



Teserakt

Company presentation – 20180908

Mission

Make encryption a standard for IoT, in the same way that it is now a standard for mobile messaging.

Teserakt AG

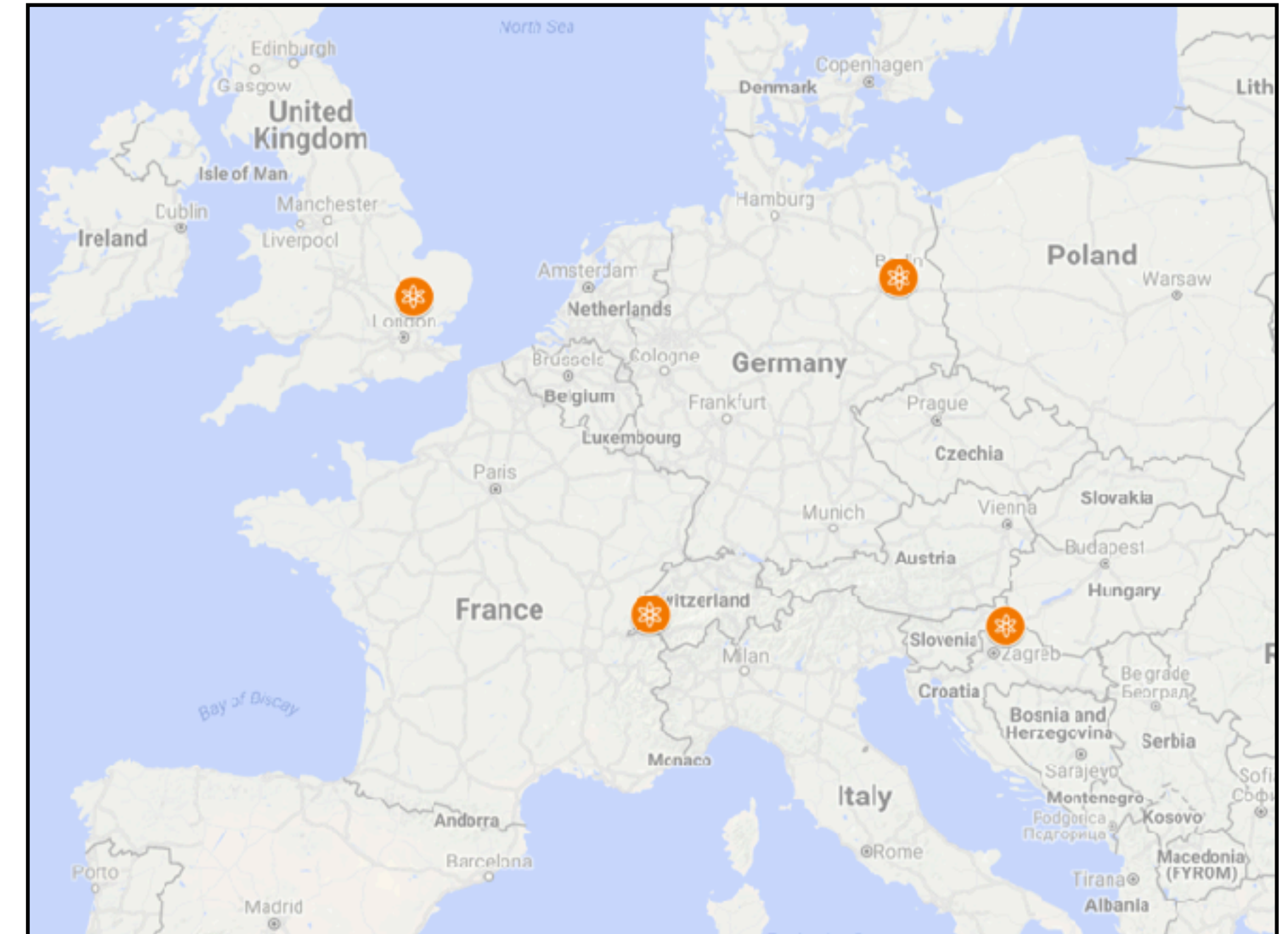
Founded in August 2018

HQ in **Lausanne, Switzerland**

Specialists based in:

- Berlin, Germany
- Cambridge, UK
- Varazdin, Croatia

Seed funded, fully owned by founders



Founders

Jean-Philippe Aumasson

Leading cryptography expert, PhD, author of the reference book *Serious Cryptography*, designer of widely used cryptosystems, speaker at leading international conferences. 12 years experience in applied cryptography in academic and industrial environments.

Alan Duric

Serial entrepreneur, secure digital communications pioneer, co-founder of leading secure messaging application Wire (CTO then CEO), co-founder of Camino Networks (acquired by Skype), co-founder of Telio Holding, contributor to IETF, ETSI, and ITU standards.

Problem addressed

Machine-to-machine (M2M) security

Hard because of:

- *Physical limitations*: Chip frequency, memory, network latency, bandwidth, storage space
- *Inadequate tools*: Legacy systems such as TLS and PKIs, built-in crypto is weak or inexistent
- *Key management*: How to securely provision keys to devices, avoid global keys, rotate keys?

Why bother?

Protect business and privacy-sensitive data that transits on third-party/cloud infrastructure

Enable new applications and use cases so far impossible because of the data breach risk

Internet of Things: Convenient

But Insecure

The IoT threat to privacy

Posted Aug 14, 2016 by [Christine Bannan](#)

Insecure IoT devices to be prohibited, US Federal purchases restricted

First product: E4

Secure communication over MQTT, software-only

MQTT is the main IoT/M2M protocol, industry standard

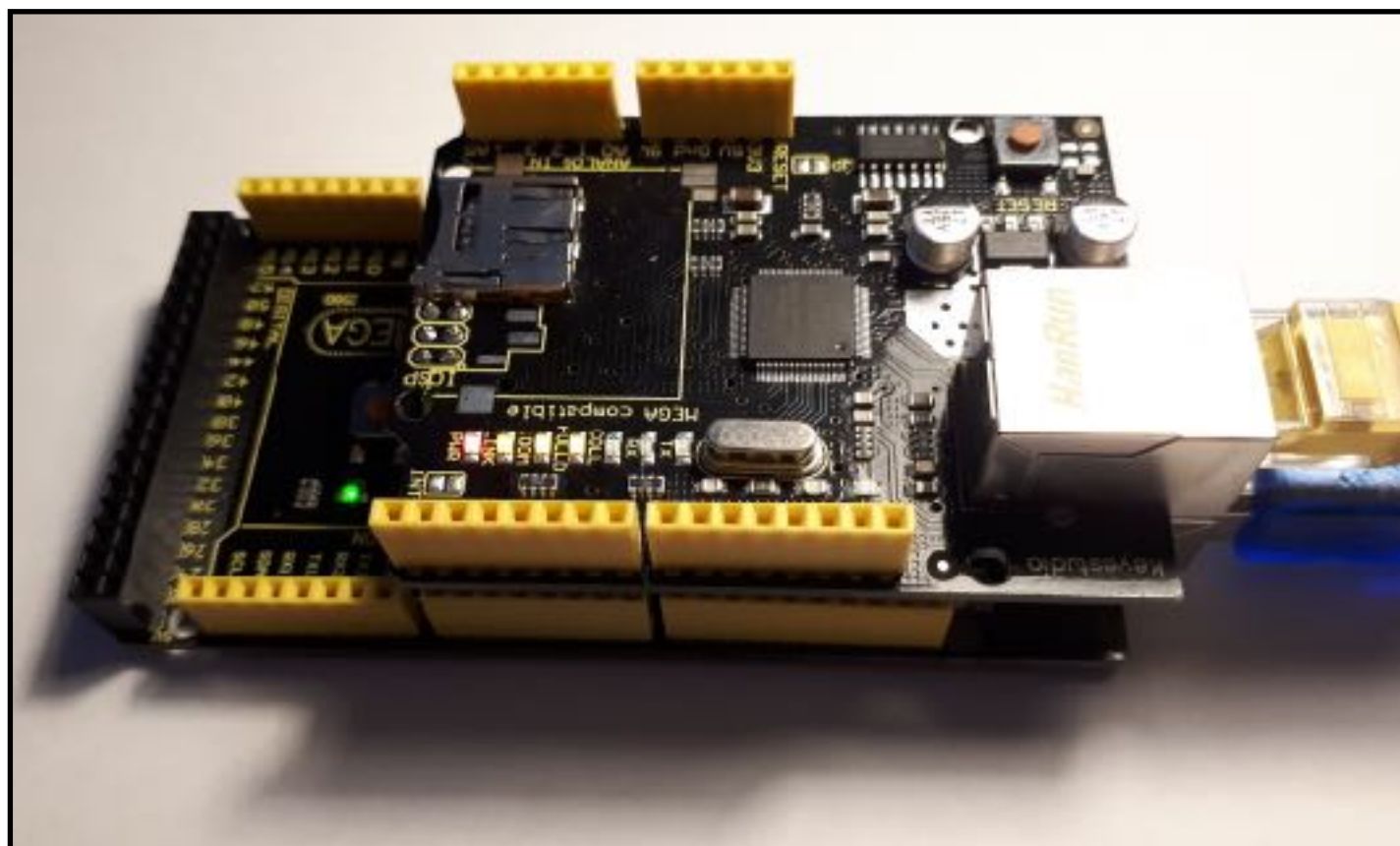
- Used in connected cars, drones, power plants, etc.
- The only IoT protocol supported by cloud platforms



First product: E4

Client software library:

Encryption layer between transport layer and business logic layer.



Key management server:

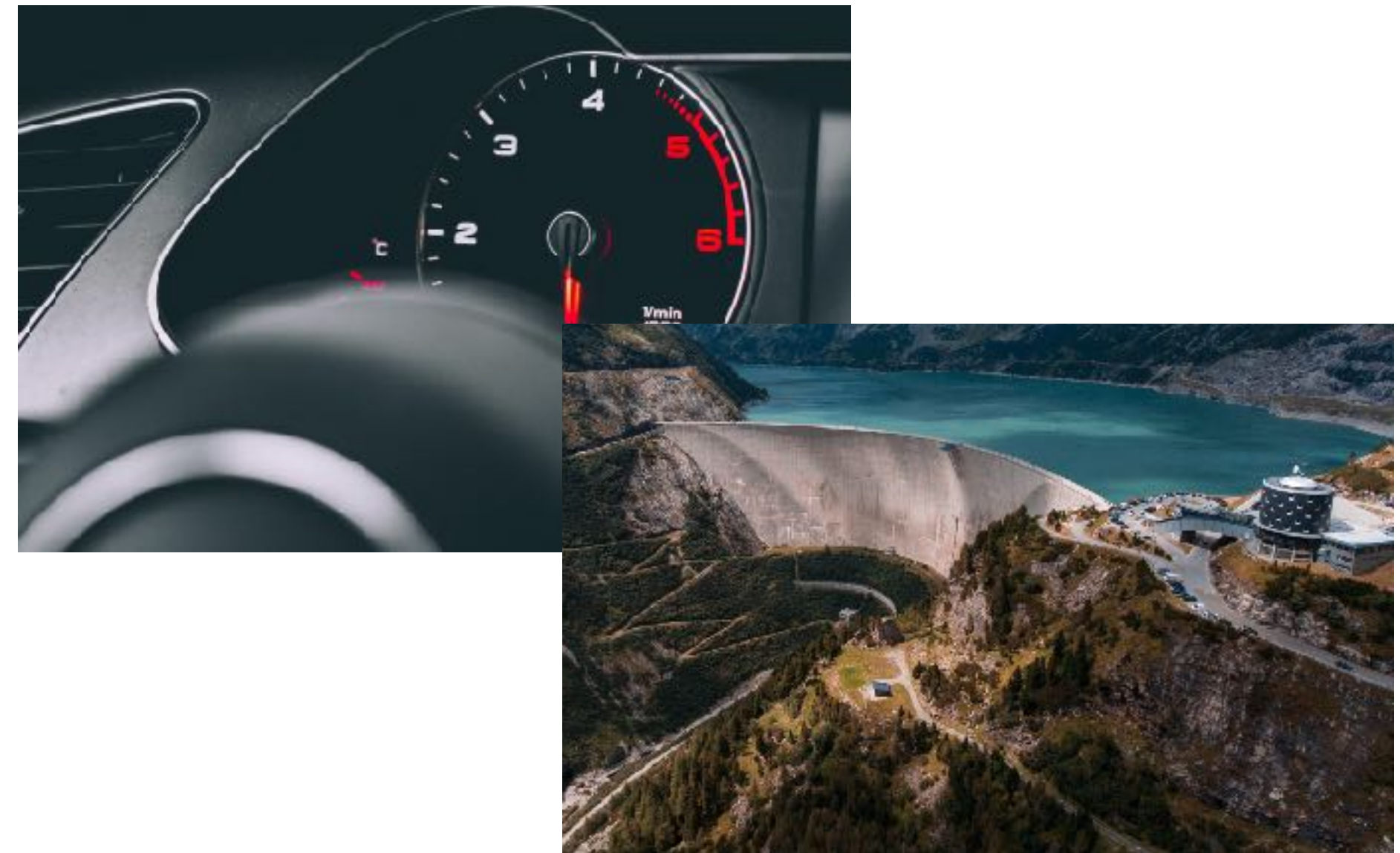
Remotely manages keys, automates key rotation, web UI and CLI.

DATE	COMMAND	PAYLOAD
23/05/2018, 13:01:55	topic_list	<pre>{ "payload": { 1 item "cmdType": string "topic_list" }}</pre>
23/05/2018, 13:01:55	remove_topic	<pre>{ "payload": { 2 items "cmdType": string "remove_topic" "topic": string "My new topic" }}</pre>
23/05/2018, 13:01:56	topic_client_list	<pre>{ "payload": { 2 items "cmdType": string "topic_client_list" "topic": string "My new topic" }}</pre>

Industries

MQTT used for M2M transmissions in:

- Automotive, V2*
- Healthcare
- Oil and gas
- Transportation
- Supply chain
- Energy, smart grid



Sales model

Key management server:

- One-time fee (integration, license)
- Yearly M&S fee

Client software:

- Per-device license fee
- Depends on the device type and number

We can adapt our solution to other protocols than MQTT, please contact us for details.



Teserakt

*Want to try our solutions or see a demo? Any questions?
Contact us at contact@teserakt.io*