AVNET SILICA

Capability Insights
Security

Security

INTRODUCTION

The strength and resilience of any chain can only be judged by looking at its weakest link – and this dictum is particularly true for IoT security. Companies have made significant progress over the last few years in terms of IT security – even though there is still room for improvement in this area. But IoT brings with it a different set of challenges, especially in the industrial sector.

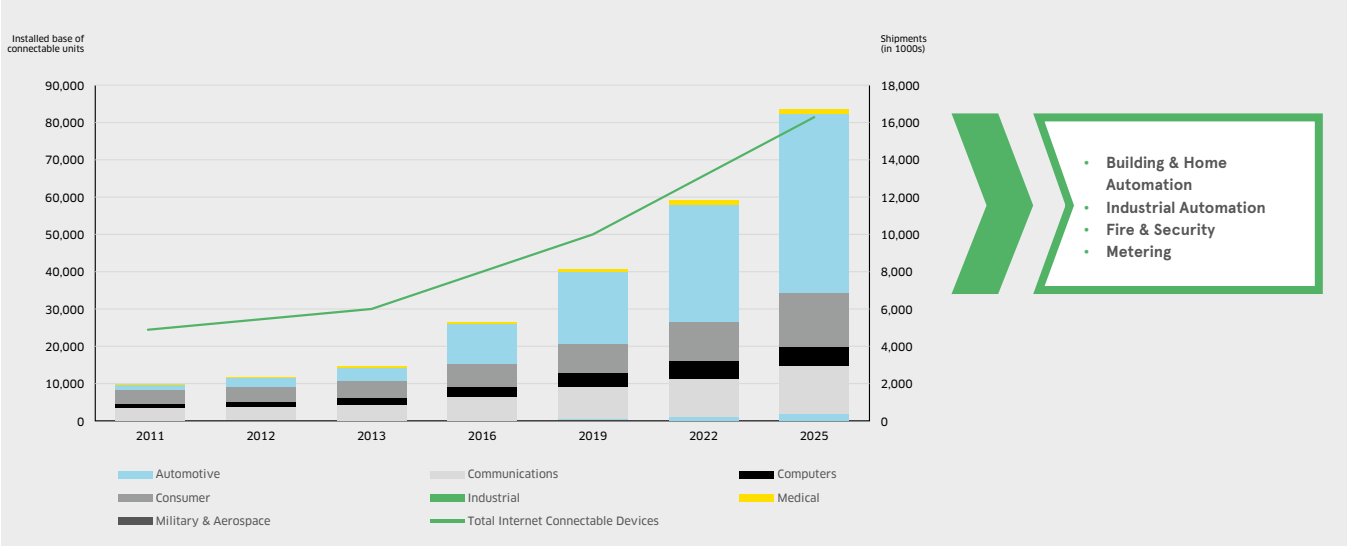
In addition to securing the connection of computers and smartphones/tablets to corporate networks, industrial IoT also aims at connecting sensors, machines, robots to these IT networks, most often in remote facilities, securely and in a seamless way.

While this is a well-known problem with established solutions in an all-IPv6 world, the low-power sensors and devices deploying under the IoT banner are not yet compatible with the Internet (IP) protocols (such as IPv6 and 6LoWPAN) and are not expected to be until 2025. This produces the dual challenge of implementing security protocols that work for non-IP devices now and IPv6 devices later.

For the same reason users of the Internet do not "http" but "https" instead, machines, sensors and devices connecting to servers through the Internet need exactly the same kind of end-to-end security in order to comply with IT security standards. Since most of these sensors, devices and machines do not talk IPv6 yet, the challenge is to tailor adequate security protocols providing this end-to-end security while meeting power consumption and cost constraints of these devices.

Along with the more obvious threats – such as industrial espionage, which seems to be in the headlines practically every day – attacks on industrial plants could also turn off or alter safety systems, with potentially catastrophic results. From the perspective of the industrial manufacturer, a corollary to the security issue is cost.

The IoT Opportunity – Highest Growth in Industrial



Source: IHS - Internet Connected Devices

Industrial use cases:
The reason why most industrial products could actually benefit from "security technologies and products" may not be evident. Real life use cases:

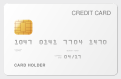
- Brand protection – product warranty
- Usage/feature control
- Remote firmware update in a field-deployed machine or device
- Deployment of local networks
- Connected devices and machines (IoT, IIoT)

Regardless of your business, failing to answer one of these questions may result in a serious problem for your profitability and long-term growth:

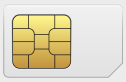
- How to prevent non-authorized accessories or consumables from connecting to my devices?
- How to make sure my customers will purchase consumables from me and not a cheap competitor?
- How to discriminate between my original device/board and a fake copy?
- How to make sure my production is not counterfeited?
- How to feel confident warranting products, knowing no one can misuse them with off-spec accessories?
- How to prevent over-usage of my consumables for health/safety/security reasons?
- How to make sure only an authorized firmware is downloaded into my devices once deployed in the field?
- How to make sure no one reprograms my devices in order to change/control/unlock functions?
- How to make sure no one can duplicate my production even if they have my firmware publicly available on the web?
- How to make sure no one impersonates my firmware with an infected pseudo-official version?
- How to automate the installation and provisioning of devices or machines in local networks or with distant servers?
- How to automate secure and remote distribution and renewal of local or distant network keys?
- How to achieve truly end-to-end security equivalent to HTTPS on the Internet?

eSecurity in your everyday life

- VISA / MASTERCARD



- Cell phone 2G/3G/4G

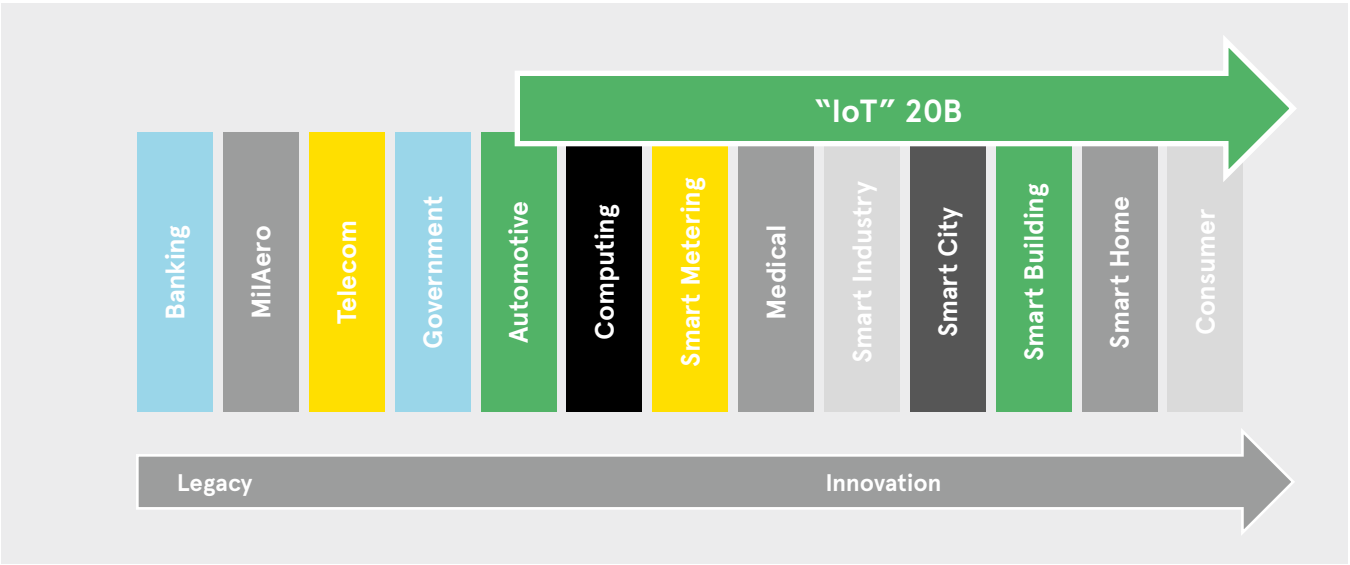


- https://

What are the key areas needing protection?

- **Access to systems and devices** – authentication – especially as most companies never bother to renew default AES keys programmed at the factory in their embedded devices! This is particularly important when adding and provisioning a new component in a remote system or upgrading a sensitive component like a motherboard. It is also essential to minimize the risk of device spoofing, where the attacker infiltrates a system by impersonating the behaviour of an authorised device or user.
- **Intellectual property** – the foundations of the company's survival need across the board protection for both hardware and software. This is particularly important when you outsource manufacturing to another company or country as it helps you ensure protection from other people **copying or counterfeiting your IP**.
- **Communications** – integrity & confidentiality – protection of data transmission from sensor to server in order to prevent hackers and eavesdropping across your factory and IT systems
- **Logistics supporting unique devices** – to facilitate personalisation and configuration in the field while securing the entire supply chain. Two important functions in the logistical area are the automated distribution and regular replacement of access keys along with secure remote management, both of which maintain protection while reducing the cost and effort of personalising configurable systems.

HW Security: Where to expect the big numbers from?



Secure elements: part of a complete solution

Secure elements are tiny components connecting as peripherals to host MCUs/MPUs and featuring:

- Personalized certificates
- Secure hosting of secret keys
- Handling of cryptography primitives

Secure elements, working together with secure personalisation logistics, can make it much easier for manufacturers to secure every component on every leg of its journey to the internet (local LAN, WAN, IP and so on). With this combination, customers can personalise and provision their connected devices, sensors, and machines to local or remote servers. Crucially, they can do this cost-effectively!

How can Avnet Silica help?

Strong innovation

Building on its long tradition of innovation, together with partners Morpho and Trusted Objects, Avnet Silica has developed a personalised secure element for customers needing an easier and more cost-effective way to secure their IoT devices end to end. Also, Avnet Silica is currently developing its own stacks and APIs able to handle TLS derivatives and easy provisioning schemes. These run on various radio links together with UbiquiOS™ technology (in which Avnet Silica is a development partner) and Avnet Services.

Strong expertise

Avnet Silica, together with its partners, offers customers unparalleled expertise in addressing personalisation and security challenges in their IoT initiatives. Customers benefit from our close partnerships, most going back many years, with some of the world's leading secure element manufacturers, including Infineon Technologies, STMicroelectronics, Morpho, Trusted Objects, NXP, Maxim Integrated, and Microchip.

Strong corporate resources

In May 2016, Avnet Silica launched its personalisation centre near Munich. Customers benefit from our personalisation expertise at this site, whether they require small or large volumes of secure elements. This centre ensures that customers not wishing to perform personalisation implementations themselves can outsource it cost-effectively to our experts.

A strong backbone

Customers benefit from the Avnet Silica vision due to our unique positioning. We have unparalleled knowledge and experience encompassing both IT and embedded technologies. In addition, we have multiple strong partnerships with the world's leading technology providers along with the expertise to integrate them efficiently. But that's not all! Together, we can develop viable security solutions reaching from sensor to server that comply with both IT and embedded hardware standards. Naturally, we also work closely with Avnet Logistics and other Avnet speedboats in EMEA for the benefit of all our customers.

Networking and security: the importance of "end-to-end"

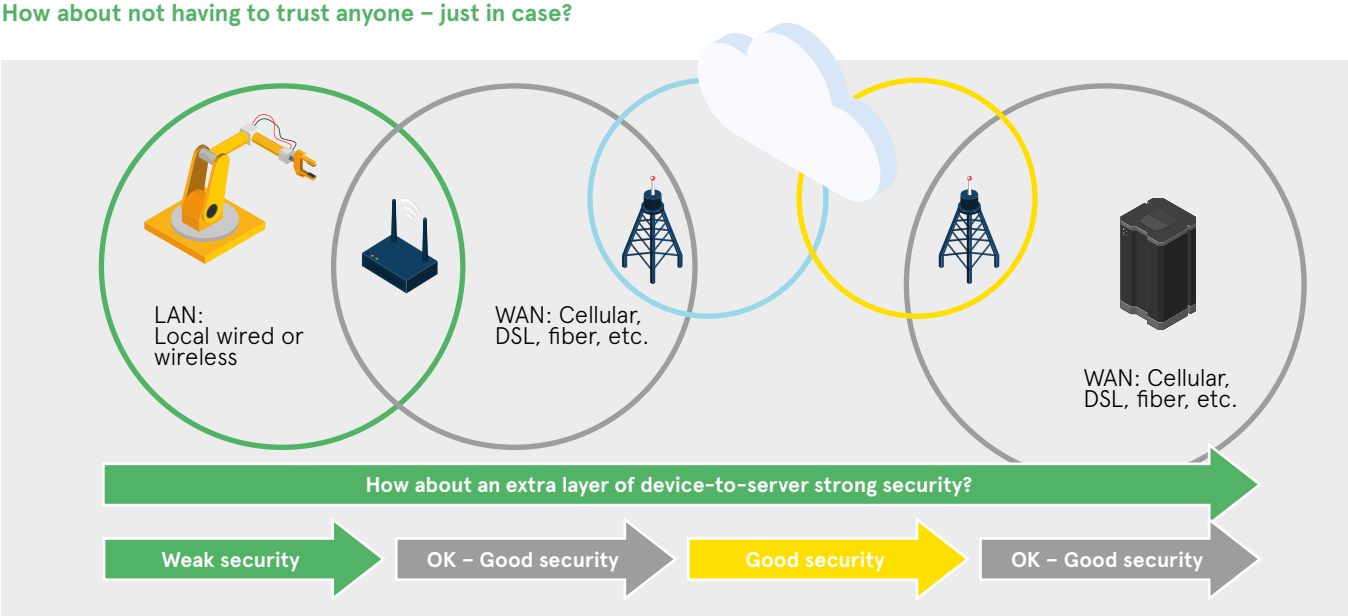
Link and network security are being addressed by every single communication and networking technology at different levels of the protocol stacks such as IPsec for IP, WPA for 802.11, 802.15.4, Bluetooth, and so on. However they should not be mistaken for end-to-end application security.

Indeed, having a WPA-secured WiFi connection to a local router is definitely not sufficient to "http" privately into a distant server, bearing in mind that most local network keys are hardly ever renewed.

As illustrated below, it is fairly common that the data generated by a sensor or a machine will be conveyed through many different networks of different sorts belonging to a variety of service providers before reaching the targeted application server.

This is why an end-to-end security scheme is needed in order to ensure equivalent mutual authentication and privacy as with https on IP networks.

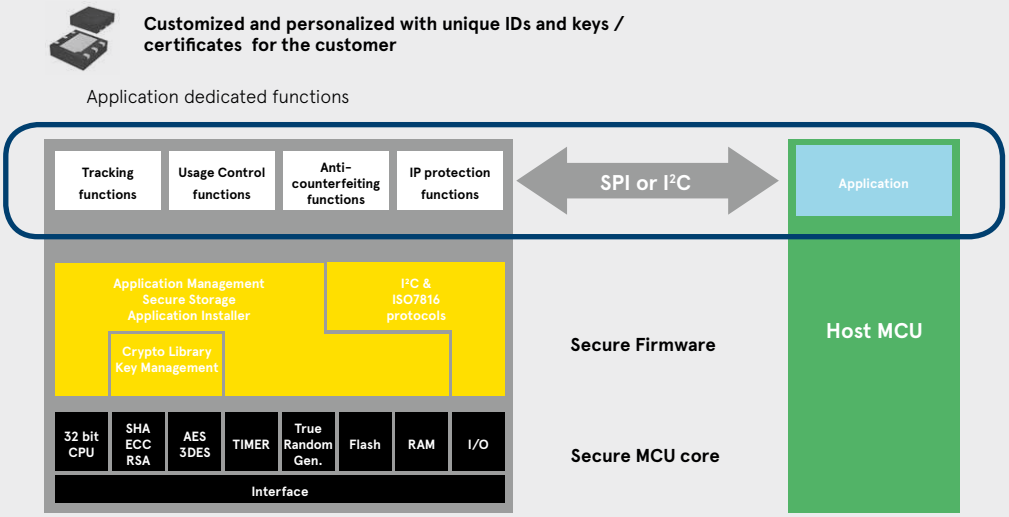
How about not having to trust anyone – just in case?



