CYBERCRYPT.

# **IS YOUR PRODUCT DESIGNED TO WITHSTAND** THE THREATS OF THE FUTURE?

An outlook on how to secure innovative technologies

SECURE PRODUCT DESIGN FOR **EVERY INDUSTRY**

## TABLE OF
# CONTENT

SETTING THE SCENE

# TECHNOLOGY IS GETTING SMARTER

## BUT SO ARE ATTACKERS

In the last decade, technology has advanced rapidly. Today, we live in a world of smart, connected devices. This unprecedented pervasiveness of computation and complexity has led to an equally unprecedented increase in attack surface and attack potential.

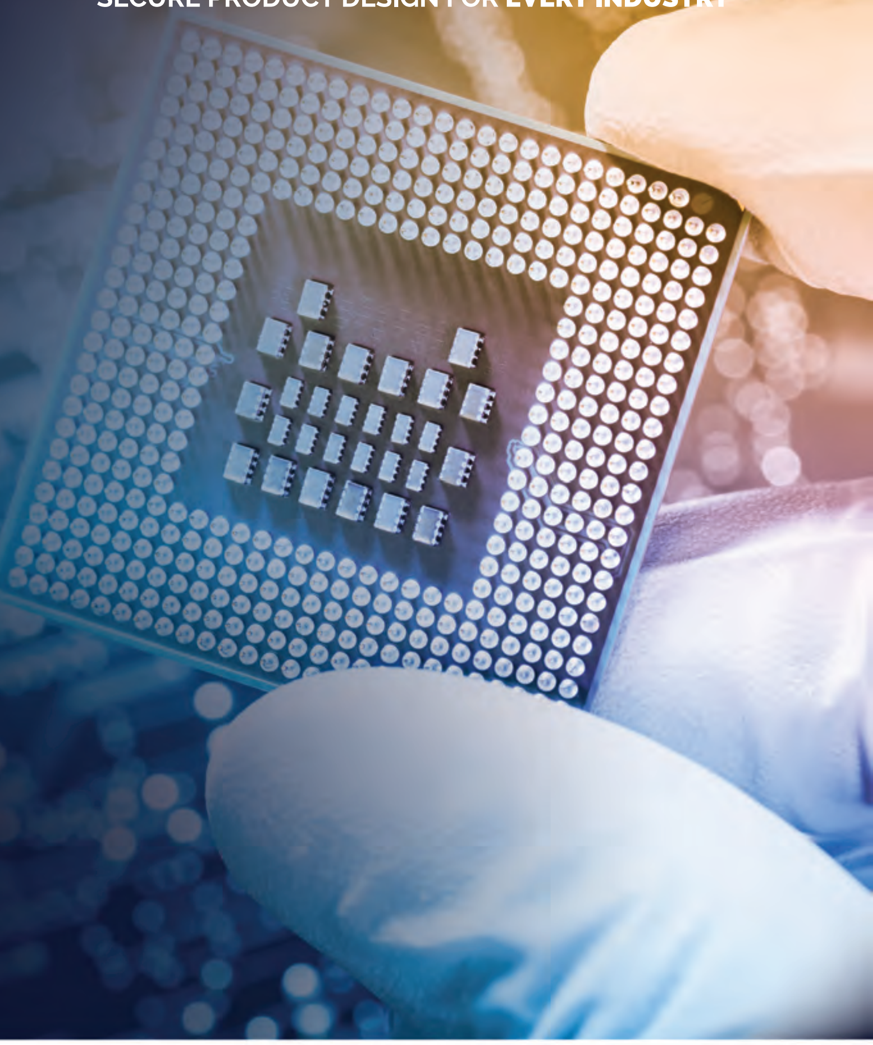
Product development companies cannot stand by and be at the mercy of this technological change.

To provide the necessary resiliency, product developers must understand the risk of adopting these novel technologies and how to properly apply security measures.

