Security Aspects

White Paper on How to Make State of the Art Electronic Designs
Committed to excellence

Content

General Data Protection Regulation ........................................... 4
Cryptography in a Nutshell ....................................................... 6
Encryption Technologies – The Key to Security ...................... 8
Security ICs ........................................................................... 12
Wireless Data Transport ......................................................... 16
   WiFi ............................................................................. 22
   Bluetooth EDR vs. Bluetooth LE vs. Bluetooth 5 .......... 24
   Bluetooth Mesh Networking .............................................. 26
   Thread vs. Zigbee vs. other 2.4 GHz Mesh Solutions ........ 28
   Security at Cellular Wireless Technologies ..................... 30
Data Storage ........................................................................... 32
   Silent Data Corruption – The Neglected Hazard .......... 32
   Intel’s Security Solutions – Designing for Data Integrity .. 34
   RAID – Redundant Array of Independent Disks ............ 35
   ECC – Error Correction Code ........................................... 35
   What Needs to be Borne in Mind when Selecting Security Media? 36
   Apcare’s Security Solutions .............................................. 38
   Swissbit’s Security Solutions ............................................. 40
   Transcend’s Hardware-based AES Solution .................... 42
   Seagate’s Security Solutions ............................................. 45
Data Processing ....................................................................... 46
   Central Processing Unit Security ...................................... 46
   Security on ARM Based Embedded Boards .................. 58
   Security Features on Standard x86 Based Boards ........... 60
   Secure Software Solution from Advantech, Acronis, McAfee .. 64
   Advantech Complete Bundle Solution – SUSI .................. 67
   Secure Power Supply ....................................................... 68
   The Defenses of the Standard Microcontroller ............... 70
   Security in General Purpose Microcontrollers ............... 72
   Security of Automotive MCUs ......................................... 78
   Security of In-Circuit-Programmer for Off-Site Production ... 84
   IoT Connected Applications with Speakers .................... 86
Social Engineering ................................................................... 88
   Avoiding Visual and Printed Spy on Displays, Keyboards and Number Pads 88
   RUTRONIK EMBEDDED .................................................. 93
   Secure Entry Systems .................................................... 94

Our Product Portfolio

Semiconductors ................................................................. Boards & Systems
Passive Components .......................................................... Storage Technologies
Electronic Components .................................................... Wireless Technologies
Displays & Monitors ...........................................................

Our Innovation Centers

RUTRONIK AUTOMOTIVE RUTRONIK EMBEDDED RUTRONIK POWER RUTRONIK SMART

Follow us

www.facebook.com/rutronik
https://twitter.com/Rutronik
https://youtube.com/user/Rutronik24
www.linkedin.com/company/rutronik
Get Your Rutronik App

www.rutronik玩家们.com

Committed to excellence

Consult – Know-how. Built-in.
The Technical Competence from RUTRONIK

Worldwide and individual consulting on the spot: by competent sales staff, application engineers and product specialists.

The Product Portfolio from RUTRONIK

Wide product range of semiconductors, passive and electromechanical components, displays & monitors, boards & systems, storage and wireless technologies for optimum coverage of your needs.

The Delivery Service from RUTRONIK

Innovative and flexible solutions: from supply chain management to individual logistics systems.

Quality Management without Compromise

The integrated management system (IMS) encompasses quality control, environmental protection and occupational health and safety.

One Leak in Security Could be One Leak Too Much

Adding security to a device costs extra money, time, power consumption and makes everything worse. The only reason for adding security to a device is the need to improve marketing – security components help to sell more products. To participate in the evolution of Industry 4.0, the Internet of Things and cloud technologies to make devices, portfolios and your ecosystem smarter, you have to start thinking about security in another way.

If your products are connected, they are the perfect target to destroy your company’s reputation. If your products do not fulfill the requirements of the European General Data Protection Regulation (GDPR), the impending fine could make your company going bankrupt.

The battle between companies will start in the second half of 2018 and we expect a wave of legal actions. Last but not least: if a third party gets control over your products, a damage of life and goods could be the result.

As the leading high tech distributor we decided not to build a single security division. We think it’s not the right way to have a security specialist on board who is managing the security semiconductors and helping our customers from all over the world if they have need for adding a security solution.

We believe that security will be mandatory for the complete design, in all layers, regarding data transmission, data processing and data storage. It affects hardware, software and virtual services. Having in mind that one leak, one little mistake, one delay of making an update could destroy human life, causing a commercial collision and destroy your business from one moment to the next. We take security very seriously and added this way of thinking to all our product managers in all product divisions.

When it comes to security, there is no one-size-fits-all solution. Thorough risk analyses have to be carried out to identify the specific threats to individual systems. In most cases, secure identities are exposed to a high level of threat as they are used to protect know-how and intellectual property, safeguard the integrity of systems and protect stored data and data distributed over networks.

If you thought SECURITY is only useful for marketing reasons, then we hope that this security brochure will change your point of view. It should make you aware about some more aspects and motivate you to make contact with us to talk about your individual needs and tailored solutions.

Enjoy reading and discover new aspects of security!
General Data Protection Regulation

If you want to sell your electronic products within the European Union, you should be aware of this new law about the protection of personal data. This law is already valid and will be mandatory to follow from May 2018 onwards. It is important to know that some courts of justice have already issued judgments regarding the definition of personal data.

For example all data which enters or leaves the motor control box of a car and the levels of all operating fluids are defined as personal data – even though they are indirectly personal and do not clearly belong to a specific person. In addition the meaning of “state of the art” was defined by the German Federal Office for Information Security (BSI) as the best available technology or products to satisfy the requirements of the law. We recommend reading the complete GDPR, but here are some quotes as extracts:

Article 25 — Data Protection by Design and by Default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.

Article 32 – Security of Processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
   a) the pseudonymisation and encryption of personal data;
   b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 83 – General Conditions for Imposing Administrative fines

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
   a) the obligations of the controller and the processor pursuant to Articles ... 25, ...32, ...;

How to Protect Your Business

The effects of this law for your electronic product design are hard to predict. We recommend using the most secure components to avoid getting accused by your competitors later on. Some aspects about how to choose the right technologies to be on the safe side (as best as possible by today) can be found on the next pages.
Cryptography in a Nutshell

The Kerckhoffs’ Principle
In cryptography, Kerckhoffs’ principle (also called Kerckhoff’s desideratum, Kerckhoff’s assumption, axiom, or law) has already been stated by Dutch cryptographer Auguste Kerckhoffs in the year 1883 and is still valid:

- A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.
  - It is much more difficult to keep an algorithm secret than a key.
  - It is more difficult to replace one compromised algorithm with another than a compromised key.
  - Secret algorithms can be reconstructed by reverse engineering from software or hardware implementations.
  - It is easier to hide a backdoor in “secret” encryption methods.
  - Bugs in public algorithms are more easily discovered when as many people as possible deal with them.

This principle is used in all relevant cryptographic methods – independent if they are symmetric, asymmetric or hybrid.

Most Popular Cryptographic Algorithms

Symmetric Cryptographic Algorithms
- Encryption and decryption with one single key (Secret-Key-Cryptography)
- Key must be present during encryption and decryption
- Key must be exchanged in advance (side channel)
- Keys must be stored safe
- 128 bit keys are considered as safe, 256 bit is considered as future proof
- Fast encryption method
- Examples of algorithms: AES, Rijndael, Blowfish, RC4/5/5a/6, 3DES, DES, A5, CAST, IDEA
- Examples of applications: WPA2 (IEEE802.11), IPsec-VPN, OpenSSL

Asymmetric Cryptographic Algorithms
- Encryption and decryption with different keys (Public-Key-Cryptography)
- Generation of a pair of keys (private key and public key)
- Private key does not need to be exchanged
- Encrypt data with public key, decrypt data with private key
- Sign data with private key, check signature with public key
- Based on one-way function
- Trapdoor function (easy to compute in one direction, yet difficult to compute in the opposite direction as long as no “Trapdoor” information is known)
- Potential attack by reversing the one-way function (not by trying to find out the key)
- Only 2048 Bit Keys (RSA) or 256 Bit keys (ECC) considered to be sufficient
- Slow encryption method (RSA is approximately 1000 times slower than symmetric encryption like AES)

Hash Cryptographic Algorithms
- The algorithm uses the net data to calculate a fixed size of another data packet, called hash value (128 bit to 512 bit are usual)
- The hash value is always unique. The algorithm will not create the same hash value when another data source is used
- It’s not possible to calculate the net data when only having the hash file
- Examples of algorithms: SHA, CRC, MD4, MD5, MD2, Tiger, RIPEMD
- Examples of applications: testing the integrity of files, making passwords more secure, creation of digital signatures and it’s also part of asymmetric algorithms

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are both hybrid encryption protocols for a safe and secure data transfer via the internet. SSL was the former protocol. After SSL 3.0, TLS 1.0 followed as successor. (TLS 1.0 is sometimes also known as SSL 3.1.) Currently the latest standard is TLS 1.3.

SSL and TLS have basically two tasks. The first is to guarantee the reliability of the connected server through a certificate. The second is an encrypted data exchange between client and server.

Hybrid Cryptographic Algorithms
- A hybrid algorithm uses asymmetric session key creation algorithms, but a symmetric algorithm to encrypt the data.
- At the end it’s a compromise using the biggest advantage of both methods
- Examples of algorithms: SSL, TLS
- Examples of applications: very often used to protect internet sessions. The SSL/TLS is used on top of TCP/IP, but below the application layer for websites, E-Mail or file transfer
- Very often the application protocol is renamed when it’s based on a cryptographic protected session – for example HTTPS is the encrypted version of HTTP
Encryption Technologies
The Key to Security

In order to understand encryption, it is helpful to consider what its aims are. These are focused on three key areas: authenticity, confidentiality, integrity. When a user wirelessly connects multiple products in his home, for example, it is important that only authorized products can join the network, and that both the data in the network and the complete system are protected.

That is to say, protection must be in place against unauthorized access to the network (authenticity), data tapping (confidentiality) and manipulation (integrity). State-of-the-art cryptography covers all three aspects. It is available in two fundamentally different modes: symmetric and asymmetric encryption.

**Symmetric Encryption**

In symmetric encryption, the same key is used for both encryption and decryption. The best-known and most frequently used encryption method is AES (Advanced Encryption Standard). AES works with either 128, 192 or 256 bit keys. Even 128 bit AES keys are classed as secure according to the current state of the art.

It is noteworthy that the principle of modern cryptography formulated by Auguste Kerckhoffs in 1883 still holds true: The security of an encryption method is founded on the secrecy of the key and not on the secrecy of the algorithm. This is particularly important in relation to a symmetric encryption method such as AES, as the same key is used on both ends (encryption and decryption). If the key is known, or is disclosed, the entire encryption process is nullified.

Consequently, the greatest challenge of AES lies in the management of the keys. In this, above all it must be ensured that the keys are generated using a genuine random generator; that they are deposited in a secure element; and that they cannot be intercepted the first time they are transferred.

**Asymmetric Encryption**

Asymmetric encryption always uses two different keys: a private key and a public key. They are always generated as a pair. The private key remains permanently with the originator of the keys, while the public key goes to the receiving party. The recipient can use the public key to encrypt messages which can only be decrypted with the linked private key. The private key can also generate a signature by which the recipient can uniquely identify the sender using the linked public key.

Asymmetric encryption is based on one-way mathematical functions. They must be as simple as possible to calculate, but very complex to reverse. Continually increasing computing power is also steadily improving the ability of computers to calculate complex reversing functions. To ensure adequate security, the keys therefore must have a certain length. Keys with 2048 bits, such as RSA 2048, are currently classed as secure. Because encryption and decryption speeds decrease as keys get longer, asymmetric methods are only practical for handling small amounts of data.

**Elliptic Curves for More Speed**

An alternative to this conventional asymmetric encryption is Elliptic Curve Cryptography (ECC). It is based on the same approach, but utilizes points on elliptic curves. That makes computing operations much more complex, so ensuring that even 256 bit keys offer a secure level according to the current state of the art. And ECC 256 does not take much more time than comparably secure symmetric methods.

**Security Is Always a System**

The issue of security is often neglected in relation to embedded systems especially. The result: Industrial spies can use hacked devices to penetrate the entire corporate network, gain access to the company’s intellectual property (IP) and business secrets, and manipulate data. Users of smart home devices might unintentionally disclose information to potential thieves through their security cameras, or even open doors and windows for them by way of automated control systems. Automobiles are also subject to multiple products in his home, for example, it is important that only authorized products can join the network, and that both the data in the network and the complete system are protected.

That is to say, protection must be in place against unauthorized access to the network (authenticity), data tapping (confidentiality) and manipulation (integrity). State-of-the-art cryptography covers all three aspects. It is available in two fundamentally different modes: symmetric and asymmetric encryption.

**Symmetric Encryption**

In symmetric encryption, the same key is used for both encryption and decryption. The best-known and most frequently used encryption method is AES (Advanced Encryption Standard). AES works with either 128, 192 or 256 bit keys. Even 128 bit AES keys are classed as secure according to the current state of the art.

It is noteworthy that the principle of modern cryptography formulated by Auguste Kerckhoffs in 1883 still holds true: The security of an encryption method is founded on the secrecy of the key and not on the secrecy of the algorithm. This is particularly important in relation to a symmetric encryption method such as AES, as the same key is used on both ends (encryption and decryption). If the key is known, or is disclosed, the entire encryption process is nullified.

Consequently, the greatest challenge of AES lies in the management of the keys. In this, above all it must be ensured that the keys are generated using a genuine random generator; that they are deposited in a secure element; and that they cannot be intercepted the first time they are transferred.

**Asymmetric Encryption**

Asymmetric encryption always uses two different keys: a private key and a public key. They are always generated as a pair. The private key remains permanently with the originator of the keys, while the public key goes to the receiving party. The recipient can use the public key to encrypt messages which can only be decrypted with the linked private key. The private key can also generate a signature by which the recipient can uniquely identify the sender using the linked public key.

Asymmetric encryption is based on one-way mathematical functions. They must be as simple as possible to calculate, but very complex to reverse. Continually increasing computing power is also steadily improving the ability of computers to calculate complex reversing functions. To ensure adequate security, the keys therefore must have a certain length. Keys with 2048 bits, such as RSA 2048, are currently classed as secure. Because encryption and decryption speeds decrease as keys get longer, asymmetric methods are only practical for handling small amounts of data.

**Elliptic Curves for More Speed**

An alternative to this conventional asymmetric encryption is Elliptic Curve Cryptography (ECC). It is based on the same approach, but utilizes points on elliptic curves. That makes computing operations much more complex, so ensuring that even 256 bit keys offer a secure level according to the current state of the art. And ECC 256 does not take much more time than comparably secure symmetric methods.
Encryption Technologies
The Key to Security

Hybrid Encryption Eliminates Disadvantages
If symmetric encryption of user data is chosen, but the security it offers is not adequate, it can be improved by means of hybrid encryption. In this, the symmetric key is sent again in encrypted form by means of an asymmetric public key. This means only the authorized recipient is able to decrypt the symmetric key with the matching private key.

At the same time, the sender of the symmetric key can use his private key to generate a signature which enables the recipient to uniquely identify him using the matching public key. Once these keys have been exchanged and decrypted, the foundation has been laid for symmetrically encrypted communications.

This combination method eliminates the disadvantages of the two separate methods – namely the insecure key transfer of symmetric encryption and the slower speed of asymmetric encryption.

Hardware or Software?
Each encryption method can be implemented by software or hardware. Software-based encryption entails the major disadvantage that the program is not an autonomous self-contained unit, but is always dependent on its environment, such as the operating system. It is susceptible to errors and attacks as a result. And there is another negative: As the microcontroller or processor of an embedded system additionally has to handle the complex encryption and decryption, loss of performance is inevitable.

The opposite case is represented by encryption using specially developed ICs. Their sole function is encryption, so there is no performance loss. Many encryption ICs are additionally protected against physical attacks. The security of those components – and also of the keys – is thus independent of the security of the overall system.

Encryption ICs in different designs meet the requirements of a range of applications: Simple authentication chips, such as from the Infineon Optiga Trust series, use asymmetric encryption (ECC 163), and are good choice for the authentication of original accessories in consumer electronics for example. The Optiga Trust E series with ECC 256 and SHA 256 assures authentication of medical equipment, in smart homes, in industry, or in cloud computing. In this context, the authentication for license management for example.

The Optiga Trust P series with ECC 521 and RSA 2048 features a Java-based operating system, in which dedicated applets can be programmed. The STSAFE (ECC 384, SHA 384, AES 256) products from STMicroelectronics also offer the highest protection, based – among other features – on secure authentication, encrypted communications, secure depositing of keys, and protection when running firmware updates.

Standardized Trusted Platform Modules (TPMs) combine highly complex encryption and secure depositing of large numbers of keys and signatures with protection against physical readout of the data stored in them. They are offered by Infineon for example.

Encrypted Smart Home
A simple practical example illustrates the use of encryption ICs: In a smart home, simple authentication chips such as the Optiga Trust SLS ensure that only authorized devices – such as shutter controls or surveillance cameras installed by the user – are able to log in to the central smart home gateway.

An STSAFE Secure microcontroller encrypts the communications between the cameras and the central gateway. A TPM in the central gateway assures key storage, firmware updates, and the transfer of all data to the Cloud. As a result, the homeowner can be certain that authenticity, confidentiality and integrity are assured.

ST offers the security you need to protect your application
ST provides customers and partners with a broad portfolio of security building blocks, to help protect everything from branded products and intellectual property to manufacturing processes, production equipment and access control in the workplace.

ST offers security solutions that are adapted to the needs of your application, covering all market needs with a range of flexible and scalable secure solutions.

STM32 family of general-purpose microcontrollers with advanced security features:
• Security monitoring and services isolation
• Secure firmware upgrade
• Cryptographic accelerators for selected families
• HW independent cryptographic libraries

STSAFE secure elements, connected to general purpose MPU and designed to ensure strong secure key storage, device identity, system and network integrity:
• Authentication
• Secure connection establishment
• Secure storage
• Certified & tamper resistant
• LPWAN secure connection & keys distribution

www.st.com/stm32 www.st.com/stsafe
Have you ever thought about if your secret keys are stored/hidden safe enough? Attackers could easily gain access to valuable software code, key material or sensitive data. If you are using so far just a common MCU or module with no special hardware crypto functions, anybody could hire a company like Circuit Engineering Company Limited or Mikatech Innovative Limited to get your software knowledge or the data stored inside. Already the name of their homepages “ic-cracker.com” or “break-ic.com” gives a hint in what kind of business they are working.

What if Your Secure System was Designed from Insecure Components?

In the end, the overall security of your system is determined by the weakest link. Even if you implement a protocol which is probably secured, your system could be broken if the key can be easily extracted from the hardware by simple physical attacks.

Therefore, if you do not already use a Security MCU, we recommend to integrate a hardware Crypto IC into your design. The purpose of a hardware security IC is to act as the keystone of a security subsystem, eliminating the need to protect the rest of the system with hardware or software security measures.

A crypto and authentication IC keeps your secret keys hidden against attacks. They are tamper-resistant and hardened against physical attacks through different measures like an active shielding, randomized layout and mechanisms which force to stop operation if they detect abnormal conditions. They can furthermore be used as brand protection and enable secured boot and secured DFU (Device Firmware Update).

An opponent with unlimited resources in terms of time, equipment and knowledge can even break any chip protection. The question is how practical it would be. If it takes too much time and financial resources well beyond the expected gain, then your defense has won. IC attackers would most probably switch to other products rather than spending time and money on breaking your IC.

So if you want to be on the safe side, think about integrating a security hardware IC, so you have a comprehensively secured system/product. And last but not least, integrating a security IC means also that you do not have any performance losses as your microcontroller has to do the complex de- and encrypt tasks.
**Security ICs**

**STMicroelectronics STSAFE Embedded Security Solutions**

Running on a Common Criteria EAL5+ platform, STSAFE-A is a highly secure authentication solution whose security is certified by independent parties. Its command set is tailored to address strong authentication, establish a secure channel in the scope of a TLS session, verify signatures, and offer secure storage as well as decrement counters for usage monitoring. It is particularly well suited for applications heavily exposed to fraud and counterfeiting attacks, such as printers, game controllers, phone accessories, and Internet of Things networks and devices. By offering a complete solution ranging from an internally-developed secure operating system embedded in the security microcontroller, example code for integrating solutions in the applicative environment, and personalization services for storing confidential customer data in the secure microcontroller, ST offers seamless integration of security measures for customers who might not be experts in secure systems.

**Infineon OPTIGA™ Embedded Security Solutions**

Infineon OPTIGA™ embedded security solutions are scalable, easy-to-integrate security for your embedded project. The OPTIGA™ Trust family includes turnkey products for smaller platforms as well as programmable solutions, while OPTIGA™ TPM (Trusted Platform Module) products are ideal for embedded PC, mobile and computing applications. All OPTIGA™ TPM products comply with the Trusted Computing Group (TCG) standards.

The OPTIGA™ Trust product family offers a full range of security chips to address individual needs in the field of embedded authentication and brand protection and further security applications. Whether you are looking for a turnkey security chip enabling fast and easy integration or a feature-rich programmable solution, OPTIGA™ Trust has the perfect match for your business model.

OPTIGA™ TPM (Trusted Platform Module) offers a broad portfolio of standardized security controllers to protect the integrity and authenticity of embedded devices and systems. With a secured key store and support for a variety of encryption algorithms, OPTIGA™ TPM security chips provide robust protection for critical data and processes through their rich functionality.

