAR, DSL, FIBER, ETC
TLS DERIVATIVES CONSTRAINED TO NETWORKS
WEAK SECURITY
OK SECURITY
GOOD SECURITY
OK SECURITY

HOW DOES END-TO-END IoT SECURITY WORK? BY ENSURING THESE THREE FUNCTIONS THROUGHOUT THE PROCESS:

- **Mutual authentication:** devices and servers should and can prove true and unique identities to each other
- **Message integrity:** messages sent between devices and servers should be able to be sent safely so that they can't be hacked, altered or changed by an interfering party
- **Message confidentiality:** messages should also be able to be coded so only parties authorized to receive them can read what they say—a main center of data privacy

Since we want to automate communications and operations of these connected devices, we want to get rid of human interactions to get closer and closer to proactivity.

Take for example safe web surfing. When browsing the web with a tablet, a user needs to make sure the website that's being visited is authenticated to ensure there's no phishing. This is done automatically by HTTPS: my web browser is capable of authenticating the web site it wants to download content from by checking the validity of an ID document called a certificate presented by the web site to my web browser. If this certificate has been issued to the web site by an authority also trusted by my web browser, the light will turn green and my web browser will confidently connect. This is a one-way authentication process.

Because there is always a human being on the browser side, the web service will focus on authenticating this human being to complete the 2-way authentication process. This is commonly done with passwords, side-channel SMS, email validation, PIN codes, etc.

Connected objects need a simpler and automated way to mutually authenticate to their distant server the way that humans do—and faster than ever in a world where everything is connected and end users want access to information at the drop of a hat. One-way authentication (via the device authentication of destination server) is insufficient. Two-way authentication is mandatory: the server should also be capable of authenticating devices that request connection in an automated way. Public key infrastructure based on certificates with secure provisioning into both secure elements as well as secure processors in the factory and destination servers is the only working and widely recognized solution.

IoT security summed up into one word: identity

In the world of IoT, security really comes down to identity.

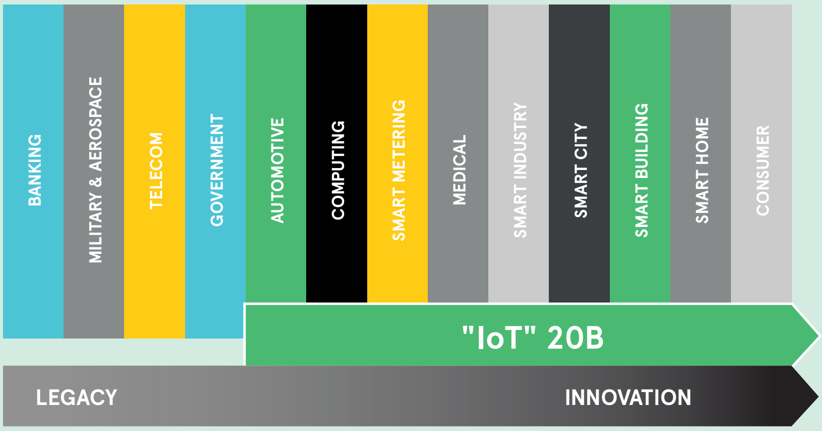
We, as people, trust communication with other people or machines we don’t know by verifying the institution with which someone or something is aligned.

Say a citizen of Spain wants to travel to the United States. Because the U.S. trusts that EU-member Spain can issue reliable passports, the U.S. customs agent would simply trust a valid passport, authenticate it and confirm it matches the traveler—rather than calling Spain’s embassy.

In the IoT, machines are doing the communication but the same concept applies.

If each has a unique trusted identity and appropriate documents proving that identity, they can exchange information as safely as humans do.

WHERE IoT IDENTITY MATTERS



We are giving every single device and server it is connecting into a “passport” in the form of a certificate. This identity measure is signed by an authority (the Certificate Authority, or CA) trusted by both sides so that they can recognize and securely authenticate one another within the circle of trust (the Public Key Infrastructure, or PKI). Within this PKI, a protocol like TLS can automatically open and maintain a secure end-to-end channel between the device and the server.

In Intranet-of-Things schemes, like early industrial deployments of connected sensors and machines inside the same company, this identity can be in the form of a custom file format. In full-out IoT deployments with devices crossing boundaries between applications, companies and services, this identity needs to be standardized.

At Avnet, we recommend adopting the X.509 certificate document format for this purpose. Whether the IP communication is handled by TLS or a non-IP Bluetooth, Zigbee or other system, X.509 is the de facto standard adopted by PKIs, IT and the IoT platforms these devices ultimately connect into.

It's not just an element—it's a whole, upgradeable security stack

In fact, trusted service providers have a key role for your deployment in terms of lifecycle management via an entire security stack, including:

- Certificate issuance services equivalent to passport issuance
- Certificate registration services equivalent to maintaining a social security database for instance
- Certificate administration services such as on-demand validity check, revocation, renewal, equivalent to what banking systems do in the background every time we pay with a credit card
- Key management services like distributing secret keys in an appropriate way to distant factories, devices in the field equivalent to sending Visa or phone SIM PIN codes in a mail to an end-user

Here's the key: for a secure solution, you need a secure stack. What's more, the whole stack holds together if and only if the device MCU or processor runs authorized software and firmware.

VISA/MASTERCARD

CELL PHONE 2G/3G/4G

HTTPS://

eSECURITY IN YOUR EVERYDAY LIFE

This can only be accomplished by a secure boot process during which the software and firmware integrity and origin is checked before execution. We also need to provide tools for our devices to upgrade remotely.

There is no such thing as software-based security alone. In everything we do, the root of trust requires hardened silicon to best resist to attacks of all sorts. This is where the hardened silicon comes in with secure elements and processors.

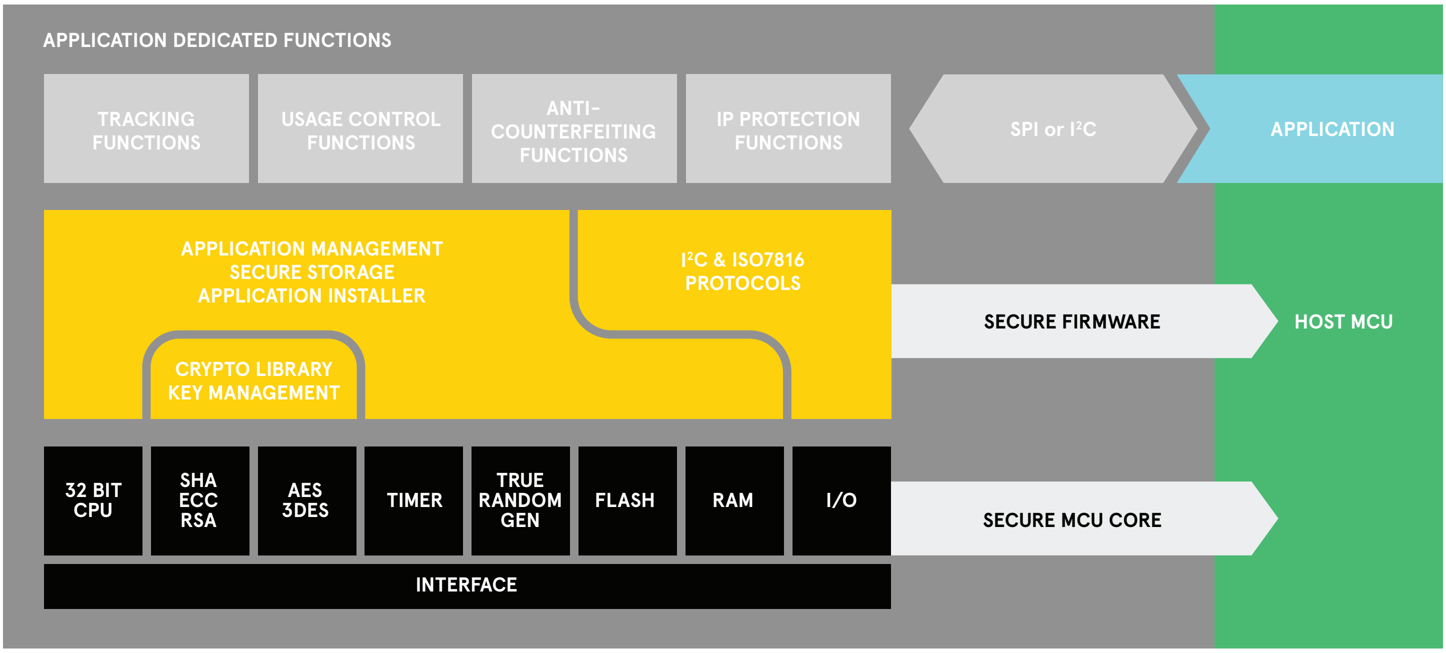
Secure elements are tiny components connecting as peripherals to host MCUs/MPUs. Secure processors are MCUs or MPUs embedding a secure element function serving as a hardware root of trust to a secure boot engine and embedded crypto functions. Most advanced designs take advantage of multicores to implement compartmentalization between a small trusted computing base and different layers of stacks up to application containers, as well as a memory management unit (MMU) arbitrating access to certain memory areas based on rules which cannot be violated, hardware firewalls to prevent exploiting a faulty implementation of an Ethernet stack for instance to hack a strategic negotiation of TLS.