That is why companies need to bring the latest cryptographic and security advances to their product architecture to ensure that the products meet the highest protection standards throughout their entire lifecycle.

APPLICATION PERSPECTIVES

# SECURITY BY DESIGN FOR FUTURE TECHNOLOGIES



At **CYBERCRYPT**, we combine decades of experience in cryptography, secure architecture and security analysis to keep your product protected.

We have built cryptography and security into some of the world's most innovative products within industries like transportation, fintech, healthcare and energy infrastructure, preventing the fatal consequences of attackers gaining access to valuable, sensitive information.

We know how the threats to future technology are increasing - and **we have learned that for future technologies to work,** they must be based on a robust security architecture.

1. Blockchain and Distributed Ledgers
2. Intelligent Medical Devices
3. Drone Technology
4. Renewable Energy
5. In-app Protection

## APPLICATION PERSPECTIVES

### 1 BLOCKCHAIN AND DISTRIBUTED LEDGERS

### TRUST IN TRANSACTIONS STILL DEPENDS ON REAL-WORLD CRYPTOGRAPHIC SECURITY

Blockchain technology is revolutionizing how transactions take place and has already transformed several industry sectors such as finance and banking. Transactions between people have historically been facilitated with the help of intermediaries. But with blockchain's distributed ledger technology, we are now seeing decentralized systems that can help document transactions. This means that the blockchain network becomes the trusted party and the need for an intermediary is eliminated, meaning that people can now conduct transactions with one another without having to go through a formal institution.

Yet, for blockchain platforms to work, transactions must still be based on trust – and they can only provide trust if they are secure. That is why distributed ledger technology must be built on state-of-the-art cryptographic primitives with strong security guarantees against outside threats. Technology such as mobile banking applications and cloud-based trading platforms access and authorize financial transactions in potentially hostile environments, which makes it mandatory that these technologies are designed with a high security standard in mind.

### HOW CAN WE HELP?

We have extensive experience in designing strong cryptography for blockchain and cryptocurrency applications, minimizing security risks in both client and server software.

