# CRYPTOGRAPHY SERVICES
## Research and Development

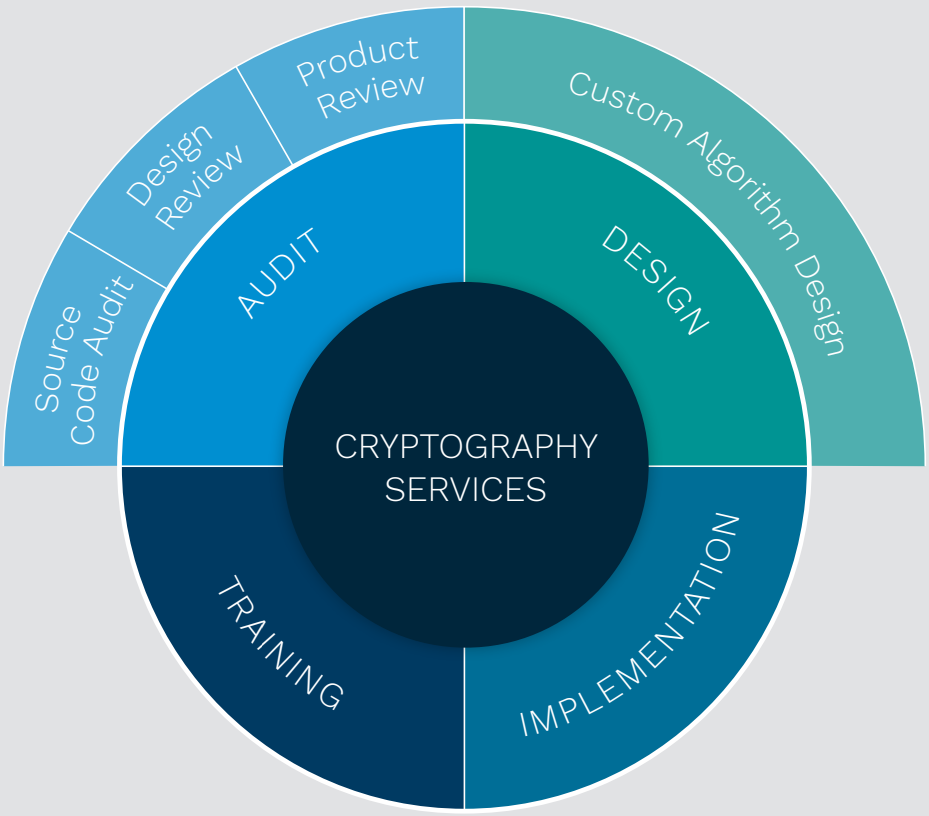
KUDELSKI SECURITY

### Access independent, world-class cryptography audits and implementation expertise to obtain target security levels for your products and systems.

Cryptography is a critical component of modern systems, ensuring secure communications, data confidentiality, and program integrity. Since its founding in 1951, the Kudelski Group has been a market leader in cryptography engineering and research, providing services to secure and monetize digital content. Extending this expertise to our broader base of cybersecurity clients, we offer services that span a wide range of areas, including algorithm design (proprietary ciphers for smart cards, popular open-source designs such as BLAKE2), implementation (efficient software and hardware code, side-channel defenses), and review (review of third-party products, source code audits).

### Recent Cryptography Projects

- Kudelski Security performed the independent review of the Wire secure communications app. Download the complete report here.
- Kudelski Security was part of the first team to find vulnerabilities in the Signal messaging app. Read more about it here.
- Kudelski Security's principal cryptographer, Jean-Philippe Aumasson, was part of the team that designed the popular hash algorithm BLAKE2 and the pseudo random function family SipHash.
- We presented the following research at Black Hat: "SGX Secure Enclaves in Practice: Security and Crypto Review". Download the presentation here.



## How We Engage

Cryptography services can be delivered on a per-application contract or through a yearly retainer.

### Identify Services

An account manager will help identify the services that best fit your needs – source code, design, or product review; algorithm design; implementation assistance; or training.

### Define Scope & Goals

A Kudelski Security cryptography expert will meet with you to define the scope and specific goals for the engagement. Project planning proceeds according to the requested service and desired outcomes.

### Establish the Team

For cryptography services, the team will typically contain the following roles:

- Project manager
- Principal cryptographer
- Technical staff

## Cryptography Services

Kudelski Security employs world-class cryptography experts, designing widely used algorithms such as BLAKE2 and SipHash, performing side-channel attacks at a nation state level, and developing enduring countermeasures. We offer this expertise to our clients to help protect their systems, data, and sensitive customer information.

- **Audit:** Kudelski Security can perform three types of audits: source code review, design review, and product review. Cryptographic software implementations require a review by cryptography experts, because they can be vulnerable to specific bugs that won't be detected by code analyzers and standard code reviews. We use manual code review as well as internal automated tools to provide you with a detailed cryptography gap analysis, and then assist your developers to implement fixes.
- **Design:** We can design custom cryptographic algorithms that match your requirements in terms of security, performance, target platform, and features. Custom algorithms can serve to enforce intellectual property rights (if the algorithm includes copyrighted material or patented techniques), to complicate reverse engineering, or to prevent emulation on certain platforms.
- **Implementation:** Cryptographic algorithms require unique skills in order to create implementations that are fast and secure. Without proper controls, cryptographic implementations can be vulnerable to side-channel attacks, exploiting for example, information leaks from the execution time, or sensitivity to attacker-induced faults. We can help you assess the required level of security for your cryptographic components and put in place the required countermeasures.
- **Training:** We offer a one- or two-day training to teach developers the most relevant aspects of modern cryptography, with a focus on software applications and real vulnerabilities.

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

Info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY