IoT Security solutions & services

Smart Security for Smart Objects

www.trusted-objects.com
Trusted Objects

- Founded by digital security experts (smart card)
- Development of cyber security solutions for the IoT market
- Critical expertise on digital security for connected devices

Hardware-based security solutions and security services have a track record of successes since more than 30 years; they offer security, privacy and convenience to consumers and industries.

Trusted Objects and its key partners are deploying digital security in IoT ecosystem and enabling end-to-end security from the device to the cloud.

Our solutions are embedded into many IoT applications, including asset tracking, utilities, e-health and smart cities.
It is all about trust!

Security and privacy are critical challenges ahead as IoT deployment is happening now.

We must ensure that businesses and consumers trust the IoT ecosystem: trust the connected devices, trust the communication, trust the cloud services.

Selecting a security solution is a trade-off between risks, costs, technical performances and efforts required.

<table>
<thead>
<tr>
<th>Security Solutions</th>
<th>Key applications</th>
<th>Security functions</th>
<th>Certified products</th>
<th>Power consumption</th>
<th>Average cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Memory</td>
<td>Counterfeiting Brand protection</td>
<td>Identification</td>
<td>No</td>
<td>⚪️</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td>Connected devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication IC</td>
<td>Entry level SIM Counterfeiting</td>
<td>Identification</td>
<td>Yes</td>
<td>⚪️</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td>Wearables/BLE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Execution</td>
<td>Mobile Phones Connected devices</td>
<td>Safe boot Authentication Encryption</td>
<td>No</td>
<td>⚪️</td>
<td>$$$</td>
</tr>
<tr>
<td>Environment</td>
<td></td>
<td>Secure storage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure Element</td>
<td>SIM Banking &amp; ID Connected devices</td>
<td>Safe boot Authentication Encryption</td>
<td>Yes</td>
<td>⚪️</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secure storage</td>
<td>EMVCo CC EAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Platform</td>
<td>PC Mobile Automotive</td>
<td>Safe boot Authentication Encryption</td>
<td>Yes</td>
<td>⚪️</td>
<td>$$$</td>
</tr>
<tr>
<td>Module</td>
<td></td>
<td>Secure storage</td>
<td>CC EAL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Trusted Objects is making your decision easy with highly secure solutions, well adapted to your requirements, easy to integrate and cost effective.
Why choosing Trusted Objects?

- Offering the best protection against logical and physical attacks
- Cost-effectiveness: affordable price adder to get the highest level of security
- Best in class technical performances: reduced footprint, low power consumption, 32 bit computing performances
- Set of tools to reduce the efforts needed to design and integrate our solution into your system
- Reactivity and flexibility, because your IoT project is unique

Minimized costs
Optimized performances
Simplified integration
The solutions developed by Trusted Objects consist in dedicated Secure Elements (SE), the TO136 family, enabling a set of security features to protect IoT connected devices against physical and logical attacks.

**Secure element hardware: 32-bit CPU with 136K Bytes Flash**
- Optimized package with small footprint (DFN6 in 3x3 mm)
- Ultra-low power (2.4 mA in active mode, 0mA in sleep mode)
- EMVCo certification, compliance with CC EAL 5+

**Secure firmware: optimized native code with state of the art cryptography algorithms**
- AES-128, ECC 256-bit (Elliptic Curve Cryptography)
- Customized firmware to meet specific security requirements
- Free user memory for secure storage: from 17 KB up to 40 KB

**Specific applets for IoT applications**
- Qualified connectivity stacks: Sigfox, LoRaWAN (specification V1.1)
- TLS-based SE solution with MCU stack for https connectivity
- Power interrupt mechanism, I2C secure link
Security of standard LPWAN devices is based on software libraries implementation inside the main MCU. Trusted Objects security solutions offer an extra layer of security that enables additional security features including strong authentication, payload encryption & decryption, secure storage and more.
 Demand, especially for smart home and wearable applications, is growing for end-to-end security between IP or non-IP IoT devices and servers. Trusted Objects’ effective response is to implement a security scheme based on the proven TLS standard (Transport Layer Security).

**TLS for IP or non-IP IoT devices**
- TLS standard for IP IoT devices
- TLS lite for non-IP IoT devices (BLE, WM-Bus, proprietary local protocol, ...)

**TO136 benefits**
- Root of trust for TLS
- Secure certificate storage
- Securing keys generation
- Secure encrypt/decrypt algorithm implementation
Trusted Objects expertise on digital security helps customers accelerating the development, implementation and management of security in their IoT project.
**Fast sampling**
*Trusted Objects delivers Secure Element samples within days for your Proof of Concept.*

- Secret keys generation in secure environment
- Sample generation based on your specification
- Samples personalized with your app and standardized keys

**Benefits**
- Eases Proof of Concept
- Simplifies application developers job
- Fast delivery

**Customer provisioning**
*Trusted Objects provides customers with specific solutions for keys provisioning at their own premises.*

- Secret keys generation in secure environment
- Secret keys provisioning:
  - By programming
  - Over the air
- Secure element personalization
- Secure element personalized according to your specification

**Benefits**
- Secure key loading on IoT device at customer premises
- Specific solution interfacing with customer programming tools
- Flexibility and simple inventory management
TO136 Secure Elements family

Full range of TO136 Secure Elements to support all LPWAN choices, TLS needs and specific requirements.

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TO136-LoRaWAN-ABP</td>
<td>TO136 for securing LoRaWAN-based products and personnalized for a specific application server and a specific network operator</td>
</tr>
<tr>
<td>TO136-LoRaWAN-OTAA</td>
<td>TO136 for securing LoRaWAN-based products and personnalized for a specific application server and activable with any operator over the air</td>
</tr>
<tr>
<td>TO136-SIGFOX</td>
<td>TO136 for securing Sigfox-based products and personalized for your Sigfox device</td>
</tr>
<tr>
<td>TO136-TLS</td>
<td>TLS based TO136 solution within full TLS-stack</td>
</tr>
<tr>
<td>TO136-TLS-UBIQUIOS</td>
<td>TLS based TO136 solution with UbiquiOS TLS stack in the IoT device MCU</td>
</tr>
<tr>
<td>TO136 GENERIC</td>
<td>TO136 for strong authentication, encryption/decryption, secure storage, ECIES (Elliptic Curve Integrated Encryption Scheme)</td>
</tr>
<tr>
<td>TO136-SPECIFIC</td>
<td>TO136 secure firmware customized for your own application</td>
</tr>
</tbody>
</table>
Get in touch!

- TO136 datasheet
- Application notes
- Integration manuals
- Generic samples box

Evaluation boards:
- LoRaWan evaluation board
- Sigfox evaluation board
- TLS evaluation board
- TO136 starter kit

Documentation and samples:

Development platform, POC:
- LoRaWAN POC platform
- Sigfox POC platform
- TLS POC platform
Contacts

**Trusted Objects France**
Europarc de Pichaury, Bât. B8
1330 rue Guillibert de la Lauzière
13290 Aix en Provence - France
Phone: +33 4 42 39 86 30 - contact@trusted-object.com

**Trusted Objects PTE LTD**
51 Goldhill Plaza, 308900 Singapore

**Trusted Objects USA**
2018

Trusted Objects solutions are deployed by Avnet

![Avnet Logo](image)