PHYTEC

Always the right level of
security for your product.

Embedded Security

Security is a continuous process that accompanies your project from development to the end of life in all of its changing phases. The starting point for this is our many years of experience in module development and in the most diverse security requirements of our customer projects.

Take advantage of our expertise to reach your goal faster and more cost-effectively. See security as an opportunity to stand out from the competition.

Smarter. Faster. Easier.

Your Specifications:

Our solutions are the result of your requirements, which we have collected from projects we have already carried out. The requirements are versatile. However, they can often be traced back to common points.

- **Know-how protection** (application, algorithms, hardware circuitry, licenses)
- **Legal compliance**
- **Protection against misuse of your devices** (for example, in the cloud)
- **Networking your devices**
- **Secure data acquisition and transmission**

Our Offer to You:

Our software offers are freely accessible and use open-source solutions. (However, for signing bootloaders, which are verified by the controllers, we have to resort to manufacturer-specific solutions in some cases).

- **Consulting | Workshops**
- **BSP features in our standard BSP and customized solutions**
- **Secure initialization (provisioning) –** the way to ensure your product is secure in an environment worthy of trust
- **Software Life cycle Management**

What the law says:

Cybercrime is real and the demands of law enforcement are many, diverse, and depend on the use of your end product. The following laws must be observed when placing IT products on the market:

- **Cybersecurity Act** – where all products are classified into classes according to the security level
- **Product liability laws** and the state of the technology
- **Federal Data Protection Act BDSG**
- **IT Security Law** for Critical Infrastructures (KRITIS)

Together we can determine the legal requirements relevant to your project and decide on a solution.

How We Work:

We prefer a comprehensive approach and work according to the IEC 62443.
(A short introduction to IEC 62443, orientation guide of the ZVEI can be found at: www.phytec.de/software/security/).

IEC 62443 differentiates between the typical roles in industry: the manufacturer, the integrator, and the operator. The standard implicitly (but often not explicitly) derives certain procedures and concepts from these roles.

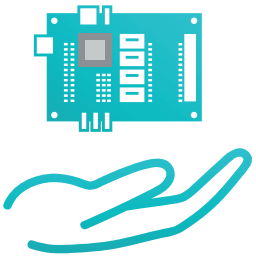
The methods can be applied both to existing facilities/ products (brownfield) and to completely newly designed facilities/products (greenfield).
That is why a specific risk analysis of processes and roles is always the first step, in order to clarify what needs to be achieved. For us, the greatest challenge results from the multitude of potential applications and locations of our products.

In order to make this process as cost effective as possible for you, we work with a certain selection of basic methods and features to realize even the most diverse requirements.
We use the safety levels specified in the IEC 62443 standard and the resulting requirements so that we have a common understanding with you.

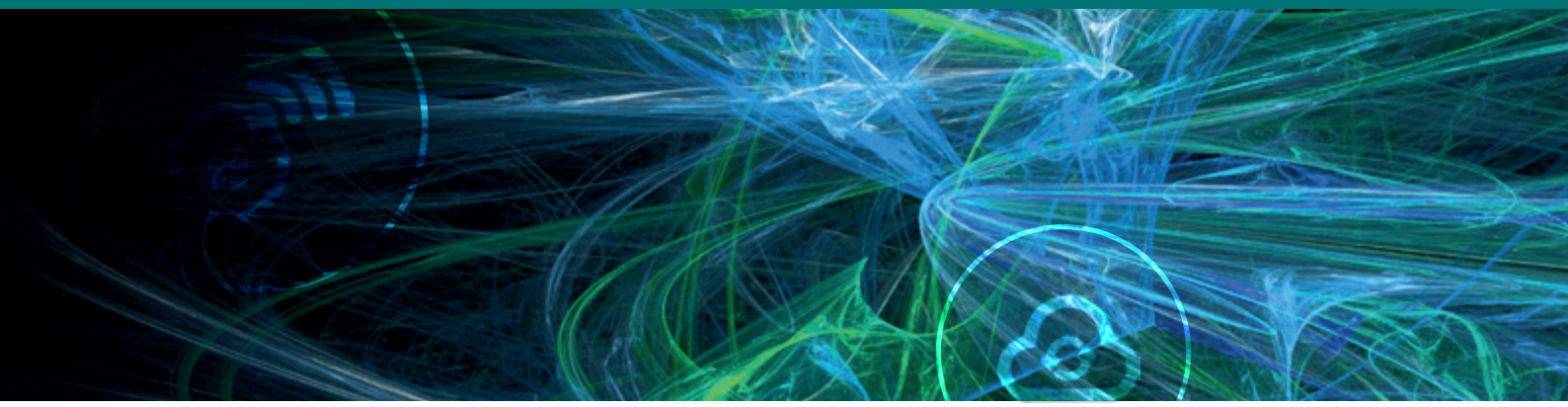
Furthermore, we consider the Top 10 threats according to the BSI and the Top 10 IOT recommendations of the OWASP. Your product is then classified accordingly and the risks relevant to you in your product class are taken into account. Finally, the corresponding concepts and solutions are selected and evaluated.

