

Secure IoT and M2M with the iBadge Device Identity Management

Cloud technology and mobile devices are sounding the bell for the new IoT and M2M (machine to machine) era. But with it come the omnipresent security threats to your devices and to your data, and thus to the well-being of your business. IKV's **iBadge Device Identity Management** is the best defense against counterfeit devices.

IoT devices possess the following characteristics:

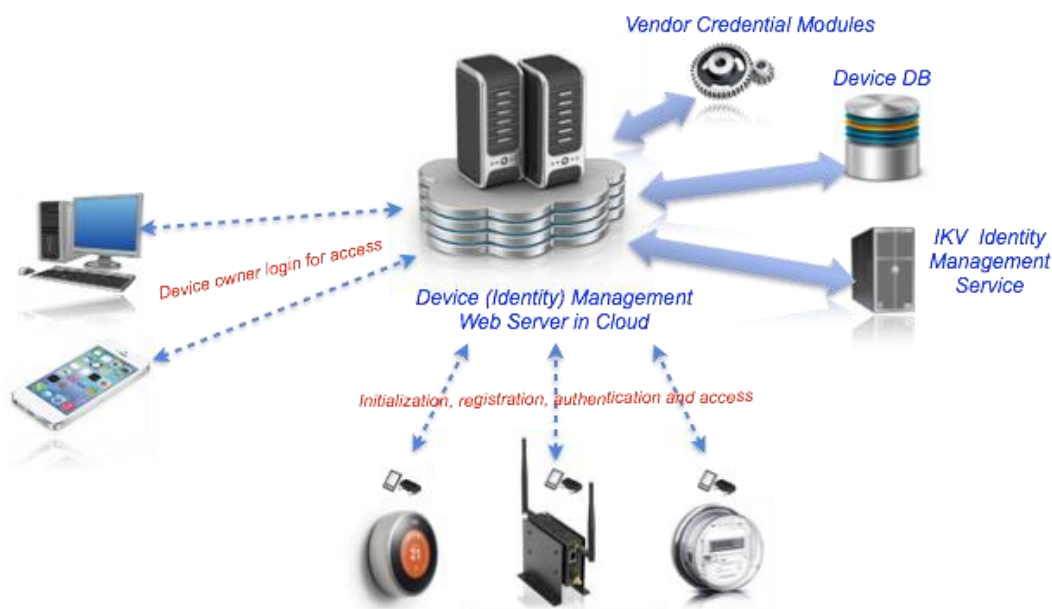
- Limited calculation capabilities
- Limited power supply
- Low production cost
- Can automatically connect to a network, and process data (device intelligence)
- Possesses a pre-installed control agent

These characteristics have the following implications:

1. High costs for burning and maintaining device specific information (like MAC address and device ID)
2. Difficult management of large production volumes
3. Simple software and hardware architecture, without differentiation
4. No sophisticated protection mechanism possible on a firmware level

This causes problems for vendors with high production volumes, as it often obstructs investors, and makes it difficult to make profit. This often means that devices lack efficient identity management mechanisms.

Our **iBadge Device Identity Management** uses a strong cryptographic authentication chip of low unit cost, and offers a cloud-based platform for authentication and management. Based on this solid foundation, vendors and service providers can thus provide device security that is second to none.

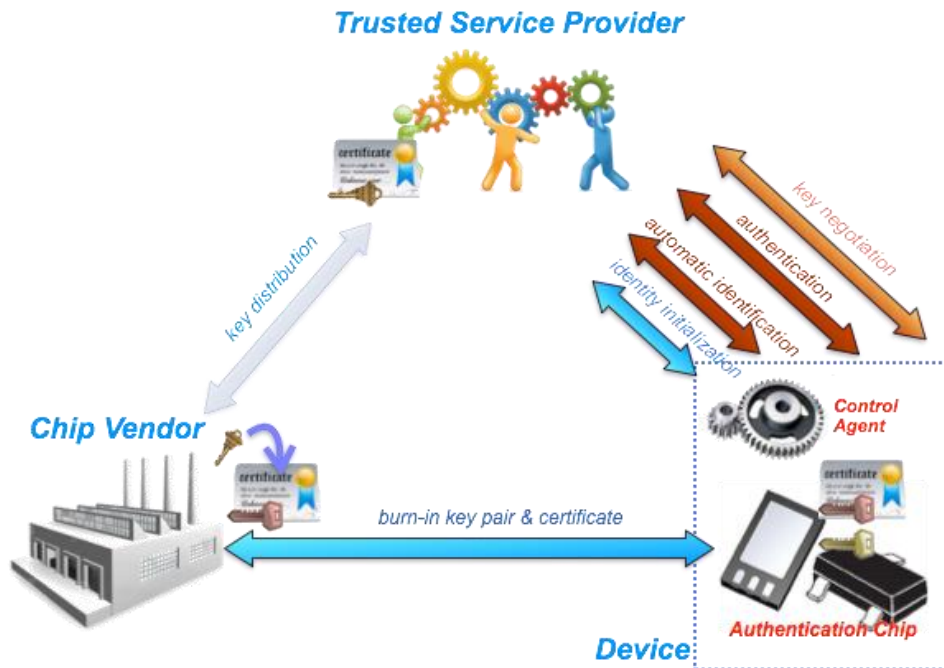


Devices equipped with the **iBadge Device Identity Management** system possess the following capabilities:

- No manual work is required during the production process
- A unique chip identifier and authentication key
- No need for complicated cryptographic algorithms in the firmware
- Device management via web-browser or smart-phone app
- Easy management of device ID and other data, through our back-end module

The **iBadge Device Identity Management** system facilitates:

- Device authentication
- Controlled device updates
- Inter-device communications
- Counterfeit protection



Special features of the **iBadge Device Identity Management** system:

- The unique identifier and cryptographic key are burned into the device during packaging and testing
- Strong authentication using Elliptic Curve Cryptography
- Flexible control agent, fit for all kinds of devices
- After each successful authentication, a unique session key is generated
- We offer support for the server side, including authentication libraries and a ready-to-use cloud-based web-service, device ID databases, device and server HTTP interfaces and an API for device management.

We also offer a complete **iBadge** system with integrated Wi-Fi, to further reduce the integration effort necessary for our customers. Currently we are working on integrating our products with manufacturers of other 2.4G/PAN (BLE, ZigBee...) communication modules.



IKV-Tech (InfoKeyVault Technology) is the currently only company in Taiwan specializing in hardware-based IT security services. Our vision is to protect global customers' digital assets with professionalism and creativity.

iBadge Device Identity Management is a hardware identification solution designed for IoT applications, Please contact us for further information.

Email: ikvinfo@email.ikv-tech.com

Website: <http://www.ikv-tech.com/en>

Contact Us: <http://www.ikv-tech.com/en/contact-us>