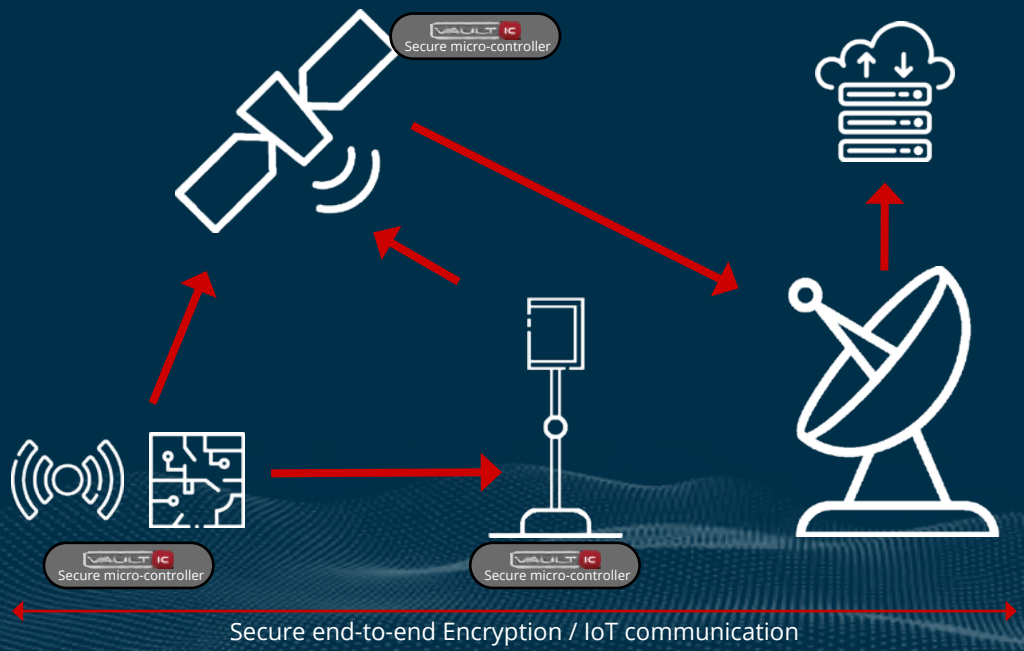
WISeSat

Powered by FOSSA - Secured by WISeKey

IoT sensor deployments are limited today by the restrictions of ground-based networks.

IoT ecosystems face the challenge of security and data privacy.

WISeSat is the first cost effective and secure IoT connectivity solution anywhere on Earth using picosatellites and low-power sensors. Its aim is to answer the needs of any large IoT deployment in Smart Farming, Energy, Logistics and more.



1 The distributed sensors collect and encrypt the data with a secret key that only the client knows.

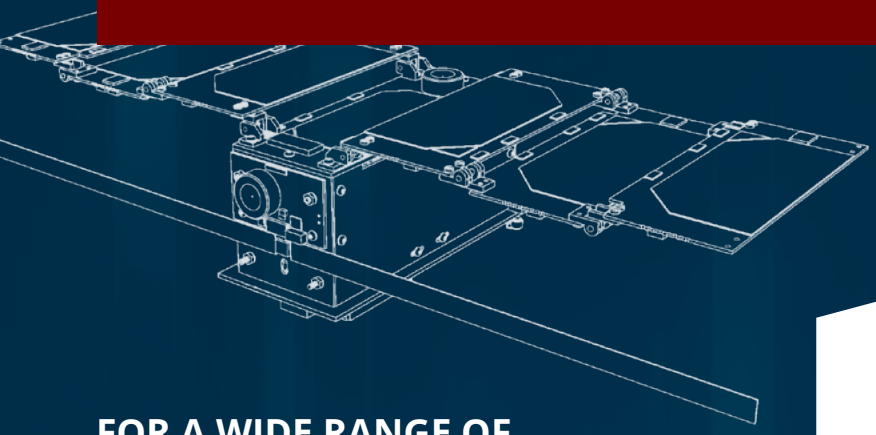
2 This encrypted data is sent to the satellite, where it is received and routed automatically to the ground station.

3 The ground station receives the encrypted data, and sends it to the network server.

4 The network server can decrypt the content and show the data for analysis.

Why WISeSat?

- Connect anywhere and everywhere on Earth.
- Cost competitive even compared to traditional ground-based solutions.
- FIPS 140-3 CMVP secure elements to secure devices, data & transmission.
- Backward compatibility for “brown-field” deployment on existing ecosystems.
- Seamless integration into ecosystems already using ground-based connectivity.
- Customized and scalable.



FOR A WIDE RANGE OF APPLICATIONS

Smart Farming: Track, monitor and control machines, crops and cattle continuously and securely no matter where they are.

Energy: Ensure a continuous and precise follow-up of your infrastructure all across the deployed area including deserts, oceans or any other remote environment.

Logistics: Track and monitor the exact location, tampering status, temperature, etc., of any merchandise or mobile asset across the whole supply chain without any blind spot.

IIoT: Collect data and monitor production and maintenance on remote industrial facilities anywhere on earth.

TRUSTWORTHY INTERACTIONS WITHIN THE IOT SYSTEM

Interactions between sensors, gateways, ground stations and satellites require trust. Trust is built by applying the following guidelines:

- Make sure you know who you are talking to.
- Are the devices allowed to communicate?
- Do we prevent others from listening in?
- Do we make sure that what was sent was received?

WISeSAT incorporates these requirements (Certificate-based Authentication (PKI), Authorization, Encryption and Integrity) by using various keys and cryptographic mechanisms (symmetric and asymmetric) and by protecting them with Secure Elements.

Contact information
WISeKey: sales@wisekey.com
FOSSA Systems: contact@fossa.systems