The different security levels are defined according to the available means and an attacker's intention.

SECURITY LEVEL (SL)	INFRINGEMENTS	MEANS	RESSOURCES (TIME, MONEY)	FEATURES	MOTIVATION	DESCRIPTION
0	no security necessary					No prevention of user errors.
1	on occasion, accidental	none	individual	none (System error)	Error	Prevention of general and accidental user errors
2	intentional, targeted	simple, general IT knowledge	low	general	low	Prevention of simple attacks with cheap available means (single offenders)
3	intentional, targeted	highly sophisticated	moderate	System specific	moderate	Prevention of medium attacks (hacker group)
4	intentional, targeted	highly sophisticated	advanced	System specific	high	Prevention of major attacks (states / organizations)



In practice, reaching even the first safety level is already a significant improvement in protecting your product.
This level can prevent security gaps caused by application errors. DIN 62443, as the basis for the assessment of security levels, is also suitable for classification according to the ESCO Cybersecurity Act, which will be introduced in 2020 for manufacturers of technical devices.



Our Offer
Workshops and Consultation

At PHYTEC, we can advise you on an individual basis on security issues relating to your project. Even the choice of controller has an influence on the available security features of your end product. We would be happy to support you in selecting the controller and possible additional modules. Together, we determine the necessary protective measures for your product.

WORKSHOPS

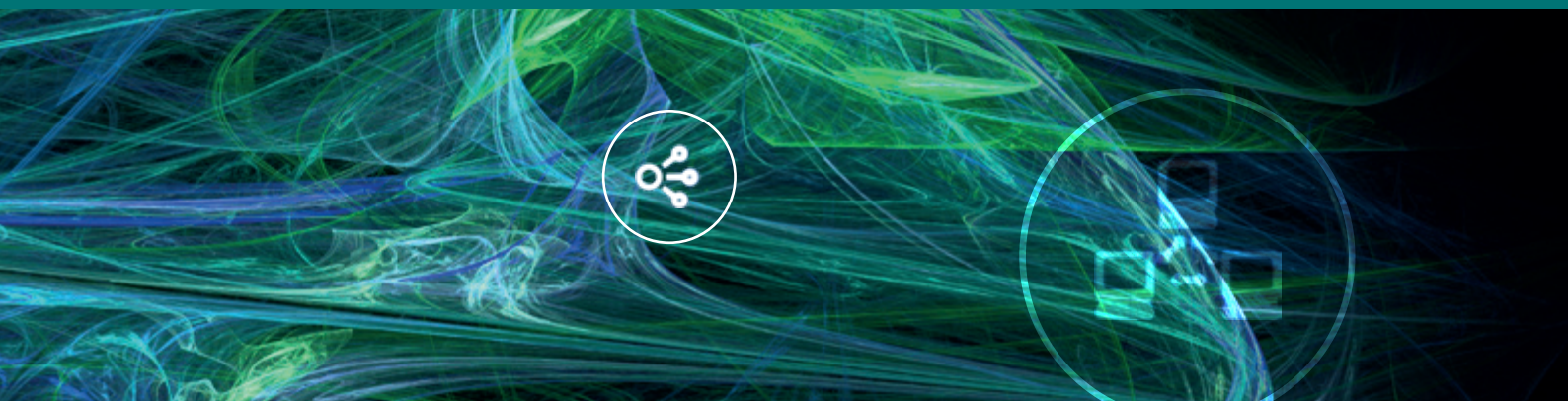
For a better introduction to the topic, we offer regular workshops on the subject of security. In these workshops you will get a comprehensive overview of the topic. Topics of our workshops include:

