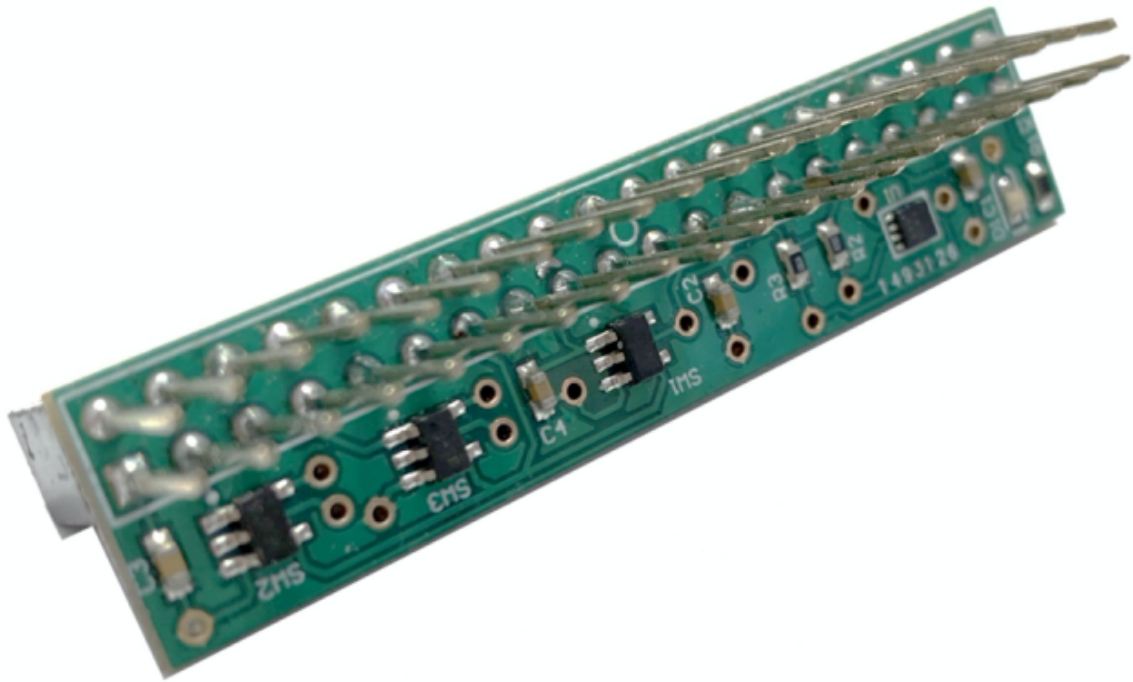


Kudelski IoT keySTREAM PicoSE Development Kit



Features

Kudelski IoT keySTREAM provides multiple features to easily secure and manage your IoT ecosystem with trusted functions.

- Kudelski IoT keySTREAM: end-to-end security management for IoT solutions
- Built in Kudelski IoT's Secure Element - the PicoSE – 800
- Unique, immutable and unclonable identity
- Late provisioning, end-to-end data protection
- Secure Data, Decisions, Commands, and Actions.
- Revocation & Refurbishment

Description

Kudelski IoT keySTREAM is a device-to-cloud solution for securing all the key assets of your IoT ecosystem, end to end and during its entire lifecycle. You can securely connect, manage & update your Raspberry Pi Computer board with Kudelski IoT keySTREAM PicoSE Development Kit.




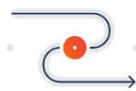
Kudelski IoT keySTREAM PicoSE Development Kit provides you with functions to identify, secure, manage and authorize your Raspberry Pi Computers, protect your data, control access and actively secure them over time. Kudelski IoT keySTREAM Development Kit's shield is built to be stacked on a Raspberry Pi and allows stacking even more cool HATs with its Arduino compatible connectors. With Kudelski IoT keySTREAM, you can easily secure and manage your IoT ecosystem with trusted functions.

We recommend you also add [Raspberry Pi 4 Computer 8GB](#) and [Raspberry Pi Sense HAT](#) to get started with Kudelski IoT keySTREAM.



In addition, Kudelski IoT keySTREAM provides advanced security features like secure boot, device commissioning, zero-touch provisioning to major cloud platforms, firmware over the air (FOTA) updates, key rotation, transferring security ownership and command authentication. Kudelski IoT also provides Managed Security Services to help ensure the active security lifecycle management of IoT ecosystems.

