KALTIOT SMART IOT

WHITE PAPER

Kaltio Technologies OY
Version 2.0

Kaltiot Disclaimer

This document is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any code, functionality, or material, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Kaltiot's products remains at the sole discretion of Kaltiot.

Table of Contents

1. Introduction

A decade ago there were about 500 million devices connected to the Internet. Today there are 10 to 20 billion. In few next years, the number can easily be doubled. The rise of the connected objects known as the Internet of Things (IoT) will rival past technologies (such as steam engines, electricity) and change the playground on many areas. Some old technologies and business models fade away, while new industries/models spawn. IoT starts a new age of data.

To the forward-thinking organizations, the Internet of Things, is a game changing evolution. It is the economic and technical significance. It helps the organizations to prepare, adapt and thrive in this new economic age. Industrial and utility components, sensors, consumer products, vehicles, goods and everyday objects are being connected to Internet to provide information on their location, usage and conditions around them.

These connected ***Things*** can see, hear, feel and smell the world around them. Intelligence embedded to household appliances, cars, personal items, clothing, medical devices, infrastructure, and factory equipment generates vast amounts of valuable data that can be collected, networked and analyzed for a wide range of personal, business, and societal advances. It enables the organizations to integrate this information into their processes to make more intelligent decisions, reduce costs, and create new revenue streams.

Kaltio Technologies Oy (“Kaltiot”) welcomes you and your organization to the new world of the Internet of Things, where your connected ***Things***, along with your processes and people, are all connected enabling solutions which were previously not possible.

We provide a seamless view of your systems, devices and deployed ***Things*** in a secure cloud service for a monthly Opex fee. Our world-class IoT solution called **“Kaltiot Smart IoT”** shorten your time-to-IoT-enablement significantly by providing easy to deploy Kaltiot Smart Gateway SDK, easy to use device management, fully functioning backend and interface to your Business Intelligence (“BI”) solutions with bi-directional secured data transfers.

Whether you have few hundreds or tens of millions of ***Things*** constantly sending and receiving data, Kaltiot Smart IoT easily scales up to meet your needs while protecting your valuable data.

This white paper will introduce you to the Internet of Things and suggest how you can easily start implementing this exciting technology today to further enhance your organization process. This white paper focuses on how **Kaltiot Smart IoT** provides an integrated Internet of Things platform, which can revolutionize the industrial world by increasing operating effectiveness and revenue, while at the same time reducing costs and helping to address compliance related needs.

2. Business Value of the Internet of *Things*

Moving from Machine-to-Machine (M2M) based systems to Smart Connectivity solutions like **Kaltiot Smart IoT** helps organizations to provide higher magnitude of connected ***Things*** than traditional internet based M2M solutions.

Kaltio Smart IoT helps organizations to orchestrate massive amount of data streams integrated to business processes. IoT will increase your organization revenue and reduce costs. It can:

- reduce manual work required in inspecting equipment's
- reduce costs in travel and automation
- provide information for preventative maintenances and less maintenance activities thus reducing downtime
- provide tracking information and increase on time delivery
- improve customer experience and customer service
- improve safety and security
- improve quality and efficiency
- create new business models

Every organization will have to become data-centric in its approach and outlook. How well this massive data from IoT ***Things*** will be utilized, will determine the organization competitive advantage and future success. This analyzed data gives e.g.:

- Business a greater insight into its processes and products than ever before
- Marketer insight how consumers are responding to the latest campaigns and product offerings

- Supply-chain manager information about efficiency and possible security issues
- Production manager information on manufacturing efficiency and processes

Let's have a short look at insurance industry as an example. In every day operation, they collect and analyze massive amounts of data to understand and to mitigate risks. Adding IoT information in transporting would enable them to collect real time information on weather conditions, quality of road surfaces, travelling speeds, speed limits, driver behavior, car/vehicle data, locations, etc. Analyzing transporting information could lead to different insurance policies, categories or services offered.

It could create many new business opportunities. A driver with aggressive driving style history might have different agreements and insurance levels than others. Or they might have to pay more on getting same level of insurances. Insurance company could get relevant information on accidents immediately and depending on their services and agreements, the Insurance Company could alert rescue, police, medic ambulance to the exact place of accident and possibly save some life or further injuries. The Insurance Company could even know when their customers are at risk or their property are stolen and where that stolen property is located at.

