ELIoTPro

Bringing cybersecurity
for IoT to the next level

Problem

IoT security measures are not good enough:

- Cyber-attacks, phishing attacks, data and identity thefts occurring on a massive scale.
- IoT devices are vulnerable against cyber-attacks.
- Safety issues are hampering growth and use of IoT solutions globally.
- IoT Devices can't support existing security solutions.
- Over 50% of consumers worldwide are concerned about IoT security.
- Compliance with new cybersecurity legislation will soon be mandatory

Solution

ELIoT Pro – is the next generation end-to-end cyber security solution.
Comprising secure Human to Machine (H2M) authentication, Machine to Machine (M2M) authentication with Lightweight Encryption and Self Healing AI, **ELIoT Pro protects users, IoT devices and data.**

Key Features

ELIoT Pro is a fully integrated IoT cybersecurity platform featuring an architecture for User and Device Authentication as well as IoT System Self Healing comprising 3 layers:

1. H2M Authentication

- ✓ Smartphone-based login using ultra-sound
- ✓ Ready for voice-activated IoT hubs
- ✓ No user credentials for hackers to steal
- ✓ No phishing or man-in-the-middle attacks

2. M2M Encryption and Authentication

- ✓ Minimum computation IoT cypher, authenticates and protects simple end-point devices and data

3. Self-Healing

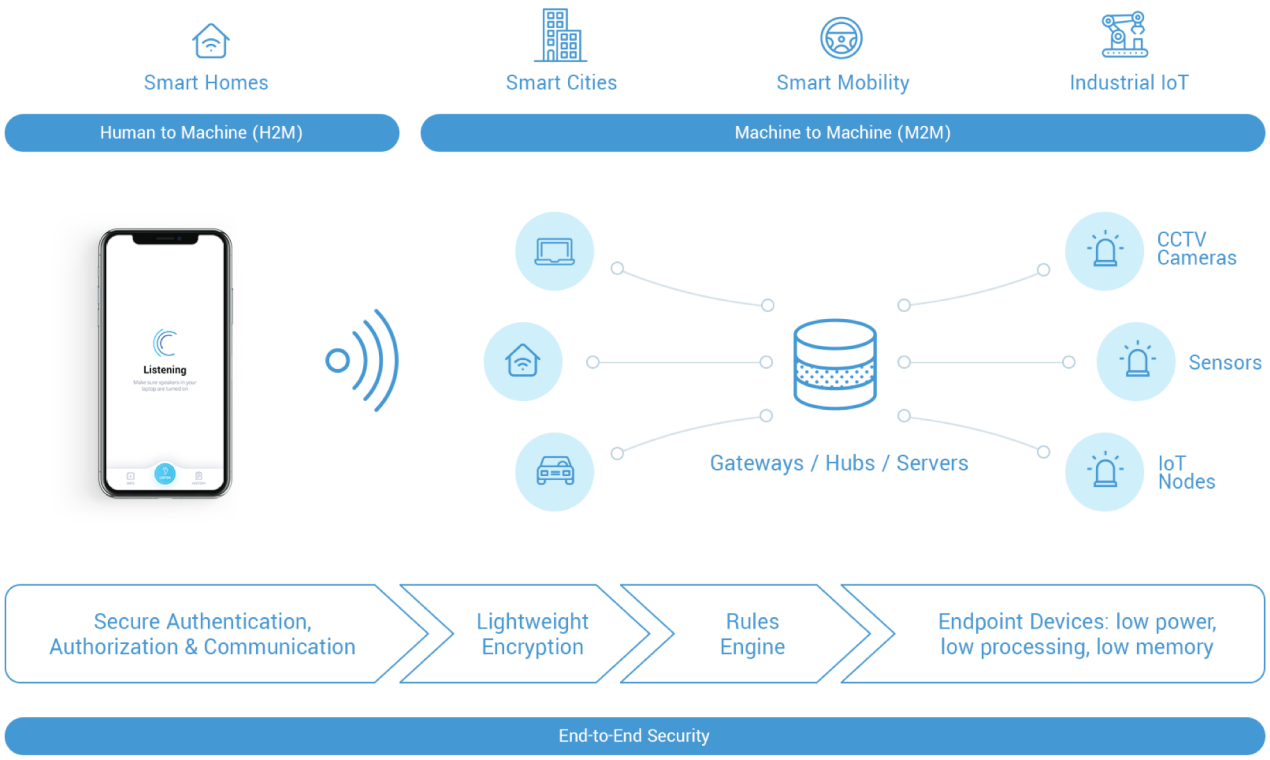
- ✓ Predictive AI analytics to detect anomalous behavior and anticipate device/system failure

ELIoT Pro is a comprehensive, end-to-end cybersecurity solution for IoT networks. No other system provides simultaneous protection of users, devices, systems and data.