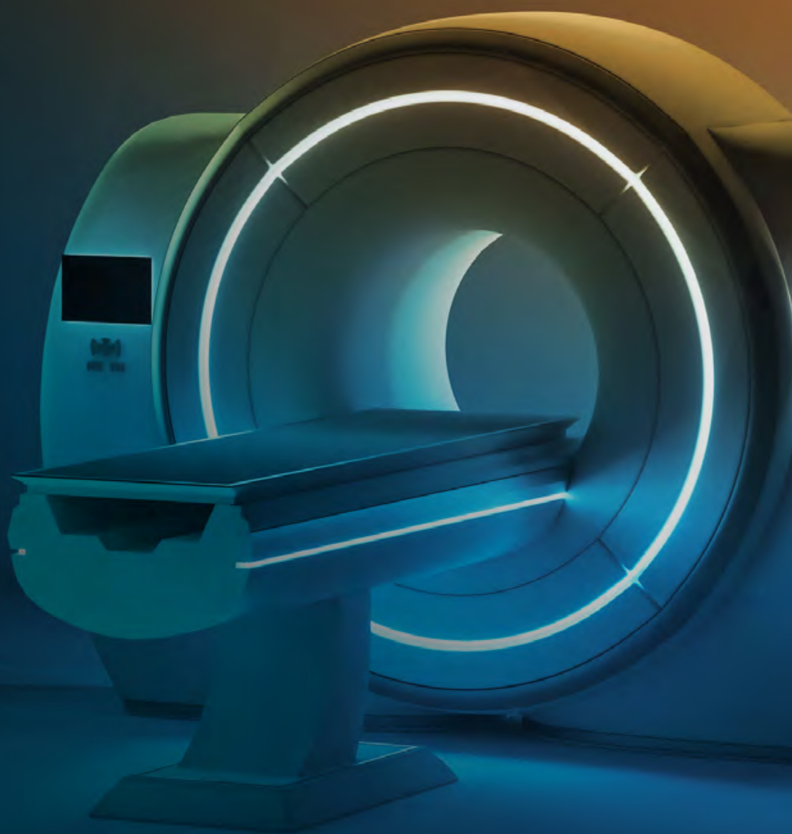
## APPLICATION PERSPECTIVES

### 2 INTELLIGENT MEDICAL DEVICES

SIMPLIFYING LIFE, BUT POTENTIALLY LIFE-THREATENING

The healthcare sector is undergoing exciting technological advancement. We are now starting to see implementation of truly innovative solutions, such as surgical robots and AI software that can provide actionable insights by diagnosing and detecting early symptoms. While these future technologies and other interconnected medical devices will help simplify the lives of patients and healthcare professionals radically, human life may also be at stake if they are attacked and controlled by unauthorized individuals.

One of the potential threats to medical devices is in their actual operation; another is that they contain vast medical records with highly sensitive patient data. Consequently, it is crucial that this data is generated, processed, and archived securely to keep confidential patient information safe and in compliance with new data protection legislation.



### HOW CAN WE HELP?

With our proven process and unique cryptographic skills, we are able to provide defense-in-depth security architectures for medical devices and help evaluate and improve protection standards.

APPLICATION PERSPECTIVES

## 3 DRONE TECHNOLOGY

AT YOUR SERVICE, IF SECURED

Drones have been used for governmental purposes for years, helping personnel on military or humanitarian missions abroad to reach remote places unnoticed in an efficient and effective way. Equipped with thermal cameras, drones can be used for search and rescue operations or to help gather information about hostile activity. In recent years, we have seen investments in unmanned aerial systems soar, as the accessibility of drones has expanded significantly – from fighting war to forecasting weather and carrying out quick deliveries. Technology is moving fast and future generations of drones are expected to incorporate highly intelligent piloting software to enable full autonomy. In fact, technology is almost moving faster than regulations. And this poses a great risk if unauthorized individuals gain access.

Proper security architectures, strong cryptographic primitives, and electronic protective measures can mitigate the risks of passive and active remote attacks such as eavesdropping and manipulating communication. However, potentially even more critical is the threat of an adversary obtaining physical access to a drone, e.g. as a result of a shutdown over the enemy territory. On a military operation, it can be devastating for the entire fleet and may put military personnel in great danger.

### HOW CAN WE HELP?

Our technologies help protect cryptographic implementations in FPGA or software - even if the adversary has full access to and control of the implementation and execution environment.

## APPLICATION PERSPECTIVES

### 4 RENEWABLE ENERGY

### SAVING THE ENVIRONMENT DEMANDS STRONGER SECURITY

Investment in renewable energy has increased rapidly in the last decade and is forecast to continue to grow to help conquer global warming. Thanks to digitalization and increased interconnectivity, the huge amount of data coming from wind turbine generators (WTGs), SCADA systems, and distribution networks is used to make operations run more efficiently, meaning greater benefits in terms of reach, cost, and environmental impact. However, it also means that the technology has become a popular target for cyber criminals. We have seen multiple attacks on energy infrastructures in recent years. For example, in December 2015, a Ukrainian power grid was attacked by malware that switched off 30 substations and led to 73 MWh of electricity being lost and 225 000 households being left in the dark.

More recently, in January 2018, Schneider Electric discovered a remote access Trojan RAT in the TRITON/TRISIS malware that infected safety instrument systems (SISs) using privilege escalation techniques. From experience, we have learned that access control systems, antivirus software, firewalls, and state-of-the-art Intrusion Detection Systems (IDSs) are no longer enough to protect energy plants from Advanced Persistent Threats (APTs).

A common feature in the abovementioned attacks is the lack of a suitable security architecture providing defense-in-depth. Even though security measures such as user authentication, remote access via VPN, or network isolation might be implemented, the compromise of just one of them can lead to the compromise of the entire system. By employing a tailored security architecture, all the previously mentioned SCADA attacks could have been prevented.