**OPTIGA™ Embedded Security Family**

<table>
<thead>
<tr>
<th>Family</th>
<th>OPTIGA™ Trust B</th>
<th>OPTIGA™ Trust E</th>
<th>OPTIGA™ Trust A</th>
<th>OPTIGA™ Trust P</th>
<th>OPTIGA™ TPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>SLE 92150</td>
<td>SLS 32AW</td>
<td>SLS 32AW100</td>
<td>SLS 326CA031</td>
<td>SLS 326CA</td>
</tr>
<tr>
<td>Security Level</td>
<td>Basic</td>
<td>CC EAL 6+ *</td>
<td>CC EAL 6+ *</td>
<td>CC EAL 5+</td>
<td>CC EAL 4+</td>
</tr>
<tr>
<td>Functionality</td>
<td>Authentication</td>
<td>Authentication</td>
<td>Connected device security</td>
<td>Programmable</td>
<td>TCG standard</td>
</tr>
<tr>
<td>NVM (Data)</td>
<td>448 Byte</td>
<td>3 kByte</td>
<td>10 kByte</td>
<td>150 kByte **</td>
<td>64 kByte</td>
</tr>
<tr>
<td>Cryptography – Private key stored in secure HRI</td>
<td>ECC163</td>
<td>ECC256</td>
<td>ECC284</td>
<td>ECC256</td>
<td>ECC256, RSA2K</td>
</tr>
<tr>
<td>Type of Host System</td>
<td>MCU without OS / proprietary OS / RTOS</td>
<td>Embedded Linux</td>
<td>Windows / Linux</td>
<td>Windows / Linux</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>SW</td>
<td>FC</td>
<td>FC</td>
<td>UART</td>
<td>UART, SPI, LPC</td>
</tr>
<tr>
<td>System Integration</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Platform vendor</td>
</tr>
</tbody>
</table>

* Based on certified HRI  ** Code & Data  Done by IFX  Customer Implementation, support by IFX  ** Launch Q1/2018

**The right security for IoT**

Protect your embedded project with the OPTIGA™ product family

Security is more than data protection – in many cases, security measures also enable new business models and services such as remote feature management. However, performance and security requirements vary considerably from one embedded project to another.

To reflect this diversity, our proven OPTIGA™ product family allows you to match security functionality to your specific application needs. Designed for ease of integration, this proven, scalable family ranges from authentication solutions (OPTIGA™ Trust family) to advanced implementations based on our Trusted Platform Modules (OPTIGA™ TPM).

Check out our OPTIGA™ product family and make your embedded solution a secured success: www.infineon.com/iot-security

**Rutronik can offer Infineon OPTIGA™ solutions as a chip to make your own embedded system build on your own PCB, as well as offering ready to use embedded boards and standard mainboards with already having Infineon OPTIGA™ technology on board.**

**Infineon OPTIGA™ Embedded Security Solutions**

Infineon OPTIGA™ embedded security solutions are scalable, easy-to-integrate security for your embedded project. The OPTIGA™ Trust family includes turnkey products for smaller platforms as well as programmable solutions, while OPTIGA™ TPM (Trusted Platform Module) products are ideal for embedded PC, mobile and computing applications. All OPTIGA™ TPM products comply with the Trusted Computing Group (TCG) standards.

The OPTIGA™ Trust product family offers a full range of security chips to address individual needs in the field of embedded authentication and brand protection and further security applications. Whether you are looking for a turnkey security chip enabling fast and easy integration or a feature-rich programmable solution, OPTIGA™ Trust has the perfect match for your business model.

OPTIGA™ TPM (Trusted Platform Module) offers a broad portfolio of standardized security controllers to protect the integrity and authenticity of embedded devices and systems. With a secured key store and support for a variety of encryption algorithms, OPTIGA™ TPM security chips provide robust protection for critical data and processes through their rich functionality.
Wireless Data Transport

Wireless communication is used nowadays in many different applications, accepted by users, and trusted as a secure way of communication. Security risks like cable breaks, cable oxidation, loose connection, cable fire, theft of copper cable, vandalism or reconnection and monitoring a communication are more unlikely than at wired solutions. Nevertheless there are still some security aspects of different wireless technologies which should be known.

Jamming Detection
Jamming devices could be found in dark market places and they could be made by you easily. A jamming device is transmitting random codes with as much power as possible on the same frequency spectrum of the wireless connection which should be disturbed. The use of a jamming device is forbidden in most cases. It could be used to avoid closing a car on the supermarket parking lot or to disturb the alarm system of a house. For security reasons you should make sure that the transmission of the data was successful. Therefore you should implement an acknowledgement feature in your communication process. Further there are wireless products available in the market, which have already an implemented jamming detection feature. All cellular and GNSS modules (GPRS, UMTS, LTE, etc.) from the manufacturer Telit have this feature. In the case of detecting a jamming signal which prevents the connection to the mobile network operator base station, the modules are able to react locally with emergency measures.

Unidirectional vs. Bidirectional
Unidirectional and bidirectional describe the way two electronic devices communicate. Unidirectional means that there is only one receiver on one side and a transmitter on the other. A typical example is a car key. The car key is able to send the orders Open/Close etc. so the car receives the information, but there is no communication from the car towards the key to tell e.g. that the command has been received. Another example is the radio broadcast: on one side you have the speaker as a transmitter and on the other the audience with their receivers. Bidirectional communication contains a receiver and transmitter on both sides – a so called transceiver. This configuration allows a duplex communication. There are three security reasons to use a bidirectional transceiver: after sending your data you can receive an acknowledgement data packet to make sure that your data has been received successfully. This ensures that your communication partner has been in range and no disturbances occurred. The second reason to use a transceiver is the possibility to exchange security keys in order to make sure that you are sending the data to the right subscriber. You can avoid man-in-the-middle attacks and you can establish an encrypted connection to avoid that anybody else can listen. The third reason is the already mentioned possibility to make jamming detection by using the receiver before transmitting data. Independent of the security aspects there are further advantages of using a transceiver, like adjusting the transmit power level to save energy and an automatic resend of data packets in case of reception problems.

General Security Strategy Regarding Frequencies and Protocols
Mobile network operators have bought own frequency ranges to offer GSM, LTE and other services to you. For all other kind of common used wireless technologies you will use licensed free and public available frequencies – so called ISM-bands (Industrial, Scientific, Medical Bands). Bluetooth, Wi-Fi, ZigBee, ANT, SigFox, LoRa, Thread, RFID, NFC and all the other known technologies are working within these frequency areas. The three most popular ISM-bands in Europe for standard applications are 433 MHz, 868 MHz and 2.4 GHz. You should be aware that the allowed transmission power, the available bandwidth and the allowed duty cycle are different and it has an impact to the security of your communication as well.

For example: the 868 MHz band has a bandwidth of 600 kHz, while the 2.4 GHz band has space for ca. 85 MHz. That means you can in general establish more data channels in parallel at 2.4 GHz, just for the case that some frequency areas are already used by others. The 868 MHz band has a more strict regulated duty cycle than the 433 MHz band. That means you have restrictions on the durations of sending data. On the one hand this could be a problem if your duty cycle capacity is already being used but you need to send another important data packet. If you think it would be better to use 433 MHz because of the missing restriction, then think about what could happen if you send this important further data packet when another application is already using this frequency channel all the time – for example a 433 MHz headphone system, which streams audio on this channel permanently. If you will use a popular wireless standard, many of these aspects have already been solved. 2.4 GHz technologies based on IEEE802.15.4 specification (like ZigBee, Thread and some others) are using 16 channels with 5 MHz modulation per channel. That makes them robust against small signal disturbances. Wi-Fi is using 20 MHz per channel, which is even more robust. Classic Bluetooth is using the same frequencies splitted into 79 channels with 1 MHz each. To make sure that the connection will be robust as well, it changes the used channel 1600 times per second. With this strategy Bluetooth makes sure not to stay on a busy channel. Bluetooth Low Energy doesn’t change the channel without having detected a disturbance, but it uses 2 MHz per channel as a compromise.

Conclusion: If you use a standardized wireless technology, like Bluetooth for example, you cannot choose the features by yourself and you have to trust the community. But if you want to create your own proprietary wireless technology, you should be aware about each of the seven layers of the ISO-OSI model in communication system. Our recommendation is to check the regulations at the ETSI website to be aware about the advantages and disadvantages of the different ISM-Bands. After this, you should look for established and proofed software from experienced specialists. In addition to the well-known wireless technologies, Rutronik can also help to get an overview of the features from protocols like RFDP4A, ShockBurst, WDP, Gazell, SNAP® or the smartphone supported ANT™ and ANT BLAZETM.
Wireless Data Transport

RFID and NFC

RFID transponders are available in different frequency ranges: Low frequency (LF, 125 kHz), high frequency (HF, 13.56 MHz) and ultra-high frequency (UHF, 868 MHz). UHF tags are often readable over distances of more than one meter and it is possible to detect hundreds of them at once. That is why this technology is often used for car windshields or logistic applications. The reading range of HF transponders is usually only a few centimeters.

That makes this technology perfect for security applications like payment or to identify individuals. NFC uses specialized protocols, but is based on HF RFID as well. A RFID transponder is a memory that gets the energy for reading and writing from the electromagnetic field. The memory contains two main areas: one area contains a unique identification number (UID). This 64-bit code is only available once in the world. It was defined and programmed by the creation of the silicon and it cannot be changed or erased. The UID code is often used for products to identify if a device is an original device or not. You can also link the set of a database to a specific UID code, like the personal number of an employee or the name of a team member.

The second area inside the memory can be programmed by the user. It can be used to save non static information, like the data of the last inspection, who conducted the inspection, and other useful information. In some RFID transponders this memory area can be split into sub-areas. Each of these sub-areas can be individually protected by different codes to protect it against unwanted reading and/or writing.

A further variant of RFID transponders are the dual interface memories. Dual interface means the wireless interface (to connect the antenna directly) and a second interface to connect a microcontroller. The interface to connect a microcontroller can be I²C or SPI, depending on the product. Also the memory size, the memory technology (EEPROM or FeRAM) and the supported protocols (ISO15693, ISO14443A/B, ISO18092, etc) could be chosen differently.

A dual interface RFID transponder allows programming the memory without having powered the microcontroller. After powering the microcontroller, it can read inside the memory what has happened while it was sleeping.

For example, the STMicroelectronics M24LR04E-R provides a special protection mechanism based on passwords. In RF mode, each memory sector of the M24LR04E-R can be individually protected by one out of three available passwords, and each sector can also have read/write access conditions set.

Rutronik offers RFID/NFC solutions from STMicroelectronics, Fujitsu, Panasonic, Murata, Toshiba and Melexis. As an example, ST provides an exhaustive offer of NFC products and solutions including ST21NFC state-of-the-art Controller and ST54 System in Package, integrating the widely deployed ST33 Secure Element, to address secure mobile transaction applications. It’s already pre-certified for most of payment and transit schemes including EMVCo, PBOC, Visa, MC, Amex, Discover, and MIFARE® allowing customers to easily and quickly ensure security in mobile transactions. Therefore a complete development ecosystem is available including reference designs, expansion boards, pre-certification services and integration into the most popular TSMs to help reduce the time to market as well as development costs.
Wireless Data Transport

Wireless SoCs and Wireless SoMs
It has become very popular during the last years to use System-on-Chips or System-on-Modules with an integrated wireless transceiver.

The reason is, that the supplier of these components has full control about the microcontroller, the peripherals, the memory, the wireless transmitter and wireless receiver blocks and in case of a module also regarding the antenna performance. As a result the supplier can offer wireless protocols tailored for his own chip. The customer doesn’t need to take care to adapt the software to hardware, because it was already developed for this setup.

Rutronik can offer Wireless-SoCs from Nordic Semiconductor, Renesas, Infineon, Toshiba and ST. Equivalent modules, including antenna, crystals, pre-certifications etc., are available from Telit, InsightSiP, Dynastream, Fujitsu, Redpine Signals and RF Digital.

There are solutions available with 8 bit, 16 bit and 32 bit MCU, different memory sizes, USB, ADC, NFC, Sub-GHz, 2.4 GHz and a lot of other features you can choose of.

Taking an example: For the SoC named nRF52840 and its 3rd party module variants, there are free wireless stacks available, like Thread (IPv6 based home automation), Gazell (open source star network), ANT (lowest power mesh network), Bluetooth Mesh, Bluetooth 5 (including high speed and long range modes) and a lot of other features you can choose of.

ARM-CryptoCell-310 is an integrated security core that consists of both HW and SW components. It provides a comprehensive security infrastructure that enables system wide protection that includes use cases inside and outside the device.

It has a cryptographic hardware engine, providing CPU host offloading, operation acceleration and power consumption reduction.

Security is a paramount consideration for the design of connectable IoT devices today and in the future. Security must be a design consideration from the ground up in any truly secure application.

Algorithm Family | Identification Code
---|---
Stream Cipher | Cha Cha
MAC | Poly 1305
Key agreement | SBP
AES | FPS107
NIST SP 800-38A
NIST SP 800-38B
NIST SP 800-38C
ISO/IEC 9791
Hash | FPS180-3
RSA | RFC2104
Diffie-Hellman | ANSI X9.42
ECC | ANSI X9.63
IEEE 1363
ANS X9.62
Ed25519
Curve25519
FIPS-1864
NIST SP 800-56A rev.2
NIST 800-90B3
AIS-31 (Class “P2 High”)
PRNG | AIS-20 (Class “A4 high”)
TRNG | ANSI X9.83
General | FIPS 140-2
PrNG

There are cryptography and security services available. Platform Security Library and Device Lifecycle is available, as well as a management infrastructure and a Secure Boot to avoid load-codes at startup.

So the CryptoCell-310 Nordic Semiconductor multi-layered product, hardware security and a middleware building blocks State management Key Management function called dangerous inside the nRF52840 is a consisting of a infrastructure, layer on top of it.
There are two versions of WPA2: WPA2 Enterprise Security and WPA2 Personal. Both use a strong encryption method called AES-CCMP to encrypt data transmitted over the air. The main difference between these security modes is in the authentication stage: While WPA2 Personal uses pre-shared keys (PSK), WPA2 Enterprise uses IEEE 802.1X. The WPA2 protocol is only securing traffic from device to the access point, not form device to end device. To avoid this problem there is the option of using a VPN tunnel, which provides a secure point-to-point connection across the internet on the lower communication layer (independent of the applications on higher layers in use).

**WPA2 Enterprise Security**
WPA2 Enterprise uses IEEE 802.1X authentication and is currently the most robust authentication for WLAN. It is specifically designed for the use in large organizations with many Access Points, for example hospitals or universities. It requires a RADIUS authentication server and needs a username and password. It also supports multiple accounts for each user. For both encryption and decryption the same key is used within the AES block cipher, which has a length of 128 bit. There are four stages included for one round in AES encryption, that's why it's often also called four-way handshake.

**WPA2 Personal / WPA2 PSK**
WPA2 Personal uses pre-shared keys (PSK) and is designed for small networks like for example home use. A PSK is a secret alphanumeric string associated to the Access Point (AP). The communication between the Station and the Access Point is encrypted by AES cipher with a 256 bit symmetric key. It only uses one single password/key which is generated at every session and is the most used Wi-Fi security standard. Like in WPA2 Enterprise Security, the protocol used to derive the key is called four-way handshake. The alternative cryptographic method WEPI is not secure and should not be used any more. The predecessor WPA is considered as secure, but shouldn't be used because WPA2 is qualified as even more secure.

**Examples of Secure Wi-Fi Solutions**
Some Wi-Fi examples of our portfolio with embedded security:

**ST Microelectronics SPWF04**
The SPWF04S from ST is a standalone 2.4 GHz 802.11 b/g/n Wi-Fi transceiver module. It includes the common encryption algorithms AES (128 bit & 256 bit) and hash (MD5, SHA-1 & SHA-256), as well as the public key algorithm RSA. Furthermore it supports the security protocols WEP, WPA2 Personal and WPA2 Enterprise.

**Telti GS2011, GS2101, GS2200**
The GainSpan Wi-Fi modules from Telti are based on the GainSpan SoC GS2000. It contains the security protocols WPA2 Personal and WPA2 Enterprise and uses TKIP and AES encryption. Upper layer encryption includes TLS, SSL, HTTP, PKI and digital certificates.

**Redpine Signals Wi-Fi Modules and Combined Technology Modules**
Connect-in-oTM Family modules are ready to use Wi-Fi modules, optionally having Bluetooth and ZigBee integrated as well. WEP, WPA and WPA2 are onboard, as well as HTTPPS, SSL 3.0, TLS 1.2 and the possibility to make wireless firmware updates. WiSeConnect™ Family are supporting Enterprise Security (EAP-TLS, EAP-FAST, EAP-TTLS, EAP-PEAP) on top of the features of Connect-in-oTM. The n-Link™ family offers WPA2 and Enterprise Security featured on the external host system. Software stacks are available for Linux, Android, WinCE7, WEC2013, Windows 7, Windows 10 and Windows IoT.

Further stand-alone solutions with WPA2 Personal are offered by Panasonic and Silex. Advantech, Silex and Intel are offering solutions with standard interfaces to run also Enterprise Security on the host system.

**SSID and WPS**
Most people would recommend hiding the SSID (Service Set Identifier - the name of the WLAN network) to prevent connection attempts from others. But this method is useless: when connecting to your own WLAN network / SSID, your device sends out signals containing the SSID name not crypted, so everybody in the network can sniff it anyway. A disadvantage would be the higher power consumption for all Wi-Fi nodes scanning for available Wi-Fi networks. We recommend to do it in the opposite way: use the administrators e-mail address as name for your network.

Then everybody could contact you if there is a topic on frequency management (channel adaption) or if somebody wants to ask to get the network key or adding his device to the whitelist of MAC addresses.

The feature Wi-Fi Protected Setup (WPS) was made to connect devices more easily to an access point. The WPS will exchange the WPA2 key by only using a four digit pin code, for example. This makes it much more easy to hack a WPS enabled router.

The connection will be jammed until it breaks. At the try of a reconnect there will be a fake access point offering the same SSID and WPS service. The records of the WPS procedure will be used to attack the original access point, similar to a man-in-the-middle attack. The leak was possible because the pin code was linked to the MAC address of the routers. At new routers this bug was solved. Anyway, using WPS is always more comfortable by losing some levels of security.

In general, we recommend to use the MAC filter of your access point to allow only listed devices to join your network. Use long WPA2 keys and they shouldn’t contain words of a dictionary. Check available firmware updates frequently. Disable WPS and don’t hide your SSID. Use the channels 1,6 and 11 only: These are non-overlapping. All other channels would not allow to establish three Wi-Fi networks in parallel without having double used frequency blocks. This would make at least two networks slower, because more resent packages will be necessary.
Wireless Data Transport

Bluetooth EDR vs. Bluetooth LE vs. Bluetooth 5

Bluetooth (IEEE 802.15.1) is the most used wireless standard in the 2.4 GHz ISM band. It is good for the exchange of data over short distances. Within this technology you can mainly differentiate between Bluetooth Classic (EDR) and Bluetooth Low Energy (BLE). Bluetooth 5, which was published lately, is an enhancement of Bluetooth Low Energy mainly adding modes for longer range or higher speed.

Bluetooth Classic (EDR – Enhanced Data Rate)

Bluetooth EDR is using between 21 and 79 channels depending on how much Wi-Fi networks (interferences) are detected. Each channel has a bandwidth of 1 MHz and the channels are changed 1600 times per second – always and permanently. It has Adaptive Frequency Hopping (AFH), Forward Error Correction (FEC) and a 128 bit AES-encryption.

Adaptive Frequency Hopping (AFH) is a technology that comes into action, when Bluetooth and Wi-Fi (both using the unlicensed 2.4 GHz ISM band) are competing in the same frequency band and therefore interfering each other. AFH detects these interferences and then excludes these blocked channels. At least 21 channels (21 MHz) will be used and still could influence a Wi-Fi network.

The Forward Error Correction (FEC) is a method which enables a receiver to detect and also correct errors in transmitted data. Bluetooth is still considered as secure because of the AES-128 coding.

Bluetooth Low Energy (BLE)

Bluetooth Low Energy is transmitting single data telegrams and has quick connecting times. It’s extremely energy saving and therefore perfectly for applications which for example only need to send a signal every few minutes. Like Bluetooth Classic, it is using Adaptive Frequency Hopping (AFH) and Forward Error Correction (FEC).

Each channel has a bandwidth of 2 MHz, by having 37 channels for data exchange and 3 channels for advertising. The advertising channels are placed before Wi-Fi channel 1 starts, between channel 1 and 6, and the third BLE advertising channel is placed after Wi-Fi channel 11. A further difference between BLE and classic Bluetooth is that BLE is not changing the channels permanently. Only if disturbances are detected, the channel will be changed.

Bluetooth Low Energy supports the following security concepts:

- **Pairing**: Devices create one or more shared secret keys
- **Bonding**: The act of storing the keys created during pairing for use in subsequent connections; this forms a trusted device pair
- **Device authentication**: Verification that the paired devices have trusted keys
- **Encryption**: Scrambling of plaintext message data into cipher text data
- **Message integrity**: Protects against tampering with data

Since Bluetooth Low Energy Version 4.2 there is also an increased security support implemented: the numeric comparison method and the Elliptic Curve Diffie-Hellman (EDHC) algorithm. Also the fact that private keys are not shared over the air makes this version and successors secure against passive eavesdropping, as it’s difficult to encrypt the transmitted data without.

Bluetooth 5

Bluetooth 5 is an upgrading of Bluetooth Low Energy. It could have four times the range, two times speed and eight times data transmission, but still using low energy. That makes Bluetooth 5 an attractive alternative for many Wi-Fi IoT applications, but also easier for hackers to get the transmitted data from a bigger distance in a shorter time. Till now, Bluetooth 5 only offers device authentication, but no user authentication.

The most popular products to use Bluetooth technology are SoC or SoM components because of the complexity of the wireless stack and the fast ongoing evolution and available improvements tailored to dedicated host system. Please have a look to chapter “Wireless SoCs and SoMs” in this book.
Wireless Data Transport

Bluetooth Mesh Networking

In order to keep up with rival standards like Thread or ZigBee, Bluetooth SIG decided to launch a communication standard that allows a many-to-many (m:m) connection as well as connections between devices of different suppliers. Until July 2017, there was only a star network and point-to-point Bluetooth Low Energy connection possible.

Bluetooth mesh networking supports connections up to 32,000 nodes. With that, this network is much bigger than all other mesh networks and allows bigger distances. As many benefits and improvements m:m connection has, as many security risk this brings.

One main focus while developing Bluetooth mesh networking was therefore the question how to keep this technique secure. Important to know is, that all possible security features are subject to the decision of the product designer, he can decide which of them will be integrated.

The Most Important Security Features are:
- Authentication and encryption of all Bluetooth mesh messages
- Network, application and device security are addressed independently
- Subnets of the mesh network are distinct and secure form the others
- Key refresh procedures allow the change of the security key during lifetime of the network
- Bluetooth mesh security protects the network against replay attacks
- Secure removal of nodes from the network, so that trashcan attacks are prevented
- Secure adding of devices to the network to become nodes

Nordic Semiconductor provides a Software Development Kit (SDK) for any Bluetooth Mesh development – the nRF5 SDK. It is compatible to the nRF51 and nRF52 System on Chips and is perfect for the use in consumer, smart home and industrial applications.

Additionally to the Bluetooth mesh security features of the Bluetooth SIG, Bluetooth mesh devices of Nordic support a secure side-by-side and blocking device firmware updates. Next to that, a serial interface allows control of the mesh network.