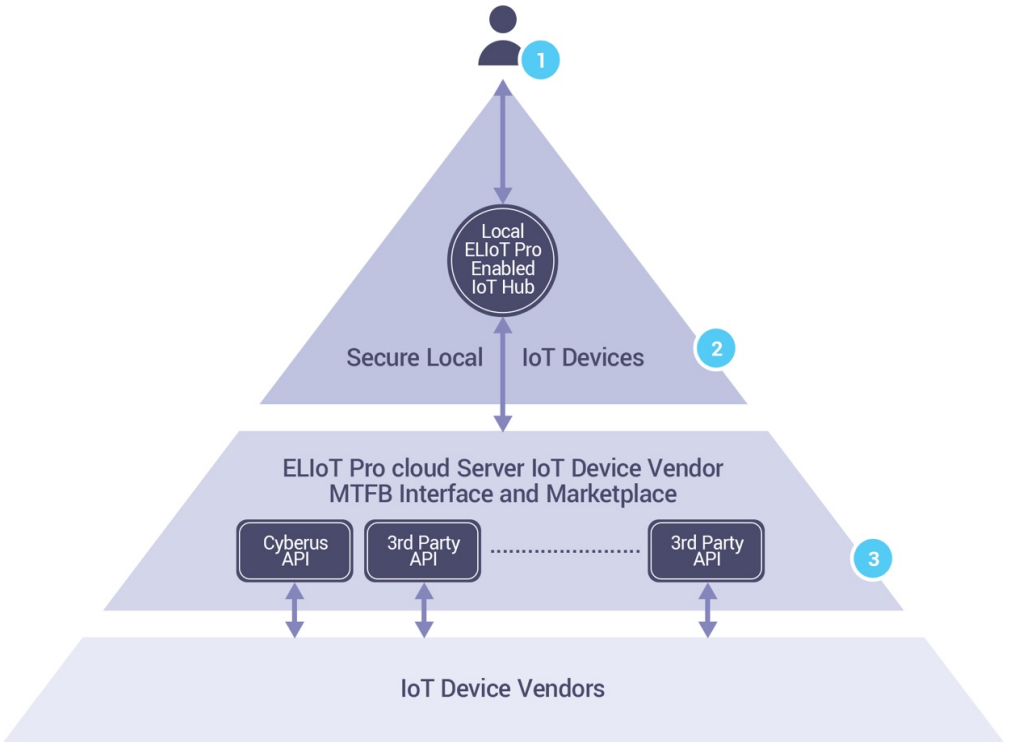
The unique approach of **ELIoT Pro** eliminates passwords and static credentials providing secure and easy authentication in Human-to-Machine and Machine-to-Machine communication.

ELIoT Pro's concept makes it a universal solution for IoT networks regardless of industry. Present use cases include **Automotive, Industrial IoT, Smart Buildings, Smart Homes** and **Smart Cities.**

System Overview



System Hierarchy



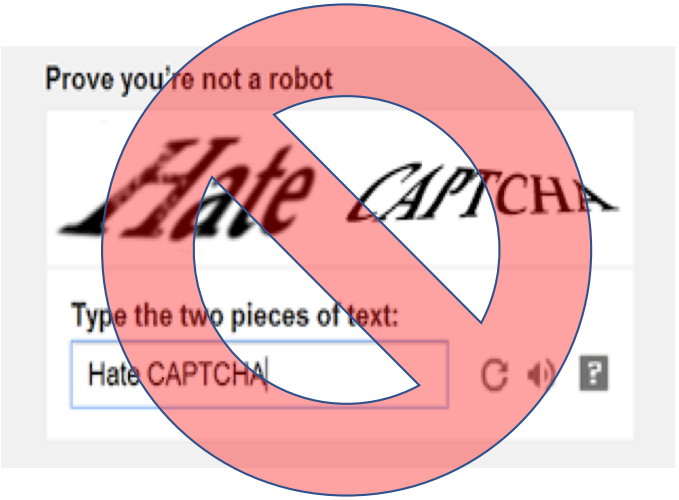
ELIoT Pro architecture for User and Device Authentication

Layer 1- Human to Machine

The Secure Human to Machine interaction (H2M) is a password-less user authentication technology based on a sonic transmission of One Time Passwords (OTP).

The technology creates a user experience that is quick, painless, and free from the friction and headaches that most users associate with “login”:

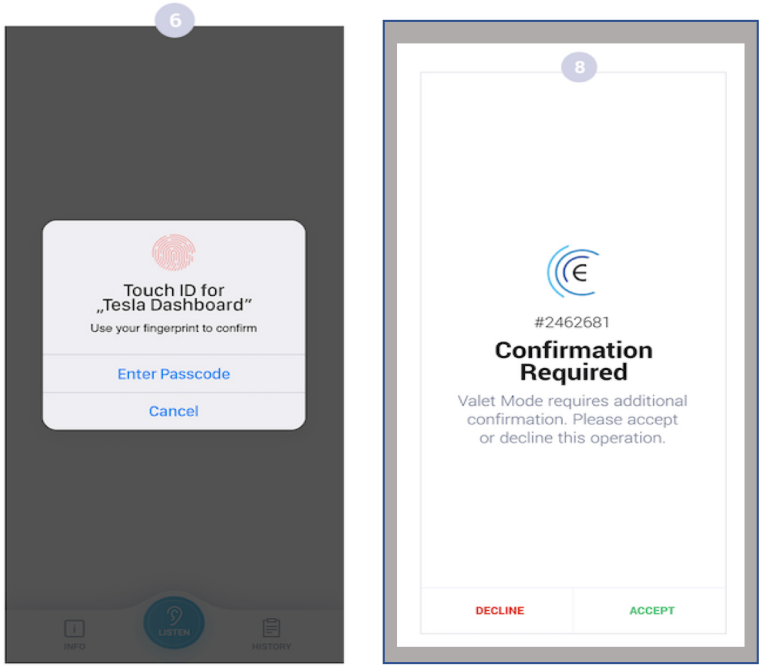
No more complex passwords to remember, reset, and manage across dozens of websites.
No more Captcha!
No more worrying about whether accounts have been compromised.
No more waiting for “security codes” to show up via SMS or hard token, and then having to type these codes into the browser.



Layer 1- Human to Machine

The **ELIoT Pro H2M** uses multiple factor authentication, Out of Band Transaction Confirmation and Cloud redundancies to be highly secure against the most common cyber attacks and hacks:

Secure against credentials theft.
Secure against phishing attacks.
Secure against Man in the Middle attacks.
Secure cloning attacks.
Secure DDOS attacks.



Layer 1- Human to Machine

With ELIoT Pro, authentication becomes as simple as opening an app and placing or holding the smartphone near the computer.

ELIoT Pro has a standalone app, as well as an SDK that can be built into existing client company apps.

To enable ELIoT Pro, the User will use the ELIoT Pro App from the iTunes or Google Play store, or integrate the ELIoT Pro App with the client app by use of the SDK.

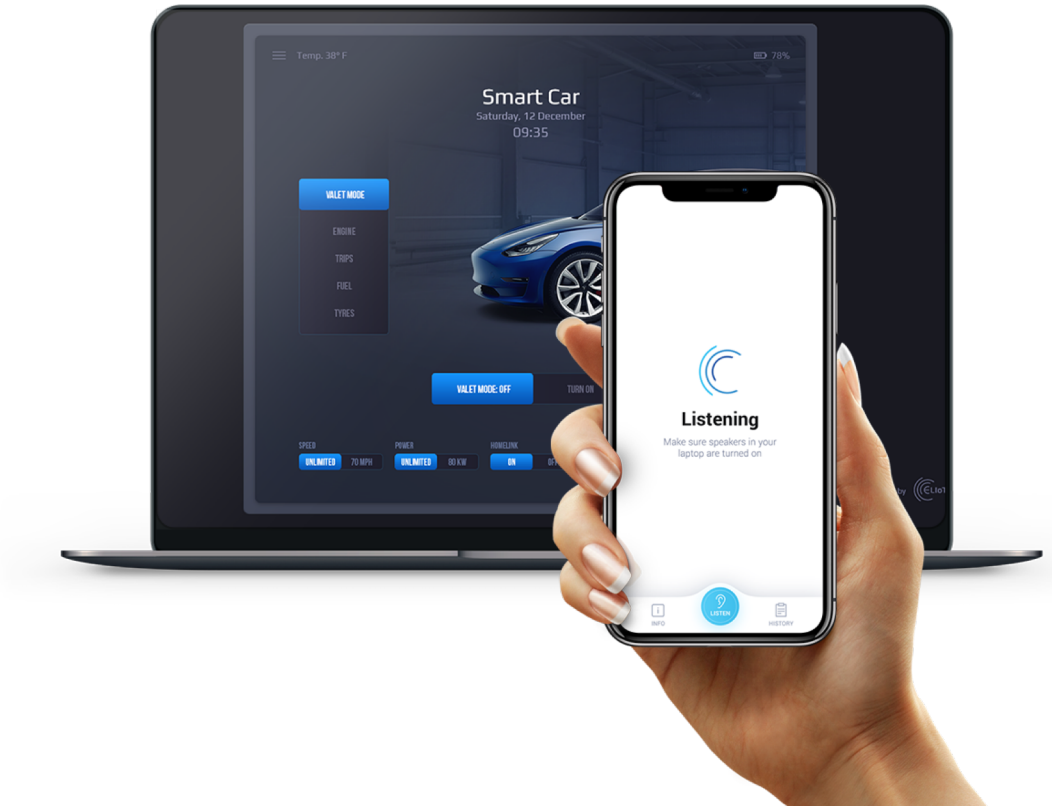
Original ELIoT Pro mobile component may be customized for Operator's needs and requirements.