2.1 Kaltiot Smart IoT is Kaltiot solution for IoT

Internet of things has brought new kind of requirements for devices which did not exists previously. These requirements are very long battery life, physically small size, low memory or network bandwidth usage and low unit price. Internet of things has also introduced security requirements like what is the impact when Internet of things-device gets hacked and important secured data cannot be leaked through hacked device.

These requirements favor for very long battery life, physically small size, low memory, low network bandwidth and low unit price without compromizing security.

Kaltiot Smart IoT has been able to implement all these new requirements. Its low memory footprint Gateway SDK library enables secure connections even on wearable

devices and optimized networking does not consume battery and bandwidth unnecessarily. Along with **Kaltiot Smart IoT** and new Iot devices, these enables new kind of business where you can have same kind of security level than you would have when are using your online bank on your desktop. This kind of security enables you to new business like remotely controlling mission critical systems which previously always required local presence. This high level of security is reached by every **Kaltiot Smart IoT** device having unique cryptographic keys, so one compromised device does endanger whole system operability.

3. Kaltiot background

Kaltiot employees has been participating in developing and building a sophisticated notification delivery system for one of the biggest mobile device manufacturer in the world. While system being robust, secure and horizontally scalable, it also made huge impact on device by reducing battery consumption and the amount of data transfers. Win-win situation to manufacturer, device users and 3rd party service providers. This notification system is a success story with tens of million users and over billions monthly notifications delivered on monthly bases. It is still used by world biggest social media companies.

4. Kaltiot Smart IoT technology

Kaltiot Smart IoT is an Internet of Things (“IoT”) turnkey messaging system solution. It provides always online functionality even to constrained connected ***Things*** and lossy wireless networks while protecting connections with strong security. Kaltiot Smart Gateway SDK uses extremely lightweight secure protocol for connecting to Kaltiot Smart IoT cloud. It reduces the bandwidth usage and power consumption. Gateway SDK provides self-provision to the system with identity and access control. Kaltiot Smart IoT provides secure HTTP API for accessing your ***Things*** data. It can be stored for further big data analysis. Kaltiot Smart IoT offers cost-efficient solution that scales easily up and down based on your needs, whether your system is small or large.

Kaltiot Smart IoT is a combination of several components working together to form a two-way end-to-end secure data message delivery channel between connected ***Things*** and organization BI systems. This enables organizations to get critical data with

minimum latency, save it to their own data storage and to further analyze it for different purposes.

Kaltiot Smart IoT has following built-in security features: secure connection using strong ciphers, client authentication, revoking devices that are physically hacked, individual client keys and certificates and automatic certificate renewal.

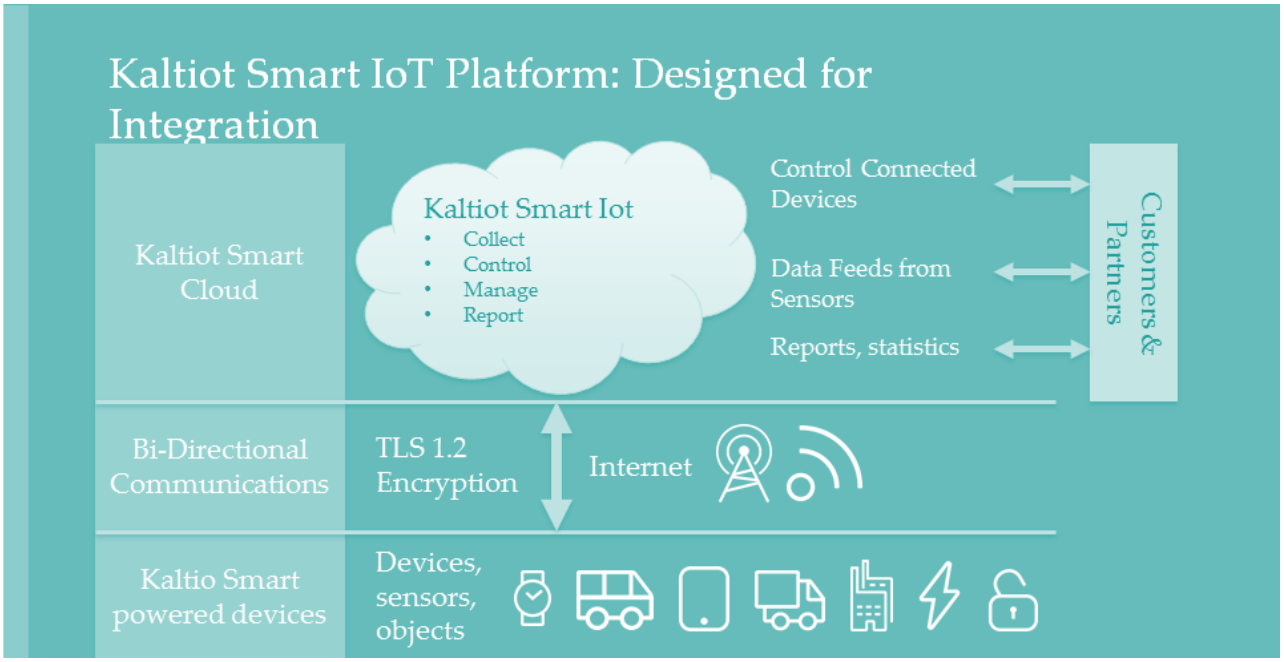
4.1 Kaltiot Smart IoT Platform: Designed for Integration