DESIGN TRUSTWORTHY IoT APPLICATIONS WITH ROBUST LEVELS OF SECURITY

Designed to address the inherent security challenges that are faced in IoT, the nRF52840 advanced multi-protocol SoC (supporting Bluetooth 5, ANT, 802.15.4, and 2.4GHz proprietary) incorporates the ARM® CryptoCell-310 cryptographic accelerator offering best-in-class security for Cortex-M based SoCs.

ARM CryptoCell-310 is an integrated security core that consists of SW and HW accelerator for symmetric and asymmetric cryptography including NIST recommended standards for key exchange, hash generation and data encryption. It includes a FIPS compliant True Random Number Generator (TRNG) and implementations for Cha Cha, ECC (with multiple curves), AES, RSA, SHA and others.

The nRF52840 SoC also supports read/write/erase protection for memory that can be reserved for cryptographic keys. On-chip memory protection module is to protect stored bootloader code memory from flash write/erase.

Secure boot - Using a combination of HW supported cryptographic functions and memory protection, secure boot to establish a root of trust is able to be implemented.

Secure OTA DFU – Using a combination of on-chip security accelerators, memory protection features and bootloader SW implementations, Over-The-Air Device Firmware Update (OTA DFU) is supported for secure, authenticated deployment of firmware images.
Wireless Data Transport

Thread vs. ZigBee vs. Other 2.4 GHz Mesh Solutions

Further technologies are available to build up wireless mesh networks. Some protocols are based on top of the IEEE802.15.4 specification (PHY and MAC layer specification). The advantage is the possibility to change the transceiver from one supplier to another, so you are more independent than using a single source. The disadvantage is the specification itself. The DSSS modulation, having 5 MHz per channel and only 16 channels available is very often not the perfect choice for an application because it needs more energy and frequency resources than other modulation schemes. Also IEEE802.15.4 solutions are often based on SoCs instead of separated transceivers and microcontroller. In case of using a SoC, the advantage of being independent from a single source is not given.

**Thread**

Thread is based on IEEE 802.15.4. At the network and transport layers Thread uses a combination of IPv6, 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), UDP (User Datagram Protocol) and DTLS (Datagram Transport Layer Security).

The application layer can be defined individually. As it is using IPv6, Thread can be used to integrate home automation devices directly to the IoT, without the need of making any protocol and address conversion. IPv6 has a strong encryption and authentication mechanism integrated – the IPsec. Part of this security protocol is:

- Interoperability
- Cryptographic protection of the transmitted data
- Access control
- Integrity of data
- Authentication of transmitter (user authentication)
- Encryption
- Authentication of keys
- Administration of keys (key management)

For the Nordic Semiconductor nRF52840 there is a free Thread stack available, which could be used in parallel to Bluetooth 5, ANT and others at the same time. The Thread Group has some strong market drivers in its board, so we would not wonder if it will be the de facto standard for home applications soon.

**ZigBee**

Also ZigBee is based on IEEE 802.15.4. The network, transport and application layers are defined by the ZigBee Alliance. ZigBee is already widely adopted and includes a mature application layer called the ZigBee Cluster Library. ZigBee uses the counter mode (CTR) encryption, which has a 128 bit AES length and the cipher block chaining (CBC) with a 128 bit AES for the generation of the message integrity code (MIC). Within ZigBee a Trust Center (TC) device is determining and approving who wants to join the network. The Trust Center either instructs the router to authenticate the joined device or force it to leave. There are three types of ZigBee security keys to protect the data: link, network and master/application keys. All of them are symmetric.

- Keypair (endpoint keys)
- Network key
- Master key

ZigBee is already widely used in building automation. For certified Telit ZigBee PRO protocol stack. They are suited for home automation and control applications as well as building automation.

**ANT, ANT BLAZE and ANT+**

ANT is a wireless sensor network protocol with ultra-low-power consumption and communication over short distances. As it is very compact, it requires few memory capacities and therefore reduces system costs. The ANT protocol was developed to connect coin cell battery powered sensors (small data packets). ANT supports different network topologies like peer-to-peer, star, tree and mesh. ANT has a network key integrated, which ensures that only devices with the same valid network key can communicate with each other. ANT will be placed on top of the PHY and MAC layer of the ICs from Nordic Semiconductor, using GFSK modulation (1 MHz per channel, channel will be changed only if disturbances are detected). On top of ANT you can choose if you want to make your own application layer or you can choose one of the defined ANT+ stacks. ANT+ application stacks are available for a lot of standard sensors and services. Using ANT+ makes you part of the ecosystem and being compatible to other companies giving security and allows to make your communication very efficiency in regards to energy consumption.

Important to know: ANT is supported by most of the Android based smartphones. There is also a small USB stick available to integrate computers to the network. Further there is a combined stack of ANT and Bluetooth LE available, which enables further connectivity possibilities.

For the Nordic Semiconductor nRF52840 there is a free Thread stack available, which could be used in parallel to Bluetooth 5, ANT and others at the same time. The Thread Group has some strong market drivers in its board, so we would not wonder if it will be the de facto standard for home applications soon.

**Be Aware:**

In 2016 scientists from the Weizmann Institute of Science in Israel and from the Canadian Dalhouse University found a security hole within the wireless Zigbee standard, extracted a security key and put manipulated firmware ("worm") on to the Philips hue bulb. Through that, they were able to control the lightbulbs. This is a serious problem regarding security, as this "worm" can "infect" all other wireless devices in the same network.

The Telit ZE61 (100 mW, long range) modules enable the certified Telit ZigBee PRO protocol stack. They are suited for home automation and control applications as well as building automation.

There are two categories. The general purpose category provides the most cost effective module solution for ANT and ANT+ applications. And the premium category adds the capability to run licensed IoT technologies such as ANT BLAZE. This series offer advanced burst data transfer mode with up to 60 kbps and optional the 128 bit AES encryption mode.

**Gazell and ShockBurst**

Gazell is a free low-power open source protocol for the 2.4 GHz ISM band developed by Nordic Semiconductor, which is implemented on top of the Enhanced ShockBurst (ESB) protocol. It is robust against interferences as it has channel hopping functionality. It supports the star network topology between a single host and up to eight devices. Data transfer within Gazell or ShockBurst is carried out bidirectional. To prevent data loss, Gazell and ShockBurst includes packet buffering, packet acknowledgement and automatic packet retransmission of lost packets.

**ANT**

An antenna is a wireless sensor network protocol with ultra-low-power consumption and communication over short distances. As it is very compact, it requires few memory capacities and therefore reduces system costs. The ANT protocol was developed to connect coin cell battery powered sensors (small data packets). ANT supports different network topologies like peer-to-peer, star, tree and mesh. ANT has a network key integrated, which ensures that only devices with the same valid network key can communicate with each other. ANT will be placed on top of the PHY and MAC layer of the ICs from Nordic Semiconductor, using GFSK modulation (1 MHz per channel, channel will be changed only if disturbances are detected). On top of ANT you can choose if you want to make your own application layer or you can choose one of the defined ANT+ stacks. ANT+ application stacks are available for a lot of standard sensors and services. Using ANT+ makes you part of the ecosystem and being compatible to other companies giving security and allows to make your communication very efficiency in regards to energy consumption.

Important to know: ANT is supported by most of the Android based smartphones. There is also a small USB stick available to integrate computers to the network. Further there is a combined stack of ANT and Bluetooth LE available, which enables further connectivity possibilities.

Most of the SoCs by Nordic Semiconductor supports ANT. Regarding SoMs we recommend to use a module from Dynastream. This supplier is the only one who has full control about the protocol and standardized profiles. The D52 ANT SoC Module Series supports dual protocol ANT and Bluetooth Low Energy.
Wireless Data Transport

Security at Cellular Wireless Technologies

Within a mobile cell, there are many members who transfer their data for and back to a base station and therefore for and back to the internet, different safety aspects have to be considered. First of all a secure protocol needs to be in place for encryption and authentication aspects, so the transferred data can't be read out by anyone else and the sender and receiver can be trusted. Secondly the SIM Card needs to have an up-to-date encryption standard so the end nodes can't be attacked by an unauthorized third party.

Telit's one stop one shop philosophy brings a great choice, from different Cellular Hardware solutions, like the xE910 and xE866 family which can be combined with the right SIM Card solution and IoT Portal from Telit, especially created for industrial applications.

What Could Happen If You Choose the Wrong Module?

The biggest German motorists' club, ADAC, was able to hack the BMW ConnectedCar system in the beginning of 2015. They were able to remotely unlock 2.2 million vehicles of BMW, Mini and Rolls-Royce by using the internal GSM module. The communication was using the same symmetric key for all cars, based on DES with a 56 bit key. To sign the messages, three methods were implemented: DES CBC-MAC, HMAC-SHA1 and HMAC-SHA256. The algorithm used is indicated in the header of the message. To sign and encrypt data, 16 pairs of two 64 bit keys each are used. Which key pair is being used is also noted in the header of the message. It was not clear why BMW was using DES encryption as this algorithm has been considered broken for some time. Its block length is shorter compared to several other crypto algorithms, leading to shorter messages. The surprising thing about what had happened was that the cellular connection between the vehicle and the BMW servers could be logged without problems in an emulated network. The car had sent a simple HTTP Get request; there was no encryption with SSL or TLS in transit. We want to mention that the used module inside the car box was not a module from Telit. At that time Telit has already offered SSL/TLS as a standard. The disclosure of the vulnerabilities was coordinated by ADAC with BMW to give the company enough time to secure their services. A configuration change to enable encryption in transit for ConnectedDrive data has now been triggered via cellular connection. According to BMW, the certificate of the server is now being checked as a consequence of this. However, car owners cannot be sure if their car has received this change. To find out, owners can contact a BMW hotline at 0 89 / 1 25 01 60 10. Owners can also trigger the change manually by selecting Update Services in the car's main menu.

was that the cellular connection between the vehicle and the BMW servers could be logged without problems in an emulated network.

The car had sent a simple HTTP Get request; there was no encryption with SSL or TLS in transit. We want to mention that the used module inside the car box was not a module from Telit. At that time Telit has already offered SSL/TLS as a standard. The disclosure of the vulnerabilities was coordinated by ADAC with BMW to give the company enough time to secure their services. A configuration change to enable encryption in transit for ConnectedDrive data has now been triggered via cellular connection. According to BMW, the certificate of the server is now being checked as a consequence of this. However, car owners cannot be sure if their car has received this change. To find out, owners can contact a BMW hotline at 0 89 / 1 25 01 60 10. Owners can also trigger the change manually by selecting Update Services in the car’s main menu.

M2M SIM Cards with Higher Level Security

Each SIM Card has basically the same function: to identify and register the owner in a cellular network. The SIM Card buffers the secure keys in order to acknowledge the owners identity and to encrypt and decrypt all the data/communication. Unfortunately not all SIM Cards use a secure encryption system and the software is not implemented well enough, so they can be easily hacked. We recommend: Keep your fingers away from SIM Cards which have only DES (Data Encryption Standard) as encryption standard. It is not considered safe enough.

We recommend, check for SIM Cards, like the one from Telit with high security levels.

Telit’s SIM cards offer 2G, 3G & 4G LTE custom plans for data, SMS & voice on tier-one networks. The terms of use are simple – one agreement with predictable pricing and no hidden fees or roaming charges. Furthermore Telit offers a 24/7 support with dedicated IoT experts and an account team. The SIM cards offer a multi-layer security & VPN connections. A 4-8 digit PIN protection preserves the system from use of unwanted third. The VPN solution uses IPSec, an encryption protocol in order to transfer data packets with the highest security level by using tunnels. Furthermore the SIM cards are manufactured in heavily audited production sites. The IoT NOC (Network Operation Center) from Telit works 24/7/365 and monitors all the operations. It works reactive as well as proactive and alerts to customers on misbehavior devices. Telit works with different MNOs (Mobile Network Operators) all around the globe, like Vodafone, Telefonica, at&t, Verizon, Sprint, Tele2 and Rogers. This enables roaming across different regions & networks around the world so the connection will not be lost.
Data Storage

Silent Data Corruption – The Neglected Hazard

Generally we can distinguish between two types of errors: the ones that are detected and those that are not. Although all types of errors are unwanted, at least detected errors are a known variable. Unlike detected errors, undetected errors give no notification, no warning and leave no logging information, which makes it extremely difficult to implement error-correction routines.

Silent errors can result in unreported data corruption, which has the capability of destroying data or rendering the data completely useless. These errors pose a serious threat now and in the future when considering the projected amount of data that will be generated from IoT, Industry 4.0 and many more industries. A study conducted some years ago by CERN revealed that undiscovered errors can occur every 10^{10} bits on average. More recent studies have produced similar average values. Larger capacities are not a solution to the problem, as modern hard disks simply multiply the 1/10^{10} error count several times over.

Silent data corruption can be costly and occur more frequently than expected

Silent data corruption events may occur more frequently than perceived and can seriously impact a business on multiple levels. Approximately 11 drivers per 1000 can experience silent data corruption in a year and up to 10% of catastrophic storage system failures have been linked to silent data corruption. This unwanted scenario can lead to multiple negative consequences, such as operations being carried out incorrectly or data being lost completely. A business affected by a silent data event scenario can experience significant downtime and in the worst case loss of business. It is estimated that retrieving the data and servicing the data center due to downtime has an average cost of $8,850 per minute. A prime example of costs and business risk associated with silent data corruption is Amazon’s 36 hour S3 cloud server downtime in 2008, which left many businesses with partially or fully broken websites, apps and devices. This and many other examples highlight the vast potential damage that silent data corruption can have on your business.

The Causes of Silent Data Corruption

Cosmic Rays

For SSDs cosmic rays are the main source of worry for silent errors. Protons and heavy ions originate from the sun and stars and interact with the atmosphere to create neutrons. The neutrons multiply quickly in a cascading reaction and once reaching the earth, they pass through a person with approximately 10 neutrons/second. In rare circumstances, these high-energy particles can strike integrated circuits, such as a SSD, causing bits to flip in the silicon of the flash cell.

Neutron and Alpha Particles

Generally, neutrons do not carry electrical charges. However, if a neutron gets close enough to a Silicon nucleus, there is a chance that the Silicon nucleus turns into an excited state. An excited Silicon nucleus has a tendency to disintegrate while generating a shower of particles. The shower can be made of more alpha particles or heavier particles which is a carbon nucleus. For these extra electrons and particles, which were generated from alpha particles interaction with electrons in the silicon substrate, are created close enough to a source or a drain junction, these electrons can essentially get sucked into the output of the transistor, creating a current pulse. These pulses are lower than neutron particles, but last longer – 60 to 100 picoseconds. Alpha particles occur less frequently than neutron particles, but, because they generate electric hole-pairs every time, they cause errors at about the same rate as cosmic rays. Susceptibility to these particles varies on the SSD component. As the larger nucleus travel through the substrate, they create a large amount of charge. The charge creates a current pulse in the transistor, which results in a bit flip.

SSD Susceptibilities to Particle Incursions

Essentially, scaling down of geometries increases the susceptibility to particle current pulse. In a Solid State Drive (SSD) the controller and DRAM are the most vulnerable components to a bit flip. Bit flips in these components can apparently make firmware code execute incorrectly, causing silent errors and other problems. On the other hand, flash memory in SSDs is fairly insensitive to these kinds of errors. The NAND is loaded with ECC protection, and enterprise drives (among others!) have end-to-end data protection.

Ideally, the data written by the host goes through the CPU logic and SRAM, which are located in the controller, and the controller picks an available and suitable position on the NAND to write the data. This way the data goes through the transfer buffer and makes it into the NAND completely intact. If the user wants to read the data then the order is simply reversed. However, in case of incorrect behavior in an SSD we know three bit flip scenarios:

1. The bit flip can occur in transit if upstream of NAND ECC
2. The bit flip can happen in the controllers cache, which results in the controller performing the wrong instruction
3. The bit flip might occur in the CPU logic, which can cause wrong sector reads, missed instructions and/or controller hang.
Data Storage

Intel’s Security Solutions – Designing for Data Integrity

Server customers have extremely rigorous specifications for silent errors. Usually they allow as few as silent error per 1025 bits, or one per billion drives. Simply put, server customers have close to zero tolerance for silent errors. Consequently, Intel wants to eliminate bit flips completely and reduce them to a bare minimum in order to fulfill the customer’s rigorous requirements. This is achieved by implementing quality control and testing procedures that go beyond the basics. To combat faulty execution, Intel designed firmware that validates its own operation. If a critical operation cannot be verified and data corruption is possible, the drive locks down, which prevents the possibility to compromise the data's integrity.

Validating Silent Data Corruption Requirements

Apart from rigorous hardware selection and software implementation processes Intel also goes above and beyond in their testing capabilities. Intel owns a neutron particle testing facility – the Los Alamos Neutron Science Center. Intel’s science center allows Intel to perform neutron and alpha particle tests beyond the standardized guideline by the industry. While traditional tests have a RDT limit of 10^-18 Intel uses measurements as low and accurate as 10^-22. This way Intel exposes their SSDs to high intensity particle beams detecting to 0.000001 % per year. At measured conditions, less than 1 drive per 1,000,000 per year will experience silent data corruption.

Intel – A Trusted Partner for Unparalleled Reliability & Integrity

The Intel Advantage – Security and Integrity for Your Data

Besides offering integrity and reliability against unknown and known errors, Intel also includes features in their SSD products that keep your data safe and secure. The hardware encrypted 256 bits Advanced Encryption Standard (AES). AES is a cypher with different key and block sizes that helps to keep data safe from unwanted access. The block size is set to 128 bits while the key has up to three lengths: 128, 192 and 256 bits. Out of the three key lengths 256 bits offers the highest level of security, due to the large number of bits being used in the key. Hardware encryption offers an additional layer of security, because all the data is encrypted prior to being stored in the SSDs flash memory. Once the data has been encrypted and written into the flash memory, the data becomes almost impossible to decrypt without the original encryption key. The AES 256 bit encryption feature is considered to be so secure that it has even been approved by the National Security Agency (NSA) for securing top secret information.

RAID – Redundant Array of Independent Disks

RAID systems are one option to prevent data loss. A RAID system consists of multiple physical mass storage devices, ordinarily hard disks or solid state disks, which are then organized into a single logical drive. A RAID system requires at least two storage media to be operated as a unified storage medium in order to increase reliability. There are different RAID levels, with RAID 1 having a specified reliability rate of 0.00001%. In a RAID 1 system, two disks are written with identical data, containing all of a system’s data. If one of the two disks fails, the second disk can continue to supply all of the data. A RAID 1 system is especially indispensable in real-time systems where security and safety are critical.

ECC – Error Correction Code

Another way to prevent memory corruption is to employ error correction methods such as ECC (error correction code). RAM and memory modules in particular feature models that offer additional ECC RAM. Especially in applications where the memory needs to process a large number of write and read operations, errors can arise when writing, causing the wrong data to be stored and possibly crashes to occur. Such RAM should be an essential feature of any server or storage system. With ECC, an additional redundant byte is generated for each 8-byte word before writing. This byte is used to detect errors when data is written and transferred, and to correct them where possible.
Data Storage

Data Storage – What Needs to be Borne in Mind when Selecting Storage Media?

Storage of personal data should be subject to adequate security measures. Companies are required to adopt suitable technical and administrative measures to protect such data, and also to document such measures.

Hardware-based Data Protection

Hardware-based data protection differs from software-based data protection in that it provides a much higher degree of security. Computer centers are very willing to implement software-based security measures, amongst other things for reasons of scalability and cost reduction. However, in such cases the assumption is made that an attacker cannot access the hardware under any circumstances. In embedded scenarios, the hardware is generally very close to the customer and very prone to attack. Hardware-based security measures are of crucial significance here.

Authentication

The implementation and administration of roles and access rights are determined by strong authentication. Whereas hardware can be configured so that access is determined through authentication by means of a retry counter, no software is capable of withstanding so-called ‘brute-force’ attacks. There are many common examples of a dual strategy, also referred to as two-factor authentication, including the procedure to switch on a mobile telephone or obtain cash from an automatic teller machine. In the latter case, a transaction is only authorized when a user can supply a data carrier that cannot be copied and the matching PIN. Whenever confidence and securing valuables is concerned, data protection involves hardware.

Encryption

In addition to authentication, data encryption within a data carrier is also advantageous. Where software encryption is involved, the key is necessarily present on the processing machine. This represents a risk, because these days any environment can be virtualized using open source software, and this means that it is, in principle, possible to examine encryption software while it is executing. In other words, as soon as an application can be separated from the target platform, purely software-based data protection concepts prove to have weaknesses. Such risks do not exist where hardware-based encryption is used – or only to a very limited extent.

Much sensitive data is stored externally – in other words, physically removed from a company’s own IT infrastructure. If such information also involves personal data, the same requirements in respect of protection apply. In all these circumstances, an adequate degree of security must be provided for. This means, it makes no difference whether the data is to be found on laptops, smartphones, in third-party offices or on a central server. A case in point is to be seen in the encryption of data on mobile devices. If such a device is stolen or gets lost, the data should not be accessible to anyone else, and preferably remotely deletable. Any encryption implemented to this end should only be decryptable by the company itself.

Comprehensive security measures such as encryption are very beneficial. If it is possible to prove that all lost, stolen or in any other way endangered personal data has been made inaccessible to all unauthorized persons, it is not necessary to inform the authorities of the data protection issue, nor the affected persons. This means that the security requirements can be fulfilled more easily and the risk of financial loss and an image problem can be minimized.

The measures include protection against unauthorized access to the data, as well as ensuring availability and a sufficient degree of robustness for the systems involved. In other words, the data should be protected against inadvertent impairment or loss of the body of information. In this connection, attention needs to be paid not only to storing the information, but also to removing it, i.e. to its permanent deletion. Scenarios in which this aspect may gain in relevance include requirement to do so by an authorized party, replacement of storage media and theft. Following evaluation of the security level needed to address the risks involved, a suitable technical solution must be found that meets current engineering standards.

Hardware-based Data Protection

Hardware-based data protection differs from software-based data protection in that it provides a much higher degree of security. Computer centers are very willing to implement software-based security measures, amongst other things for reasons of scalability and cost reduction. However, in such cases the assumption is made that an attacker cannot access the hardware under any circumstances. In embedded scenarios, the hardware is generally very close to the customer and very prone to attack. Hardware-based security measures are of crucial significance here.