Layer 1- Human to Machine

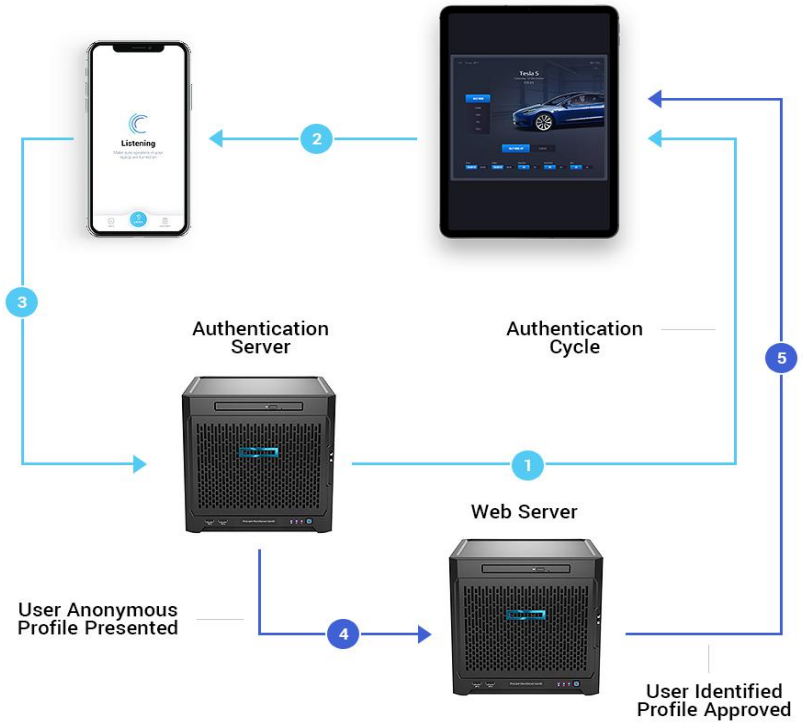
The secret of ELIoT Pro is the credential-free authentication, to secure Human to Machine interaction.

Logon is available via web or Operating System interface.

The authentication protocol is versatile as it can be used in laptop to mobile, laptop to laptop, mobile to mobile or POS to mobile.



Layer 1- Human to Machine



ELIoT Pro H2M authentication loop

Layer 1- Human to Machine

Voice Activated Networks:
IoT User interaction is increasingly done via voice control using Smart Speaker technology.

ELIoT Pro has been configured to strongly authenticate human users in voice-controlled environments to support secure voice transactions.

The ELIoT Pro Smart Speaker integration provides a secure, noise resilient user authentication system, which overcomes all the weaknesses inherent in voice authentication and other biometric user authentication.

Current ELIoT Pro H2M is integrated with Alexa to transmit a sonic OTP to the ELIoT Pro mobile app, when an authentication event is requested by the user.

Layer 2: Machine to Machine

The **ELIoT Pro** Secure Machine to Machine interaction (M2M) proprietary Lightweight Encryption (LE) and authentication protocol allows IoT devices to be robustly authenticated and to communicate securely to IoT hubs or directly with each other without the use of any preset passwords. The minimal computational requirements of LE are ideal for secure communications to the IoT edge devices which run on minimal processing and battery power.

Today's IoT security systems discriminate against the vast majority of end-point devices and provide security only to the minority that meet large memory and substantial computational power requirements.

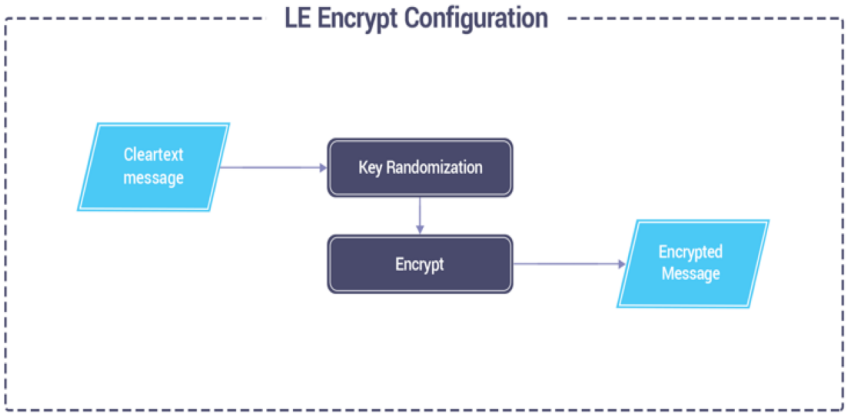
The computational power and memory storage of the majority of IoT devices are among the main problems for securing IoT networks, since these devices limit or exclude the use of demanding encryption methodologies.