- **Legal aspects** - standards and guidelines - what does the law require?
- **Basics** (security pyramid) - from the module to the runtime - Which protection measures are available?
- **Security by Design** - Developing secure products - How is security considered in the product development process?
- **System security** - Analysis and implementation – Security requirements
- **Secure initialization** - Security features in production - How do your keys get access to the module?
- **Software Lifecycle Management** - Software maintenance and updates after delivery - How do you provide your product

The concepts of security are based on confidentiality and on individually adapted concepts.

We are happy to offer you individually customized workshops and project consulting. You can find our next workshop dates here:

www.phytec.eu/events



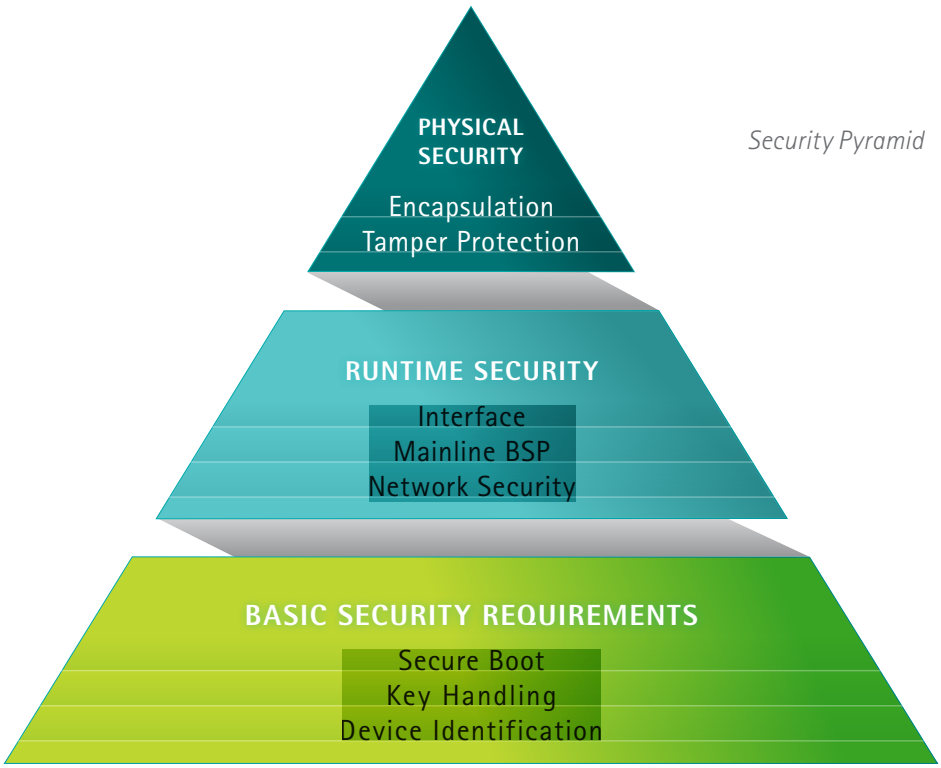
CONSULTATION

Many things can already be realized with the features of the controller, peripherals, memory, and operating system. We use solutions from different hardware manufacturers. For software, we rely on open source solutions. Our starting point is the knowledge of these features and the concepts and solutions behind security.

