achelos
the experts in eID

Security is the key element

Your Partner in End-To-End Security for M2M and IoT

M2M Trends

In the coming decade, market experts forecast exponential increase of M2M, IoT devices and applications.

Gartner, Inc. forecasts that 6.4 billion connected things will be in use worldwide in 2016, up 30 percent from 2015, and will reach 20.8 billion by 2020. In 2016, 5.5 million new things will get connected every day. Furthermore, Gartner estimates that the Internet of Things (IoT) will support total services spending of $235 billion in 2016, up 22 percent from 2015. (www.gartner.com)

The main threats to a successful M2M implementation are reliability, availability, and security. Security, in this case, is most critical, and mostly overlooked in the interest of reducing costs and decreasing of time to market.

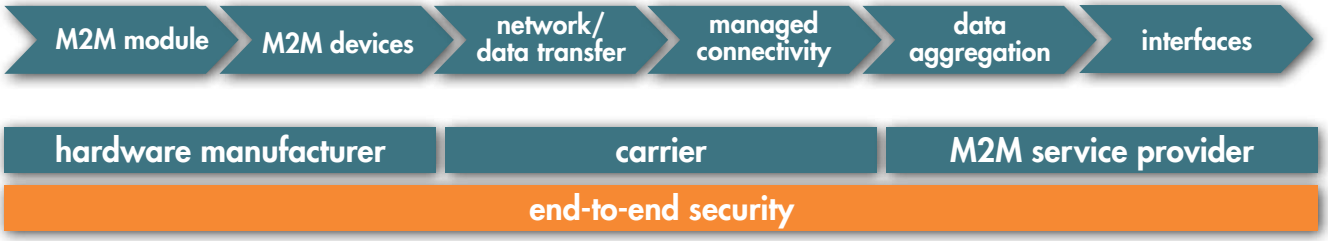
IoT provides a tremendous opportunity and is affecting most industries and markets. This technology trend requires standards and services with an end-to-end approach focused on security.

Main Fields of Application

Main fields of application for M2M markets in the near future:

- mechanical engineering
- production
- automotive
- healthcare
- building services engineering
- security, remote maintenance & remote control
- POS/payment
- logistics, tracking and tracing
- vending machines
- traffic management, public transport
- agricultural engines
- consumer devices
- metering

M2M value chain



Security is a key element of the value chain and is, in the same time, the mostly unnoticed. Application and service developers focus on features, forgetting the importance of the safety of service usage. Every link of the value chain is a key element in the assurance of data security and privacy. Only if all links and the complete value chain are secured on commonly accepted standards the security of the service can be guaranteed.

achelos
the experts in eID

The overall goal is Security

Connectivity is one of the weaknesses of a connected device by nature: when disconnected from the infra-structure, a device stops to deliver the service or, in the worst case, provides an incorrect service. Hence one of the key objectives of M2M and IoT service providers is to ensure stable and reliable connectivity of the devices. M2M and IoT services are not only limited to secure connectivity, they are in addition an attractive target for security attacks for various reasons:

- The majority of devices will be unattended during most of their operational lifetime, making M2M applications attractive to hackers, and a relatively easy target.
- The devices will be used in vital and critical business processes, requiring ultimate accuracy and reliability, especially in health and automotive applications.
- The number of connected M2M and IoT devices will grow at a much faster rate, compared to consumer devices, and will rapidly outgrow their number. That opens new possibilities for fraudulent activities, for example using the hacked devices for Denial of Service (DoS) attacks.
- The life time of connected devices will be longer in comparison to consumer devices. Security measures have a limited lifespan and (remote) regular security maintenance (e.g., in form of software or credential updates) will thus be vital.
- A small, hacked M2M or IoT device may open a door for attack on a major critical service, like power supply or traffic management. Therefore, security of the devices is a crucial factor for seamless M2M service operation.
- Device security is also a key factor for guaranteeing privacy of human users. A human user may not consider autonomously operating devices in his proximity (e.g., car or home appliances) as a potential source of danger for his privacy. And this fact makes these devices an ideal target for malicious actions.