This hardware then features:

- Personalized certificates and corresponding secret private keys
- Secure hosting of secret keys
- Handling of cryptography primitives running all necessary functions using these secret keys for the stacks calling them: key derivation and renewal, signature, verification, encryption, decryption of messages and firmware, etc.
- State-of-the-art security certification by standard bodies like Common Criteria (CC) or EMVco (Mastercard Visa)
- Some may handle a complete TLS stack, support mechanisms for a secure boot, the capability to cipher and decipher at a high data rate, fast memory encryption and decryption, etc.

They function in IoT connected devices the way a chip on your banking card, the SIM card in your cellphone or the trusted platform module in your computer's motherboard do, keeping your secret credentials safely and able to prove their identity when asked.

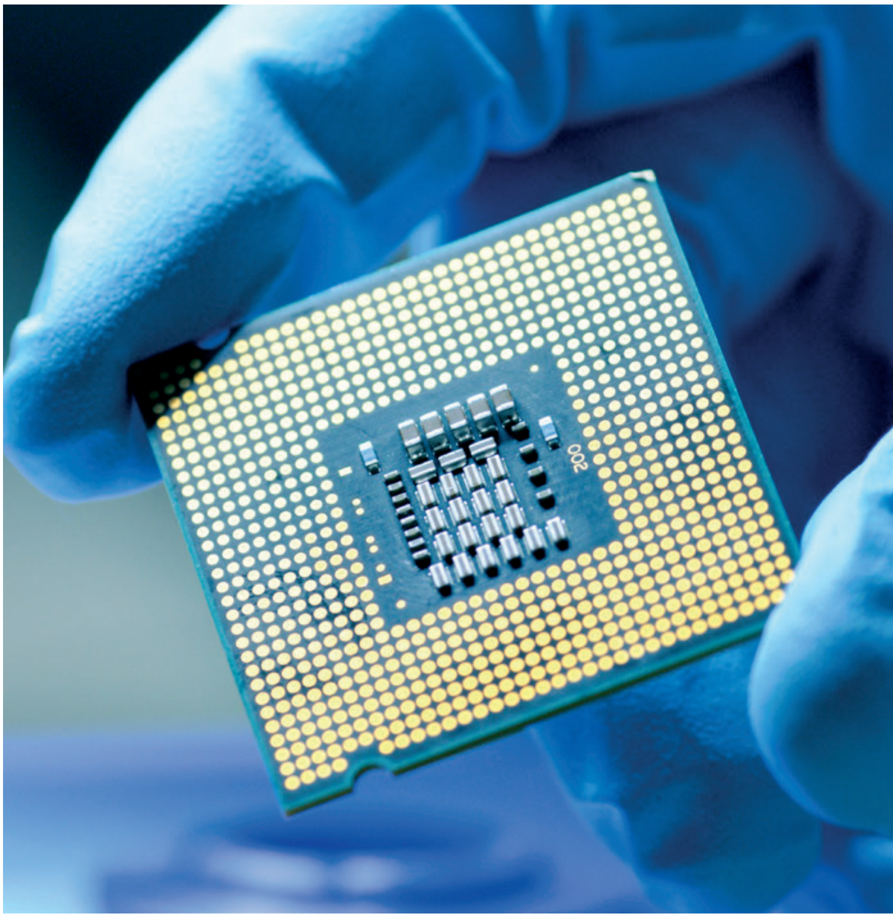
CUSTOMIZED AND PERSONALIZED WITH UNIQUE IDs AND KEYS / CERTIFICATES FOR THE CUSTOMER



Some processors and MCUs also embed a security core able to play the root of trust for the various functions supported by the chip itself. The first feature they offer is often a secure boot process during which the integrity and signature of the firmware is checked every time the processor resets. Hardware memory management prevents from writing and erasing inside the program memory for all other processes.

A security supervisor will watch for any abnormal behavior of the CPU, such as brutal temperature drops useful to freeze and dump a RAM, stack overflows or unsupported mnemonics useful to stall a CPU in undocumented or test states.

Hardware firewalls will also maintain a clean isolated trusted computing zone, separate kernel, OS, stacks and compartmentalize applications in order to avoid for instance a lousy open-source Ethernet stack leaking access to a sensitive TLS negotiation. Needless to say that all these mechanisms have to rely on X.509-certificate / private key pairs generated and administrated within a consistent Public Key Infrastructure.



Security systems don't have the luxury of video or connectivity standards, both of which are able to evolve in time with improvements, innovations and breakthroughs while maintaining ascending compatibility and slow obsolescence. Especially in the eyes of end users, security can only exist state-of-the-art. There is a good reason why a security standard like SSL/TLS has had six new releases since 1994: weaknesses and flaws discovered and exploited by hackers need an immediate fix—and the market won't take "we'll do it later" for an answer.

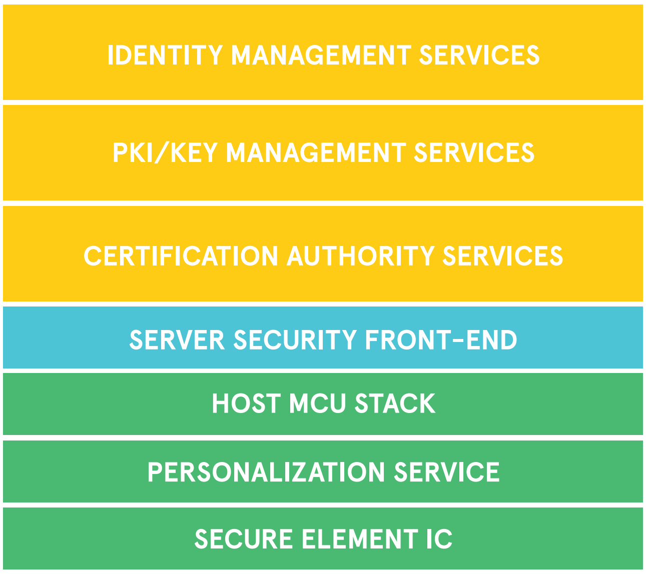
This calls for a very important property of secure devices: they need to embed mechanisms supporting upgrades, not only of their application software or firmware but also their operating system, their kernel, and their security subsystem whether an embedded secure core or a distinct secure element. Moreover, these upgrades should only be possible via a very secure channel from a very secure administration platform with administration rights and credentials keeping track of every device in the field. Implementing real security in your IoT solution will require up to 7 layers and as many partners that you will need to orchestrate and maintain to hold everything together in the long run.

Having a system that not only builds in security at every layer, but also ensures your IoT solution is future-proofed through lifecycle maintenance means that your IoT solution can be competitive today and stay competitive in the future as this nearly half a trillion market continues to grow.

It's difficult to build up an end-to-end security system. From the silicon up to identity management, identifying partners and negotiating business-models, it's a lot to manage. That's why we encourage those looking to deploy to think of the pros and cons of building an internal IoT infrastructure versus buying from an experienced technology solutions provider. For instance, Avnet customers have told us that getting access to all these services was limited to a privileged market until quite recently.

The consult-develop-deploy process is crucial to creating an environment where a new IoT solution can succeed. If you feel like there are some questions you can't answer from the above, find the right partner to help you assess security end-to-end. An end-to-end partner like Avnet anticipates new technologies and future best practices, partners with leading suppliers to give you access to the best components and services as well as spearheads the best fit solution you need with one objective: help you focus on what you do best while we take care of the rest.

THE IoT SECURITY STACK



IDENTITY MANAGEMENT SERVICES

PKI/KEY MANAGEMENT SERVICES

CERTIFICATION AUTHORITY SERVICES

SERVER SECURITY FRONT-END

HOST MCU STACK

PERSONALIZATION SERVICE

SECURE ELEMENT IC

SO, YOU'VE GOT SOME ANSWERS. NOW, HERE'S A WAY TO GET YOU STARTED.

IoT security questionnaire

THERE ARE THREE MAIN SECTIONS OF AN IOT DEPLOYMENT: CONSULT, DEVELOP AND DEPLOY. HERE ARE THE SECURITY QUESTIONS YOU SHOULD ASK AT EACH STEP:

CONSULT

First, you have to make a big decision on whether you'll build an internal team to execute your IoT solution or buy it through exporting the work to an external partner. That way, you'll be able to properly scope out the road ahead for final deployment in order to get initial buy in from the executives who might have the ROI rather than the security stack in mind.