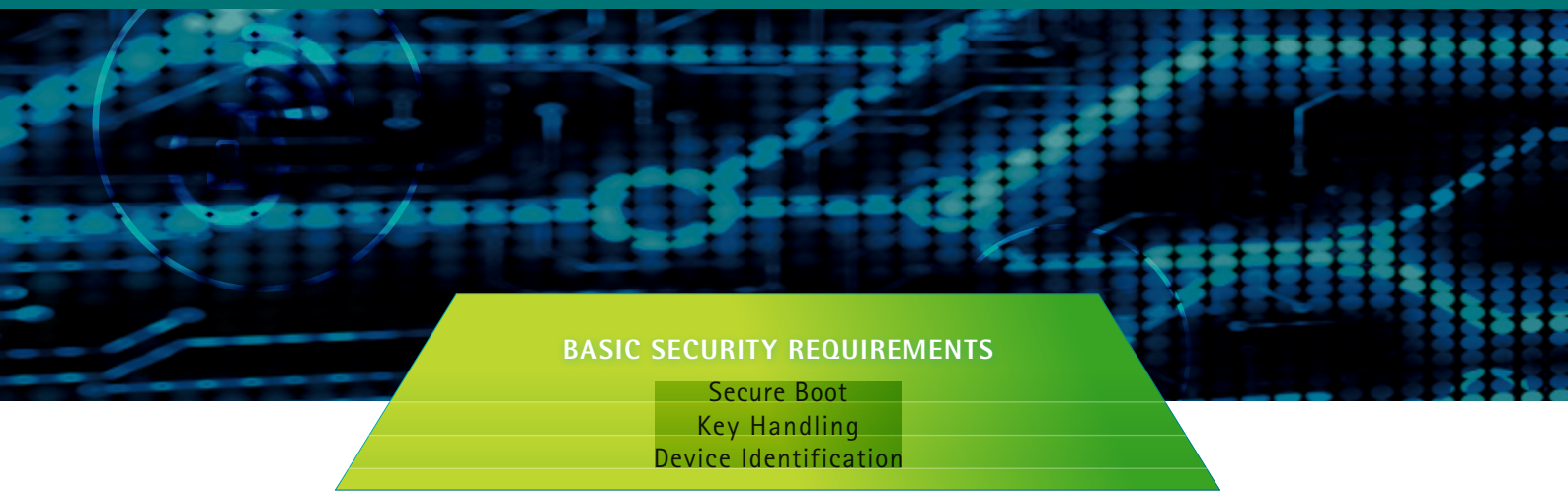
There are different solutions depending on the application:

- Secure-Boot ensures that only trustworthy software is executed on your module
- Depending on the application, the use of crypto chips / secure elements is recommended for the storage of keys and certificates (key handling)
- A unique identity may be required to identify your devices on networks
- When communicating via the network, we recommend the use of TLS for encryption
- The use of Mainline Linux allows for the long-term care of the product

All possible measures to defend against attacks can be roughly divided into three areas.



Security Pyramid



The BASIC SECURITY REQUIREMENTS are the cornerstone for a secured embedded Linux system.

Secure Boot
The use of Secure Boot ensures that only confidential, signed software can be executed on the hardware module. Secure Boot is the core of the Chain of Trust. With the help of this chain of trust, only verified software is guaranteed to be used right up to the end application.

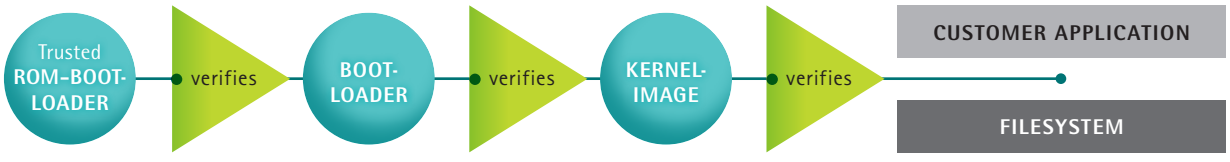
Trusted Execution Environment (op-tee)
ARM TrustZone is a feature for SoCs and processors in the ARM processor families Cortex-A and Cortex-M. The TrustZone has two separate domains (normal world and secure world). In the secure world, the keys are stored, which can only be accessed via an API from the normal Linux world. The TrustZone is the basis for the Trusted Execution Environment, of which op-tee is an open source implementation.

eMMC with Replay Protected Memory Block
Secret data can be stored in the RPMB partition, which is protected against unauthorized access.