### HOW CAN WE HELP?

We design security architectures that are tailored for your systems. By design, these security architectures provide defense-in-depth, ensuring that the failure or compromise of a single component does not give the attacker complete control over the entire system.

## APPLICATION PERSPECTIVES

### 5 IN-APP PROTECTION

SAFEGUARDING THE IP AND SECURING FEATURE ACTIVATION IN YOUR APPLICATION

With modern architectures migrating software logic to the client side, the proliferation of mobile applications has empowered users by driving faster and easier-to-access consumption of services. As seen in many industries, such as financial services, gaming, entertainment (DRM), healthcare, and insurance, these critical and high-value applications run in untrusted environments.

Based on a zero-trust approach, in-app protection technologies protect the application from the inside. Self-defending capabilities like application shielding and anti-malware techniques are installed into client-side applications and software running on connected devices. Code obfuscation prevents both the intellectual property (IP) and sensitive data from being exposed during reverse engineering attacks. In parallel, anti-tampering techniques are used to monitor the surrounding environment and detect malicious activities.

Enterprises developing consumer-facing applications that contain unique IP, paid content, or feature activation capabilities need novel and comprehensive tailor-made solutions to minimize the risks of revenue loss.

**HOW CAN WE HELP?**

We make bespoke in-app protection tools comprising countermeasures against static, dynamic, and symbolic analysis and supporting iOS as well as Android.

# OUR KEY LEARNINGS FOR YOUR INSPIRATION

From working with technological applications across multiple industries, we have seen that future threats and attacks are increasing and for many product development companies, there is still room for security enhancements in their product designs. Good security starts with a thorough analysis and implementation plan, as well as continuously keeping the developers and the product at the forefront of security standards. We have collected a selection of our key learnings for your inspiration here.

> The IOTA Foundation is honored and excited to be collaborating with CYBERCRYPT, to ensure we achieve world-leading security for the IOTA protocol
>
> **DAVID SONSTEBO**
>
> Co-Founder, IOTA Fountation

## 1

### Invest in evaluation and analysis to ensure effectiveness and efficiency

Before commencing a security project, it is worthwhile investing in evaluation and analysis of current countermeasures. Vulnerabilities will vary and require different actions, depending on product technology, lifecycle stage, and the environment in which the product operates.
By identifiying these, you will ensure more efficient development and implementation.

## 2

### Involve the right competences in product development processes

When creating innovative technology, the product design can be highly complex. This can make it difficult to assess adequate security measures while working with actual product realization. To prevent security enhancements from delaying the development process and increasing the time to market, it is crucial to involve key personnel with cryptographic security competencies, as early as possible.

## 3

### Develop a lifecycle view of your product's security

It is important to remember that the journey toward secure product design does not stop when the product is launched in the market. To fight off future threats and attacks, your product should meet security needs throughout its entire lifecycle. We recommend developing a product security roadmap to identify security needs and ensure that security levels are always accordingly up to date.

## 4

### Engage key personnel in continuous training and education

The field of secure product design and development is constantly evolving, and ensuring high security standards demands up-to-date cryptographic expertise. Few companies are set up to handle this issue on their own. But by continuously training and educating your key personnel and assisting them with documentation, your company can remain on top of future security risks.

## 5

### Bring the security of your product in at the strategic level

Securing your product design from attacks is a great investment — and its risks clearly outweigh the risks of not doing anything. The consequences of not being able to protect your product from attackers can be costly and threaten the entire company. Therefore, it is critical that stakeholders with strategic responsibilities are involved in the process and educated on the importance of prioritizing protection of critical assets in product design.

# WORLD-LEADING EXPERTS IN SECURE PRODUCT DESIGN

Founded by expert cryptographers, CYBERCRYPT provides decades of extensive experience to even the most technologically advanced products. Our mission is to mitigate the risk of attacks on products associated with current and future threats.

That is why we put security at the center of everything we do. We provide expert services and tailored solutions so that you can deliver secure products to the market – while safeguarding your critical assets.

At CYBERCRYPT, we establish the foundations of product security using innovative, advanced cryptographic solutions. We strive to go above conventional security through proper analysis, detailed security design and structured implementation, to elevate the security of your product.

**1**

YOUR PRODUCT WITH

**CONVENTIONAL**

SECURITY

**2**

ANALYSIS, DESIGN, AND IMPLEMENTATION TO

**ENHANCE**

SECURITY

**3**

YOUR PRODUCT WITH

**ELEVATED**

SECURITY

# WE PLAN FOR YOUR PRODUCT'S LONG-TERM PROTECTION

Our work is anchored in understanding your technological needs and bringing the latest cryptographic and security standards to your product. By implementing cryptography and security resilience, we ensure that your products meet the highest protection standards throughout their lifecycle.

## SECURITY EVALUATION

A thorough analysis of the security of your product's architecture and implementation will ensure that all security enhancements to your product design process are applied most effectively and efficiently.

## SECURE PRODUCT DESIGN

To secure your product, we align your cryptographic needs using product roadmaps – helping you comply with current regulations while creating high-quality documentation standards.

## IMPLEMENTATION AND DEVELOPMENT

We support the implementation of software, code, or algorithms in your production environment via a detailed project plan carried out in coordination with your responsible teams.

## LIFECYCLE SUPPORT

Your product should have its protection needs met throughout its lifecycle. By training your key personnel and assisting with documentation, we help you remain at the forefront of security offerings.

# WHAT ARE YOUR SECURITY NEEDS?

With five decades of experience collaborating across multiple project types, we can help you secure your product and adapt our process to your critical assets and your specific product.

## I NEED TO SECURE A NEW PRODUCT

Whether it is an autonomous vehicle, a mobile application, or an internet-connected medical device, our cryptography and security experts can help secure your product. Having built cryptography and security into some of the world's most innovative products and projects, we can help your development team navigate the complex world of cryptography and product security testing, allowing you to resolve security issues and build the best possible security into your product – before it reaches the market.

## I NEED TO SECURE AN EXISTING PRODUCT

To improve an existing product or application, you must be fully aware of the latest security and cryptographic standards. We help you meet security requirements as determined by our threat model,  without impacting performance or usability. Based on the most up-to-date cryptanalysis techniques and security product testing, we provide a quantitative design that will get your project to the right security level.

## I NEED MECHANISMS TO SECURE STORAGE, CONFIGURATION, OR COMMUNICATION

You have an existing storage component, product configuration, or communication protocol that requires elevated security. With us by your side, you will meet security requirements as determined by your threat model — without impacting performance and usability. Based on the most up-to-date cryptanalytic techniques and security product testing, our quantitative design ensures your storage, configuration, or communication reaches the right security.

## I NEED NEW, IMPROVED CRYPTOGRAPHIC ALGORITHMS OR TECHNIQUES

You have an idea or prototype that requires a new and innovative cryptographic algorithm or protocol. However, you also know that designing such a primitive is costly and requires specialist help — from experts who understand your needs and know that existing cryptographic standards will not be right for your project. With our extensive experience in designing customized cryptography, we can reach the optimal security for your product.

ABOUT US

# WE ARE THE CRYPTOGRAPHY AND SECURITY EXPERTS

## WE ARE HERE TO KEEP YOU AND YOUR PRODUCT SAFE

The innovative and connected technologies of our future are generating great excitement and potential, but also great risk of threats and attacks that will exploit the vulnerabilities in product designs. And the security challenges that come with this call for novel technologies.

At CYBERCRYPT, we are here to help protect your product from attackers. Please feel free to reach out to one of our experts, if you want to know more.

# CYBERCRYPT.

Providing decades of extensive experience to our customers, we establish the foundations of **cryptography and software security.**

+45 53 73 74 00
info@cyber-crypt.com
cyber-crypt.com