KUDELSKI IoT THINGS

Semiconductor Manufacturer Services & Solutions

We ensure the security and robustness of our semiconductor clients' products based on more than 25 years of research, analysis, development and operational excellence. We have a unique portfolio of services and solutions that give SoC manufacturers critical insights and proven technologies to help them meet the quickly evolving regulatory and customer expectations around security.

OUR MISSION

We empower you to build and sell secure products throughout their entire lifecycle

Build secure, validated chipsets

We make your product secure by offering design, security assessment and pre-certification support, as well as a Secure IP block that enables advanced, efficient key management and late provisioning for any connected device.

Enable efficient lifecycle management

We provide the technology foundations and infrastructure required to effectively manage security risks and operational complexity. We provide means to efficiently and securely handle key material both in-factory, as well as simplifying in-field provisioning.

SECURING THE FUTURE OF IoT

Our products and services

SECURITY CONSULTING SERVICES

We work with you to assess your security threats and opportunities and help you create a product that is secure by design.

IoT SECURITY LAB SERVICES

We assess the security of your new and existing products and provide actionable insights.

SECURE IP HARDWARE ROOT OF TRUST

We provide core technology to implement robust security foundations into your SoC.

keySTREAM LIFECYCLE MANAGEMENT

We provide a proven system enabling you and your customers to manage the entire security lifecycle of your product(s).

HOLISTIC 360° OFFERING

Ingredients for building a secure chipset, from design to operations

Secure IP – a Kudelski HW Root of Trust

Immutable device identity

HW key protection and key management

Secure storage, isolation, anti-tampering

Cryptographic functions

Secure interfaces

Security services for SoC and device

Support for Secure Boot and lifecycle management

Threat Assessment & Risk Analysis

Identification of assets, risks, probabilities and impact

System- and device-wide threat analysis

Market-specific TARA such as ISO 21434, IEC 62443, EN 303645, ED203A

Lab Evaluation

Validate the effectiveness of countermeasures and security controls

Non-invasive low-cost attacks

State of the art side channel attacks

Electrical and EM glitch, DPA, laser multi-location, multi-temporal hardware attacks

keySTREAM Lifecycle Management

Onboarding and provisioning

PKI-as-a-service

Security monitoring

Secure Firmware Updates

JTAG management

Validation & Certification

Remediation analysis

CSPN certification (accredited lab)

PSA and SESIP pre-certification support

Secure Design and Development

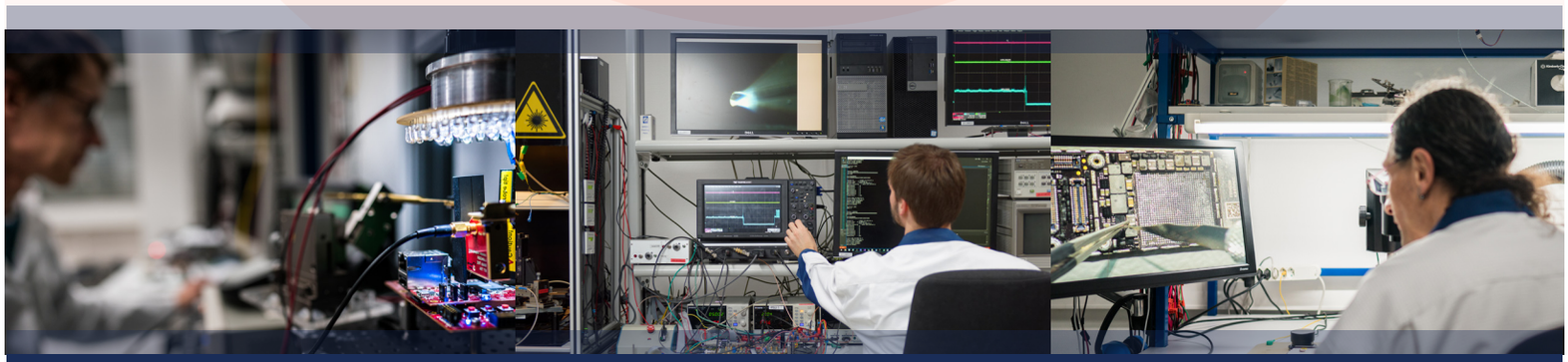
Architecture assessment

Security consulting

ROM and firmware review

Tailored research program

Licensing of test tools



Security is in our DNA – Our IoT experience is rooted in our 30+ years protecting high-value data and business models.

For protecting Digital TV services, we have developed highly robust and efficient hardware – the NAGRA On-Chip Security (NOCS) for set-top boxes and smart TVs. This is integrated with over 500 different chips and with over 100 million chipsets deployed. Kudelski has also developed custom security chips for smart cards, as well as IP sub-systems for integrated SIM SoC.

 V1.4

www.kudelski-iot.com