Device Identification
For communication with your devices in networks, reliable device identification is a basic requirement. For this purpose, we are working on a process for secure crypto chip initialization, among other things.

TPM and Secure Elements
Crypto chips and secure elements such as the TPM chip make it possible to store and manage cryptographic keys. The private keys are stored in a tamper-proof manner, regardless of the software used.

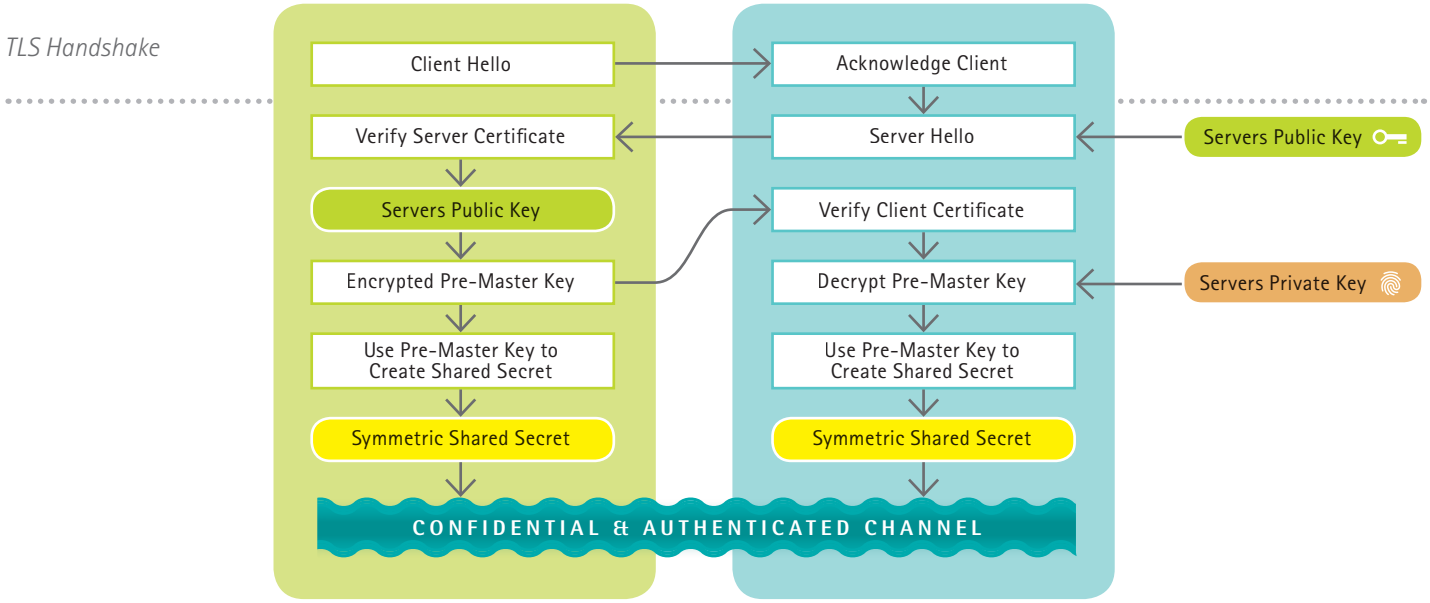
NXP CAAM
With Secure Boot enabled, NXP's CAAM module offers similar functionality to a TPM chip, but without the certified physical protection.



Chain-of-Trust

Features:
- *Trusted ROM Bootloader checks the software image before it is executed*
- *Use of RSA-4096 key pairs and SHA-256 signatures*
- *These algorithms meet the requirements of the BSI (German Federal Office for Information Security) and NIST (National Institute of Standards and Technology) until 2030 and beyond*
- *Basis for the establishment of a Trusted Execution Environment (TEE) and the ARM TrustZone®*

Runtime Security



Network Security

When devices communicate with a server or with each other, the connection must be secure. TLS is the most common protocol and application-independent method for implementing an encrypted connection.