Bridging the gap between Embedded and IT

Solutions

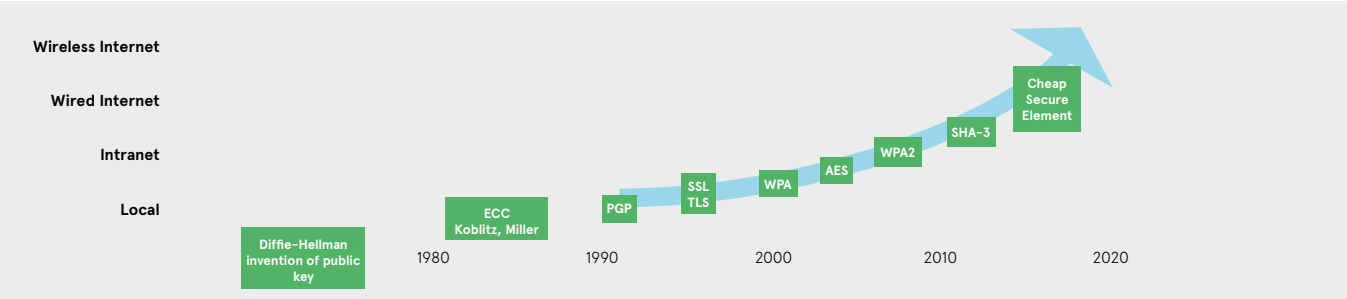
So much for our background and infrastructure. As further proof of our innovative capabilities, we've put our money where our mouth is. At Avnet Silica, we've invested no less than 1M € in a unique, high-security platform developed in collaboration with our partners Morpho and Trusted Objects. The first product on the platform is based on a low-cost, low-power, secure 32-bit microcontroller from Morpho, with a certification from EMVCo (Europay Mastercard Visa) and firmware from Trusted Objects. It is delivered in a range of standard packages, making it an easy-to-integrate companion chip in any sensor, device, or gateway.



Secure Elements

Avnet Silica personalizes the secure elements with unique IDs, certificates and keys, tailored to the exact requirements of our customers. We program the components in our Avnet Silica secure warehouse and can produce quantities as low as 1000 or as high as 5 million. Once they're ready, our sister speedboat Avnet Logistics delivers them to you. The ready-to-use secure element can then be embedded into the objects throughout your IoT chain, providing an extra level of strong security on top of those already present in your networks and other assets.

Enterprises: network evolution driving security



Your benefits

With our cutting-edge solutions, you can dramatically accelerate your IoT and Industry 4.0 initiatives without being hindered by security worries. In all your industrial applications, you maintain full control, at all times, over the flow, storage and processing of data produced and used by your devices – without ever exposing it to the outside world.

Authenticator chips

		Usage Counter	ECDSA	SHA
Infineon	Optiga™ Trust B	Yes	Yes	256
Maxim	DS28EL15	No	No	256
Maxim	DS28C36	Yes	Yes	256
Microchip	ATECC108	Yes	Yes	256
Microchip	ATSHA204	Yes	No	256
NXP	A1006	No	Yes	224

General purpose secure elements

		Custom FW / commands	TLS and X509 certificates	Personalization	Certification
Infineon	Trust E SLS 32AIA	No	No	1 Infineon certificate	CC EAL6+
Maxim	MAXQ1061	No	X509	1 Maxim certificate	CC EAL4+
Microchip	ATECC508	No	proprietary	1 Microchip certificate	No
NXP	A070CM	No	X509	2 NXP certificates 72 AES keys	CC EAL5+
Idemia & Trusted Objects	TO136	Yes	X509 + short certificate	AVS unlimited PKI certificates AES keys etc.	EMVco
STMicroelectronics	STSAFEA100	No	X509	n ST certificates	CC EAL5+

Security partners

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

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
braunschweig@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: +39 055 436 039 2
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 06 413 115 1
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: +7 812 635 81 11
Fax: +7 812 635 81 12
stpetersburg@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

FSC Mixed Sources
Product group from well-managed forests and other controlled sources
www.fsc.org Cert no. IC-COC-100065
© 1996 Forest Stewardship Council

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.