Authentication

The implementation and administration of roles and access rights are determined by strong authentication. Whereas hardware can be configured so that access is determined through authentication by means of a retry counter, no software is capable of withstanding so-called ‘brute-force’ attacks. There are many common examples of a dual strategy, also referred to as two-factor authentication, including the procedure to switch on a mobile telephone or obtain cash from an automatic teller machine. In the latter case, a transaction is only authorized when a user can supply a data carrier that cannot be copied and the matching PIN. Whenever confidence and securing valuables is concerned, data protection involves hardware.

Encryption

In addition to authentication, data encryption within a data carrier is also advantageous. Where software encryption is involved, the key is necessarily present on the processing machine. This represents a risk, because these days any environment can be virtualized using open source software, and this means that it is, in principle, possible to examine encryption software while it is executing. In other words, as soon as an application can be separated from the target platform, purely software-based data protection concepts prove to have weaknesses. Such risks do not exist where hardware-based encryption is used – or only to a very limited extent.

Much sensitive data is stored externally – in other words, physically removed from a company’s own IT infrastructure. If such information also involves personal data, the same requirements in respect of protection apply. In all these circumstances, an adequate degree of security must be provided for. This means, it makes no difference whether the data is to be found on laptops, smartphones, in third-party offices or on a central server. A case in point is to be seen in the encryption of data on mobile devices. If such a device is stolen or gets lost, the data should not be accessible to anyone else, and preferably remotely deletable. Any encryption implemented to this end should only be decryptable by the company itself.

Comprehensive security measures such as encryption are very beneficial. If it is possible to prove that all lost, stolen or in any other way endangered personal data has been made inaccessible to all unauthorized persons, it is not necessary to inform the authorities of the data protection issue, nor the affected persons. This means that the security requirements can be fulfilled more easily and the risk of financial loss and an image problem can be minimized.

The measures include protection against unauthorized access to the data, as well as ensuring availability and a sufficient degree of robustness for the systems involved. In other words, the data should be protected against inadvertent impairment or loss of the body of information. In this connection, attention needs to be paid not only to storing the information, but also to removing it, i.e. to its permanent deletion. Scenarios in which this aspect may gain in relevance include requirement to do so by an authorized party, replacement of storage media and theft. Following evaluation of the security level needed to address the risks involved, a suitable technical solution must be found that meets current engineering standards.

Hardware-based Data Protection

Hardware-based data protection differs from software-based data protection in that it provides a much higher degree of security. Computer centers are very willing to implement software-based security measures, amongst other things for reasons of scalability and cost reduction. However, in such cases the assumption is made that an attacker cannot access the hardware under any circumstances. In embedded scenarios, the hardware is generally very close to the customer and very prone to attack. Hardware-based security measures are of crucial significance here.

Authentication

The implementation and administration of roles and access rights are determined by strong authentication. Whereas hardware can be configured so that access is determined through authentication by means of a retry counter, no software is capable of withstanding so-called ‘brute-force’ attacks. There are many common examples of a dual strategy, also referred to as two-factor authentication, including the procedure to switch on a mobile telephone or obtain cash from an automatic teller machine. In the latter case, a transaction is only authorized when a user can supply a data carrier that cannot be copied and the matching PIN. Whenever confidence and securing valuables is concerned, data protection involves hardware.

Encryption

In addition to authentication, data encryption within a data carrier is also advantageous. Where software encryption is involved, the key is necessarily present on the processing machine. This represents a risk, because these days any environment can be virtualized using open source software, and this means that it is, in principle, possible to examine encryption software while it is executing. In other words, as soon as an application can be separated from the target platform, purely software-based data protection concepts prove to have weaknesses. Such risks do not exist where hardware-based encryption is used – or only to a very limited extent.

Much sensitive data is stored externally – in other words, physically removed from a company’s own IT infrastructure. If such information also involves personal data, the same requirements in respect of protection apply. In all these circumstances, an adequate degree of security must be provided for. This means, it makes no difference whether the data is to be found on laptops, smartphones, in third-party offices or on a central server. A case in point is to be seen in the encryption of data on mobile devices. If such a device is stolen or gets lost, the data should not be accessible to anyone else, and preferably remotely deletable. Any encryption implemented to this end should only be decryptable by the company itself.

Comprehensive security measures such as encryption are very beneficial. If it is possible to prove that all lost, stolen or in any other way endangered personal data has been made inaccessible to all unauthorized persons, it is not necessary to inform the authorities of the data protection issue, nor the affected persons. This means that the security requirements can be fulfilled more easily and the risk of financial loss and an image problem can be minimized.
Apacer’s Security Solutions

Apacer’s CoreSecurity is a proprietary data protection technology developed to elevate the data security level through customized firmware and prevent data leakage for higher reliability of storage devices. CoreSecurity is a proprietary data protection technology built into Apacer SSD products. It is crucial for mission-critical applications, where data erase, drive sanitization, and reliability of data storage are essentially required. CoreSecurity provides the following three types of technologies designed with exclusive software commands to meet clients’ requirements of a high level of data protection.

CoreDestroyer Technology

The CoreDestroyer Technology terminates all the data in the drive, even the firmware and the management table. The drive would be unable to perform its functions. To bring the SSD back to life, firmware reloading is necessary.

CoreEraser Technology

Apacer’s Core Eraser Technology provides highly comprehensive drive sanitization measures, developed to securely and thoroughly erase data in operating blocks. The CoreEraser comes in three classes of block sanitizations and can be implemented through vendor software command or hardware architect.

Class 1: Quick Erase eliminates FAT (File Allocation Table) and the MBR (Master Boot Record) in LBA that manages partition tables and boot sector during system start-up process. With both of the MBR and FAT erased, the drive would appear as uninitialized on operating system.

Class 2: Full Erase Function has a more comprehensive Quick Erase, where all contents of the user blocks, free blocks, MBR and FAT table are erased after the procedure is completed. Drive will be reinitialized upon the completion of the erase action. The device will behave as a raw disk as cells in the drive would display “FF” (or “00”).

Class 3: MIL Erase includes a list of globally certified drive purge methods that meet the military and industrial standards, such as NSA 9-12. The process would sanitize the MBR, FAT tables as well as user & free blocks by erasing the blocks, overwriting with random data, then verify. These certified erase features are widely approved in military applications, while providing confidence in secure data erase.

CoreProtector

The widespread adoption of SSDs over HDDs in mission critical applications may attract potential data theft. In order to reinforce data security, Apacer introduces the CoreProtector technology that integrates multiple layers of protection for your valuable data.

Class 1 Data Protect: Apacer SSDs come with a unique 512-byte Security Key when they leave the factory. The key is activated whenever the host boots up. The host BIOS can retrieve the 512-byte key data and the host user can use it as password identification for accessing certain application programs or booting up process. Failure to match the key will result in aborted operations.

Class 2 Write Protect: Apacer implements the Virtual Write scheme that allows write commands to go through the flash controller and data temporarily stored. The OS can then function normally but since the whole process is virtual, no data has actually been written into the flash. When the host system is reset or rebooted, all the temporarily stored data will be lost and nowhere to be found in the system. Since the Virtual Write scheme runs at device level, it requires no software of driver installation and is independent from the host OS.

Class 3 Device Protect: Developed as a more comprehensive security solution, Device protect can be considered as Write protect scheme integrated with read protection that prevents unauthorized accesses to read files in the device. When enabled, the Device Protect scheme would allow read commands to go through flash controller, but no actual data in the device can be read during the whole process. Without the proper way to disable the protection, unauthorized read attempts would receive only invalid data, indicated as “FFh” or “00h”.

Class 4 Boot Protect: Boot Protect Technology is the ultimate security class of Apacer CoreProtector series that restricts the unauthorized from accessing the computer system. Users can set access code during the system booting process so that no one else would be able to access their operating system and SSDs without the correct access code. Boot Protect technology is also ideally applicable for SSDs with multiple OS-run storage zones that are independent from one another. For instance, if a SSD is divided into two storage zones with OS installed in each, the host can decide which zone to access by entering the corresponding access code.
Swissbit’s Security Solutions

Convenience for developers: The products offer tangible hardware security using a plug and play approach. The flash memory can be used by any host to store and retrieve data on the cards at high speed. At the same time, various security functions on the card can be activated to protect any data. IT legislation is very strict regarding requirements for maintaining current technological standards when it comes to the storage of personal or system-critical data. With the aid of secure Swissbit products, it is very easy to enhance security in existing products or provide even greater flexibility in new products.

Valuable data such as sensitive files, e-mails, photos, OS images, firmware updates, log files and audit trails can be protected by encryption, authentication and specific access protection, and subsequent manipulation can be prevented. Data streams for M2M communication (IoT), medicine and video surveillance can be protected against third-party access as confidential data on the storage medium with the aid of a secure, high speed memory card.

Swissbit’s DP (data protection) security product series is based on a security extension for the Swissbit durabit™ firmware. The Swissbit Security Interface enables solution providers to build applications for various platforms. An SDK is available to develop applications on Windows and Linux PC platforms.

Smart card technology is one of the most reliable technologies for protecting data, e.g. through secure device login, data encryption, speech encryption, cloud authentication and many other technologies. The large number of application areas brings about benefits for solution providers such as achieving autonomy with respect to third parties, extremely high security levels and flexibility.

Typical Areas of Application

Industrial equipment is suffering new threats that require countermeasures. Domains like copy protection, license management, counterfeiting protection, system integrity and data protection now need responses, that can be easily solved by using Swissbit security products while data retention and endurance still meet the highest requirements of industrial customers.

Body-worn Cameras and Dashcams

Mobile police units and vehicles are increasingly being equipped with cameras. Strong encryption of the data and strong authentication protect the registered data against loss and unauthorized access.

More and more organizations that have to do with road traffic, such as security firms, public transport operators, taxi companies etc., register data that could contain personal information and therefore needs to be protected against falling into the wrong hands. This requires that the data can only be evaluated by the data protection officer, and that this is verifiable. Such data can be protected adequately and risks minimized by separating the registration and reproduction processes into different roles.

Reliable Boot-up

Secure booting up of devices is required under circumstances in which there is a need to ensure that the device in question always boots up in a particular way or as configured through a given policy. This is normally done by means of a CD ROM or comparable methods.

However, for embedded and IoT devices, this option is precluded simply on size grounds. As an alternative, SD and microSD memory cards with enhanced functionality can be used. It is also possible to provide these cards with unique identifiers and define privileges that determine whether and under which conditions the data can be read at all.

Of course, the card content can be managed by the card administrator. For critical infrastructures such as in power stations or energy distribution networks, legislators have laid down strict definitions for the run-time environment and its traceability.

Copy Protection and License Management

Developing high-quality, sophisticated software is expensive. According to the VDMA (German Mechanical Engineering Industry Association), the German economy suffers huge losses in turnover every year.

The protection of intellectual property includes the need to protect embedded and IoT devices. In particular, the trend towards unification of hardware platforms has the effect of making protection of software the only means of differentiation between competitors, so that it now has the highest priority. Protection against copy is considerably enhanced through making access to storage media content on strong authentication. Content is only readable within the context of a defined usage scenario, and attacks are much less likely to succeed.

The unique identification of each storage device can be enhanced to such an extent through certificates or encryption that even if software is misappropriated, it will not function without a secure memory card. The aim, therefore, is to provide for enough additional security through viable means without unreasonably increasing product and processing costs during the life-cycle stages.
Data Storage

Transcend’s Hardware-based AES Solution

For applications that handle especially sensitive data or require special levels of confidentiality, Transcend offers hardware-based AES encryption on several SSD models for various 2.5”, M.2, and mSATA models.

Transcend Information’s SSDs equipped with hardware-based AES encryption offer considerably more professional data protection and performance compared to alternative programs that utilize software-based or firmware-based encryption.

With hardware-based encryption, all data is encrypted before being stored in NAND flash memory (See Figure 1). After the encrypted data has been written into the flash memory, it becomes virtually impossible to decrypt the data without the original encryption key. Performance is also improved compared to software-based solutions, since hardware-based encryption does not require system resources to perform the encryption/decryption process.

Transcend Information offers a variety of SSDs equipped with hardware-based AES encryption, thereby enabling reliable handling of sensitive data and enhanced data security.

From securing personal data, such as credit card information or medical records, to protecting sensitive corporate information, Transcend Information’s SSDs with hardware-based encryption mechanisms provide an excellent solution that guarantees data protection.

TCG OPAL Specifications

The Trusted Computing Group (TCG) is an organization whose members work together to formulate industry standards with the intention that these should enjoy cross-industry validity. TCG’s Storage Work Group created the Opal Security Subsystem Class (SSC) as a class of security management protocols for storage devices. It applies mainly to products used in PCs and notebooks. The class defines specifications concerning file management on storage devices, and defines multi-stage access levels for data management and protection. Devices conforming to Opal SSC specifications may be referred to as TCG Opal devices, a mark of trustworthiness.

TCG Opal Features

Opal is a comprehensive set of guidelines. The target audience includes manufacturers of storage devices, software vendors, system integrators, and academia. These specifications cover the manufacture of storage devices, system setup, management, administration, and use. They require password protection and hierarchical storage management in order to guarantee data security and protection.

Advantages of Opal

1. In a hierarchically managed system, access privileges can be assigned to certain persons by means of passwords. This minimizes the chance of data being stolen, tampered with, or lost.

2. All security functions take place within the device itself. They do not need to pass through the host operating system. They do not exploit system resources, making for faster and more secure execution. In addition, compatibility problems can no longer arise.

With increasing volumes of data, information security is becoming one of the most important issues for both business and private users. The TCG designed Opal to address both software and hardware aspects of security, and take account of the need for hierarchical management approaches. From the manufacturer to the user, Opal is a standard that serves the needs of everyone.

Transcend’s AES SSDs are compliant with the TCG Opal 2.0 standards, and can be customized to meet specific customer needs as required.
Data Storage

Transcend’s Hardware-based AES Solution

Hardware Purge

In addition to data encryption, Transcend Information offers a variety of SATA III SSD models that can be equipped with a hardware purge function, ensuring quick and irrevocable erasure of data.

Hardware purge refers to the effective, hardware-based erasure of all data blocks in flash memory, which returns the SSD to its original state at the time of manufacture.

Whereas software-based methods utilize the ATA ‘erase’ command to delete data, a hardware purge constitutes a different kind of access via an external switch that is connected with the controller’s General Purpose Input/Output (GPIO) interfaces. Here, the voltage levels of all the installed flash memory units are switched from High to Low at the same time.

The erase function is activated and all data present on the SSD is simultaneously deleted through short-circuiting the hardware purge pins (see Figure 1). Erased data is absolutely non-recoverable, meaning that this procedure reliably and irrevocably destroys confidential information.

The hardware purge pin is connected to the designated pin of the controller’s GPIO (see Figure 2). Customized firmware settings are required to support the hardware purge pin.

With Transcend’s hardware purge feature, sensitive data can be securely, permanently and effectively deleted.

Seagate’s Security Solution

Locking Down Firmware

Firmware is a very attractive target for cybercriminals, because it cannot be scanned by anti-virus programs.

Therefore the ‘Secure Download and Diagnostics’ feature is now standard on every Seagate hard disk. It prevents unauthorized access to the firmware of a drive, as well as preventing manipulation of executable firmware code and sensitive system-level data.

Therefore customers can be sure that the devices are free of malware, and provide evidence of this to authorities.

Encryption

Encryption keeps data protected even in cases where a hard disk is lost, gets stolen or misplaced. Also, your customers can minimize the risks for the affected persons, and this plays a major role when it comes to weighing up whether the authorities have to be informed or not. Seagate’s self-encrypting storage media can delete the key required for decryption, so that all the data on a disk are rendered illegible in less than one second. Subsequently, the disk can be returned, reused or disposed of without any risk. Also, self-encrypting hard disks lock down automatically as soon as they are removed from a system, or when the disk or the system is switched off. This represents an additional degree of protection for the stored data.

Simple Data Deletion Prior to Disposal

Companies and institutions are responsible for the entire life cycle of the personal data in their possession, from its initial acquisition until its deletion. So what actually happens when a storage medium reaches the end of its service life?

Overwriting data on such a medium is expensive and can block valuable resources for days at a time. Demagnetization of media is complicated and risky. Physically shredding media is expensive, environmentally questionable and also involves a lot of effort. Long-term storage of media at another location is expensive and also risky.

The intelligent solution is called Seagate Instant Secure Erase. It is part of the SeaTools suite and is an aid to IT specialists involved in data deletion and media sanitization. It provides for secure, fast and problem-free disposal of storage media.

Figure 1: Hardware purge pin

Figure 2: Hardware purge pin
**Data Processing**

Central Processing Unit Security

These days it is not a matter of “if” but when private data begins to roam outside of your secure perimeter. In 2016 there were over 1.3 billion registered data breaches and with the new European data protection regulation to be introduced in 2018, it becomes even more essential to protect users identity, to prevent and detect malware, to protect your data and have resiliency and recovery features. Intel has numerous hardware- and software-based solutions that address security issues and help reduce data compromise and data loss, providing protection at the point of creation and throughout the data lifecycle.

**Intel® AES New Instructions (Intel® AES NI)**
- Encryption instruction set for improvement and acceleration of AES data encryption in hardware with Intel® Xeon® or Core™ processor families
- Implemented intensive sub-steps of AES algorithm in hardware
- Strengthens and accelerates execution of AES applications
- Accelerate encryption and decryption
- Improve key generation and matrix manipulation
- Minimizes application performance concerns inherent in traditional cryptographic processing
- Provides enhanced security by addressing side channel attacks on AES associated with traditional software methods of table look-ups

**Best Way to Secure Business-critical Data Within the Following Fields:**
- Network traffic
- Personal data
- Corporate IT infrastructure

**Intel® Secure Key**
- Intel® 64 Architecture instruction RDRAND and its underlying Digital Random Number Generator (DRNG) hardware implementation
- RDSEED instruction is part of the Intel® Secure Key
- Digital Random Number Generator is a key enabler for Information Security Applications
- Cryptographic protocols rely on RNGs for generating keys and fresh session values to prevent replay attacks
- Can be used to fix this weakness, thus significantly increasing cryptographic robustness
- RDRAND has been engineered to meet existing security standards and can be used in general for information security standards

**Other Uses of Digital Random Number Generation Include**
- Communication
- Gaming
- Secure disk wiping or document shredding
- Protecting online services against RNG attacks

**Intel® Execute Disable Bit**
- Security feature that can help to reduce system exposure to viruses
- Allows the processor to classify areas in memory where application code can or cannot execute
- When code wants to insert in the buffer, the processor disables code execution, preventing damage and worm propagation
- Usage needs a PC or server with a processor with Execute Disable Bit capability and a supporting operating system

**Intel® Trusted Execution Technology (Intel® TXT)**
- Hardware-based Technology for enhancing Server Platform Security
- High virtualized increased data center or high workloads will be shared across physical infrastructure
- More trusted infrastructure is the key to maintain the assurance and controlling
- Visibility of the security and workloads within the data center
- New control capabilities

**Intel® Memory Protection Extensions (Intel® MPX)**
- Set of extensions to the x86 instruction set architecture
- With compiler, runtime library and operating system support
- Brings increased security to software by checking pointer references whose normal compile-time intentions are maliciously exploited at runtime due to buffer overflows
- Two-level address translation is used for storing bounds in memory
- Top layer consists of a Bounds Directory (BD) created on the application startup
- Each BD entry is either empty or contains a pointer to a dynamically created Bounds Table (BT), which in turn contains a set of pointer bounds along with the linear addresses of the pointers
- Bounds load (BINDLX) and store (BINDSTX) instructions transparently perform the address translation and access bounds in the proper BT entry

**Architecture Includes Two Configuration Registers**
- BNDCFGx
  - BNDCFGU in user space
  - BNDCFGx in Kernel
- BNDSTATUS status register
  - Provides a memory address
  - Provides an error code

**Intel® AES New Instructions (Intel® AES NI)**

**Intel® Secure Key**

**Intel® Execute Disable Bit**

**Intel® Trusted Execution Technology (Intel® TXT)**

**Intel® Memory Protection Extensions (Intel® MPX)**

**Central Processing Unit Security**

These days it is not a matter of “if” but when private data begins to roam outside of your secure perimeter. In 2016 there were over 1.3 billion registered data breaches and with the new European data protection regulation to be introduced in 2018, it becomes even more essential to protect users identity, to prevent and detect malware, to protect your data and have resiliency and recovery features. Intel has numerous hardware- and software-based solutions that address security issues and help reduce data compromise and data loss, providing protection at the point of creation and throughout the data lifecycle.

**Intel® AES New Instructions (Intel® AES NI)**
- Encryption instruction set for improvement and acceleration of AES data encryption in hardware with Intel® Xeon® or Core™ processor families
- Implemented intensive sub-steps of AES algorithm in hardware
- Strengthens and accelerates execution of AES applications
- Accelerate encryption and decryption
- Improve key generation and matrix manipulation
- Minimizes application performance concerns inherent in traditional cryptographic processing
- Provides enhanced security by addressing side channel attacks on AES associated with traditional software methods of table look-ups

**Best Way to Secure Business-critical Data Within the Following Fields:**
- Network traffic
- Personal data
- Corporate IT infrastructure

**Intel® Secure Key**
- Intel® 64 Architecture instruction RDRAND and its underlying Digital Random Number Generator (DRNG) hardware implementation
- RDSEED instruction is part of the Intel® Secure Key
- Digital Random Number Generator is a key enabler for Information Security Applications
- Cryptographic protocols rely on RNGs for generating keys and fresh session values to prevent replay attacks
- Can be used to fix this weakness, thus significantly increasing cryptographic robustness
- RDRAND has been engineered to meet existing security standards and can be used in general for information security standards

**Other Uses of Digital Random Number Generation Include**
- Communication
- Gaming
- Secure disk wiping or document shredding
- Protecting online services against RNG attacks

**Intel® Execute Disable Bit**
- Security feature that can help to reduce system exposure to viruses
- Allows the processor to classify areas in memory where application code can or cannot execute
- When code wants to insert in the buffer, the processor disables code execution, preventing damage and worm propagation
- Usage needs a PC or server with a processor with Execute Disable Bit capability and a supporting operating system

**Intel® Trusted Execution Technology (Intel® TXT)**
- Hardware-based Technology for enhancing Server Platform Security
- High virtualized increased data center or high workloads will be shared across physical infrastructure
- More trusted infrastructure is the key to maintain the assurance and controlling
- Visibility of the security and workloads within the data center
- New control capabilities

**Intel® Memory Protection Extensions (Intel® MPX)**
- Set of extensions to the x86 instruction set architecture
- With compiler, runtime library and operating system support
- Brings increased security to software by checking pointer references whose normal compile-time intentions are maliciously exploited at runtime due to buffer overflows
- Two-level address translation is used for storing bounds in memory
- Top layer consists of a Bounds Directory (BD) created on the application startup
- Each BD entry is either empty or contains a pointer to a dynamically created Bounds Table (BT), which in turn contains a set of pointer bounds along with the linear addresses of the pointers
- Bounds load (BNDLDX) and store (BNDSTX) instructions transparently perform the address translation and access bounds in the proper BT entry

**Architecture Includes Two Configuration Registers**
- BNDCFGx
  - BNDCFGU in user space
  - BNDCFGx in Kernel
- BNDSTATUS status register
  - Provides a memory address
  - Provides an error code
Data Processing

Central Processing Unit Security

Intel® Software Guard Extensions (Intel® SGX)
- Intel technology for application developers who are seeking to
  protect selected code and data from disclosure or modification
- Protection possible through the use of enclaves, which are
  protected areas of execution in memory
- Application code can be put into an enclave by special instructions
- Software is available to developers via the Intel® SGX Software
  Development Kit (SDK)
- Collection of APIs, libraries, documentation, sample source
  code, and tools that allows software developers to create and
  debug Intel SGX enabled applications in C and C++

Application Code Executing Within an Intel SGX Enclave
- Introduced with 7th generation of Intel Core and Xeon E3 v5
  processors for data center servers
- Usage of the full processor power possible
- Possibility of cold boot
- Uses hardware-based mechanisms to respond to remote
  attestation challenges that validate its integrity
- Synchronization with parent application
- Can be used with standard development tools
- Supports initial data center use

Intel® Transactional Synchronization Extensions – New Instructions (TSX-NI)
- Programmer-specified code regions are executed transactional
- Memory operations will appear and be occurred when viewed
  from other logical processors, after successful execution
- A processor makes architectural updates performed within the
  region visible to other logical processors only on a successful
  commit, a process referred to as an atomic commit
- Serialization through lock-protected critical section if required
- Synchronization of hidden applications with exposing

Intel® ECC Memory Support
- Detect and correct the internal data corruption
- ECC memory maintains a memory system immune to single-bit
  errors
- Data that is read from each word is always the same as the data
  that had been written to it, even if one or more bits actually
  stored have been flipped to the wrong state
- Most non-ECC memory cannot detect errors although some
  non-ECC memory with parity support allows detection but not
  correction
- Supported by integrated memory controller at Intel® Xeon®
  processors and some application specific Intel® Atom processors

Intel® vPro™ Technology
- Allows PCs to be fixed and maintained remotely
- Service providers can use vPro to solve problems after entering
  a key sequence
- Ability to access a computer even if it has been turned off within
  a wired or secure wireless network
- Laptops outside the internal network can be accessed with the
  newest versions of software
- Possibility for remotely operating system security patches and
  BIOS updates

Intel® Boot Guard
- Provides reliable information about the state of the system
- Hardware implemented
- Processor is called Trusted Platform Module (TPM)
- First verification of signatures happens by code on the CPU
- Possibility to emulate a "properly" booted system
- A key which is written in the CPU makes it possible to lock
  down the boot block
- In “Measured Boot” mode, Boot Guard creates a hash over the
  bootblock and sends it off to the TPM
- Value is stored in TPM registers, which aren’t writable by code
  running on CPU
- Supposed to prevent replay attacks with possibility to fake a
  certain Boot Guard state if an attacker manages to disable Boot
  Guard altogether

Intel® Identity-Protection-Technology
- Will be managed with hardware based certificates and PIN for
  a safe Protected-Transaction-Display (PTD)
- With multifactor-authentification (MFA)
- Framework for the basis of identification and access manage-
  ment, which could be integrated in the IT-infrastructure
- Flexibility in access management for different users and
  applications
- MFA Engine based on the firmware guarantees the given access
- The authentication occurs between user, system and network
- "Walk-Away Lock": Bluetooth device connected to the PC for
  ability to block and unblock the system
- "Domain/OS-Login": required key for the system login saved in
  the hardware, which secures the user, system and network for
  malware attacks
- "VPN-Login": similar to “Domain/OS-Login” secures the
  hardware based VPN-authentication and system from malware
  due to file all relevant keys in the hardware
### Intel® Atom® Embedded

<table>
<thead>
<tr>
<th>Type</th>
<th>Intel® Atom® x5-E8000 Processor</th>
<th>Intel® Atom® x5-E8900 Processor</th>
<th>Intel® Atom® x5-E8940 Processor</th>
<th>Intel® Atom® x7-E8950 Processor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Name</td>
<td>Braswell</td>
<td>Apollo Lake</td>
<td>Apollo Lake</td>
<td>Apollo Lake</td>
</tr>
<tr>
<td>Package Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Cores</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td># of Threads</td>
<td>4</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Processor Frequency</td>
<td>1.04 GHz</td>
<td>1.30 GHz</td>
<td>1.60 GHz</td>
<td>1.60 GHz</td>
</tr>
<tr>
<td>TDP</td>
<td>5 W</td>
<td>6.5 W</td>
<td>9.5 W</td>
<td>12 W</td>
</tr>
<tr>
<td>Memory Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Types</td>
<td>DDR3L</td>
<td>DDR3L, LPDDR4</td>
<td>DDR3L, LPDDR4</td>
<td>DDR3L, LPDDR4</td>
</tr>
<tr>
<td>ECC Memory Supported</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Graphics Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sockets Supported</td>
<td>FCBGA1170</td>
<td>FCBGA1296</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package Size</td>
<td>25 mm x 27 mm</td>
<td>24 mm x 31 mm</td>
<td>24 mm x 31 mm</td>
<td>24 mm x 31 mm</td>
</tr>
<tr>
<td>Power specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>-40°C to 85°C</td>
<td>-40°C to 85°C</td>
<td>-40°C to 85°C</td>
<td>-40°C to 85°C</td>
</tr>
</tbody>
</table>

### Intel® Pentium® Embedded

<table>
<thead>
<tr>
<th>Type</th>
<th>Intel® Pentium® Processor N3710</th>
<th>Intel® Pentium® Processor N4200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Name</td>
<td>Braswell</td>
<td>Apollo Lake</td>
</tr>
<tr>
<td>Package Specifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Cores</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td># of Threads</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Processor Frequency</td>
<td>1.60 GHz</td>
<td>1.10 GHz</td>
</tr>
<tr>
<td>TDP</td>
<td>1.04 GHz</td>
<td>2.40 GHz</td>
</tr>
<tr>
<td>Memory Specifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Types</td>
<td>DDR3L, LPDDR3</td>
<td>DDR3L, DDR4, LPDDR4, LPDDR4</td>
</tr>
<tr>
<td>ECC Memory Supported</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Graphics Specifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package Specifications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sockets Supported</td>
<td>FCBGA1170</td>
<td>FCBGA1296</td>
</tr>
<tr>
<td>Package Size</td>
<td>25 mm x 27 mm</td>
<td>24 mm x 33 mm</td>
</tr>
</tbody>
</table>

### Intel® Celeron® Embedded

<table>
<thead>
<tr>
<th>Type</th>
<th>Intel® Celeron® Processor N3965U</th>
<th>Intel® Celeron® Processor N3935</th>
<th>Intel® Celeron® Processor N3900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Name</td>
<td>Kaby Lake</td>
<td>Apollo Lake</td>
<td>Braswell</td>
</tr>
<tr>
<td>Package Specifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Cores</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td># of Threads</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Processor Frequency</td>
<td>2.20 GHz</td>
<td>1.10 GHz</td>
<td>1.60 GHz</td>
</tr>
<tr>
<td>TDP</td>
<td>15 W</td>
<td>6 W</td>
<td>4 W</td>
</tr>
<tr>
<td>Memory Specifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Types</td>
<td>DDR3L, LPDDR3</td>
<td>DDR3L, DDR4, LPDDR4, LPDDR4</td>
<td></td>
</tr>
<tr>
<td>ECC Memory Supported</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Graphics Specifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package Specifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sockets Supported</td>
<td>FCBGA1296</td>
<td>FCBGA1296</td>
<td>FCBGA1400</td>
</tr>
<tr>
<td>Package Size</td>
<td>24 mm x 24 mm</td>
<td>24 mm x 28 mm</td>
<td>28 mm x 28 mm</td>
</tr>
</tbody>
</table>

---

**Data Processing**

**Central Processing Unit Security**
## Intel® Core™ Embedded

| Type | Intel® Core™ (i3-7100U) Processor | Intel® Core™ (i3-7100E) Processor | Intel® Core™ (i3-7101TE) Processor | Intel® Core™ (i3-7102E) Processor | Intel® Core™ (i5-7300U) Processor | Intel® Core™ (i5-7440EQ) Processor | Intel® Core™ (i5-7442EQ) Processor | Intel® Core™ (i5-7500T) Processor | Intel® Core™ (i5-7500) Processor | Intel® Core™ (i7-7600U) Processor | Intel® Core™ (i7-7700T) Processor | Intel® Core™ (i7-7700) Processor | Intel® Core™ (i7-7820EQ) Processor |
|------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|
| Code Name | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake | Kaby Lake |
| Vertical Segment | Embedded | Embedded | Embedded | Embedded | Embedded | Embedded | Embedded | Embedded | Embedded | Embedded | Embedded | Embedded | Embedded | Embedded |
| Processor Number | i3-7100U | i3-7100E | i3-7101TE | i3-7102E | i3-7440EQ | i3-7442EQ | i5-7500T | i5-7500 | i7-7600U | i7-7700T | i7-7700 | i7-7820EQ | i7-7820EQ |
| Lithography | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm | 14 nm |
| Performance | | | | | | | | | | | | | |
| # of Cores | 2 | 2 | 2 | 2 | 4 | 4 | 4 | 4 | 2 | 4 | 4 | 4 | 4 | 4 |
| Processor Base Frequency | 2.40 GHz | 2.90 GHz | 3.40 GHz | 3.90 GHz | 2.10 GHz | 2.60 GHz | 2.90 GHz | 2.10 GHz | 2.70 GHz | 3.40 GHz | 2.80 GHz | 2.90 GHz | 3.60 GHz | 3.00 GHz |
| TDP | 15 W | 35 W | 35 W | 54 W | 15 W | 45 W | 25 W | 35 W | 65 W | 15 W | 35 W | 65 W | 45 W |
| Memory Specifications | | | | | | | | | | | | | |
| Memory Types | DDR4, LPDDR3, DDR3L | DDR4, DDR3L | DDR4 | DDR4, LPDDR3, DDR3L | DDR4 | DDR4 | DDR4 | DDR4, DDR3L | DDR4 | DDR4 | DDR4, DDR3L | DDR4 | DDR4, DDR3L | DDR4 |
| ECC Memory Supported | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Package Specifications | | | | | | | | | | | | | |
| Package Supported | FBGA1356 | FCBA1440 | FCBA1440 | FCBA1440 | FCBA1440 | FCBA1440 | FCBA1440 | FCBA1440 | FCBA1440 | FCBA1440 | FCBA1440 | FCBA1440 | FCBA1440 |
| Package Size | 42 mm x 24 mm | 42 mm x 28 mm | 37.5 mm x 37.5 mm | 37.5 mm x 37.5 mm | 42 mm x 28 mm | 42 mm x 28 mm | 42 mm x 28 mm | 42 mm x 28 mm | 37.5 mm x 37.5 mm | 37.5 mm x 37.5 mm | 42 mm x 28 mm | 37.5 mm x 37.5 mm | 37.5 mm x 37.5 mm |
| Security & Reliability | | | | | | | | | | | | | |
| AES New Instructions | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Secure Boot | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Software Guard Extensions (Intel® SGX) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Memory Protection Extensions (Intel® MPX) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Trusted Execution Technology | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Execute Disable Bit | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| OS Guard | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Stable Image Platform Program (SIPP) | No | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Device Protection Technology | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Device Protection Technology with Boot Guard | No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

### Data Processing

#### Central Processing Unit Security

- **Intel® vPro™ Technology**: No, No, No, No, No, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes
- **Intel® Virtualization Technology (VT-x)**: Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes
- **Intel® Virtualization Technology (VT-d)**: Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes
- **Intel® VT-x with EPT**: Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes
- **Intel® TSX-NI**: No, No, No, No, No, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes
- **Intel® 64**: Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes
- **Instruction Set**: 64 bit, 64 bit, 64 bit, 64 bit, 64 bit, 64 bit, 64 bit, 64 bit, 64 bit, 64 bit, 64 bit, 64 bit, 64 bit, 64 bit
- **Security & Reliability**: Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes, Yes
### Intel® Xeon® E3 Embedded

<table>
<thead>
<tr>
<th>Type</th>
<th>Intel® Xeon® Processor E3-1505M v6</th>
<th>Intel® Xeon® Processor E3-1505L v6</th>
<th>Intel® Xeon® Processor E3-1501L v6</th>
<th>Intel® Xeon® Processor E3-1501M v6</th>
<th>Intel® Xeon® Processor E3-1275 v6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Name</td>
<td>Kaby Lake</td>
<td>Kaby Lake</td>
<td>Kaby Lake</td>
<td>Kaby Lake</td>
<td>Kaby Lake</td>
</tr>
<tr>
<td>Essentials</td>
<td>Embedded</td>
<td>Embedded</td>
<td>Embedded</td>
<td>Embedded</td>
<td>Embedded</td>
</tr>
<tr>
<td>Processor Number</td>
<td>E3-1505MV6</td>
<td>E3-1505LV6</td>
<td>E3-1501LV6</td>
<td>E3-1501MV6</td>
<td>E3-1275V6</td>
</tr>
<tr>
<td>Lithography</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
</tr>
<tr>
<td>Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Cores</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td># of Threads</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Processor Base Frequency</td>
<td>3.00 GHz</td>
<td>2.20 GHz</td>
<td>2.10 GHz</td>
<td>2.90 GHz</td>
<td>3.80 GHz</td>
</tr>
<tr>
<td>TDP</td>
<td>45 W</td>
<td>25 W</td>
<td>25 W</td>
<td>45 W</td>
<td>73 W</td>
</tr>
<tr>
<td>Memory Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Types</td>
<td>DDR4, LPDDR3, DDR3L</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4, DDR3L</td>
</tr>
<tr>
<td>ECC Memory Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Graphics Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Package Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sockets Supported</td>
<td>FCBGA1440</td>
<td>FCBGA1440</td>
<td>FCBGA1440</td>
<td>FCBGA1440</td>
<td>FCBGA1440</td>
</tr>
<tr>
<td>Package Size</td>
<td>42 mm x 28 mm</td>
<td>42 mm x 28 mm</td>
<td>42 mm x 28 mm</td>
<td>42 mm x 28 mm</td>
<td>37.5 mm x 37.5 mm</td>
</tr>
<tr>
<td>Advanced Technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intel® AMT™ Technology</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® Hyper-Threading Technology</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® Virtualization Technology (VT-c)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® Virtualization Technology (VT-d)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® VT-x with EPT</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® TSX/N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® 64</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Instruction Set</td>
<td>64 bit</td>
<td>64 bit</td>
<td>64 bit</td>
<td>64 bit</td>
<td>64 bit</td>
</tr>
</tbody>
</table>

### Intel® Xeon® D Embedded

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Name</td>
<td>Broadwell</td>
<td>Broadwell</td>
<td>Broadwell</td>
<td>Broadwell</td>
<td>Broadwell</td>
<td>Broadwell</td>
</tr>
<tr>
<td>Essentials</td>
<td>Embedded</td>
<td>Embedded</td>
<td>Embedded</td>
<td>Embedded</td>
<td>Embedded</td>
<td>Embedded</td>
</tr>
<tr>
<td>Processor Number</td>
<td>D-1529</td>
<td>D-1539</td>
<td>D-1557</td>
<td>D-1559</td>
<td>D-1567</td>
<td>D-1577</td>
</tr>
<tr>
<td>Lithography</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
</tr>
<tr>
<td>Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Cores</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td># of Threads</td>
<td>8</td>
<td>16</td>
<td>24</td>
<td>24</td>
<td>24</td>
<td>32</td>
</tr>
<tr>
<td>Processor Base Frequency</td>
<td>1.30 GHz</td>
<td>1.60 GHz</td>
<td>1.50 GHz</td>
<td>1.50 GHz</td>
<td>2.10 GHz</td>
<td>1.30 GHz</td>
</tr>
<tr>
<td>TDP</td>
<td>20 W</td>
<td>35 W</td>
<td>45 W</td>
<td>45 W</td>
<td>65 W</td>
<td>45 W</td>
</tr>
<tr>
<td>Memory Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Types</td>
<td>DDR4, DDR3</td>
<td>DDR4, DDR3</td>
<td>DDR4, DDR3</td>
<td>DDR4, DDR3</td>
<td>DDR4, DDR3</td>
<td>DDR4, DDR3</td>
</tr>
<tr>
<td>ECC Memory Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Graphics Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processor Graphics</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Package Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sockets Supported</td>
<td>FCBGA1667</td>
<td>FCBGA1667</td>
<td>FCBGA1667</td>
<td>FCBGA1667</td>
<td>FCBGA1667</td>
<td>FCBGA1667</td>
</tr>
<tr>
<td>Package Size</td>
<td>37.5 mm x 37.5 mm</td>
<td>37.5 mm x 37.5 mm</td>
<td>37.5 mm x 37.5 mm</td>
<td>37.5 mm x 37.5 mm</td>
<td>37.5 mm x 37.5 mm</td>
<td>37.5 mm x 37.5 mm</td>
</tr>
<tr>
<td>Advanced Technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intel® Virtualization Technology (VT-x)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® Virtualization Technology (VT-d)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® VT-x with EPT</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® TSX/N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® 64</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Instruction Set</td>
<td>64 bit</td>
<td>64 bit</td>
<td>64 bit</td>
<td>64 bit</td>
<td>64 bit</td>
<td>64 bit</td>
</tr>
<tr>
<td>Security &amp; Reliability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intel® AES New Instructions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure Key</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Intel® Trusted Execution Technology</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Execute Disable Bit</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GS Guard</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Central Processing Unit Security**

- **Data Processing**
- **Central Processing Unit Security**
### Intel® Xeon® Scalable Processors

<table>
<thead>
<tr>
<th>Type</th>
<th>Intel® Xeon® Platinum 8160T</th>
<th>Intel® Xeon® Gold 6138T</th>
<th>Intel® Xeon® Gold 6130T</th>
<th>Intel® Xeon® Gold 6126T</th>
<th>Intel® Xeon® Gold 5120T</th>
<th>Intel® Xeon® Gold 5119T</th>
<th>Intel® Xeon® Gold 4116T</th>
<th>Intel® Xeon® Gold 4114T</th>
<th>Intel® Xeon® Silver 4110T</th>
<th>Intel® Xeon® Silver 4109T</th>
<th>Intel® Xeon® Bronze 3106</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Name</td>
<td>Skylake</td>
<td>Skylake</td>
<td>Skylake</td>
<td>Skylake</td>
<td>Skylake</td>
<td>Skylake</td>
<td>Skylake</td>
<td>Skylake</td>
<td>Skylake</td>
<td>Skylake</td>
<td>Skylake</td>
</tr>
<tr>
<td>Vertical Segment</td>
<td>Server</td>
<td>Server</td>
<td>Server</td>
<td>Server</td>
<td>Server</td>
<td>Server</td>
<td>Server</td>
<td>Server</td>
<td>Server</td>
<td>Server</td>
<td>Server</td>
</tr>
<tr>
<td>Lithography</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
<td>14 nm</td>
</tr>
<tr>
<td>Processor Number</td>
<td>8160T</td>
<td>6138T</td>
<td>6130T</td>
<td>6126T</td>
<td>5120T</td>
<td>5119T</td>
<td>4116T</td>
<td>4114T</td>
<td>4110T</td>
<td>4109T</td>
<td>3106</td>
</tr>
<tr>
<td># of Cores</td>
<td>24</td>
<td>20</td>
<td>20</td>
<td>16</td>
<td>16</td>
<td>12</td>
<td>24</td>
<td>24</td>
<td>12</td>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td>Processor Base Frequency</td>
<td>2.10 GHz</td>
<td>2.00 GHz</td>
<td>2.00 GHz</td>
<td>2.10 GHz</td>
<td>2.10 GHz</td>
<td>2.60 GHz</td>
<td>2.60 GHz</td>
<td>2.20 GHz</td>
<td>1.90 GHz</td>
<td>2.30 GHz</td>
<td>2.10 GHz</td>
</tr>
<tr>
<td>TDP</td>
<td>150 W</td>
<td>125 W</td>
<td>125 W</td>
<td>125 W</td>
<td>125 W</td>
<td>125 W</td>
<td>125 W</td>
<td>105 W</td>
<td>105 W</td>
<td>85 W</td>
<td>85 W</td>
</tr>
<tr>
<td>Memory Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Type</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
<td>DDR4</td>
</tr>
<tr>
<td>ECC Memory Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Package Specifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Packages Supported</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
<td>FCLGA3647</td>
</tr>
<tr>
<td>Package Size</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
<td>76.0 mm x 56.5 mm</td>
</tr>
</tbody>
</table>

### Advanced Technologies

- **Intel® vPro™ Technology**: Yes
- **Intel® Virtualization Technology (VT-x)**: Yes
- **Intel® TSX-NI**: Yes
- **Intel® 64**: Yes
- **Intel® AES New Instructions**: Yes
- **Intel® Trusted Execution Technology**: Yes
- **Intel® Run-Safe Technology**: Yes
- **Mode-based Execute Control (MBC)**: Yes
- **Execute Disable Bit**: Yes

### Security & Reliability

- **Intel® AES New Instructions**: Yes
- **Intel® Trusted Execution Technology**: Yes
- **Intel® Run-Safe Technology**: Yes
- **Mode-based Execute Control (MBC)**: Yes
Secure Boot
F&S makes it easy to get a higher security level for your application. The key is Secure Boot. Secure Boot ensures that only genuine or authentic software is allowed to run on your board. Furthermore, it supports encrypted boot including image cloning protection and, depending on the use case, image confidentiality. In short, using Secure Boot on your platform prevents hackers from altering the boot process.

F&S provides two different offers for the Secure Boot:
- **Secure Boot as a Service**
  Signing and Encrypting of the images will be managed by F&S
- **Secure Boot as a Package**
  Signing and Encrypting of the images will be managed by customer

Secure Boot is the concept of protecting the system from manipulation and the software from decrypting. Both procedures can be used for the boot loader as well as for the device tree and kernel.

The software developed by F&S makes the software of NXP simplify the process of signing and encryption.