Kaltiot Smart IoT platform has been designed for integration towards organizations BI systems. This system contains the HTTP Rest API, where your organization can connect your BI systems. It enables bi-directional communication between your connected ***Things*** and your BI systems. Getting data streams allows your organization to store received data and then use that data for analysis. These data streams can be:

- Session ID's
- Persistent or non-persistent web socket to one single or all your connected ***Things***
- Get all your devices identities
- Send data from your BI systems to one single or group of connected ***Things***

The HTTP Rest API allows you to send command messages or queries to your connected ***Things*** either one at a time or more than one connected objects at the same time. If a connected object is not online, message will be delivered once connection has been re-established.

Kaltiot provides a private channel between your connected ***Things*** and your organization BI systems.



4.2 Kaltiot Smart Gateway SDK

Kaltiot Smart Gatewat SDK helps organizations to get their objects connected to Kaltiot Smart IoT for delivering their data towards their own organization. The Gateway SDK takes care of everything needed for secure communication to **Kaltiot Smart IoT** backend.

We have gone through the needs of the end customer and made it easy to use. We have packed in to our SDK all the needed components, which do almost everything from fetching unique identity to security to using network in the most optimal way. All the connected ***Things*** need to do is to connect to Gateway SDK. We will ensure your ***Things*** are connected in the most secured way and messages are both delivered and sent.

Gateway SDK is written in C for easy portability, excellent performance and low memory usage to the embedded devices.

Automatic Provisioning: Ability to create unique identity, certificates, and credentials required to go online without human intervention.

Identity Management: Gets unique identifier for the Gateway SDK and the ***Things*** connected to SDK.

Certificate Management: Fetches unique certificate for the Gateway SDK. Renews the out of date certificate automatically.

Network Management: always online and finds out the optimal keep alive for the network it is in. Reconnecting when there is disconnection. Thus optimizing the battery/power usage.

Kaltiot Smart IoT Protocol: Abstraction layer on top of MQTT, which hides the complexity of identity, certificate, messaging to the application.

TLS 1.2: **Kaltiot Smart IoT** uses ECC based key exchange and authentication, which provides equal security with smaller key sizes compared to RSA.

Advantages: **Kaltiot Smart Gateway SDK** helps you easily and quickly connect your object to **Kaltiot Smart IoT Cloud.** Its binary size is approximately 250 kilo bytes including TLS and TCP code. It needs 20 kilo bytes of RAM to operate, including TLS and TCP consumption.

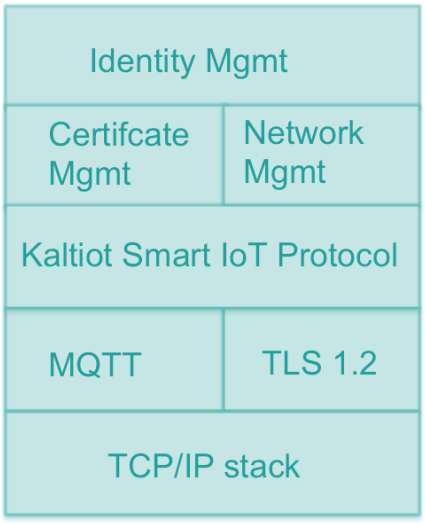


Figure: Client Stack (layered diagram)

4.3 Data Communication & Encryption

Nearly all connected ***Things*** are usually behind operator or organization NAT/FW, where TCP brings advantages over UDP. Kaltiot has evaluated and tested various connectivity solutions and chosen TCP with TLS 1.2 encryption. For always connected ***Things***, which need real-time push, below is a list of comparison with most important behaviors.