- Establishing a secure connection regardless of the application or protocol used
- TLS (SSL) is recognized as best practice and industry standard for encrypted communication

General recommendations to increase application safety:

- Only run services that you really need on your device
- Closes all ports and selectively opens required ports only
- Always use password-protected logins (including COM and Telnet interfaces)
- Use standard protocols for data transmission
- Use common (open source) implementations of encryption methods (no proprietary development)

Mainline Linux

Linux is our first choice as an operating system for industrial serial use. One of PHYTEC's clear goals is to provide our customers with the advantages of a mainline board support package as early as possible: stable code, quick bug/security fixes as well as the maintenance and further development of mainline drivers by the community.

Mainline is a guarantee for the maintenance of current operating system versions, even after many years. We often offer both a vendor and a mainline BSP simultaneously. This way you can decide when to start with Mainline.

- Mainline BSPs for PHYTEC Boards
  - Annual BSP updates with all mainline security patches
  - The latest kernel version with current security patches is included
  - The latest Yocto-Minor releases are included
- LTS kernel in the BSPs for PHYTEC products
- Offers customer-specific tests with continuous integration

Interfaces

All interfaces accessible in the end product are a potential security risk for embedded systems.

- Only use interfaces that are required
- User-dependent access to interfaces
- Use of encrypted connection

YOUR SECURITY PROJECT

Do you have questions about security or need specific support foryour project?

Our security experts are happy to help you!

Physical Security

In addition to attacks via interfaces or the network connections, direct manipulation of the hardware also poses a security risk. The following procedures are available to protect your electronics from physical attacks:

Tamper Protection
- Protects sensitive data like encryption or private keys
- Deletes data permanently if the device is manipulated
- Various designs are possible

Encapsulation (resin casting)
- Physical access to individual components is prevented
- Detection of the components and parts used is prevented
- Reverse engineering via electrical measurements is not possible

BSP-Features / Customer BSP

The PHYTEC BSP is already equipped with many functions that you can use to protect your product. In our standard BSPs, PHYTEC supplies Yocto recipes for Barebox and FIT Image, as well as preparations for file system locking with the CAAM module.

Features that you can use with our BSPs:
- Secure Boot for Barebox (i.MX 6)
- Secure Boot for u-boot (i.MX 7, i.MX 8)
- Signed Linux kernel as FIT image
- CAAM module for file system encryption

We can help you with the selection of the right controller for your project
contact@phytec.de | www.phytec.eu

Additional features and concepts that are not part of the standard BSP can be created for you in the form of individual customer BSPs.

*Legend Overview Table: ✔ = Feature is supported by the controller ✘ = Feature is not supported by the controller ? = No information available (Premium) = Secure Boot with key handling of TI and minimum quantity · (Standard) = Secure Boot can be used by everyone, separate part number · * limited ■ Advance performance in process / available · ■ Advance performance not planned / not possibl e · ☐ Implementation on request*

Comparison Table: Controller Security Features

			Texas Instruments				NXP					Rockchip	ST
	Explanation	Hardware Support Available	AM 335x	AM571x AM572x	AM574 (PP)	AM 654x* (PP)	i.MX6 i.MX 6UL	i.MX 6ULL	i.MX7	i.MX8 QM	i.MX8M / i.MX8MM (mini)	RK3288	STM32 MP15x
Basic Security Requirements													
Secure Boot	Ensure that only verified SW is started	✔	✘ * (Premium)	✘ * (Premium)	✔ (Standard)	✔ (Standard)	✔	✔	✔	✔	✔	✔	✔ (in STM32 MP15xC)
Hardware Acceleration	Support of HW-based encryption	✔	✔ * limited	✔ * limited	?	✔	✔	✔ * limited	✔	✔	✔	✔	✔ (in STM32 MP15xC)
Secure Debug	Prevent debug access to security relevant system parts	check individually	✘	✘	✔	?	✔	✔	✔	✔	✔	✔	✔
True Random Generator			✘	✘			✔	✔	✔	✔	✘ PRNG certifiable by the CAVP of the NIST	✘	✔
Security Co-Processor	Completely independent security unit	check individually	✘	✘	✘	✔	✘	✘	✘ Cortex-M4 for Safety	✔	✘ Cortex-M4 for Safety	✘	✘ Cortex-M4 for Safety
Boot Fuses	Boot medium and order can be determined by FUSES		✘	✘			✔	✔	✔	✔	✔	✘	✔
Runtime Security													
One-Time Programming	One-time setting of security settings	✔	✔ * limited	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Cryptographic acceleration	Cryptographic co-processor with private key	✔	✘	✘	✘	✘	✔	✘ (DCP)	✔	✔	✔	✘	✘
Secure On-Chip RAM	More secure in RAM directly in controller	✔	✘	✘	?	✔	✔	✘	✔	?	?	✘	?
Trusted Execution Environment	Access protection for installed RAM memory	✔	✘	✔	✔	?	✔	✔	✔	✔	✔	✔	✔
Physical Security													
External Memory Protection	Access protection for installed RAM memory	check individually	✘	✘	✔	✔	✔	✔	✔	✔	✔	✘	
Tamper PINs	For implementation of Tamper Protection (manipulation detection)	check individually	✘	✘	?	?	✔ * UL G3 Only	✔	✔	✔	✔	✘	✔