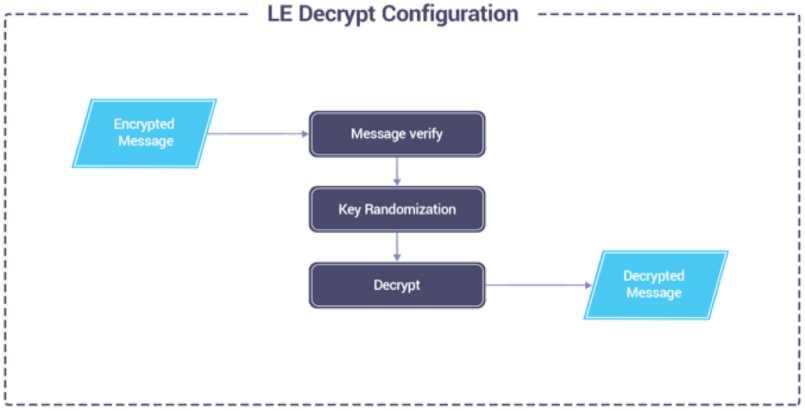
Also, device battery life is affected by computing activities and memory usage. Examples include sensors in remote locations that run on batteries and have limited memory and computation capabilities. This creates a vulnerability for an entire IoT environment.

The **ELIoT Pro** Lightweight Encryption (LE) is IoT Platform and Communication Protocol agnostic.

Layer 2: Machine to Machine

The ELIoT Pro Lightweight Encryption (LE) provides an encryption algorithm which can run on even the smallest ARM type processor with minimal memory needs. LE incorporates the concept of ‘entanglement’, its unique characteristic that sets it apart from other solutions in the cyber security world. Devices communicating via LE accumulate a type of hashed record of previous interactions similar to blockchain node records. This allows devices to build “trust” in the other devices on the IoT network.





Layer 2: Machine to Machine

Test results of Lightweight Encryption (LE) against AES 128 & AES 256 in - ARM system profiling.

Algorithm	Compiler options	Input size (bytes)	Iterations	Avg. encryption time	Avg. decryption time	Avg. time total	Throughput Mbps
LE	-DNDEBUG -O3	1,048,576 (1 MB)	1	54 ms	39 ms	93 ms	86.02
AES 128	-DNDEBUG -O3	1,048,576 (1 MB)	1	128 ms	85 ms	213 ms	37.56
AES 256	-DNDEBUG -O3	1,048,576 (1 MB)	1	139 ms	100 ms	239 ms	33.47
LE	-DNDEBUG -O3	1,048,576 (1 MB)	1000	25,506 ms	20,217 ms	45,723 ms	174.97
AES 128	-DNDEBUG -O3	1,048,576 (1 MB)	1000	81,082 ms	86,198 ms	167,280 ms	47.82
AES 256	-DNDEBUG -O3	1,048,576 (1 MB)	1000	95,910 ms	100,732 ms	196,642 ms	40.68

LE

ELIoT Pro’s performance beats currently used algorithms and allows for improved security in a wide range of IoT devices that would otherwise have either substandard encryption or no encryption at all.

Layer 3: Data Analytics

Layer 3 analyzes IoT system data to predict system and device failure, detect anomalous behavior and identify possible attacks. Layer 3 is designed to create a “Self Healing” capability for IoT systems by setting operating limits on devices, ingesting Mean Time Between Failure (MTBF) data and cyber attack patterns to feed an AI mechanism which can predict and mitigate system failure.

Layer 3 is comprised of 3 key components:

1. A Rules Engine and Flight Envelope parameters, to set and control device operating limits.
2. An IoT Device Vendor Interface for ingestion of MTBF data. The IoT Device Vendor Interface also supports automatic device purchase for replacement and provisioning.
3. An AI engine for predictive analytics and anomaly detection.

Compliance

ELIoT Pro provides technology features that are compliant with the most recent and projected legislative initiatives, designed to implement cybersecurity requirements for IoT systems, both in Europe and in the US. Among them are:

- EU Cybersecurity Act – ENISA (EU);
- S.B.327 - Security of Connected Devices (US);
- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (US);
- Code of Practice for Consumer IoT Security (UK).

ELIoT Pro by design is also compliant with EU Data Privacy regulations including GDPR. This has been confirmed by the European Commission's Directorate-General during ELIoT Pro's Horizon 2020 grant application evaluation.

Types of Installation

ELIoT Pro can be installed as a full Cloud/SaaS, On-Premise or Hybrid solution, depending on the Client preference.

Cloud/SaaS Solution
ELIoT Pro H2M Cloud/SaaS solution is the simplest, least expensive and fastest installation/deployment for a Client. Using the ELIoT Pro H2M API (for web-based logins) and/or the ELIoT Pro H2M SDK (for mobile-only logins) a Client can quickly and easily install ELIoT Pro H2M for their users.
ELIoT Pro H2M Authentication Servers are hosted on Amazon Web Services (AWS).

On-Premise Solution
For a large enterprise installation, a Client may prefer to have an On-Premise installation – meaning the ELIoT Pro H2M Authentication servers will be located within the Client's IT ecosystem, behind their firewalls.

Hybrid Solution
ELIoT Pro H2M Authentication Servers are located in the Cloud and users' data is anonymized. Servers with data bases containing Client's users' personal data and Web Server will be located within the Client's IT ecosystem, behind their firewalls.

SaaS/Cloud Solution	Fast install at AWS Servers in Frankfurt, DE
Enterprise Solution	Custom on-premise install with „white label” option
License fee	Based on # of devices
Pricing	Flexible

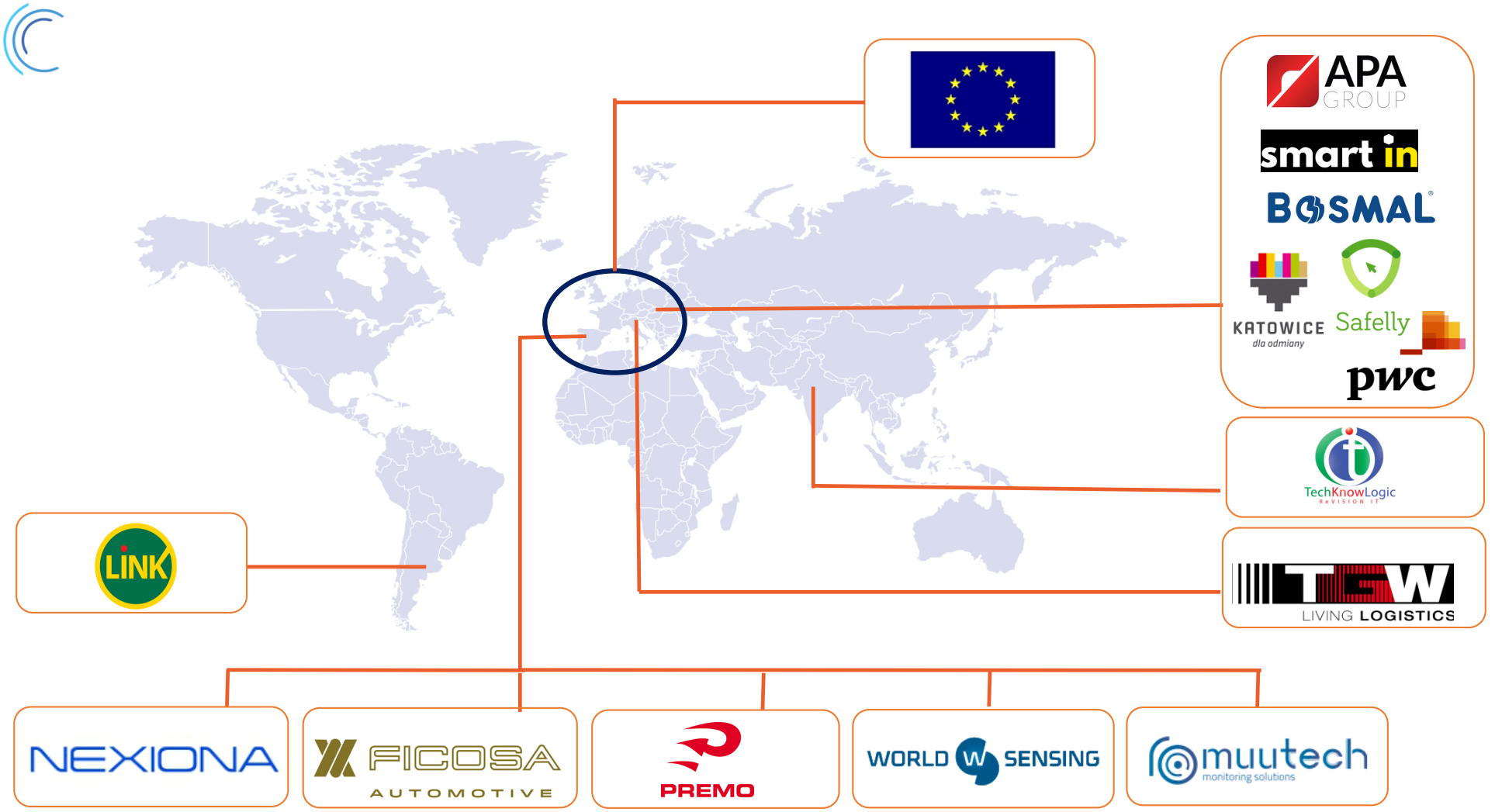
Advantages & Features

- ✓ Easy & Secure – great UX!
- ✓ One-click login & authentication
- ✓ Authentication of both sides
- ✓ Multi-factor authentication

- ✓ Strong encryption
- ✓ Eliminates passwords
- ✓ Eliminates 80% of breaches
- ✓ Eliminates „password sharing”

- ✓ Easy on-boarding
- ✓ + 60% cost effective vs competition
- ✓ Revenue enhancer
- ✓ Highly targeted loyalty link

- ✓ For Web & Mobile services
- ✓ Easy integration with API + SDK
- ✓ Perfect for SSO
- ✓ For employees and customers


APA GROUP
smart in
BOSMAL
KATOWICE dla odmiany
Safelly
pwc
TechKnowLogic
LINK
TGW LIVING LOGISTICS
NEXIONA
FICOSA AUTOMOTIVE
PREMO
WORLD SENSING
muutech monitoring solutions

The project ELIoT Pro has received EUR 1,9 M funding to finish development and enter the market from the European Union’s Horizon 2020 research and innovation program under grant agreement No 822641

Selected Use Cases

Smart Buildings

Together with our partner **APA GROUP** Cyberus Labs has integrated ELIoT Pro with their Building Management System “NAZCA” to provide secure user authentication to smart building system.

NAZCA is a management and optimization system for building automation processes, which allows business benefits to be maximized. This universal technology automates information flow processes, replacing: BMS (Building Management System), SMS (Security Management System) and EMS (Energy Management System) systems.

Advantages of the system include its clarity and convenient use, adaptation to any building and the ability to create a system distributed among many computers, making the system limitless in terms of size and effectiveness.

Smart Buildings

NAZCA efficiently combines all information into a single, cohesive picture, allowing convenient building management and full process control, and it may be operated from any mobile device with Internet access

ELIoT Pro user authentication component will be used also at the APA GROUP HQ at their fully automated smart office “BLACK HOUSE” in Gliwice, Poland.

ELIoT Pro will provide for NAZCA a secure user authentication which overcomes all the weaknesses of using static credentials such as passwords and biometrics. ELIoT Pro will provide also Machine to Machine authentication between components of the NAZCA system and data encryption with use of the Lightweight Encryption.

User authentication is integrated with NAZCA Operating System and uses ELIoT Pro mobile app technology.

https://apagroup.pl/industry/?lang=en

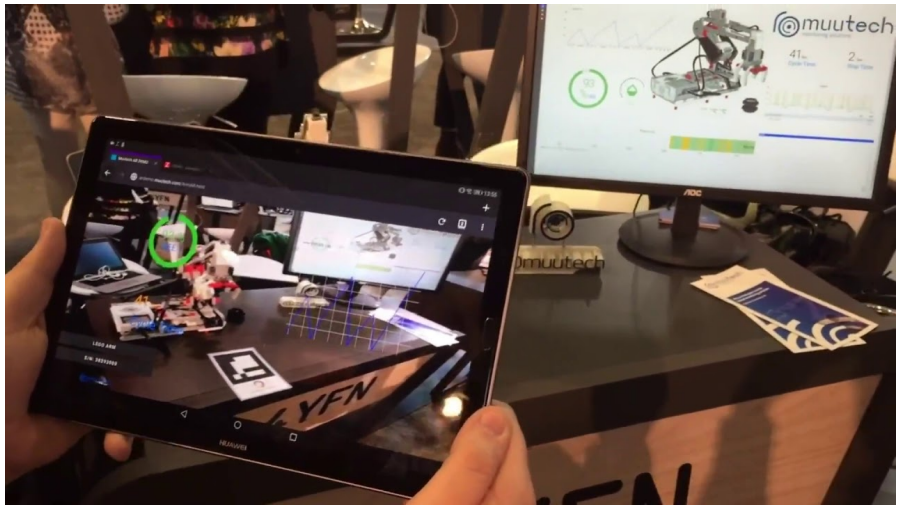
Industrial IoT

Muutech has integrated ELIoT Pro's Human to Machine user authentication component with their web-based assets monitoring platform. ELIoT Pro will provide Muutech's clients with a passwordless, multifactor, one-touch secure login with use of the ELIoT Pro's original mobile app.

Muutech Monitoring Solutions offers monitoring systems focused to IT, industrial and production environments. Muutech's platform is a tool which gathers and shows information originated from diverse sources.

Muutech's systems complement perfectly with countless sensors and actuators that offers us the possibility of positioning even in places of very difficult access.

Through dynamic customized dashboards they help to know at any time the status of the client's information systems.



https://www.muutech.com/en/

Industrial IoT

NEXIONA
CONNECTOCRATS

Barcelona based IIoT company **Nexiona** is a young but already established middleware provider. Cyberus Labs is working closely with Nexiona to integrate ELIoT Pro's Lightweight Encryption and Machine to Machine credentials free, secure authentication with Nexiona's MIMETIQ platform dedicated to a large Industrial IoT networks.

Next step in cooperation will be implementation also of ELIoT Pro's passwordless, multifactor, secure user's login.

Nexiona very quickly became a main Player in the Industrial IoT landscape thanks to the unique value proposal addressed to customers looking for Privacy and Ownership in IoT data. **MIIMETIQ® is a** can be installed in any infrastructure, can understand any data/system protocol, it's efficient from few devices and scalable to millions of devices, offering also a full flexibility in data modelling.

https://www.nexiona.com/

Industrial IoT & Automotive

Bosmal has integrated ELIoT Pro's Human to Machine user authentication component for its cutting-edge smart production plant system for automotive industry. ELIoT Pro will provide to Bosmal's system a passwordless, multifactor, one-touch secure login with use of the ELIoT Pro's original mobile app to enable authorized users to login, manage and control the production processes in the IoT environment.

Bosmal Automotive Research and Development Institute Ltd specializes in conducting research and development as well as manufacturing activities for domestic and foreign companies, mainly in the automotive sector.
The Institute has extensive experience in the field of cooperation with both final car manufacturers as well as with cooperating factories manufacturing parts and assemblies for the main assembly and for the aftermarket.

https://www.bosmal.eu/

Industrial IoT & Automotive

As a next step **Bosmal** and **Cyberus Labs** are working to integrate in Bosmal's smart production plant system also other ELIoT Pro's components.

The first will be the Lightweight Encryption to provide internal and external connection protection by Machine to Machine credentials-free authentication between components of the plant, as well as encryption of the traffic between plant's components and the external world.

Also ELIoT Pro's Flight Envelope and malfunction detection offered by ELIoT Pro's Rules Engine will provide additional security features Bosmal's system.

The first presentation of joint project is planned for the 4Q 2019. In 2020 companies will cooperate in another joint project dedicated to smart cars' access and user login system powered by ELIoT Pro.

https://www.bosmal.eu/

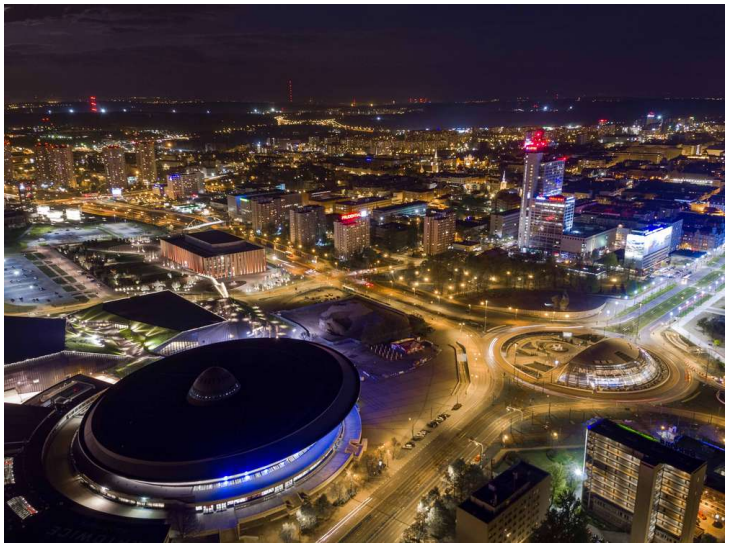
Smart City

ELIoT Pro's security features have been also appreciated by **City of Katowice**. This ex-heavy and coal mining industry city is turning at the moment into the most modern centres of the technology development in Poland. City of Katowice is also a pioneer in introducing Smart City components in Poland.

Cyberus Labs in the partnership with **Katowice City Office** is running the pilot implementation of ELIoT Pro's components: human user authentication, Lightweight Encryption's Machine to Machine authentication and data encryption as well as devices performance monitoring with the use of ELIoT Pro's Rules Engine on the different smart city systems that are already installed in Katowice.

The first public presentation of this pilot implementation is planned for the 4Q 2019.

KATOWICE
for a change



https://www.katowice.eu/

Industrial IoT & Smart Cities

Together with **Smartin**, Cyberus Labs is integrating Human to Machine user authentication component of ELIoT Pro with Smartin's smart assets management and monitoring systems. Cyberus Labs provides Smartin's clients with a passwordless, multifactor, one-touch secure login with an mobile app to smart environments' management systems – both web and OS-based ones.

Smartin is a provider of monitoring and management systems for a smart environments: monitoring and survelliance, property and asset management, data analytics including Industrial IoT, Smart Buildings and Smart Cities.

Smartin provides also cybersecurity services to their clients. Smartin's clients portfolio includes companies form the public sector in Poland – energy & utilities providers, public infrastructure operators.

"At Smartin, we believe that by implementing state-of-the-art, intelligent technologies, we can essentially help the effectiveness of industry, quality of life and security in our cities. We implement intelligent monitoring and analysis systems; especially in the field of comprehensive solutions for video monitoring and decision support for municipal and security services."

http://smart-in.eu

(Smart) Banking and Fintech

Argentina based **Red Link** has integrated Cyberus Labs' original, passwordless user authentication system Cyberus Key with its Innovation Lab program.

It was the pioneer integration of a multifactor, password free user login system in the banking industry. In Red Link's Innovation Labs corporate clients experience combination of the ease of use and security of Cyberus Key.

Recently Red Link and Cyberus Labs are exploring the possibility of expanding cooperation into the field of Smart Banking with use of ELIoT Pro.

Red Link caters for key financial entities, credit card companies and other customers providing ATM, home banking, corporate banking, mobile and safety solutions, information processing and tax and collection services.

https://www.redlink.com.ar/en/

CYBERUS LABS Sp. z o.o.
Address: ul. Warszawska 6/309, 40-006 Katowice, Poland
www.cyberuslabs.com, office@cyberuslabs.com, +48 692 437 857