

presented by
EBVElektronik
| An Avnet Company |



Spotlight on embedded security

Keeping up with the Internet of Things

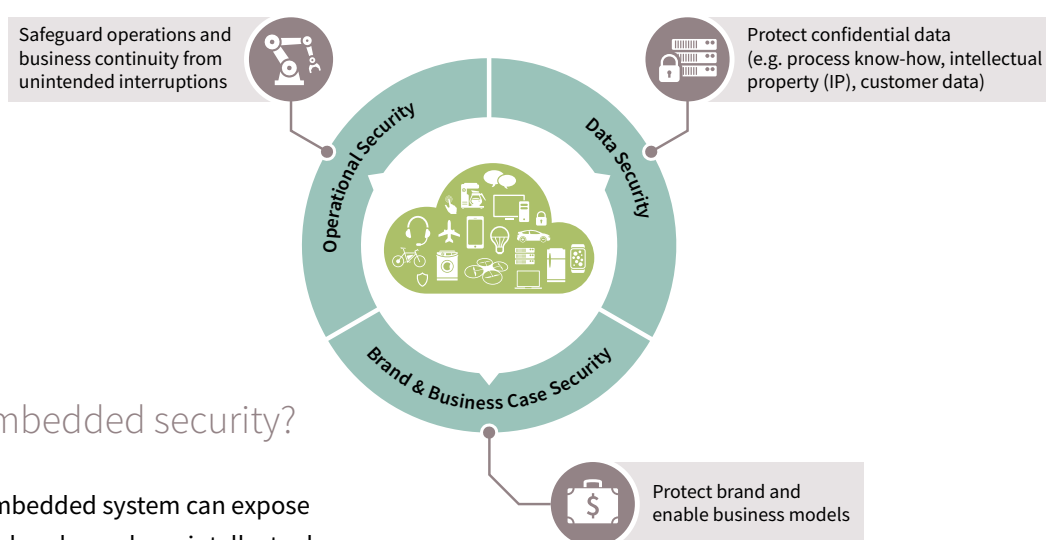
www.infineon.com/embedded-security



Rising concerns about embedded security

Embedded systems are becoming ubiquitous. Trends such as the Internet of Things (IoT) and machine-to-machine communication (M2M) mean that the number of connected devices and machines is increasing. Many of these – from small household appliances through large communication networks to complex, industrial automation systems – are controlled by special-purpose, embedded computing systems.

As it continues to gather pace, the networking trend promises greater convenience and comfort for users, plus new business and service models for companies. However, security in this embedded world often lags far behind. Security vulnerabilities are rising dramatically as the attack surface widens and manufacturers struggle to protect sensitive data, intellectual property (IP) and process integrity.



Why do we need embedded security?

A successful attack on an embedded system can expose confidential information such as know-how, intellectual property, customer data and process intelligence. In addition, it can interrupt operations, compromise business continuity and even endanger a company's brand image, success and very existence.

Challenges

- › Protect systems against increasingly sophisticated and determined hacker attacks
- › Balance financial constraints with the value of protected assets
- › Find reliable, trustworthy functionality that is easy to implement
- › Increase system security without compromising usability

Opportunities

- › Develop new business and service models
- › Carve out an image-building competitive differentiator
- › Reduce security investment by building on partner know-how
- › Increase production site flexibility through improved control across the supply chain



The answer

With its OPTIGA™ family, Infineon offers easy-to-integrate, scalable and customizable turnkey solutions to meet your embedded security challenges. As a trusted advisor, we help you reduce complexity and implementation costs. Rather than investing in security know-how and infrastructure yourself, you can build on our vast and proven expertise in hardware-based security solutions.



Protection against digital threats

Software alone is not enough to protect embedded systems as it can be read, copied and distributed with relative ease. Secured hardware is needed to reliably store data and software code, detect manipulation and encrypt data for safe storage and processing. You can rely on our solutions to establish a hardware-based root of trust that renders embedded software trustworthy.

Our OPTIGA™ portfolio achieves this by supporting the following three key security-critical functions:

> Authentication

Our OPTIGA™ security ICs authenticate people and devices so information is exchanged between authorized individuals and devices only

> Encryption

Our security controllers protect sensitive information by encrypting it and securely storing the secret keys

> Integrity

Our security chips check platform, machine and device integrity to identify manipulation and detecting unauthorized changes

By building a root of trust in security architectures, our semiconductor-based solutions create immense value for consumers and enterprises – giving all stakeholders the peace of mind needed to fully leverage the potential offered by the Internet of Things.