### Protection of Intellectual Property
- Boot code cannot be read out

### Protection against Manipulation
- Only certified software is accepted

#### Features
- Modifying file contents can be accepted only in completed operations (state-transition)
- During modification transitions can also be accomplished by using explicit calls within the application (FlushFileBuffers)

---

F3S – Failsafe Flash Filesystem
The Failsafe Flash Filesystem is a filesystem that is especially designed to be robust against (abrupt) electrical power outages. Data modifications of a file will be written in several, definable transactions, where each change only will be committed completely. Unfinished operations will be revoked. It’s designed for NAND-Flash-Memories particularly. In contrary to other file systems it is able to guarantee a reliability in transaction on file-level. The user has the option to define the point of validation of modified data, in easiest case by closing the file-handle. In this way important data can be stored permanently and safely.

#### Features
- Modifying file contents can be accepted only in completed operations (state-transition)
- During modification transitions can also be accomplished by using explicit calls within the application (FlushFileBuffers)
WATCH DOG

PC systems can use the “WATCHDOG” function. The term “WATCHDOG” is usually used for a component of a system that monitors the function of other components. If a possible fault is detected, it is either signaled according to the system agreement or a corresponding step instruction is initiated which corrects the current problem. The signal or jumper commands directly serve as a trigger for other cooperating system components to solve the problem. The integrated controllers are completely independent of CPU and software. For this reason, the WATCHDOG can act as a reliable monitor to monitor the regular WATCHDOG RESET event that must be performed by operating system tasks or by the SystemGuard utility. If the retrigger events do not arrive in time, a malfunction of hardware or software must be accepted, then the system is restarted.

Benefits

- Additional reliability
- The watchdog itself is independent of the operating system and any application software
- Additional BIOS POST watchdog and/or BIOS BOOT watchdog
- Easy set-up of watchdog functionality possible via BIOS setup and SystemGuard utility
- Integration into customer applications through programming interface

Supported Mainboards

<table>
<thead>
<tr>
<th>Mainboard</th>
<th>BIOS POST WATCHDOG</th>
<th>BIOS Boot WATCHDOG</th>
<th>OS WATCHDOG</th>
</tr>
</thead>
<tbody>
<tr>
<td>D3313-S</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>D344x-S</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>D3417-B</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>D3402-B</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>D3598-B</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Fujitsu implements the following three various WATCHDOGS:

- BIOS POST WATCHDOG
- BIOS (OS) Boot WATCHDOG
- Operating System Runtime WATCHDOG

Please note, that the implementation of the various WATCHDOG features depends on the mainboard model. All three WATCHDOGS are physical identical, but they are handled by different application levels.

The mainboards provide full BIOS POST-, Operating System Boot-, and Operating System-Runtime watchdog supervision.

How to handle the different WATCHDOG levels?

- BIOS POST WATCHDOG
  - No user interaction possible
  - POST WATCHDOG is always enabled

- BIOS Boot WATCHDOG
  - Set WATCHDOG in BIOS Setup
    - 0 = WD disabled
    - 1–255 = WD enabled (timeout = 1–255 minutes)

- OS WATCHDOG
  - Use "WATCHDOG software agent" to stop or retrigger the WATCHDOG during OS runtime

The following diagram shows the sequence after powering on the system.
Erase Disk
Erase Disk is a Fujitsu Technology Solutions feature embedded in the system firmware to erase all data reliably from a hard disk. The main purpose of this feature is to delete all data from the hard disk before it will be changed or the complete system will be sold. It can be also used whenever a hard disk should be deleted, for example before a new operating system will be installed.

The great benefits against other software are
- No additional cost, because it is included in the system
- A part of the BIOS can’t get lost during the lifetime of the board

Description
This application itself is called EraseDisk and it is a part of the UEFI Firmware at the end of the PowerOnSelfTest (POST).

To erase all data from the hard disk you have to do the following steps

1. The application can only be selected and deleted if you have set an Admin password
2. Start the BIOS and set the switch from EraseDisk to enable. After reboot you have to enter your admin password for security purpose
3. A dialog will be displayed which allows you to select a specific, several or all hard disk – depending on the number of attached hard disks in the system
4. Select a hard disk which shall be deleted

EraseDisk offers you four different options how to delete your hard disk from “fast” to “very secure”
- Zero Pattern (1 pass) overwrite the flash with “0” in 1 pass
- German BSI / VSITR (7 pass) 6 pass overwrite with changing numbers, last pass with “010101”
- DoD 5220.22-M ECE (7 pass) 7 pass overwrite with random numbers, (DoD=Department of Defense)
- Guttmann (35 pass) 35 pass overwrite with certain values after a certain pattern, not more up today

5. Select hard disk deletion algorithm

After the hard disk deletion process, the user can select as follows which tasks he will be executed by the system.
- Reset password
- Load Setup Defaults
- Shutdown System

6. Select desired tasks

The deletion process will start now. The complete disk erase can be recorded as an audit proof protocol and copied to an external USB drive.

Depending on the selected algorithm the duration ranges from 10 sec. until 10 min. per GByte.

Full Disk Encryption
Full disk encryption (FDE) is a security tool whereby every bit of data is encrypted on the hard disk drive. Encryption involves converting information into unreadable code, which cannot be deciphered easily by unauthorized users. Thus full disk encryption prevents unauthorized access to the stored data.

FUJITSU OEM Mainboards are able to support this feature which is mainly a HDD feature.

Trusted Platform Module
Trusted Platform Module (TPM) is a security feature available on selected Fujitsu OEM Mainboards. The TPM itself is a computer chip (microcontroller) which securely stores information, such as passwords, certificates or encryption keys, used to authenticate your PC or laptop. A TPM can also store information regarding your PC or laptop, enabling you to determine whether your device is trustworthy and has not been breached.

All Fujitsu Skylake-based mainboards provide TPM V2.0 as recommended for MS Windows 10.

<table>
<thead>
<tr>
<th>Type</th>
<th>Win7 (x32/x64) Legacy</th>
<th>Win7 (x32) UEFI</th>
<th>Win7 (x64) UEFI</th>
<th>Win8.1 (x32/x64) Legacy</th>
<th>Win8.1 (x32/x64) UEFI</th>
<th>Win10 (x32/x64) Legacy</th>
<th>Win10 (x32/x64) UEFI</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPM 2.0 Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1) MS Hotfix required: Update to add support for TPM 2.0 in Windows 7 and Windows Server 2008: https://support.microsoft.com/en-us/kb/2920188
Advantech attach great importance to deliver the highest level of threat visibility & protection for their customers – we are not alone

Embedded security solutions from Advantech and those partners, world leading companies like McAfee, Acronis and SUSI help manufacturers to ensure their products and devices are protected from cyberthreats and attacks. Embedded systems and device security solutions span a range of technologies, including application whitelisting, antiviruses and anti-malware protection, device management, and encryption. Solutions can be tailored to meet the specific design requirements for a manufacturer’s embedded device and its architectures.

Acronis True Image 2017 – The No.1 Personal Backup Software
Acronis True Image 2017 is an integrated software suite that ensures the security of all of the information on your PC. It can back up your documents, photos, e-mail, and selected partitions, and even the entire disk drive, including operating system, applications, settings, and all of your data.

- Back up everything in just two clicks
- Get the fastest backup and recovery available
- Protect mobile, social and remote data

Easy Image Backup
Protect everything easily: operating system, programs, settings, files, and boot information.

Simple Two-click Backup
Back up to external drives, network shares, and cloud with just two clicks.

Dual-Protection™
Back up locally to your external drives, network shares, and store copies in the Acronis Cloud.

Mobile Backup
Back up all your phones and tablets to your Windows PC and/or to Acronis Cloud. Manage all devices from touch friendly online dashboard. Migrate your data from Android to iOS and back. Better than native backup!

Remote Backup
Back up remote computers easily and safely.

Social Backup
Protect Facebook photos and posts with automatic, incremental social backup.

More than just Backup – Use powerful features and tools above and beyond backup
- Clone disks and create exact replicas of your system disk to faster or larger storage devices
- Migrate your system to a new computer with Acronis Universal Restore
- Archive files from your computer to cloud storage or an external drive to free up disk space
- Find selected files within backups and archives with powerful search
- Synchronise files between multiple computers and access the most important data any time
- Safely try new software and drivers and roll back to a previous configuration with Try & Decide
- Securely delete temporary files, purge recycle bin, and free disk space with system cleanup

Cloud Features
Get the following benefits when your purchase includes Acronis Cloud Storage:
- Back up files, folders, and full disk images to the Acronis Cloud
- Archive files to the cloud
- Search backup files in the cloud
- Back up mobile devices to the cloud
- Synchronise files to the cloud and between computers
- Gain additional protection with the 3-2-1 rule: Have 3 copies of your data; on 2 different types of storage; 1 being in the cloud
- Implement additional ransomware protection by having a copy in a location not reachable by a virus on your local computer

The Original Full Image Backup
- 14 years & more than 5.5 million users worldwide!
- Back up everything with one solution.

Acronis is faster than all competitors with backup technology to local drives. Cloud archives, backups, and synchronisation take advantage of your entire broadband capability.
- Full image backup
- Multi-platform backup to PC and cloud
- Modern disk drive and NAS device support
- Full computer recovery to dissimilar hardware
- Remote backup plans
- Cloud and local archive
- File synchronisation

... and much more!
McAfee Deliver the Solution

McAfee is one of the world’s leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies’ products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

Data Processing
Secure Software Solution

Advantech Complete Bundle Solution for Security of Embedded Systems – SUSI

SUSI – A Bridge to Simplify & Enhance H/W & Application Implementation Efficiency.

When developers try to write an application that involves hardware entry, they have to study the specifications to write the drivers. This is a time-consuming job and requires lots of expertise. Advantech has done all the hard work for customers with creation of a suite of Software APIs (Application Programming Interfaces), which is called Secured & Unified Smart Interface (SUSI). SUSI provides not only the underlying drivers required but also a rich set of user-friendly, intelligent and integrated interfaces, which speeds up development, enhances security and offers add-on value for Advantech platforms.

McAfee Whitelisting Technology

McAfee Embedded Security Solution is ideal for protecting systems that are fixed-function in terms of CPU or memory resources. Embedded security solutions from McAfee help manufacturers ensure their products and devices are protected from cyberthreats and attacks.

Features
- Low overhead because dynamic whitelisting eliminates manual effort
- Low impact on system performance
- Low CPU and memory requirements
- Low ownership costs result from no-need-to-manage as long as devices are operating well

Key Features 1: Application Control
- Protects against zero-day attacks
- Only authorized software is allowed to run
- Prevents all unauthorized applications from being executed
- Makes sure the machine does what it should do
- Automatically accepts new software added through authorized process

Key Feature 2: Change Control
- Sets access rights for who or which application can access protected data
- Prevents outages resulting from unplanned changes

Key Feature 3: ePolicy Orchestrator
- Fast time to remote deployment/configuration
- Reporting
- Central management
- Compliance requirements
- Monitors data of managed clients

Advantech Complete Bundle Solution for Security of Embedded Systems – SUSI

SUSI – A Bridge to Simplify & Enhance H/W & Application Implementation Efficiency.

When developers try to write an application that involves hardware entry, they have to study the specifications to write the drivers. This is a time-consuming job and requires lots of expertise. Advantech has done all the hard work for customers with creation of a suite of Software APIs (Application Programming Interfaces), which is called Secured & Unified Smart Interface (SUSI). SUSI provides not only the underlying drivers required but also a rich set of user-friendly, intelligent and integrated interfaces, which speeds up development, enhances security and offers add-on value for Advantech platforms.

McAfee Whitelisting Technology

McAfee Embedded Security Solution is ideal for protecting systems that are fixed-function in terms of CPU or memory resources. Embedded security solutions from McAfee help manufacturers ensure their products and devices are protected from cyberthreats and attacks.

Features
- Low overhead because dynamic whitelisting eliminates manual effort
- Low impact on system performance
- Low CPU and memory requirements
- Low ownership costs result from no-need-to-manage as long as devices are operating well

Key Features 1: Application Control
- Protects against zero-day attacks
- Only authorized software is allowed to run
- Prevents all unauthorized applications from being executed
- Makes sure the machine does what it should do
- Automatically accepts new software added through authorized process

Key Feature 2: Change Control
- Sets access rights for who or which application can access protected data
- Prevents outages resulting from unplanned changes

Key Feature 3: ePolicy Orchestrator
- Fast time to remote deployment/configuration
- Reporting
- Central management
- Compliance requirements
- Monitors data of managed clients

Advantech Complete Bundle Solution for Security of Embedded Systems – SUSI

SUSI – A Bridge to Simplify & Enhance H/W & Application Implementation Efficiency.

When developers try to write an application that involves hardware entry, they have to study the specifications to write the drivers. This is a time-consuming job and requires lots of expertise. Advantech has done all the hard work for customers with creation of a suite of Software APIs (Application Programming Interfaces), which is called Secured & Unified Smart Interface (SUSI). SUSI provides not only the underlying drivers required but also a rich set of user-friendly, intelligent and integrated interfaces, which speeds up development, enhances security and offers add-on value for Advantech platforms.

McAfee Whitelisting Technology

McAfee Embedded Security Solution is ideal for protecting systems that are fixed-function in terms of CPU or memory resources. Embedded security solutions from McAfee help manufacturers ensure their products and devices are protected from cyberthreats and attacks.

Features
- Low overhead because dynamic whitelisting eliminates manual effort
- Low impact on system performance
- Low CPU and memory requirements
- Low ownership costs result from no-need-to-manage as long as devices are operating well

Key Features 1: Application Control
- Protects against zero-day attacks
- Only authorized software is allowed to run
- Prevents all unauthorized applications from being executed
- Makes sure the machine does what it should do
- Automatically accepts new software added through authorized process

Key Feature 2: Change Control
- Sets access rights for who or which application can access protected data
- Prevents outages resulting from unplanned changes

Key Feature 3: ePolicy Orchestrator
- Fast time to remote deployment/configuration
- Reporting
- Central management
- Compliance requirements
- Monitors data of managed clients
FSP

The GDPR is pushing a manufacturer to build robust systems. The basis for a system is always the power supply. Having a robust power supply can be addressed by a redundant strategy against failure of a power supply or a battery buffered power supply against failure of the power input itself. A robust power supply will help to avoid data corruption.

Redundant Power Supplies

Redundant Power Supplies for seamless switching between two or three independent Power Supplies in case of defect on one Power Supply is very important to safe data in networking servers and cloud systems.

Features
- Alert-LED identifies the defect Power Supply
- Monitoring the power supplies via software tools and PMBus functionality
- Typically less than 18ms Hold-Up-Time
- Hot swappable for replacement and maintenance
- Highest efficiency and reliability due to selected components

Uninterruptible Power Supplies

Uninterruptible Power Supplies are mandatory for systems where failures are not acceptable. They provide uninterrupted power in case of power failure and ensure the voltage quality. There are different types of UPSs.

Features
- Off-Line UPSs
  - Starts to feed the system typically 2-10 ms after power failure
- On-Line UPSs
  - draw power through the power conditioning and charging components continuously
- Line-Interactive UPSs
  - are a mixture between Off- and On-Line, they start after power failure but the main power is always conditioned by the inverter and the battery charger is connected continuously
- AVR UPSs provide an automatic voltage regulation for constant voltage and power line conditioning combined with a battery
- Highest efficiency and reliability due to selected components

Technical Data

<table>
<thead>
<tr>
<th>Type Series</th>
<th>Feature</th>
<th>Technical Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Off-Line</td>
<td>Champ RM 1k/2k/3k/6k/10k</td>
</tr>
<tr>
<td></td>
<td>On-Line</td>
<td>Proline 60/80/100A</td>
</tr>
<tr>
<td></td>
<td>Line-Interactive</td>
<td>CP750/1000/1500/2000</td>
</tr>
<tr>
<td></td>
<td>AVR</td>
<td>S940/900/1000/1300</td>
</tr>
<tr>
<td></td>
<td>Efficiency</td>
<td>83 % – 93 %</td>
</tr>
<tr>
<td></td>
<td>Battery</td>
<td>12/9 Ah</td>
</tr>
<tr>
<td></td>
<td>Indicators</td>
<td>Load level, Battery level, Line mode, Battery mode, Bipass mode, Fault indicators</td>
</tr>
<tr>
<td></td>
<td>Alarms</td>
<td>Battery mode, Low Battery, Overload, Fault</td>
</tr>
<tr>
<td></td>
<td>Dimensions</td>
<td>D x W x H (mm)</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td>Windows 2000 to Windows 10, Mac, Linux and PowerMgmt. from SNMP and Web browser</td>
</tr>
<tr>
<td></td>
<td>Input</td>
<td>110 – 280 Vac / 46–70 Hz</td>
</tr>
<tr>
<td></td>
<td>Output</td>
<td>200–240 Vac / 47–63 Hz</td>
</tr>
<tr>
<td></td>
<td>Efficiency</td>
<td>83 % – 93 %</td>
</tr>
<tr>
<td></td>
<td>Battery</td>
<td>12/9 Ah</td>
</tr>
<tr>
<td></td>
<td>Indicators</td>
<td>Load level, Battery level, Line mode, Battery mode, Bipass mode, Fault indicators</td>
</tr>
<tr>
<td></td>
<td>Alarms</td>
<td>Battery mode, Low Battery, Overload, Fault</td>
</tr>
<tr>
<td></td>
<td>Dimensions</td>
<td>D x W x H (mm)</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td>Windows 2000 to Windows 10, Mac, Linux and PowerMgmt. from SNMP and Web browser</td>
</tr>
<tr>
<td></td>
<td>Input</td>
<td>110 – 280 Vac / 46–70 Hz</td>
</tr>
<tr>
<td></td>
<td>Output</td>
<td>200–240 Vac / 47–63 Hz</td>
</tr>
<tr>
<td></td>
<td>Efficiency</td>
<td>83 % – 93 %</td>
</tr>
<tr>
<td></td>
<td>Battery</td>
<td>12/9 Ah</td>
</tr>
<tr>
<td></td>
<td>Indicators</td>
<td>Load level, Battery level, Line mode, Battery mode, Bipass mode, Fault indicators</td>
</tr>
<tr>
<td></td>
<td>Alarms</td>
<td>Battery mode, Low Battery, Overload, Fault</td>
</tr>
<tr>
<td></td>
<td>Dimensions</td>
<td>D x W x H (mm)</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td>Windows 2000 to Windows 10, Mac, Linux and PowerMgmt. from SNMP and Web browser</td>
</tr>
</tbody>
</table>
The Defenses of the Standard Microcontroller

In the midst of the rise of IoT, Industry 4.0 and robotics, microcontrollers are increasingly becoming a protective shield from tampering and cyber-attacks. Various microcontroller families are already equipped with an arsenal of security features. Once the European General Data Protection Regulation (GDPR) enters into legal force in May 2018, businesses must have implemented the data security standards specified therein. The law regulates the pseudonymization and encryption of personal data much more stringently, with new resilience and accountability provisions compared to the previous legal basis in Germany.

The GDPR affects not only manufacturers but also operating enterprises such as OEMs and network operators. As a central control and regulatory component, microcontrollers have a key role to play in networked systems. Manufacturers are already working with development processes that are certified in accordance with corresponding security standards. With a secured production chain, semiconductor manufacturers also offer their customers secure end-to-end solutions. STMicroelectronics was recently the first microelectronics component manufacturer to receive the “France Cybersecurity Label” for microcontroller solutions that combine maximum security and flexibility for a variety of target markets.

Security Takes on Different Meanings for Each Application

In security terms, the target applications can be broken down into different microcontroller categories:
- Authentication solutions and TPMs (Trusted Platform Modules), e.g. for trademark protection and IoT networks
- Banking and ID solutions for traditional smartcard enterprises in the fields of payment, personal identification, transportation and paid TV content
- Mobile security solutions for SIM-based solutions in mobile products and machine-to-machine (M2M) applications
- Automotive solutions for near-field communication (NFC, eSE) and safe driving

Integrated Data Security Features

Within the IoT and in Industry 4.0 and robotics, standard microcontrollers for industrial and consumer applications are usually used (general purpose microcontrollers). Models with integrated security features are already available in this field. Our Linecard possesses a variety of features that offer protection as regards:
- Identification theft (anti-tampering mechanisms, integrity checks, traceability)
- Throttling of data services
- Data and code interception and tampering (memory protection, rights management, debug levels, anti-tampering mechanisms, integrity checks, secure firmware updates)
- Physical or mechanical attacks (anti-tampering mechanism on module)

These features are mainly integrated into the chip and ensure robust authentication, integrity of the platform and consistent data security, thereby ensuring the privacy of the end user and providing comprehensive protection of data, IP and trademarks – thereby also satisfying the highest standards when it comes to data security in standard products. Typical target applications include printers, computers, gateways, IoT end nodes and sensors.

Hardware-Based Functions

Integrity & Safety

The cyclic redundancy check determines a check value that enables errors in data transmission or storage to be detected. This means that it is not only possible to check the integrity of the data but also verify the signature of the software while it is running.

The secured power supply monitoring system (POR [Power on RESET] / PDR [Power down RESET] / BOR [Brown out RESET] / PVD [Programmable Voltage Detector] flag status) enables the reason for a reset to be identified and ensures that it has been conducted on the basis of legitimate access. It is supplemented by the “read while writing” function for efficient tampering detection and logging.

The Clock Security System (CSS) is based on the clock and the system upon restoration, as well as internal and external clocks functioning independently of one another. The Watchdog and Window Watchdog also monitor the time windows independently of one another.

The integrity and trustworthiness of the memory contents are ensured using Error Correction Code (ECC) and parity checking. It also offers expanded protection from attacks aimed at sneaking in errors. A temperature sensor continuously monitors the ambient temperature of the IC to prevent it from deliberately being heated above its specified range, permanently damaging it.

Encryption Methods

Encryption methods protect a source text from unauthorized access by encrypting the original plaintext using a code. Breaking the code enables the hacker to decode the encrypted text. More sophisticated cryptographic methods use symmetric or asymmetric encryption. With symmetric encryption, there is only one key with encryption and decryption, meaning that the sender and receiver use the same key.

With asymmetric methods, each of the communication partners uses their own key, which is used to generate a key pair. This consists of a public key, which is used to encrypt the data, and a private key, which decrypt it.

For example: Symmetric method – Certain STM32 series have a genuine random number generator, used to generate 32 bit keys for encryption, integrated entirely into the chip.
Some microcontroller parts also have fully integrated hash only one key, key management is simpler than with asymmetric encryption. The advantage of the symmetric method is that, because there is an asymmetric encryption engine in hardware, an outstanding feature. Additionally, Renesas RX-family and Synergy S5 & S7 series offer AES-128. Such symmetric encryption standard is also available within dedicated MCU/MPU-families of few other suppliers (e.g. Renesas RX, Renesas Synergy and Toshiba TZ1000) (see cross list).

