KUDELSKI IOT THINGS | amazon alexa

Security Certification Assessment for Alexa Built-in Devices

We ensure you achieve Amazon security certification and provide actionable security advice

IN SHORT

Through more than 25 years of research and security analysis of digital systems, the Kudelski IoT Labs have developed a unique expertise to support companies in the evaluation of the security level of their products.

As an Amazon Alexa Authorized Security Lab, we perform independent security assessments to help you meet Amazon Alexa Built-In security requirements and help you pass certification.

Our actionable improvement recommendations help you improve the long-term security of your device and prevent risk to your revenue and reputation.

BASE PACKAGE

Achieve basic certification

The AVS Security Requirements require that developers implement all reasonable security measures to prevent unauthorized access to Alexa Service.

These requirements are intended to help companies creating Alexa Built-In devices be proactive in identifying and resolving potential security vulnerabilities in their devices and be prepared to distribute fixes for security issues identified after launch.

The basic assessment package analyzes and documents the compliance for the following scope:

- AVS Security Best Practices Assessment
- Hardware Analysis
- Basic Firmware Analysis
- Basic Mobile App Assessment

ADVANCED PACKAGE

Protect your product long-term

To complement the base package, the advanced package can be requested to analyze the device security with an extended scope.

By considering the system as a whole, our security experts will go beyond standard penetration testing by covering the most probable local and remote attack vectors.

The advanced package also provides:

- Base package
- \+ Advanced Firmware Analysis
- \+ Advanced Mobile App Assessment
- \+ Cloud Services Assessment
- \+ Security recommendations

The Advanced Device Security Discovery package covers the following security aspects of a device:

- Authenticity: prevent data falsification
- Integrity: avoid malicious modification of a device
- Non-repudiation: provide proof of data integrity & origin
- Confidentiality: verify that data and code does not leak
- Availability: ensure a service can be reached
- Authorization: prevent unauthorized actions CPASULE

HOW WE WORK TOGETHER

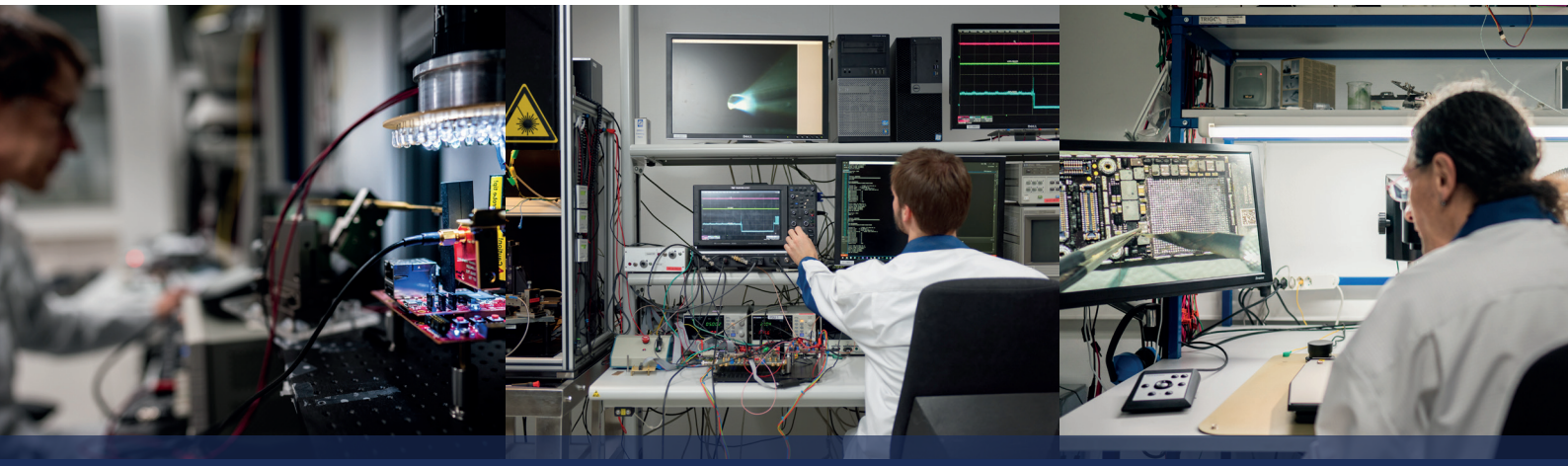
Engagement inputs and deliverables

Once an agreement is signed, we ask that you send three sample devices to be evaluated. Please also provide any relevant documentation, in addition to the Amazon AVS checklists and the self-assessment. Additional mandatory inputs are listed below.

Once the device is reviewed against Amazon AVS security requirements, we will deliver a detailed technical report describing the evaluation steps, providing details on the methodology and a compliance table to Amazon's security requirements.

At the agreed upon end of the analysis, the hardware and any provided documentation are returned to the client. When required, the hardware analysis might be destructive. Devices are returned as is, as we may conduct destructive tests as part of the analysis.

- One test sample with access enabled to debug ports (JTAG, SWD, UART, USB, etc) and the schematic describing the pinout of such interfaces
- A software maintenance update strategy describing how your company will create and distribute new software releases (cf. AVS requirement 1.4)
- A security response plan that describes how your company will proceed if a security incident arises (cf. AVS requirement 1.6)
- The companion application, if applicable, for the Android operating system



ABOUT KUDELSKI GROUP

$100B
revenues enabled annually

500M
users

$741M
revenues (2020)

3250
employees

32
offices worldwide

70
years of innovation

Kudelski IoT is the Internet of Things division of Kudelski Group and provides end-to-end IoT solutions, IoT product design, and full-lifecycle services to IoT device manufacturers, ecosystem creators and end-user companies.

These solutions and services leverage the group's 30+ years of innovation in digital business model creation; hardware, software and ecosystem design and testing; state-of-the-art security lifecycle management technologies and services and managed operation of complex system

www.kudelski-iot.com