Reaching beyond product-based security

Drawing on our 30-year, proven track record in security, our mission extends beyond inspiring our customers with reliable, tangible security products.

We build trust beyond product-based security in a number of ways. Firstly, we focus on process security. Concrete measures include security-certified design environments, dedicated security infrastructure with biometric access and a secured production environment to protect key programming in particular.

Secondly, our security experts put our market-leading products through rigorous testing. This allows us to keep track of attack trends, continuously adapt our product concepts and proactively manage the product lifecycle.

And last but not least, we have our products as well as our development and manufacturing processes certified by third parties. Most of our products have successfully completed the strict Common Criteria certification process with the German authorities.

These measures combine to give our customers easy-to-grasp proof points that empower them, in turn, to build trust among their customers.

Broad market spectrum

We understand that security needs are as varied as they are complex. Scaling from basic, single-function authentication solutions to robust certified security controllers for advanced platform integrity checks, we have developed the market's widest portfolio to support individual security needs across a broad market spectrum.

Smart home

Here we enable protection of everything from the toaster sensor to the overarching control system – for example by:

- › Securing communication between the smart home gateway and the server
- › Authenticating home automation components
- › Protecting against counterfeit home automation components

We add value to today's smart home by offering flexibility and cost savings for all implementations, building trust in new applications with ground-up, proven security capabilities and thus paving the way for new business and service models.



Connected Car

We are making cars safer and protecting sensitive user data – for example by:

- › Securing communication over telematics systems
- › Authenticating infotainment systems to enable media service models
- › Securing remote maintenance information and firmware updates

We build confidence in the connected car with optimized security solutions that synergize our long-standing automotive expertise with our extensive security know-how. This also gives you the chance to capture new business and service models.





Cloud

Information & Communication Technology

Our scalable portfolio safeguards communications and access across everything from small network switches up to enterprise-scale networks – for example by:

- > Protecting data through secured communication between networking devices
- > Securing software updates and protecting software
- > Checking integrity of devices with router-enabled network access

As a trusted partner in the ICT field, we keep our customers ahead with easy access to the latest security solutions, backed by integration and device management support delivered through our wide partner network. With our trustworthy security solutions, you can develop new business and service models.

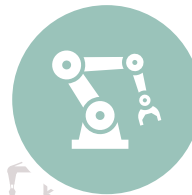


Smart factories

We are helping manufacturers to safeguard long-term success by securing everything from machine sensors to control systems – for example by:

- > Securing communication between the automation system and IT platform to protect sensitive data and IP
- > Authenticating sensors and devices in the automation network
- > Securing software or firmware updates to protect IP and prevent operational interruptions

Our synergized industrial and security expertise builds confidence in the modern smart factory with a scalable portfolio to match individual requirements. Easy access to our established security know-how and infrastructure allows you to rein in your security investment.



Use cases in focus

The depth and range of our proven portfolio cover just about every conceivable typical use case scenario. The following outlines the most typical scenarios that can benefit from our tailored offering.



Secured software and firmware updates

Software and firmware in embedded systems often need regular updates. However, it can be challenging to protect both the software itself as well as the system that is being updated. Updates protected by software only are at risk as software can be read, analyzed and modified to compromise the update or system. However, software can become trustworthy by combining it with secured hardware. Secured hardware from our OPTIGA™ family protects the processing and storage of code by means of encryption, fault and manipulation detection, and secure code and data storage.



Stored data encryption and integrity protection

Embedded devices often store sensitive user data. The integrity and confidentiality of this data can be protected by encrypting or signing it. The challenge lies in securely storing cryptographic keys. Data can be easily decrypted if an attacker manages to read out the keys. Our OPTIGA™ Trust and OPTIGA™ TPM families overcome this problem by encrypting data and storing cryptographic keys securely. The OPTIGA™ TPM also supports software and hardware integrity checks.



Authentication

Authentication is the process of identifying users, computers, devices and machines in networks and restricting access to authorized persons and non-manipulated devices. Hardware-based security can support authentication by providing secured storage for a device's credentials (cryptographic keys or passwords). We have developed a broad portfolio of OPTIGA™ products that build a root of trust in hardware devices to allow the secured authentication of devices and systems.