The encryption is based on the symmetric Advanced Encryption Standard (AES), whereas STM32F2, F4, F7, L4 series employing a key length of 128 bits (AES-128) and 256 bit (AES-256) with a variety of methods (ECB, CBC, CTR, GCM, GMAC, CMAC), while STM32L0 / L1 employing a key length of 128 bits (AES-128). Such symmetric encryption standard is also available within dedicated MCU/MPU-families of few other suppliers (e.g. Renesas RX, Renesas Synergy and Toshiba TZ1000) (see cross list).

Additionally, Renesas RX-family and Synergy S5 & S7 series offer asymmetric encryption engine in hardware, an outstanding feature. The advantage of the symmetric method is that, because there is an asymmetric encryption engine in hardware, an outstanding feature. The encryption is based on the symmetric Advanced Encryption Standard (AES), whereas STM32F2, F4, F7, L4 series employing a key length of 128 bits (AES-128) and 256 bit (AES-256) with a variety of methods (ECB, CBC, CTR, GCM, GMAC, CMAC), while STM32L0 / L1 employing a key length of 128 bits (AES-128). Such symmetric encryption standard is also available within dedicated MCU/MPU-families of few other suppliers (e.g. Renesas RX, Renesas Synergy and Toshiba TZ1000) (see cross list).

Some microcontroller series also have RTC register protection, which blocks unauthorized write operations and operates independently of the system reset, but does not include protection when writing a sequence of keypresses. If tampering is detected, the backup register ensures that the written content is automatically deleted. The communication channels can also be selectively blocked with a GPIO communication block. This prevents selected general purpose inputs/outputs (GPIO), and the block can be removed upon next reset.

Debug Block
The debug block prevents unauthorized access to the microcontroller via a debug interface. The security level can be selected for each application or requirement, although it cannot be downgraded again after that point.

Access Rights Management
Access rights confer upon users or user groups the authority to perform certain actions. To this end, the integrated memory protection unit (MPU) divides the memory into regions with different access rights and rules.

Security in General Purpose Microcontrollers

### Hardware-Based Functions

#### Encryption Methods
The encryption is based on the symmetric Advanced Encryption Standard (AES), whereas STM32F2, F4, F7, L4 series employing a key length of 128 bits (AES-128) and 256 bit (AES-256) with a variety of methods (ECB, CBC, CTR, GCM, GMAC, CMAC), while STM32L0 / L1 employing a key length of 128 bits (AES-128). Such symmetric encryption standard is also available within dedicated MCU/MPU-families of few other suppliers (e.g. Renesas RX, Renesas Synergy and Toshiba TZ1000) (see cross list).

The encryption is based on the symmetric Advanced Encryption Standard (AES), whereas STM32F2, F4, F7, L4 series employing a key length of 128 bits (AES-128) and 256 bit (AES-256) with a variety of methods (ECB, CBC, CTR, GCM, GMAC, CMAC), while STM32L0 / L1 employing a key length of 128 bits (AES-128). Such symmetric encryption standard is also available within dedicated MCU/MPU-families of few other suppliers (e.g. Renesas RX, Renesas Synergy and Toshiba TZ1000) (see cross list).

Some microcontroller parts also have fully integrated hash functions, where data is hashed and scattered, and the function maps a larger amount of input to a smaller amount of target data. There is also the keyed-hash message authentication code (HMAC). The structure of this message authentication code (MAC) is based on a cryptographic hash function. HMACs are specified in RFC (Request for Comments) 2104 and in the NIST (National Institute of Standards and Technology) standard FIPS 198.

**Anti-Tamper Mechanism**
The anti-tamper mechanism is used to defend against deliberately or unintentionally launched physical attacks against the hardware system outside of the microcontroller. The backup domain, which references various wake-up sources, ensures that protection is maintained even in low-power mode. The real-time clock (RTC) timestamps each tamper event.

Some microcontroller series also have RTC register protection, which blocks unauthorized write operations and operates independently of the system reset, but does not include protection when writing a sequence of keypresses. If tampering is detected, the backup register ensures that the written content is automatically deleted. The communication channels can also be selectively blocked with a GPIO communication block. This prevents selected general purpose inputs/outputs (GPIO), and the block can be removed upon next reset.

**Debug Block**
The debug block prevents unauthorized access to the microcontroller via a debug interface. The security level can be selected for each application or requirement, although it cannot be downgraded again after that point.

**Access Rights Management**
Access rights confer upon users or user groups the authority to perform certain actions. To this end, the integrated memory protection unit (MPU) divides the memory into regions with different access rights and rules.

### Software-Based Encryption Methods
The security functions implemented in hardware can also be supplemented with software-based solutions. Cryptographic library packages are available for different microcontroller families with a range of cryptographic algorithms. They are provided as standard in binary object format, and can also be provided in source code form under the terms of an NDA-based license. A hardware expansion is also available to provide certain groups of integrated circuits with functional support.

During data transfer, the firewall isolates the code or data component of the flash memory or SRAM from the remainder of the code executed outside of the protected area. The firewall is more restrictive than the memory protection unit (MPU) and is only integrated into the STM32L0, L4 and Renesas Synergy S5 & S7.

**Memory Protection**
Read protection is used to manage how memory is accessed. Memory dumps and backups of user IPs for instance are not permitted. Write protection enables each sector to be protected from unwanted write operations. Proprietary code protection allows each memory region to be configured as “execute only”, meaning that only code may be executed here – it is not possible to write to this region. IPs and confidential data can be securely deleted using the mass erase or secure erase functions. This function resets the memory entirely to its factory state.

**Traceability of Data**
Many microcontroller series have a specific, unique 96 bit ID to ensure that an end product is traceable. This can also be used for the diversification of security keys.

Many series also have functions enabling a secure firmware update.

For sophisticated IoT solutions, there is also the option of utilizing another on-board module – the STSAFE-A100 from STMicroelectronics or the OPTIGA family from Infineon are supplied as a ready-to-run solution with a secure operating system. This latest generation of secure microcontrollers enhances authentication and data management service security for local and remote host PCs, smart home, smart city and industrial applications, electronic entertainment devices and all kinds of other end devices, utilities and accessories.
## Security Features Built in General Purpose MCUs – Industrial & Consumer Purpose

The cross list for security features refers to MCU families whereas each sub-line within MCU family contains at least one part number with listed security features. The portfolio listed is usually silicon based / hardware integrated. Exception: the SW based methods of encryption and the Crypto HW feature.

### Table: Security Features Built in General Purpose MCUs

<table>
<thead>
<tr>
<th>Supplier</th>
<th>STMicroelectronics</th>
<th>Infineon</th>
<th>Renesas</th>
<th>Toshiba</th>
<th>EPSON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family</td>
<td>Proprietary</td>
<td>CortexM0+</td>
<td>CortexM4</td>
<td>Proprietary</td>
<td>Cortex M</td>
</tr>
<tr>
<td>Series</td>
<td>STML1/ STML5</td>
<td>STML1/ STML1</td>
<td>STML1/ STML1</td>
<td>STML1/ STML1</td>
<td>STML1/ STML1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>STML1</th>
<th>STML1</th>
<th>STML1</th>
<th>STML1</th>
<th>STML1</th>
<th>XMC1x</th>
<th>XMC4x</th>
<th>RL78</th>
<th>RX</th>
<th>RZ</th>
<th>Synergy S1</th>
<th>Synergy S3</th>
<th>Synergy S5 &amp; S7</th>
<th>TEZxxx</th>
<th>TXZ</th>
<th>S1C17</th>
<th>S1C31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity &amp; Safety</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>CRC Calculation Unit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power Supply Integrity Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read While Write</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clock Security System (CSS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error Correction Code (ECC)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parity Check</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temperature Sensor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Watchdog</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random Number Generator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hashing Functions &amp; HMAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systematic Cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric Cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric Key Generation (AKeG)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crypto Software Package</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random Number Generator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hashing Functions &amp; HMAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systematic Cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric Cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antt Tamper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup ROM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTC (Warm Timestamp)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTC Register Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Registers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QPD Configuration Locking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debug Lock</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JTAG or SW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proprietary Code Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Erase</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traceability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Update</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software FSU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes:
- **X** indicates feature available.
- **-** indicates feature not available.
- **(0)** indicates feature not available at each sub-line of mentioned MCU family.
- **RL78** indicates Renesas RL78: Device Electronic 64-bit Unique ID only.
- **Epson** indicates: Even NOT available currently, could be included in new products 6th.
## Security Features in General Purpose MCUs of STM32 Family

### Integrity & Safety 1/2

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefit</th>
<th>STM32 Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRC calculation unit</td>
<td>Used to verify data transmission or storage integrity</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4</td>
</tr>
<tr>
<td>Power Supply Integrity Monitoring</td>
<td>Ultra-safe supply monitoring (POR/PDR/BOR/PVD)</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4</td>
</tr>
<tr>
<td>Read While Write</td>
<td>For efficient tamper detection logging</td>
<td>F3,F4,L0,L1,L4</td>
</tr>
<tr>
<td>Error Correction Code (ECC)</td>
<td>Robust memory integrity</td>
<td>F3,F4,F5,F7,L1,L1,L4</td>
</tr>
<tr>
<td>Parity check</td>
<td>Memory content integrity check</td>
<td>F0,F1,L4</td>
</tr>
<tr>
<td>Temperature Sensor</td>
<td>Check if device is operating in expected temperature range.</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4</td>
</tr>
<tr>
<td>Watchdogs</td>
<td>Independent watchdog and window watchdog for software timing control</td>
<td>L0,L1,L4</td>
</tr>
</tbody>
</table>

### Crypto – Hardware

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefit</th>
<th>STM32 Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Number Generator (RNG)</td>
<td>True RNG is done entirely by the hardware. It delivers 32 bit random numbers</td>
<td>F2,F4,L0,L4,F7</td>
</tr>
<tr>
<td>Hashing Functions &amp; HMAC</td>
<td>ND5, SHA-1, SHA-2</td>
<td>F2,F4,F7</td>
</tr>
<tr>
<td>AES/128 Bits (ECB, CBC, CTR)</td>
<td>AES-128/256/512 bits (ECB, CBC, CTR, GCM, GMAC, CMAC) (only L4)</td>
<td>F2,F4,F7,L1,L4</td>
</tr>
</tbody>
</table>

### Crypto – Software

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefit</th>
<th>STM32 Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Number Generator (RNG)</td>
<td>On-chip entropy generation. Ensure strong keys, protect against replay attacks. (LM5098)</td>
<td>Based on DQRG-AES-128; F0,F1,F2,F3,F4,F7,L1,L0,L4</td>
</tr>
<tr>
<td>Hashing Functions &amp; HMAC</td>
<td>Hash algorithm provides a way to guarantee the integrity of information, verify digital signatures and message authentication codes. (ND5, SHA-1, SHA-2/256, SHA-3/512, LM5098)</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4</td>
</tr>
<tr>
<td>STM32 cryptographic library package:</td>
<td>AES/128/256/512 bits (ECB, CBC, CTR, GCM, CMAC, GMAC, CMAC) (only LL4)</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4</td>
</tr>
<tr>
<td>RSA signature function with PKCS#1v1.5</td>
<td>ECC (Elliptic Curve Cryptography): Key generation, Scalar multiplication, ECDSA (LM5098)</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4</td>
</tr>
</tbody>
</table>

### Debug Lock level 0,1,2

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefit</th>
<th>STM32 Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>JTAG or SWD</td>
<td>Prevent unauthorized access to the device through debug interfaces</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4</td>
</tr>
<tr>
<td>Memory Protection Unit (MPU)</td>
<td>The processor MPU is a component for memory protection. It divides the memory map into a number of regions with privilege permissions and access rules</td>
<td>F1,F2,F3,F4,F7,L1,L4,L4</td>
</tr>
<tr>
<td>Firewall</td>
<td>Even more restrictive than MPU. Made to protect a specific part of code or data Flash Memory, and/or to protect data into the SRAM from the rest of the code executed outside the protected area</td>
<td>L0,L4</td>
</tr>
</tbody>
</table>

### Privileges Permission Management

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefit</th>
<th>STM32 Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory Protection Unit</td>
<td>The processor MPU is a component for memory protection. It divides the memory map into a number of regions with privilege permissions and access rules</td>
<td>F1,F2,F3,F4,F7,L1,L4,L4</td>
</tr>
<tr>
<td>FireWall</td>
<td>Safety remove IPs and confidential data. Forcelfactory reset</td>
<td>L0,L4</td>
</tr>
</tbody>
</table>

### Memory Protection

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefit</th>
<th>STM32 Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Protection (RDP)</td>
<td>Global memory access control management. Prevents memory dumps, safeguarding user’s IPs</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4,L5,F0,F1,F2,F3,F4,F7,L1,L4,SRAM</td>
</tr>
<tr>
<td>Write Protection (WRP)</td>
<td>Each sectors can be protected against unwanted write operations</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4,SRAM</td>
</tr>
<tr>
<td>Proprietary Code Protection (PCROP)</td>
<td>Each Sector can be configured in “execute only,” “execute with read,” “execute with read and write,” “execute with read and write and execute only”</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4,SRAM</td>
</tr>
<tr>
<td>Device Electronic 96 Bit Unique ID</td>
<td>Enables product traceability; Can be used for security key diversification</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4</td>
</tr>
</tbody>
</table>

### Traceability

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefit</th>
<th>STM32 Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Electronic 96 Bit Unique ID</td>
<td>Enables product traceability; Can be used for security key diversification</td>
<td>F0,F1,F2,F3,F4,F7,L1,L4</td>
</tr>
</tbody>
</table>

### Secure Firmware Update

<table>
<thead>
<tr>
<th>Features</th>
<th>Benefit</th>
<th>STM32 Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software FSU</td>
<td>Secure firmware upgrade capability</td>
<td>F2,F4,F7</td>
</tr>
</tbody>
</table>
Security of Automotive MCUs – EVITA and SHE Security Features

EVITA and SHE are major security initiatives in the automotive world which define security standards. In order to harden ECUs against security attacks, the security mechanisms should prevent successful manipulation of SW, data, keys and keying material – so they must be rooted in hardware. The Secure Hardware Extension (SHE) specification known as an Automotive initiative of the HIS working before 2010 has meanwhile been accepted as an open and free standard. The SHE specification defines a portfolio of functions and a programmer’s model (API) enabling a secure zone to coexist within any electronic control unit installed in the vehicle. The most significant features inside a secure zone are storage and management of security keys, plus encapsulating authentication, encryption and decryption algorithms that application code can access through the API. These features help maximize flexibility and minimize costs.

EVITA – E-Safety Vehicle Intrusion Protected Applications

The project EVITA, which is coordinated by the Fraunhofer SIT has the aim of the provision of a cost-effective hardware security architecture fulfilling the requirements of present on-board security issues. The following general categories are considered to be protected:

- Vehicle-to-X (V2X) communication
- On-board communication between actors, sensors and electronic control unit (ECU)
- Integration of mobile devices
- Diagnosis processes
- Vehicle safety applications
- Drivers privacy

Therefore, security methods have to be implemented in hardware like hashing routines, authentication protocols and encryption algorithm. Furthermore, the ECUs have to be protected against tamper, unauthorized cloning and thievery. EVITA is an open specification to offer the benefits to the whole automotive industry. In order to harden ECUs against security vulnerabilities of V2X communications. Therefore electronic signatures must be created / verified. A very efficient asymmetric cryptographic engine is needed in order to meet the specified security performance. Sufficient for a maximum of security life time.

Full EVITA HSM

Provides the maximum level of functionality, security and performance of HSM variants. Focus on protecting in-vehicle domain against security vulnerabilities of V2X communications. Therefore electronic signatures must be created / verified. A very efficient asymmetric cryptographic engine is needed in order to meet the specified security performance. Suitable for a maximum of security life time.

Medium EVITA HSM

Focus on securing on-board communication with the ability to perform several non-time-critical asymmetric cryptographic operations in SW, e.g. in order to establish shared secrets. All internal communication protection is based on symmetric cryptographic algorithms. Compared to the full version it comes without the integrated asymmetric cryptographic building block and allows only a reduced CPU performance (e.g. 25 MHz vs. 100 MHz).

The Hardware Security Modules (HSM)

The Hardware security module (HSM) components are splitted into mandatory / optional components. Depending on the use cases, different security requirements must be considered. For cost-effective HW-solutions, three different EVITA HSM variants are specified with different security level.

- **Internal Clock**: w/ incl. external UTC synchron.
- **Internal NVM (Non Volatile Memory)**
- **Counter (16 x 64 bit)**
- **Tamper Protection (HW)**
- **Parallel Access-Multiple sessions**

**CPU internal**

- **CPU programmable**
- **CPU PRESET**

**Boot Integrity Protection:**

- **Authentication & Secure**
- **Boot Protection**

**Random Number Generator**

- **…based on PPRG w/ TRNG seed**

**Crypto algorithms, incl. key generation (HW)**

- **AES / MAC**
- **Options: ECDH, ECDH, HWRHPOOL / HWRHPOOL**

**Crypto acceleration (HW)**

- **AES**
- **ECC, HWRHPOOL**

Automotive Security Level Classification

<table>
<thead>
<tr>
<th>Type</th>
<th>SHE</th>
<th>EVITA Light</th>
<th>EVITA Medium</th>
<th>EVITA Full</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Clock</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Internal NVM (Non Volatile Memory)</td>
<td>X</td>
<td>X (optional)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Counter (16 x 64 bit)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Tamper Protection (HW)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Parallel Access-Multiple sessions</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>CPU internal</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>…CPU programmable</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>…CPU PRESET</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Boot Integrity Protection:</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Authentication &amp; Secure</td>
<td>Secure only</td>
<td>X (optional)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Random Number Generator</td>
<td>…based on PPRG w/ TRNG seed</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Crypto algorithms, incl. key generation (HW)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AES / MAC</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Options: ECDH, ECDH, HWRHPOOL / HWRHPOOL</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Crypto acceleration (HW)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Components for different EVITA HSM`s, suggested in publications

Security requirements and related functional requirements considered for EVITA

- **Integrity / authenticity of e-safety related data:**
  - in terms of origin, content, and time. Forgery of such information, tampering, or replay of this information should be at least detectable
  - Integrity / authenticity of ECU / firmware installation / configuration: Any replacement / addition of an ECU, also with related firmware or configuration to the vehicle must be authentic in terms of origin, content, and time
  - Secure execution environment:
    - Limited consequences requested on separate / more trusted zones of the platform, in case of a successful ECU attack
    - Vehicular access control:
      - Control requested in regard to the access of vehicular data and functions
    - Trusted on-board platform:
      - Integrity / authenticity of operated software has to be ensured
  - Secure in-vehicle data storage:
    - in regard to ensure access control and integrity, freshness and confidentiality of data stored within a vehicle

- **Confidentiality of certain on-board or external communication:**
  - in regard to confidentiality of existing software / firmware, updates and security credentials which must be ensured
  - **Privacy data:**
    - for personal data stored within a vehicle, contained in messages sent from vehicle to the outside
  - **Interference of security functionality:**
    - availability of bus systems, CPUs, RAM and wireless communication technologies must be ensured [2]

**Source:**


Data Processing
Microcontroller

EVITA and SHE Security Features – Automotive

The Automotive HSM
The HSM Block consists of HW embedded mandatory functional blocks:

- Secure Storage
  HW embedded Internal RAM and Internal NVM PFlash/DFlash

- Crypto HW Acceleration
  basically with HW embedded Symmetric Crypto Engine.

- Further blocks are available as option:
  - Symmetric Crypto Engine
  - Asymmetric crypto engine (optional)
  - TRNG/PRNG (optional)
  - Hash Engine (optional)
  - Counters (optional)

Secure CPU Core
CPU architecture and specific HW embedded features dedicated for highest possible security. It incorporates a Tamper – resistant processor and several security features based on dedicated hardware implementation. It is optimized for Security applications, known primarily from tamper-resistant smart cards, also suited for usage of advanced payment systems, electronic passwords and others. It is now migrating into an area of transporting, vehicle etc.

HW-Interface
enables data exchange and interrupt request exchange with application core.

Application Core
The Application Core consists of a Application CPU and Bus Interface, e.g. a CAN Interface, as well as Shared area RAM for data exchange and/or an Application NVM (PFlash/DFlash).

Interrupts are exchanged between HSM block (HW interface) and the Application Core (Application CPU Core). Data are exchanged between HSM block (HW interface) and the Application Core (“Shared area RAM”).

Source: https://www.evita-project.org/Publications/AEHR10.pdf
Security Features for Automotive & Industrial Purpose

### Security Features for STM8Ax Series

<table>
<thead>
<tr>
<th>Feature</th>
<th>STM8A-F</th>
<th>STM8B-L</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerSupply integrity monitoring</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Read White</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Clock Security System (CSS)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Error Correction Code (ECC)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Parity check</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Temperature Sensor</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Watchdogs</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Random Number Generator (RNG)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Hashing functions &amp; HMAC</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Symmetric Cryptography</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Asymmetric Cryptography</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Key Management</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>WATCHDOG</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Power Supply Int.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Internal Voltage Regulator</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Clock Security System</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Error Correction Code</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Temperature Sensor</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Watchdogs</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### Security Features for Aurix 1./2. Generation – TC2xx / TC3xx Series

<table>
<thead>
<tr>
<th>Feature</th>
<th>TC2xx</th>
<th>TC3xx / TC4xx</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerSupply integrity monitoring</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Read White</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Clock Security System (CSS)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Error Correction Code (ECC)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Parity check</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Temperature Sensor</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Watchdogs</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Random Number Generator (RNG)</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Hashing functions &amp; HMAC</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Symmetric Cryptography</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Asymmetric Cryptography</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Key Management</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>WATCHDOG</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Power Supply Int.</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Internal Voltage Regulator</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Clock Security System</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Error Correction Code</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Temperature Sensor</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Watchdogs</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

### Notes for Aurix

1. READ PFlash while WRITE DFlash, not for READ while Write inside PFlash
2. Features are available in regard to S9A
3. Standby controller: x 8 bit processor and Standby RAM available in TC3xx, NOT in TC2xx
4. Standby controller contains RTI
5. Standby controller executes its own image
6. GDS configuration is protected with safety measures (e.g., ACCEN, ENDINIT)
7. Bridge module in HSM can be understated as Firewall functionality
8. Exclusive flag applicable on HSM code and other protection layers – a Proprietary Code protection feature (PCROP)

---

Data Processing

Microcontroller
CMs have access to customer IP and large quantities of the components they are contracted to produce. It is essential that the original owner of the IP controls their IP and the production volume. Flasher SECURE does both. To prevent counterfeit devices, the Flasher reads out a unique ID from the system which it is going to program. This ID is sent to a server that is under physical control of the IP owner. This server validates the ID and determines whether a programming run is allowed. In this case, a signature is generated for the device. The signature is sent back to the Flasher which stores the signature inside the target device it programs.