achelos
the experts in eID

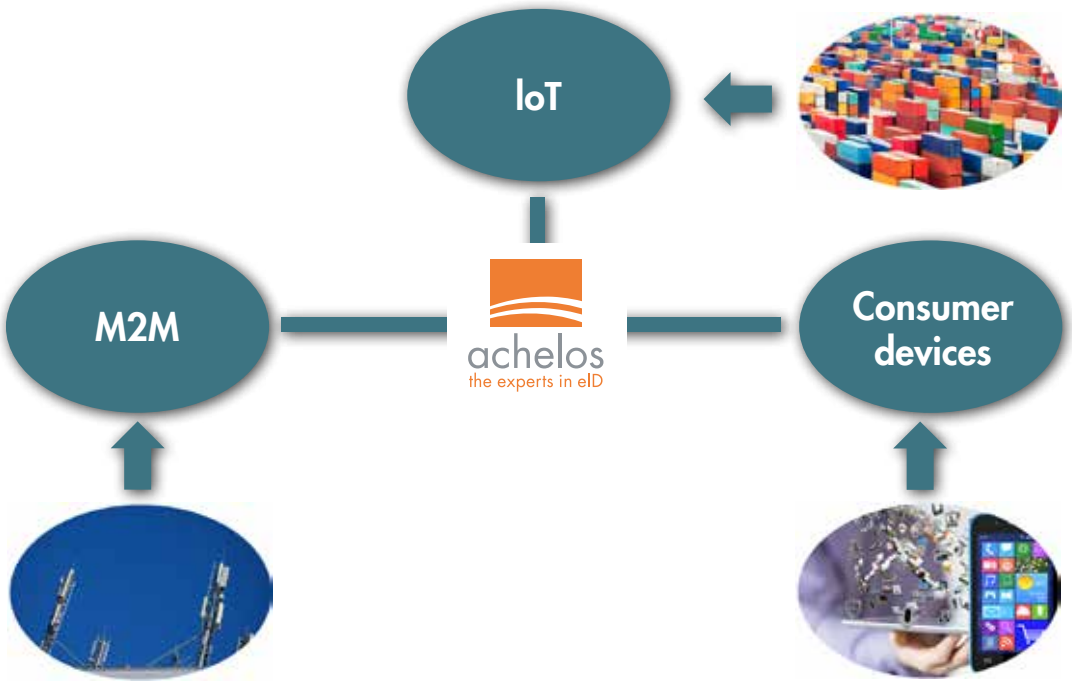
Making M2M solutions more secure

As an independent software development company, achelos focuses on end-to-end security products and services for your business. Our service offering in M2M is tailored to the customer's needs and compliant with the highest security standard defined for the M2M and IoT industry.

The elements of M2M services have to seamlessly interact with each other. Security is a key element in this complex value chain. It must be at the heart of the design and implementation of both individual component and the entire solution. The right choice of underlying technologies and components as well as the test strategy and supporting tools are the key factors for a successful service deployment.

Machine-to-machine (M2M) communication is used for automated data transmission and measurement between mechanical or electronic devices. The key components of an M2M system are: Field-deployed wireless devices with embedded sensors or RFID wireless communication networks with complementary wireless access including, but not limited to cellular communication, Wi-Fi, ZigBee, WiMAX, wireless LAN (WLAN), generic DSL (xDSL), and fiber to the x (FTTx). (www.gartner.com)

... for various market segments



achelos
the experts in eID

achelos' M2M offer consists of:

- **Security analysis**
  Our experts perform software security scans, monitor the whole M2M service value chain, detect the weak spots in security coming from (virtual) machines, sensors, terminals, service platforms and applications as well as services and processes.

  Analysing the outcome of the scan, achelos can provide tailored security solutions with a focus on connectivity, system integration, and life cycle management. The high performance Qumate Test Center, developed by achelos, is the main tool supporting the security analysis.

Qumate.World

www.qumate-world.com

- **Test concept**
  Taking security evaluation as an input, our experts can develop a security test concept tailored to the customer's use case. Our Qumate Test Center product is the core of the tailored testing environment achelos is supplying. Customers can either use Qumate and the respective test software, or receive complete test services from achelos. Upon successful conclusion of the tests, customer's service or it's components will be ready to withstand the security threats.

- **Solution for remote provisioning of secure credentials stored in a secure environment**
  The solution is aimed to manage keys, configuration data, or certificates stored in a secure area of a M2M or IoT device using the standard mechanisms defined for a given secure element type (for example, mechanisms defined by ETSI or oneM2M).

  The secure element may be represented by a SIM card (removable or embedded) or an embedded secure element (eSE). It is also possible to manage the content of a Trusted Execution Environment (TEE), but the management mechanisms are very dependent on the TEE implementation and therefore the support of a dedicated TEE requires additional study.

  Subscription Management solution for remote management of mobile network subscriptions.

  Our implementation follows the specification created by the GSM Association (GSMA, specification version 3.0) and is enriched with proprietary extensions allowing addressing of use cases not covered by GSMA.

Our solution is independent of any SIM supplier, is flexible to meet your specific business needs, and is scalable to address any deployment scenario. This includes services for integration and customization of our software components into your infrastructure as well as end-to-end testing, including security evaluation.

Benefit from our expert knowledge:
achelos is your partner in M2M security!

achelos is a member of major organizations in the IT security sector. Our experts are involved in various working groups to create, develop, and implement security standards for different segments, use cases and technical solutions:

member of bitkom · KONTIKI · IT in Germany · green IT · WIR SIND FÖRDERMITGLIED IM FNN FORUM NETZTECHNIK/NETZBETRIEB IM VDE · MITGLIED IM DIN · KogniHome · BlackBerry Associate Alliance Member