Boot process protection

Also known as secure, verified or trusted boot, boot access protection blocks unauthorized booting of computing devices to stop compromised devices from exchanging data over the Internet of Things. We deliver a range of security ICs to enhance boot protection and take the complexity out of integrity metrics management. Our OPTIGA™ TPM products integrate a root of trust in the boot process compliant with Trusted Computing Group (TCG) standards.



Secured communication

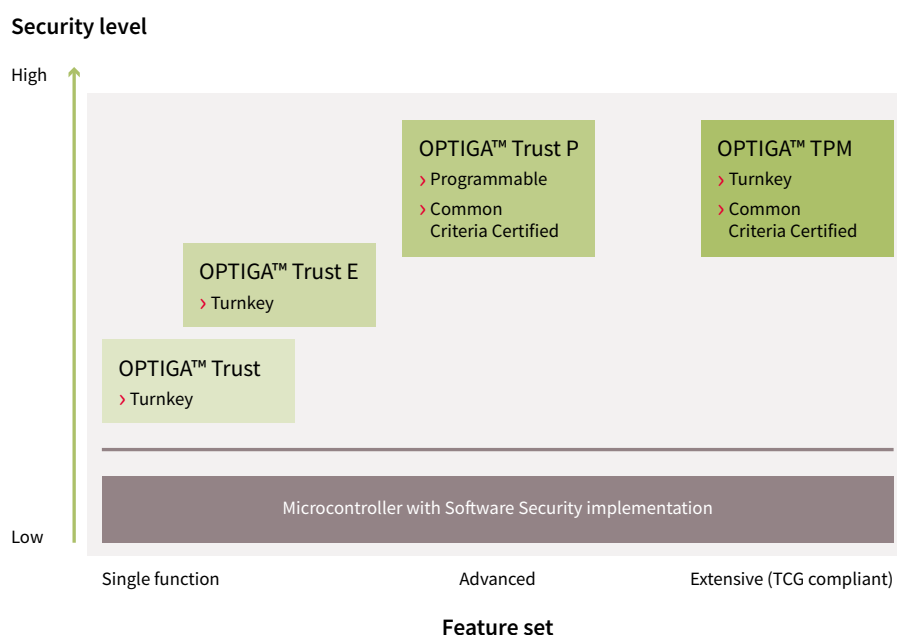
In typical embedded system architectures, devices and systems are connected across heterogeneous networks employing various standard and proprietary protocols. To protect communication against eavesdropping and message falsification, for instance, it must be secured between these systems. Our OPTIGA™ family enables secured communications by storing the keys and certificates used in communication protocols as well as supporting cryptographic operations.



Meeting today's security challenges with OPTIGA™

Our OPTIGA™ family of security solutions is designed for easy integration into embedded systems. These hardware-based security solutions scale from basic authentication functionality to complex implementations to meet

your individual and changing needs, while maximizing the return on your investment. Both our OPTIGA™ Trust and OPTIGA™ TPM product families provide proven and reliable embedded security performance.



OPTIGA™ Trust family

Trust anchor for embedded systems

Our OPTIGA™ Trust family of turnkey or programmable solutions gives you the benefit of easy and convenient integration whilst offering you the most suitable security level to protect your business model, process know-how

and IP. You can rely on OPTIGA™ Trust products to protect your embedded systems against counterfeiting, unauthorized products, intentional attacks and unintentional operator errors.

OPTIGA™ Trust

Basic authentication solution for your embedded application



OPTIGA™ Trust (SLS 10ERE) is a robust cryptographic solution for embedded systems requiring easy-to-integrate authentication features. It is designed to assist system and device manufacturers in proving the authenticity, integrity and safety of their original products. As a turnkey solution, it provides enhanced protection against aftermarket counterfeit replacements and helps to maintain OEM authenticity.