This method of secure programming is also in the best interest of the CM. The CM can now boast that the production floor will protect the customers IP.

Firmware running on the system, or an external application communicating with the system, can now verify that the system is genuine. With an additional signature for the firmware, the bootloader in the system can also verify that the firmware is genuine and unmodified. If any of the above verification fails, the device stops working. As each signature is unique for each device, it is not possible to create a non-approved system by simply copying the firmware.

The signature generation uses a proven asymmetric algorithm where the private key is not accessible by anyone but the IP owner. This prevents attackers from forging a signature for a given ID. All communication between Flasher and server is encrypted and authenticated by a secure SSL/TLS connection to prevent unauthorized access. All actions are logged and accessible through an administration interface to provide as much transparency to the IP owner as possible. Small series and mass production environments benefit from the reliability and performance of SEGGER’s in-circuit-programming solution. SEGGER’s production programmers are designed with multiple interfaces, making them easy to integrate into any production environment. In mass production environments, ATE or other production control units can easily access the Flasher for programming including serial numbers and patch data.

100% transparency & security in manufacturing management enables full control and visibility online about all CM activities:
- Account management
- Administration
- User
- Contract manufacturers
- Firmware management
- Firmware binary
- Signature key management
- Project management
- Manufactured volume
- Contract manufacturer
- Production recording
- Logging of programming records
- Report of failed programming tries

As soon as production reaches a certain volume, contract manufacturing is a serious option. Most companies are hesitant to take that route as it introduces a risk to their intellectual property. Proper application of security systems, such as Flasher SECURE, enable these companies to access the next level with confidence.
New Trend to Worry About: Ultrasonic Beaconing

There are already some hundred smartphone apps in the stores which contain ultrasonic beaconing software. If the app has the right to use the microphone of the smartphone, than it will listen in the background to audio codes in the range of 18kHz-20kHz, which cannot be heard by humans. This audio spy technology can be used to track the consumed media or to identify the people within the same room by cross-device tracking. Even more dangerous is the functionality to de-anonymize users and to detect their position.

Actually the main use case is to send personalized advertisements to public displays if a user is close. This kind of marketing can be discussed in a very controversial way of course. We want to make you aware about another scenario: a manufacturer of vending machines, video walls or other public electronic equipment containing a loudspeaker is a potential victim to become infiltrated by 3rd parties with this kind of software code – similar to the use case of DDoS-Attacks, your devices could also be used to send out ultrasonic audio signals to the purpose of others.

How to prevent this scenario? Of course you should take care that nobody can install such a software on your devices. For this you should use a mainboard with TPM and a supporting operation system, as well as security software to detect malware with a frequent update process. Nevertheless you can only be on the safe side if you prevent the emitting of such 18kHz-20kHz audio signals over the loudspeaker. Considerating cost and complexity we recommend to start by building at least a 2nd grade Butterworth filter directly connected to the speaker or – in case you use a separate amplifier – before the amplifier. In any case it should not be a digital filter in the same silicon where the beaconing code could be processed:

2nd order Butterworth (12 dB/Octave)
If you are using a 4 Ω speaker and you want a cut-off frequency of 18 kHz, then you should use $L_2 = 0.05$ mH and $C_2 = 1.56$ µF.
If you are using a 8 Ω speaker, please choose $L_2 = 0.1$ mH and $C_2 = 0.78$ µF.

To be more on the safe side, you can also try to set up the cut-off frequency to 12 kHz to reach a much lower signal at the critical 18 kHz. Therefore you can try $L_2 = 0.075$ mH and $C_2 = 2.34$ µF at a 4 Ω speaker, or $L_2 = 0.15$ mH and $C_2 = 1.17$ µF at a 8 Ω speaker.

The impedance of speaker chassis is rising at higher frequencies and is not stable or linear, so the fine tuning should be done in your individual design. Nevertheless the suggested values give you a good starting point. Here is another example to get a sharper split of amplified and not amplified frequencies, but it will increase your bill of material:

3rd Order Butterworth (18 dB/Octave)
If you are using a 4 Ω speaker and you want a cut-off frequency of 18 kHz, then you should use $L_2 = 0.05304$ mH, $L_3 = 0.01768$ mH, $C_3 = 2.94722$ µF.

For these capacities we recommend the MKP10 series from manufacturer WIMA. They are made for audio requirements up to 250 V. Some examples to order at Rutronik are the order codes KFO9094 for 1 µF, KFO8627 for 1.5 µF, KFO9244 for 2.2 µF, KFO9245 for 3.3 µF. Do not hesitate to ask for the order codes of other specifications.

Parallel to the filtering of playing these frequencies, you can also use a speaker made to avoid playing these ultrasonic beaconing signals. The PUI Audio AS09208AR-R is a wideband speaker with a frequency range of 90 Hz up to 15 kHz. The speaker has an impedance of 8 Ω and can be connected to a 10 W RMS (15 W music) amplifier. The industrial quality ensures an operational temperature range of -20°C up to 60°C, which is good enough for most places of public vending machines or video walls for example.

The picture shows the different use cases of ultrasonic beaconing technology.
Avoiding Visual Spy on Displays

Security is also an important topic in the field of visualization. Taking the easy example of an ATM, the person who is in front of the display needs to have the full view and control of his action. The viewing angle of the TFT must be designed in the way that only the user can see the proceedings on the screen. All the other persons next to the user are of course not allowed to see the transactions which are happening at that moment. So therefore the display-designers need to guarantee a restrictive viewing angle for the security of the user.

Displays are made of a front glass and rear glass, backlighting, liquid crystals and polarizers.

The viewing angles of a display are related to the rubbing angle of the LCD masking within the production. The rubbing angle itself is the trace that guides the flow of the liquid crystal inside the display to reveal the expected view.

The polarizer can be produced in a way to influence the viewing angles through his structure on the surface. Another security point in our ATM example is the fact that the user wants to quit the application without leaving any traces of finger prints on the screen. That could make a “review” of the PIN input possible. Therefore many displays use a touchscreen with an anti-fingerprint function.

Most smartphones have the AFP (Anti Finger Print) included. This special coating of the display glass or cover glass avoids traces of dust, scratches and the finger print itself.

Avoiding Visual and Printed Spy on Keyboards and Number Pads

If a user has to type in a password on a keyboard or a pin-code on a number pad, the input can be observed by Outsiders. To avoid such lack in security we recommend using a biometrical sensor to ensure the identity of an authorized user.

Fingerprint Solutions from BYD

- Product line is complete, can be used for mobile phone back, front and side
- Perfect industrial chain layout, has a good capacity to support
- Package support cutting, mobile ID design more flexible
- Support different module structure, such as
  - “Plastic package + Coating”
  - “Plastic package + Cover” and
  - “Under-glass”
- Use unique patented “synchronous excitation” capacitance detection scheme, no need for metal ring, single chip implementation, cost-effective
- Own software algorithm, without authorization fee, with ultra low FAR and FRR, the user experience is better
- For different hardware platforms and software systems , have mature development experience and production experience, technical support efficiency is high

Avoiding Visual and Printed Spying on Displays, Keyboards and Number Pads

All the digital high tech security mechanisms are useless when it comes to social engineering. If somebody wants to spy your pin-code, password or personal data on a screen, all the security on data transmission, data storage and data processing are obsolete.
Infrared Iris Scanning

Essentially, iris scanners illuminate the eyes with infrared light and a camera takes a picture. Special software then analyzes the picture to detect the iris pattern, which is unique to each individual. After rolling out its first infrared LED for iris scanners in mobile devices, Osram added a version with a slightly angled direction of emission, which aligns with the camera’s field of view. The latest infrared LED, the OsLUX SFH 4787S, is a new version that enables the iris to be illuminated even more uniformly.

Reliable Protection of Devices Thanks to Infrared Iris Scanning and Facial Recognition from Osram

This third-generation Osram IRED for iris recognition meets another need in this application: the brightness differences in the camera images should ideally only originate from the iris pattern and not be additionally caused by a gradient in the illumination. This would mean that the software needs to correct fewer artefacts when determining the iris pattern. With the SFH 4787S, Osram has thus developed an emitter with a flat light, optimizing the reflector and lens to ensure virtually constant intensity across the emitted light beam.

Apart from this, the SFH 4787S is almost identical to its predecessor, the SFH 4786S. Both are based on the compact 3.5 x 3.5 x 1.6 millimeter large OsLUX package. A wavelength of 810 nanometers (nm) delivers high-contrast images for all eye colors. The emission direction is tilted by 8°, while the emission angle is ±18°. The optical output of this highly efficient emitter is 720 milliwatts (mW) at a current of 1 amp, with a radiant intensity of 1,000 milliwatts per steradian (mW/sr).

Iris scans and facial recognition are among the most reliable biometric identification methods and are difficult to fool. Both methods require special infrared LEDs in order to provide reliable protection for mobile devices. Osram Opto Semiconductors is a technology leader in this field. Two years ago, the company was the first to launch an infrared LED that brought iris scanners to smartphones and other mobile devices.

Facial Recognition

Sensor systems for facial recognition record the user’s face and detect typical features independent of facial expressions. However, to identify these features accurately and reliably, the software requires high-quality images. This means illuminating the face brightly and evenly, without shadows – and for this method to work in a wide variety of lighting conditions. The solution lies in illuminating the face also with infrared light. Facial recognition is considered a highly secure form of biometric identification. The system records the user’s face and detects typical features independent of facial expressions.

However, to identify these features accurately and reliably, the software requires high-quality images. This means illuminating the face brightly and evenly, without shadows – and for this method to work in a wide variety of lighting conditions. The solution lies in additional illumination of the face with infrared light.

The SFH 4770S is Osram’s most compact infrared LED (IRED) in the high-power class. Its low height is of particular benefit in smartphones and tablets. The high optical output of typically 1800 mW @ 1.5 A and broad emission characteristics make this IRED ideal for facial recognition and eye-tracking systems which can activate applications in response to blinking instead of the usual double-click.

The basis for the new record emitter is the SYNIOS package which Osram introduced some time ago for LEDs in the visible spectral range for automotive applications. The package is extremely compact, measuring only 2.7 mm x 2.9 mm x 0.6 mm, and offers optimum light extraction. The SFH 4770S is the first component in which this package has been used for infrared emitters. Installed in the IRED is a 1 mm2 emitter chip with a wavelength of 850 nanometers (nm) in which two emission centers are provided with the aid of nanostack technology. Overall, the component delivers a typical optical output of 1800 mW @ 1.5 A with only one chip.

Products for Facial Recognition

Osram SFH 4770S and SFH 4716AS

Secure data transfer is possible thanks to high tech from Osram. Banking apps on smartphones, business e-mails on your laptop, and online shopping on your tablet – our mobile companions need powerful protection against unauthorized access. Special infrared LEDs from Osram Opto Semiconductors provide the basis for reliable iris and face recognition even on mobile devices. The OSLUX and SYNIOS family are used for any kind of access control.

Iris scans and facial recognition methods require special infrared LEDs in order to provide reliable protection against unauthorized access. Special infrared LEDs from Osram Opto Semiconductors provide the basis for reliable iris and face recognition even on mobile devices. The OSLUX and SYNIOS family are used for any kind of access control.

Secure data transfer is possible thanks to high tech from Osram. Banking apps on smartphones, business e-mails on your laptop, and online shopping on your tablet – our mobile companions need powerful protection against unauthorized access. Special infrared LEDs from Osram Opto Semiconductors provide the basis for reliable iris and face recognition even on mobile devices. The OSLUX and SYNIOS family are used for any kind of access control.
Human Vision Components (HVC-P2)

HVC incorporates different image sensing functions like face recognition in an easy-to-mount and compact format to provide image sensing capability to various devices.

Features
- Camera module angle of view: 2 models (50 deg. and 90 deg.) available
- Multiple Functions (10 functions): Body Detection, Face Detection, Hand Detection, Face Direction Estimation, Gaze Estimation, Blink Estimation, Age Estimation, Gender Estimation, Expression Estimation and Face Recognition
- User-friendly, easy implementation through UART or USB

Specifications

<table>
<thead>
<tr>
<th>Function</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Horizontal detection area (angle of view) 50 deg: 54°±3°; 90 deg: 94°±5°</td>
<td></td>
</tr>
<tr>
<td>Vertical detection area (angle of view) 50 deg: 41°±3°; 90 deg: 76°±5°</td>
<td></td>
</tr>
<tr>
<td>Detection distance (differs per function) 3.2 – 16.7 m (HVC-P2 50 deg), 1.6 – 8.6 m (HVC-P2 90 deg)</td>
<td></td>
</tr>
<tr>
<td>Dimensions (W x L x H) 45 x 45 x 8.2 mm (main board for both types) 25 x 25 x 8.7 mm (camera board 50 deg type) 25 x 25 x 15.7 mm (camera board 90 deg type)</td>
<td></td>
</tr>
</tbody>
</table>

Function Results

- Face detection, body detection, hand detection
- Result count (max: 35), center coordinates (X & Y), detection size (pixel), degree of confidence
- Face direction estimation
- Yaw degree, pitch degree, roll degree, degree of confidence
- Gaze estimation
- Yaw degree, pitch degree
- Blink estimation
- Blink degree (left-side eye/right-side eye)
- Age estimation
- Age, degree of confidence
- Gender estimation
- Gender, degree of confidence
- Expression estimation
- 5 expressions: "neutral", "happiness", "surprise", "anger", "sadness" and their respective scores, expression degree (positive/negative)
- Face recognition
- Individual recognition result, score
- Image output
- Choose one: none, 160 x 120 pixels, 320 x 240 pixels
- Image format: 8 bit Y data

Applicable for:
- Workplace
  - AC units targeting people
  - Robots matching people
  - Lights targeting only people
- Home
  - Home appliances matching movement of people
  - AC units targeting people
  - Robots matching people
  - Lights targeting only people
- Outdoors
  - Estimate interest and purchase behavior of people to store goods of interest
  - Vending machines recommending drinks to people

Social Engineering

Avoiding Visual and Printed Spying on Displays, Keyboards and Number Pads

Combine Technologies

Realize EMBEDDED Designs

RUTRONIK EMBEDDED brings together entire solutions to build applications for:
- Digital Signage
- Transportation
- Industrial
- Control Medical

More information: [www.rutronik.com/embedded](http://www.rutronik.com/embedded)
| embedded@rutronik.com | Tel. +49 (0) 7231 801-1776 |
Secure Entry System Based on RFID Security

Rutronik can offer a wide range of ready to use access control systems including turnstiles. The RFID reader system is already integrated and is being managed via TCP/IP. Our range of RFID identity cards, wristbands and key fobs as well as our servers from Advantech or Fujitsu can complete the whole application of a secure entry system using RFID authentication. It is safer than a pin code, because a RFID transponder cannot be copied or spied out like a pin code. Only the risk of losing the transponder or theft is given. We recommend to discuss the individual compilation of components with our product specialists.

Secure Entry Systems

A secure access to sensitive areas is the first barrier to prevent damage, theft and unauthorized operations. An entry system has very often used a pin code terminal, because it was the simplest way to grant access. A pin code is the easiest barrier to hack, so we recommend other solutions.

Social Engineering

Secure Entry System Based on 3D Face Recognition by Video Technology

Combining a turnstile with biometrical sensor technology is the safest solution. One of our latest high tech sensors is the Intel® RealSense™ Technology. This is a collection of hardware and software capabilities that allows you to interact with a device in a non-traditional manner and enables you to develop highly interactive applications or solutions.

There are three combined cameras that act like one:
- a 1080p HD camera
- an infrared camera
- an infrared laser projector
allowing them like the human eye to sense depth and track human motion.

Intel® RealSense™ technology redefines how we interact with our devices for a more natural, intuitive and immersive experience, supported by the powerful performance of Intel® processors.

The infrared projector projects an infrared grid onto the scene and the included infrared camera records the reflection on surfaces to compute the depth information and combine it with the recorded 2D camera record. With the integrated microphone array it is possible to localize sound sources in the space and perform background noise cancellation. With Intel® RealSense™ Software Development Kit and RealSense™ modules, you can create compelling, exciting applications in a variety of application areas, or you can just buy needed modules and cables separately. Face recognition, which is needed to build a secure entry system, is already available in the SDK to allow a quick time to market.
Committed to excellence

Rutronik Elektronische Bauelemente GmbH
Industriestraße 2 | 75228 Ispringen / Pforzheim
Tel. +49 7231 801-0 | Fax +49 7231 82282 | E-Mail: rutronik@rutronik.com | www.rutronik.com

Germany – Headquarters

Rutronik Elektronische Bauelemente GmbH
Tel. +49 7231 801-0 | Fax +49 7231 82282 | E-Mail: rutronik@rutronik.com | www.rutronik.com

Austria:
Rutronik Elektronische Bauelemente Ges. m. b. H.
Durasillstraße 11
4600 Wels
Tel. +43 7242 4 9491

Belgium:
Rutronik Elektronische Bauelemente GmbH
Bvd. Nikola Vaptzarov 35
Bauelemente GmbH
Tel. +49 361 2 28 36-20

Bulgaria:
Rutronik Elektronische Bauelemente GmbH
Blvd. Nikola Vaptzarov 35
Bauelemente GmbH
Tel. +49 361 2 28 36-20

Czech Republic:
Rutronik Elektronische Bauelemente CZ s.r.o.
Pražákova 1008/69, 15. floor
Brno
Tel. +420 5 4 54 24-681

Denmark:
Rutronik Elektronische Bauelemente GmbH
Herstedvesterweg 27-29
2620 Albertslund
Tel. +45 7020 19 63

Estonia:
Rutronik Elektronische Bauelemente GmbH
Tel. +370 37 26 17 80

Finland:
Rutronik Elektronische Bauelemente GmbH
Malminkaari 5
00700 Helsinki
Tel. +358 9 391 22 00

France:
Rutronik S.A.S.
6, Mail de l’Europe
Parc d’Activités de la N ballotte
78170 La Celle St Cloud
Tel. +33 5 49 52 88 88

Germany:
Rutronik Elektronische Bauelemente GmbH
Tel. +49 89 1793 44 1885

Hungary:
Rutronik Elektronische Bauelemente GmbH
ul. Bojkowska 37
Tel. +48 32 4 61 20 00

Italy:
Rutronik Italia S.r.l.
21, Via Cadlera
Centro Direzionale S.Siro
20135 Milano (MI)
Tel. +39 02 409 51-1
italia_MI@rutronik.com

Netherlands:
Rutronik Elektronische Bauelemente GmbH
Landsberger Straße 172
90449 Nürnberg
Tel. +49 911 6 8868-0

Norway:
Rutronik Elektronische Bauelemente GmbH
Mønticas, 5, 1236 Trondheim
Tel. +36 1 361 06 90

Poland:
Rutronik Polska Sp. z o.o.
ul. Bojkowska 37
44-101 Gliwice
Tel. +48 32 461 20 00

Portugal:
Rutronik Elektronische Bauelemente GmbH
Av. General Humberto Delgado
Porto Alegre, Brasil
104-012 V. N. Famalicão
Tel. +351 252 3 12-336

Romania:
Rutronik Elektronische Bauelemente GmbH
Martin Luther Str. no. 2, 3rd floor
01-785 Warszawa
Tel. +48 32 462 70-50

Russia:
Rutronik Elektronische Bauelemente GmbH
ul. Bojkowska 37
104-012 V. N. Famalicão
Tel. +351 252 3 12-336

Serbia:
Rutronik Elektronische Bauelemente GmbH
ul. Bojkowska 37
104-012 V. N. Famalicão
Tel. +351 252 3 12-336

Slovakia:
Rutronik Elektronische Bauelemente GmbH, o.z.
Lazovna 11
97401 Banska Bystrica
Tel. +421 48 472 23-00

Spain:
Rutronik Elektronische Bauelemente GmbH
Molina 5, 1236 Trzin
Tel. +39 06 228 782-1

Sweden:
Rutronik Elektronische Bauelemente GmbH
ul. Bojkowska 37
104-012 V. N. Famalicão
Tel. +351 252 3 12-336

Turkey:
Rutronik Elektronische Bauelemente GmbH
ul. Bojkowska 37
104-012 V. N. Famalicão
Tel. +351 252 3 12-336

UK:
Rutronik Elektronische Bauelemente GmbH
ul. Bojkowska 37
104-012 V. N. Famalicão
Tel. +351 252 3 12-336

United Kingdom & Ireland
Rutronik UK Ltd.
1-3 The Courtyard, Calvin Street
The Valley, Bolton, BL1 8PB
Tel. +44 1793 44 1885

International branches:

USA:
Rutronik Inc.
Parkway Centre
2745 N. Dallas Parkway
Plano TX, 75093
Tel. +1 216 328 8900

Mexico:
Rutronik Mexico S.A. DE C.V.
Av. Armando Rilaela Shapiro
No. 2001 Piso 4 A-11
Corp. Central Park Torre 1, Centro Sur
76090 QUERETARO, Qro.
Tel. +52 442 103 1800

China:
Rutronik Electronics (Shenzhen) Co., Ltd.

Shenzhen:
Room 907, Excellence Bldg.,
No. 98, Fuhan 1 Road
Futian Dist., Shenzhen
Tel +86 755 8240 7106

Shanghai:
Room 1710, Dongchen Tower
No. 60, Mudan Road
Fudong New Dist., Shanghai
Tel. +86 21 8869 910

Chengdu:
Room no. 407, 4F
No. 31 Zong Fu Street
10543 Taiwan
Tel. +886 (2) 2175 2936

Hong Kong:
Rutronik Electronics Asia HK Ltd.

Hong Kong:
54/F, Hopewell Centre
183 Queens Road East, Wan Chai
Hong Kong
Tel. +852 5337 0119

Taiwan:
Rutronik Electronics Asia HK Ltd.

Taipei (Taiwan representative office)
8F, No. 367, Fuxing N. Rd.,
Songshan Dist, Taipei City,
10543 Taiwan
Tel. +886 (2) 2175 2936

Thailand:
Rutronik Elektronische Bauelemente GmbH
2/20 Rom Kla 25/2
Rom Kla Road, Klongsamprawet
Ladkrabang, 10520 Bangkok
Tel. +66 2 737 6423