UDP vs TCP

- UDP consume more bandwidth
- UDP consume more power from connected devices
- UDP keep-a-live value is 30-180 seconds, TCP has up to several hours. This results to huge difference in data traffic and power consumption.
- Security (DTLS) on UDP can consume more RAM due to DTLS handshake requiring bigger buffers to be able to buffer incoming fragmented handshake messages

Conclusion UDP vs TCP

- TCP uses less power
- TCP uses less data
- TCP uses less memory

Another obvious solution would be to use (Open)VPN. In low signal or low quality networks, we see following:

(Open)VPN vs TCP with TLS

- (Open)VPN can consume a lot of data just to keep the connection open.
- Re-establishing (Open)VPN handshake consumes over 40KB of data, plus tunneling protocol added overhead in every packet your connected objects send.

Conclusion (Open)VPN vs TCP with TLS1.2

- TCP with TLS1.2 can reduce data costs up to 50-60 times less than (Open)VPN

4.4 Cyber threats and how Kaltiot Smart IoT tackles them

Denial of Service attacks:

- Gateway SDK: Devices does not require any listening ports or public IP's.
- Kaltiot Smart IoT Cloud: Transport layer is TCP. Cloud architecture can be distributed to multiple data-centers with automated scripts to add and remove capacity based on needs.

Botnets and malware based attacks:

- Gateway SDK: Device does not have open listening ports through which malware could get in and device is behind operator or organization NAT/FW without public IP.
- Kaltiot Smart IoT Cloud: Physically hacked devices can be revoked from the system.

Data breaches:

- Gateway SDK: Spying of the communications is prevented with strong encryption algorithms.
- Kaltiot Smart IoT Cloud: Databases are behind bastion hosts/DMZ. No user credential stored in databases. All devices connecting to cloud are required to TLS mutual authentication and then provide very long machine created passwords.

Poor physical security:

- Gateway SDK: Sensitive information is not stored in unencrypted format on the device.

Privacy concerns:

- Kaltiot Smart IoT Cloud: It is possible to run the system without identities for physical ***Things***. Collected data can be de-identified and anonymized. Data access only for authorized and authenticated entities.

Insecure software/firmware:

- Gateway SDK: Device has ability to update its software in secure manner.

Man in the middle:

- Gateway SDK: All communication is end to end encrypted.

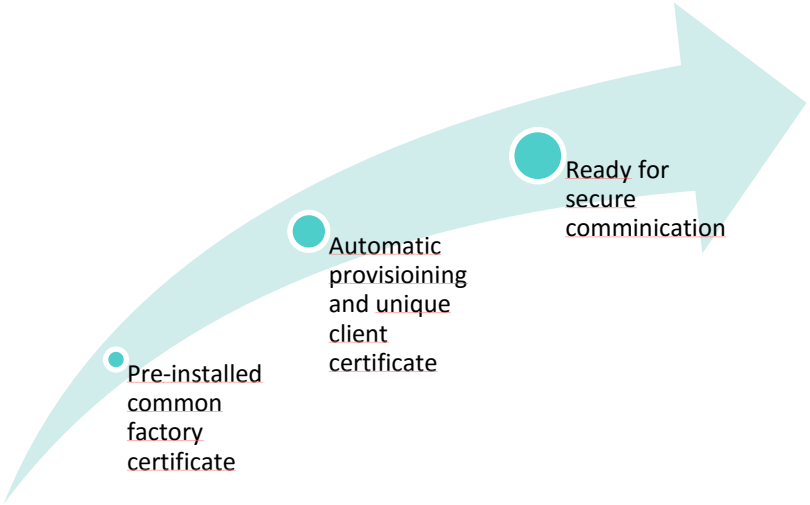
Insufficient authentication/authorization:

- Two level of authentication is used. Both server and client have to provide a valid certificate and the client certificate is unique per device. Every connected ***Things*** has unique credentials on top of certificate authentication.