Key features

- › Advanced cryptographic algorithm implemented in hardware (ECC163)
- › Turnkey solution including host-side software for easy integration
- › 3.5 kbit user memory
- › Unique asymmetric key pair per chip
- › Size-optimized PG-USON-3 package (2 x 3 mm)
- › Easy to implement Single-Wire host interface

Key benefits

- › Lower system costs due to single-chip solution
- › Increased security with asymmetric cryptography and chip-individual keys
- › Easy integration thanks to full turnkey design

Applications

- › IoT edge devices
- › Printer cartridges
- › Consumer accessories
- › Original replacement parts
- › Medical & diagnostic supply equipment



OPTIGA™ Trust E

Easy, cost-effective security solution for high-value goods



OPTIGA™ Trust E (SLS 32A1A) is a high-end turnkey security controller with full system integration support for easy and cost-effective deployment. It supports a broad range of use cases focused on the protection of services, business models and user experience. One-way authentication mechanisms uniquely identify objects and protect PKI networks.

Key features

- › High-end security controller with advanced cryptographic algorithms implemented in hardware (ECC256)
- › Turnkey solution with OS, Applet and complete host-side integration support
- › I2C interface and PG-USON-10 package (3 x 3 mm)
- › Up to 3 Kbytes user memory
- › Standard and extended temperature range -40° to +85°C
- › Compliant to USB Type-C standard

Key benefits

- › Reduced design-in and integration effort
- › Protection of IP and data
- › Protection of business models and company image
- › Safeguarding of quality and safety

Fields of application

- › Embedded systems networked over the IOT
- › Industrial control and automation
- › Medical devices & consumer electronics
- › Smart homes
- › PKI networks



OPTIGA™ Trust P

Programmable trust anchor for embedded systems



OPTIGA™ Trust P (SLJ 52ACA) is a high-security, feature-rich solution. As a fully programmable chip, it is a highly flexible and robust solution supporting the full range of functions from authentication and secured updates through key generation and access control. This hardware security microcontroller provides advanced and efficient protection against side-channel, fault-induction, and physical attacks.

Key features

- › High-end security controller with advanced cryptographic algorithms implemented in hardware (ECC521, RSA2048, TDES, AES)
- › Common Criteria EAL 5+ (high) certification
- › Programmable JavaCard operating system with reference applets for a variety of use cases and host-side support
- › 150 KB user memory
- › Small footprint VQFN-32 SMD package (5 x 5 mm)
- › ISO7816 UART interface

Key benefits

- › Secured and certified solution
- › Increased flexibility based on programmable solution with reference applets to simplify customization and integration
- › Protection of system integrity, communication and data

Applications

- › Industrial control systems
- › Energy generation and distribution systems
- › Healthcare equipment and networks
- › Consumer electronics
- › Home security and automation
- › Embedded systems networked over the IOT

OPTIGA™ TPM

Standardized, feature-rich security solution



OPTIGA™ TPM (Trusted Platform Module) is a standardized security controller that protects the integrity and authenticity of devices and systems in embedded networks. Built on proven technologies and supporting the latest TPM 2.0 standard, OPTIGA™ TPM highlights include secured storage for keys, certificates and passwords as well as dedicated key management. As the established, trusted market and innovation leader in the Trusted Computing space, we offer a broad portfolio of certified OPTIGA™ TPM security controllers based on the Trusted Computing Group (TCG) standard to suit all needs.

Key features

- > High-end security controller with advanced cryptographic algorithms implemented in hardware (e.g. RSA2048, ECC256, SHA-256)
- > Common Criteria (EAL4+) and FIPS security certification
- > Flexible integration with SPI, I2C or LPC interface support
- > Extended temperature range (-40 to +85°C) for a variety of applications
- > Easy to integrate with wide range open source support

Key benefits

- > Reduced risk based on proven technology
- > Fast time to market through concept reuse
- > Flexibility thanks to wide range of security functions as well as dedicated key management
- > Easy integration into all platform architectures and operating systems

Applications

- > PC and embedded computing
- > Network equipment
- > Industrial control systems
- > Home security and automation
- > Energy generation and distribution systems
- > Automotive electronics

Overview of OPTIGA™ TPM family

SLB 9645	SLB 9660	SLB 9665	SLB 9670
<ul style="list-style-type: none"> > TPM 1.2 > I2C interface > Based on EAL4+ certified TPM 1.2 hardware and firmware 	<ul style="list-style-type: none"> > TPM 1.2 > LPC interface > TCG and Common Criteria EAL4+ > FIPS 140-2 certified mode (certification pending) 	<ul style="list-style-type: none"> > TPM 2.0 > LPC interface > TCG and Common Criteria EAL4+ 	<ul style="list-style-type: none"> > TPM 1.2 > SPI interface > TCG and Common Criteria EAL4+

A photograph of two men in business attire sitting at a table in an office, engaged in a conversation. The man on the right is smiling and looking towards the man on the left. The background shows a bright office environment with large windows and a modern interior.