Key Handling Concept

Most methods for securing devices and software are based on asymmetric cryptography using a connected public key infrastructure (PKI). To do this, you often need a different number of certificates, with public and private keys. Managing and protecting these certificates and private keys is a big challenge. The private keys must be protected throughout their entire lifecycle.

PHYTEC is your partner for these tasks and can guarantee the security of your private keys and other secrets with its production concept.

PARTNERSHIP BUILDS TRUST

PHYTEC you can trust! As a reliable partner for the implementation of your business ideas, we make protecting your secrets a top priority. We ensure the encrypted and verified transmission of your information for the realisation of your projects.

SECURE STORAGE

We protect your company secrets throughout the entire product lifecycle. We ensure safe storage on a specially developed system that is not connected to the company network. Strict access controls ensure maximum security.

- Strict access controls
- Not on the company network
- Physically separated network connection to production (software installation)

SAFE INTRODUCTION INTO THE PRODUCT

In order to guarantee secure device initialization, PHYTEC is planing a secure zone at our new manufacturing site currently under construction. All security relevant features of your device will be enabled within the secure zone.

The use of special Hardware Security Modules (HSM) during the import process ensures that your know-how remains confidential. The transfer of cryptographic keys to your end device takes place in the security zone with special access controls. This allows us to guarantee the highest level of security: whether patent-protected software, cryptographic keys for verifying software updates, or certificates for unique device identification on the Internet. We bring your solutions securely onto your product!

- No direct access to private keys in the test environment
- Use of HSM modules to protect private keys
- Physically independent network for the entire process

PROTECT YOUR PRODUCT UNTIL DELIVERY

We take care of the protection of your products during the entire production process and during storage, after installation of your customer software. We design the procedure up to the agreed delivery time according to your requirements.

Headquarters | Subsidiaries

Germany
PHYTEC Messtechnik GmbH
D-55129 Mainz
t +49 6131 9221-32
f +49 6131 9221-33
www.phytec.de
www.phytec.eu

France
PHYTEC France SARL
F-72140 Sillé le Guillaume
t +33 2 43 29 22 33
f +33 2 43 29 22 34
www.phytec.fr

North America
PHYTEC America LLC
Bainbridge Island, WA 98110
t +1 206 780-9047
f +1 206 780-9135
www.phytec.com

India
PHYTEC Embedded Pvt. Ltd.
HSR Layout
Bangalore 560102
t +91 80 408670-46/49
www.phytec.in

China
PHYTEC Information Technology Co. Ltd.
Nanshan District, Shenzhen
518026 PRC
t +86 755 6180 2110
www.phytec.cn

Benefit from our Security Services
in the entire life cycle of your products.

Security 2020-1

- Device Identification
- Made in Germany
- Product Lifecycle Management
- Mainline BSP with LTS-Kernel

Let's talk about your project!

maik.otto@phytec.de

+ 49 (0) 6131/ 9221-32