4.5 Certificates

When you first time install SDK, you will get common factory certificate which is common for all your ***Things***. Once device goes online first time, it will automatically fetch new unique certificate which will be used until it's validity time or certificate is revoked. If certificate's validity time expires, SDK will take care of updating it automatically with the new one.

Certificates size is optimized. Average certificate will take approximately 400 bytes and only strongest cipher suites are supported (TLS1.2)



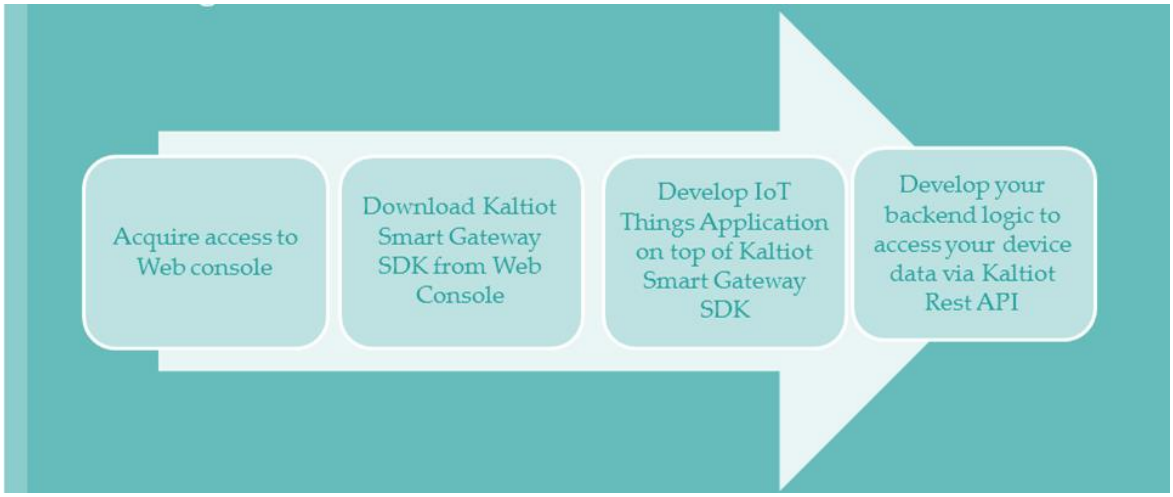
5. Taking Kaltiot Smart IoT into use

Taking any new solution into use consumes usually a lot of time and valuable resources. Therefore we're providing easy way to start using our world class solution. We can offer Kaltiot Smart IoT for testing purposes as well as for running any sized production environment.

Kaltiot offers also consultation services, where our skilled solution engineer(s) can be used for building your organization software. Our engineers will be able to assist you on various cases.

5.1 The 4 main steps for taking Kaltiot Smart IoT into use:

1. Acquire/apply access to Kaltiot Smart IoT Web Console
2. Download the Kaltiot Smart Gateway SDK from Kaltiot Smart IoT Web Console
3. Write your ***Things*** application and connect them with Kaltiot Smart Gateway SDK
4. Write your service using Kaltiot Rest API



See more details in our wiki: https://kaltiot.atlassian.net/wiki/display/KALTIOT SMART IOT/Kaltiot Smart IoT+Documentation

Abbreviations

Abbreviation	Description
BI	Business Intelligence, the set of techniques and tools for the transformation of raw data into meaningful and useful information for business analysis purposes
Constrained	Some sort of restriction, like reduced amount of memory or low power
Device	Any equipment made for particular purpose. An item of hardware
FW	Firewall, a network security system that monitors and controls both incoming and outgoing traffic
IoT	Internet of ***Things***
Kaltiot	Acronym for Kaltio Technologies Oy company based in Oulu, Finland
Latency	A measure of the time delay experienced
NAT	Network Address Translation, technique to map multiple hosts to one publicly exposed IP address
Object	A thing/device that has physical existence
Opex	Operating Expence or operating expenditure; the continuing costs of a business, in contrast to capital expenditure
Organization	Company, corporation, firm, institute, hospital, etc
Revoke	Cancel granted privileges
SDK	Software Development Kit, a software framework
Things	IoT devices, objects, sensors and gadgets that are capable of sending and receiving data
Kaltiot Smart IoT	Internet of ***Things*** messaging system