You win new customers

Reliable, proven, certified products help you to build trust and enable new business and service models.

You get what you need

Our scalable OPTIGA™ family matches security performance to your precise embedded system needs.

Trusted advisor at your side

Designers see us as a trusted advisor for their embedded security needs. When you partner with us, you can immediately put our extensive embedded security competence and dedicated security infrastructure to work for you – reducing your investment and integration effort, saving time and money and protecting your valuable assets and IP.

We complement one of the market's broadest and most scalable portfolios with a rich partner ecosystem – the Infineon Security Partner Network (ISPN) – so you can tap into a vast global network of consulting and support expertise. Ultimately, not only will our security technologies help secure the future success of your current business case, they will also open up exciting new business and service models in security-critical applications.

www.infineon.com/ISPN



You can adapt as your needs change

Tailored solutions based on open standards give you flexibility to grow and adapt.

You don't need to worry about complexity

Extending across the entire security ecosystem, our experience and dedicated infrastructure will speed up and simplify your integration effort.

You can manage your security investment

We reduce integration effort and save valuable time-to-market through standardized designs.

EBV EUROPEAN HEADQUARTERS

EBV Elektronik GmbH & Co. KG | D-85586 Poing | Im Technologiepark 2-8 | Phone: +49 (0)8121 774-0 | www.ebv.com

EBV REGIONAL OFFICES | Status November 2015

AUSTRIA

A-1120 Wien
Schönbrunner Str. 297 - 307
Phone: +43 (0)18 91 52-0
Fax: +43 (0)18 91 52-30

BELGIUM

B-1831 Diegem
Kouterveldstraat 20
Phone: +32 (0)27 16 00 10
Fax: +32 (0)27 20 81 52

BULGARIA

B-1505 Sofia
48 Sitnyakovo Blvd., Serdika
offices, 10th floor, Unit 1006
Phone: +359 2 9264 337
Fax: +359 2 9264 133

CZECH REPUBLIC

Amazon Court
Karolinska 661/4
CZ-18600 Prague
Czech Republic
Phone: +420-234 091 011
Fax: +420-234 091 010

DENMARK

DK-8230 Åbyhøj
Ved Lunden 10-12, 1. sal
Phone: +45 86 25 04 66
Fax: +45 86 25 06 60

DK-2730 Herlev

Ellekær 9, 2 tv
Phone: +45 39 69 05 11
Fax: +45 39 69 05 04

ESTONIA

E-10414 Tallinn
Niine 11
Phone: +372 625 79 90
Fax: +372 625 79 95
Cell: +372 513 22 32

FINLAND

FIN-02240 Espoo
Pihatörmä 1 a
Phone: +358 (0)927 05 27 90
Fax: +358 (0)9 27 09 54 98

FIN-90100 Oulu

Nahkatehtaankatu 2
Phone: +358 (0)85 62 49 10
Fax: +358 (0)85 62 49 15

FRANCE

F-13856 Aix-en-Provence
1330 Rue G. G. de la Lauziere
Europarc Pichauray, Bâtiment A2
Phone: +33 (0)442 39 65 40
Fax: +33 (0)442 39 65 50

F-92184 Antony Cedex (Paris)

3, rue de la Renaissance
Phone: +33 (0)140 96 30 00
Fax: +33 (0)140 96 30 30

F-35510 Cesson Sévigné (Rennes)

35, av. des Peupliers
Phone: +33 (0)299 83 00 50
Fax: +33 (0)299 83 00 60

F-67400 Illkirch Graffenstaden

35 Rue Gruninger
Phone: +33 (0)3 90 40 05 92
Fax: +33 (0)3 88 65 11 25

F-31670 Labège (Toulouse)

Immeuble Les Berges du Lac
Bat A, 45 Rue du Colombier
Phone: +33 (0)561 00 84 61
Fax: +33 (0)561 00 84 74

F-69693 Venissieux (Lyon)