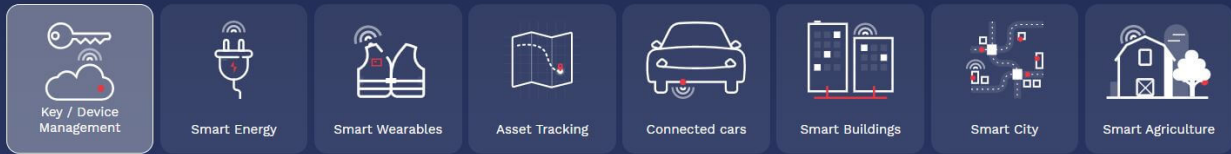
Your long-term success depends on your ability to build on trusted foundations (your data, your devices, your connectivity), along with your ability to efficiently manage and scale your IoT ecosystem.

 <p>Establish Trust Give every IoT device a unique identity that is immutable, unclonable and forms the foundation for any IoT security function.</p>	 <p>Ensure Integrity Protect data at rest and in motion, ensuring it is authentic, comes from a verified source and hasn't been tampered with.</p>
 <p>Enforce Control Prevent unauthorized commands or software from being executed on a device, and control access to data using fine-grained policies.</p>	 <p>Full product lifecycle Respond to evolving threats and new security requirements by actively managing the product from launch through end of life, using advanced security technology and services.</p>

How you can use keySTREAM to secure and enable your use-cases

Kudelski IoT keySTREAM provides trust, integrity, and control for any IoT application or uses case you wish to secure, ensuring the protection of data, safety, and revenue throughout its entire product lifecycle.

USE CASES EXPLORER



- Key / Device Management
- Smart Energy
- Smart Wearables
- Asset Tracking
- Connected cars
- Smart Buildings
- Smart City

- Smart Agriculture

Why Kudelski IoT?

Security is our DNA - 30+ years protecting high-value business models

Our IoT security expertise is rooted in our more than three decades of hardware, software and cybersecurity experience within Kudelski Group. We use those fundamental skills and expertise that we've developed in embedded and operational security to protect your key IoT assets – devices, identity, data, decisions, commands and actions – throughout the entire lifetime of the device and its ecosystem.

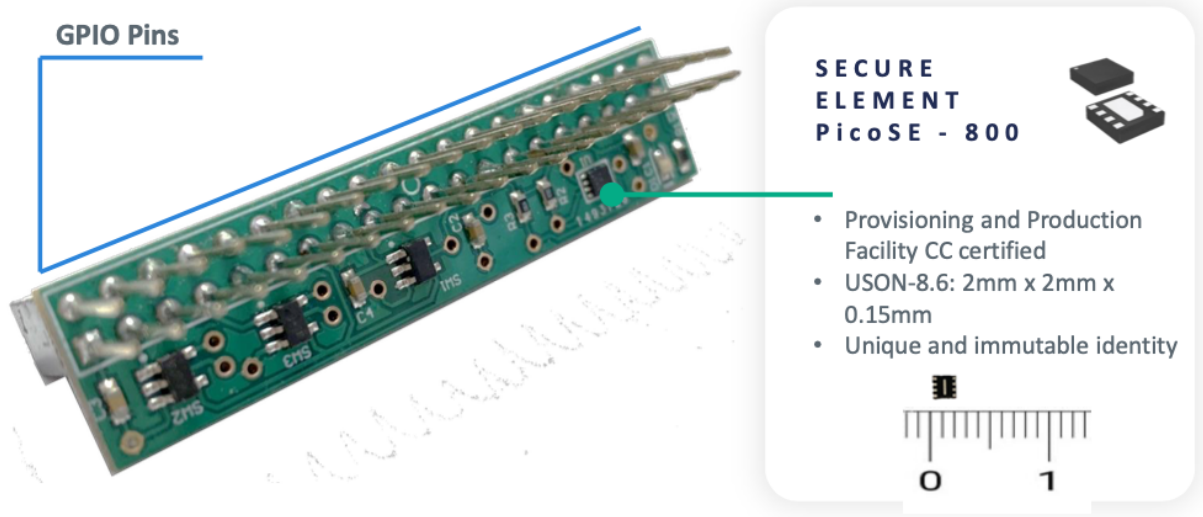
Why keySTREAM?

Embed trust, integrity & control at the root of your IoT business

We provide a device-to-cloud solution for securing all the key assets of your IoT ecosystem, end to end and during its entire lifecycle.

We integrate seamlessly with your devices and backend, enabling and securing all the applications and use cases that drive your connected business.