Ask yourself questions like:

- Which security measures do you need to comply with by law?
- What security scenarios related to this project could jeopardize your project revenue or your company revenue as a whole? (Rank them by priority, short/long term and draft a technical solution for each)
- What costs are associated with developing and deploying in terms of overall budget?
- What hardware, software and firmware considerations do you need to consider?
- What security team do you have in house ready for an IoT deployment?
- Who on your team will be the final responsible party for security of the solution?
- How will you measure success for your team in terms of security protocols?

DEVELOP

In the develop phase, you should clean up the initial plans created in the consult phase to optimize for performance and cost as well as to find the fastest, most profitable route to market.

Ask yourself questions like:

- What will you build in-house and what are you ready to outsource to partners?
- If external partners, will they outlive the 10-year smart appliance you are deploying yourself?
- Who is ensuring hardware security, including board development and logistics around manufacturing?
- Who is ensuring software and firmware security, including the software, cloud and associated analytics platform? (If you are including artificial intelligence (AI), machine learning, web platforms and applications, or data visualization, you'll need to build out this even more.)
- Who in your development team will follow through to deployment to ensure the solution's security stack works in the field?
- Do you need certifications or should you rely on already certified solutions?
- Have you considered privacy and data concerns? Do you need additional security resources?

DEPLOY

Here's where the rubber meets the road: security and data privacy plans laid out in the consult phase and created during development also come full circle in deploy.

Ask yourself questions like:

- Do you have the in-house capabilities to install, support and service on premise during the crucial weeks and months of initial implementation? Does your external partner?
- Do you have secure tech support for Wi-Fi or cellular networks, gateways, web interfaces, apps and your new cloud platform?
- Do you have plans if a critical piece is stolen days before deployment? If a protocol crucial to your system is hacked? How can you protect your system from ongoing threats?
- What is your plan to qualify your solution and check every single scenario which could make it go wrong?
- How about having a "white hats" lab proof it before you go live?

Offices

AUSTRIA
Vienna
Phone: +43 186 642 300
Fax: +43 186 642 350
wien@avnet.eu

BELGIUM
Merelbeke
Phone: +32 9 210 24 70
Fax: +32 9 210 24 87
gent@avnet.eu

BULGARIA
Sofia
sofia@avnet.eu

CZECH REPUBLIC (SLOVAKIA)
Prague
Phone: +420 234 091 031
Fax: +420 234 091 030
praha@avnet.eu

DENMARK
Herlev
Phone: +45 432 280 10
Fax: +45 432 280 11
herlev@avnet.eu

ESTONIA
(LATVIA, LITHUANIA)
Pärnu
Phone : +372 56 637737
paernu@avnet.eu

FINLAND
Espoo
Phone: +358 207 499 200
Fax: +358 207 499 280
helsinki@avnet.eu

FRANCE (TUNISIA)
Cesson Sévigné
Phone: +33 299 838 485
Fax: +33 299 838 083
rennes@avnet.eu

Illkirch
Phone: +33 390 402 020
Fax: +33 164 479 099
strasbourg@avnet.eu

Massy Cedex
Phone: +33 164 472 929
Fax: +33 164 470 084
paris@avnet.eu

Toulouse
Phone: +33 05 62 47 47
toulouse@avnet.eu

Vénissieux Cedex
Phone: +33 478 771 360
Fax: +33 478 771 399
lyon@avnet.eu

GERMANY
Berlin
Phone: +49 30 214 882 0
Fax: +49 30 214 882 33
berlin@avnet.eu

Freiburg
Phone: +49 761 881 941 0
Fax: +49 761 881 944 0
freiburg@avnet.eu

Hamburg
Phone: +49 40 608 235 922
Fax: +49 40 608 235 920
hamburg@avnet.eu

Holzwickede
Phone: +49 2301 919 0
Fax: +49 2301 919 222
holzwickede@avnet.eu

Lehrte
Phone: +49 5132 5099 0
hannover@avnet.eu

Leinfelden-Echterdingen
Phone: +49 711 782 600 1
Fax: +49 711 782 602 00
stuttgart@avnet.eu

Leipzig
Phone: +49 34204 7056 00
Fax: +49 34204 7056 11
leipzig@avnet.eu

Nürnberg
Phone: +49 911 24425 80
Fax: +49 911 24425 85
nuernberg@avnet.eu

Poing
Phone: +49 8121 777 02
Fax: +49 8121 777 531
muenchen@avnet.eu

Wiesbaden
Phone: +49 612 258 710
Fax: +49 612 258 713 33
wiesbaden@avnet.eu

HUNGARY
Budapest
Phone: +36 1 43 67215
Fax: +36 1 43 67213
budapest@avnet.eu

ITALY
Cusano Milanino
Phone: +39 02 660 921
Fax: +39 02 660 923 33
milano@avnet.eu

Firenze
Phone: +39 055 428 2301
Fax: +39 055 431 035
firenze@avnet.eu

Modena
Phone: +39 059 348 933
Fax: +39 059 344 993
modena@avnet.eu

Padova
Phone: +39 049 807 368 9
Fax: +39 049 773 464
padova@avnet.eu

Rivoli
Phone: +39 011 204 437
Fax: +39 011 242 869 9
torino@avnet.eu

Roma Tecnocittà
Phone: +39 06 412 319 10
Fax: +39 06 413 116 1
roma@avnet.eu

NETHERLANDS
Breda
Phone: +31 765 722 700
Fax: +31 765 722 707
breda@avnet.eu

NORWAY
Asker
Phone: +47 667 736 00
Fax: +47 667 736 77
asker@avnet.eu

POLAND
Gdansk
Phone: +48 58 307 81 51
Fax: +48 58 307 81 50
gdansk@avnet.eu

Katowice
Phone: +48 32 259 50 10
Fax: +48 32 259 50 11
katowice@avnet.eu

Warszawa
Phone: +48 222 565 760
Fax: +48 222 565 766
warszawa@avnet.eu

PORTUGAL
Vila Nova de Gaia
Phone: +35 1 223 779 502
Fax: +35 1 223 779 503
porto@avnet.eu

ROMANIA (BULGARIA)
Bucharest
Phone: +40 21 528 16 32
Fax: +40 21 529 68 30
bucuresti@avnet.eu

RUSSIA (BELARUS, UKRAINE)
Moscow
Phone: +7 495 737 36 70
Fax: +7 495 737 36 71
moscow@avnet.eu

Saint Petersburg
Phone: +7 812 245 1571
stpetersburg@avnet.eu

SLOVAKIA
Bratislava
Phone: +421 232 242 211
Fax: +421 232 242 210
bratislava@avnet.eu

SLOVENIA
(BOSNIA AND HERZEGOVINA,
CROATIA, MACEDONIA, MONTENEGRO,
SERBIA)
Ljubljana
Phone: +386 156 097 50
Fax: +386 156 098 78
ljubljana@avnet.eu

SPAIN
Barcelona
Phone: +34 933 278 530
Fax: +34 934 250 544
barcelona@avnet.eu

Galdàcano. Vizcaya
Phone: +34 944 572 777
Fax: +34 944 568 855
bilbao@avnet.eu

Las Matas
Phone: +34 913 727 100
Fax: +34 916 369 788
madrid@avnet.eu

SWEDEN
Sundbyberg
Phone: +46 8 587 461 00
Fax: +46 8 587 461 01
stockholm@avnet.eu

SWITZERLAND
Rothrist
Phone: +41 62 919 555 5
Fax: +41 62 919 550 0
rothrist@avnet.eu

TURKEY (GREECE, EGYPT)
Kadikoy Istanbul
Phone: +90 216 528 834 0
Fax: +90 216 528 834 4
istanbul@avnet.eu

UNITED KINGDOM (IRELAND)
Berkshire
Phone: +44 1628 512 900
Fax: +44 1628 512 999
maidenhead@avnet.eu

Bolton
Phone: +44 1204 547 170
Fax: +44 1204 547 171
bolton@avnet.eu

Bucks, Aylesbury
Phone: +44 1296 678 920
Fax: +44 1296 678 939
aylesbury@avnet.eu

Stevenage, Herts, Meadway
Phone: +44 1438 788 310
Fax: +44 1438 788 250
stevenage@avnet.eu

ISRAEL
Tel-Mond
Phone: +972 (0)9 7780280
Fax: +972 (0)3 760 1115
avnet.israel@avnet.com

SOUTH AFRICA
Cape Town
Phone: +27 (0)21 689 4141
Fax: +27 (0)21 686 4709
sales@avnet.co.za

Durban
Phone: +27 (0)31 266 8104
Fax: +27 (0)31 266 1891
sales@avnet.co.za

Johannesburg
Phone: +27 (0)11 319 8600
Fax: +27 (0)11 319 8650
sales@avnet.co.za

All trademarks and logos are the property of their respective owners. This document provides a brief overview only, no binding offers are intended. No guarantee as to the accuracy or completeness of any information. All information is subject to change, modifications and amendments without notice.