Parc Club du Moulin à Vent
33, Av. du Dr. Georges Lévy
Phone: +33 (0)472 78 02 78
Fax: +33 (0)478 00 80 81

GERMANY

D-12277 Berlin-Mariendorf
Kitzingstraße 15 - 19
Phone: +49 (0)30 74 70 05-0
Fax: +49 (0)30 74 70 05-55

D-30938 Burgwedel

Burgdorfer Straße 2
Phone: +49 (0)5139 80 87-0
Fax: +49 (0)5139 80 87-70

D-41564 Kaarst

An der Gumpgesbrücke 7
Phone: +49 (0)2131 96 77-0
Fax: +49 (0)2131 96 77-30

D-59439 Holzwickede

Wilhelmstraße 1
Phone: +49 (0)2301 943 90-0
Fax: +49 (0)2301 943 90-30

D-71229 Leonberg

Neue Ramtelstraße 4
Phone: +49 (0)7152 30 09-0
Fax: +49 (0)7152 759 58

D-90471 Nürnberg

Lina-Ammon-Straße 19B
Phone: +49 (0)911 817 669-0
Fax: +49 (0)911 817 669-20

D-85586 Poing

Im Technologiepark 2-8
Phone: +49 (0)8121 774-0
Fax: +49 (0)8121 774-422

D-04435 Schkeuditz

Airport Business Center Leipzig
Frankfurter Straße 2
Phone: +49 (0)34204 4511-0
Fax: +49 (0)34204 4511-99

D-78048 VS-Villingen

Marie-Curie-Straße 14
Phone: +49 (0)7721 998 57-0
Fax: +49 (0)7721 998 57-70

D-65205 Wiesbaden

Borsigstraße 36
Phone: +49 (0)6122 80 88-0
Fax: +49 (0)6122 80 88-99

HUNGARY

H-1117 Budapest
Budafoki út 91-93, West Irodaház
Phone: +36 1 436 72 29
Fax: +36 1 436 72 20

IRELAND

IRLDublin 12
Calmount Business Park
Unit 7, Block C
Phone: +353 (0)14 09 78 02
Fax: +353 (0)14 56 85 44

IL-40600 Tel Mond
Drorrim South Commercial Center
P.O. Box 149
Phone: +972 (0)9 778 02 60
Fax: +972 (0)9 796 68 80

ITALY

I-20092 Cinisello Balsamo (MI)
Via C. Fropa, 34
Phone: +39 02 66 09 62 90
Fax: +39 02 66 01 70 20

I-50019 Sesto Fiorentino (FI)

EBV Elektronik Srl
Via Lucchese, 84/B
Phone: +39 05 54 36 93 07
Fax: +39 05 54 26 52 40

I-41126 Modena (MO)

Via Scaglia Est, 33
Phone: +39 059 29 24 211
Fax: +39 059 29 29 486

I-80128 Napoli (NA)

Via G. Capaldo, 10
Phone: +39 081 193 016 03
Fax: +39 081 198 061 24
Cell: +39 335 8 39 05 31

I-00155 Roma

Via Edoardo D'Onofrio 212
Phone: +39 064 06 36 65/789
Fax: +39 064 06 37 77

I-35030 Sarmeola di Rubano (PD)

Piazza Adelaide Lonigo, 8/11
Phone: +39 049 89 74 701
Fax: +39 049 89 74 726

I-10144 Torino

Via Treviso, 16
Phone: +39 011 262 56 90
Fax: +39 011 262 56 91

NETHERLANDS

NL3606 AK Maarssenbroek
Planetenbaan 116
Phone: +31 (0)346 58 30 10
Fax: +31 (0)346 58 30 25

NORWAY

Postboks 101, Manglerud
Ryensvingen 3B
N-0681 Oslo
Phone: +47 22 67 17 80
Fax: +47 22 67 17 89

POLAND

80-838 Gdansk
Targ Rybny 11/12
Phone: +48 (0)58 719 21 87

02-674 Warszawa

Ul. Marynarska 11
Phone: +48 (0)22 257 47 06

PL-50-062 Wrocław

Pl. Solny 16
Phone: +48 (0)71 34-2 29-44
Fax: +48 (0)71 34-2 29-10

PORTUGAL

Unipessoal LDA
Edifício Tower Plaza
Rotunda Eng.º Edgar Cardoso, 23 - 14ºG
4400-676 Vila Nova de Gaia
Phone: +351 220 920 260
Fax: +351 220 920 261