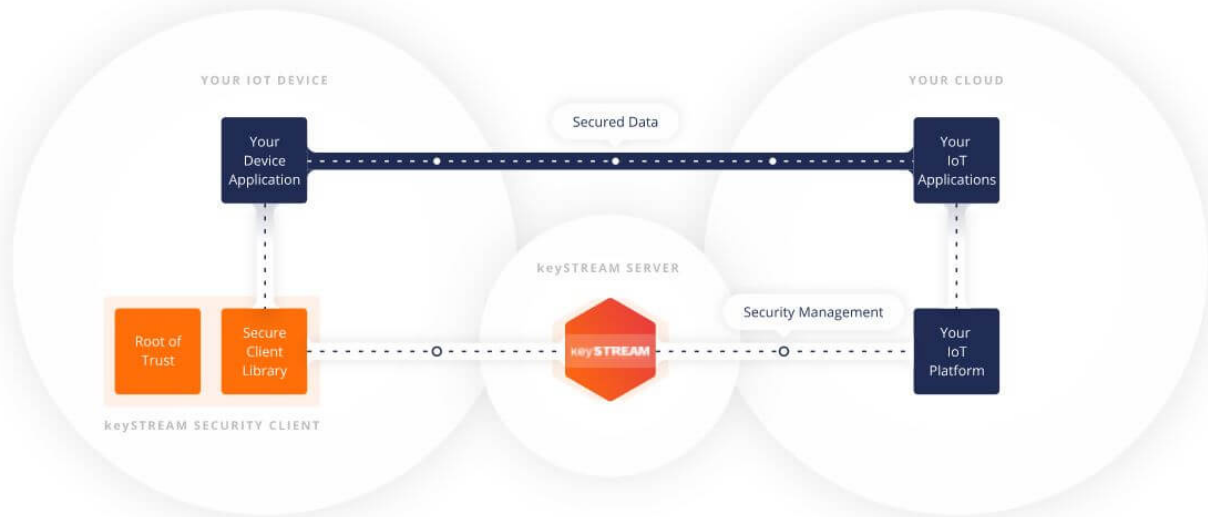
Hardware Overview



How does Kudelski IoT keySTREAM work to ensure security?

keySTREAM Secure Client with Root of Trust and Security Server secure your business end to end

keySTREAM consists of two main elements: a security client and secure server, that easily integrate with your devices and back-end platforms and applications using simple APIs.



DEVICE-SIDE
Robust device identity

One of the biggest challenges in IoT security is establishing an immutable identity (root of trust) in hardware (or software) that forms the basis for all other security use cases.

Root of Trust

The Root of Trust (RoT) is integrated in software or embedded as hardware into the device and is the foundation for all security use cases. This root of trust is personalized

when the component hosting the security is manufactured. Today we offer different security clients that bring increasing levels of robustness to the solution including Secure Elements, eSIMs and software hardened solutions.

Secure Client Library

The Secure Client Library (SCL) integrates with the device firmware and applications and acts as a driver to provide APIs to all security functions of the Root of Trust and of the Kudelski IoT Security Platform.

The Secure Client Library (SCL) is delivered as an SDK including test suites and documentation to test the SCL and SAL API integration.

BACKEND-SIDE

Secure Data, Decisions, Commands and Actions

Achieving your IoT business objectives depends on your ability to process and act on data. We create trust between all physical, digital and human assets in your IoT ecosystem and fully attest to data origin and integrity.

Security Server

The Security Server connects to your back-end platform to enable secure features by any authorized application. The server provides trusted data to the customer's backend. The data sent between the device and the cloud is identified, authenticated and traceable.

REST API

Device and Server APIs enable encryption, authentication and manage all IoT business logic. All Server functions are provided through REST APIs.

An online documentation kit is available to support the end-to-end integration of the Server and Client APIs including reference code for all functionalities of the platform.

DEVICE-SIDE

Robust device identity

One of the biggest challenges in IoT security is establishing an immutable identity (root of trust) in hardware (or software) that forms the basis for all other security use cases.

Root of Trust

The Root of Trust (RoT) is integrated into software or embedded as hardware into the device and is the foundation for all security use cases. This root of trust is personalized when the component hosting the security is manufactured. Today we offer different

security clients that bring increasing levels of robustness to the solution including Secure Elements, eSIMs and software hardened solutions.

Secure Client Library

The Secure Client Library (SCL) integrates with the device firmware and applications and acts as a driver to provide APIs to all security functions of the Root of Trust and of the Kudelski IoT Security Platform.

The Secure Client Library (SCL) is delivered as an SDK including test suites and documentation to test the SCL and SAL API integration.