ROMANIA

Construdava Business Center
Șos. Pipera-Tunari 4c
Voluntari, Ilfov (Bucharest)
RO - 077190 Romania
Phone: +40 21 529 69 11
Fax: +40 21 529 69 01

RUSSIA

RUS-620028 Ekaterinburg
Tatischeva Street 49A
Phone: +7 495 730 31 70
Fax: +7 343 311 40 46

RUS-127486 Moscow

Korovinskoye Shosse 10,
Build 2, Of.28
Phone: +7 495 730 31 70
Fax: +7 495 730 31 71

RUS-195197 St. Petersburg

Polustrovsky Prospect 43,
Office 421
Phone: +7 812 635 70 63
Fax: +7 812 635 70 64

SERBIA

Balkanska 2
SRB-11000 Belgrade
Phone: +381 11 404 9901
Fax: +381 11 404 9900
Mobile: +381 63 204 506
Mobile: +381 62 78 00 12

SLOVAKIA

SK-85101 Bratislava
Ševčenkova 34
Phone: +421 2 321 111 41
Fax: +421 2 321 111 40

SLOVENIA

SI-1000 Ljubljana
Dunajska 167
Phone: +386 (0) 1 56 09 778
Fax: +386 (0) 1 56 09 877

SOUTH AFRICA

ZA-8001 Foreshore, Cape Town
1 Mediterranean Street
5th Floor MSC House
Phone: +27 (0)21 402 19 40
Fax: +27 (0)21 419 62 56

ZA-3629 Westville

Forest Square, 11 Derby Place
Suite 4, Bauhinia Building
Phone: +27 (0)31 27 92 600
Fax: +27 (0)31 27 92 624

ZA-2157 Woodmead,

Johannesburg
Woodlands Office Park
141 Western Service Road
Building 14-2nd Floor
Phone: +27 (0)11 236 19 00
Fax: +27 (0)11 236 19 13

SPAIN

E-08014 Barcelona
c/Tarragona 149 - 157 Planta 19 1º
Phone: +34 93 473 32 00
Fax: +34 93 473 63 89

E-39005 Santander (Cantabria)

Racing nº 5 bajo
Phone: +34 94 223 67 55
Phone: +34 94 237 45 81

E-28760 Tres Cantos (Madrid)

Centro Empresarial Euronova
C/Ronda de Poniente, 4
Phone: +34 91 804 32 56
Fax: +34 91 804 41 03

SWEDEN

S-191 62 Sollentuna
Glimmervägen 14, 7 tr
Phone: +46 (0)859 47 02 30
Fax: +46 (0)859 47 02 31

SWITZERLAND

CH-8953 Dietikon
Bernstrasse 394
Phone: +41 (0)44 745 61 61
Fax: +41 (0)44 745 61 00

CH-1010 Lausanne

Av. des Boveresses 52
Phone: +41 (0)216 54 01 01
Fax: +41 (0)216 54 01 00

TURKEY

Canan Residence
Hendem Cad. No: 54 Ofis A2
Serifali Umraniye Istanbul
34775 Türkiye
Phone: +90 (0)216 52 88 310
Fax: +90 (0)216 52 88 311

UKRAINE

UA-03040 Kiev
Vasilovskaya str. 14
off. 422-423
Phone: +380 44 496 22 26
Fax: +380 44 496 22 27

UNITED KINGDOM

South East
2, The Switchback
Gardner Road
Maidenhead
Berkshire, SL6 7RJ
Phone: +44 (0)16 28 77 85 56
Fax: +44 (0)16 28 78 38 11

South West & Wales

12 Interface Business Park
Bincknoll Lane
Royal Wootton Bassett
Wiltshire, SN4 8SY
Phone: +44 (0)17 93 84 99 33
Fax: +44 (0)17 93 85 95 55

North

Manchester International
Office Centre, Suite 3E (MIOC)
Styal Road

Manchester, M22 5WB
Phone: +44 (0)16 14 99 34 34
Fax: +44 (0)16 14 99 34 74

Scotland

1st Floor
180 St. Vincent Street
Glasgow, G2 5SG
Phone: +44 (0)141 242 4820
Fax: +44 (0)141 221 1916

