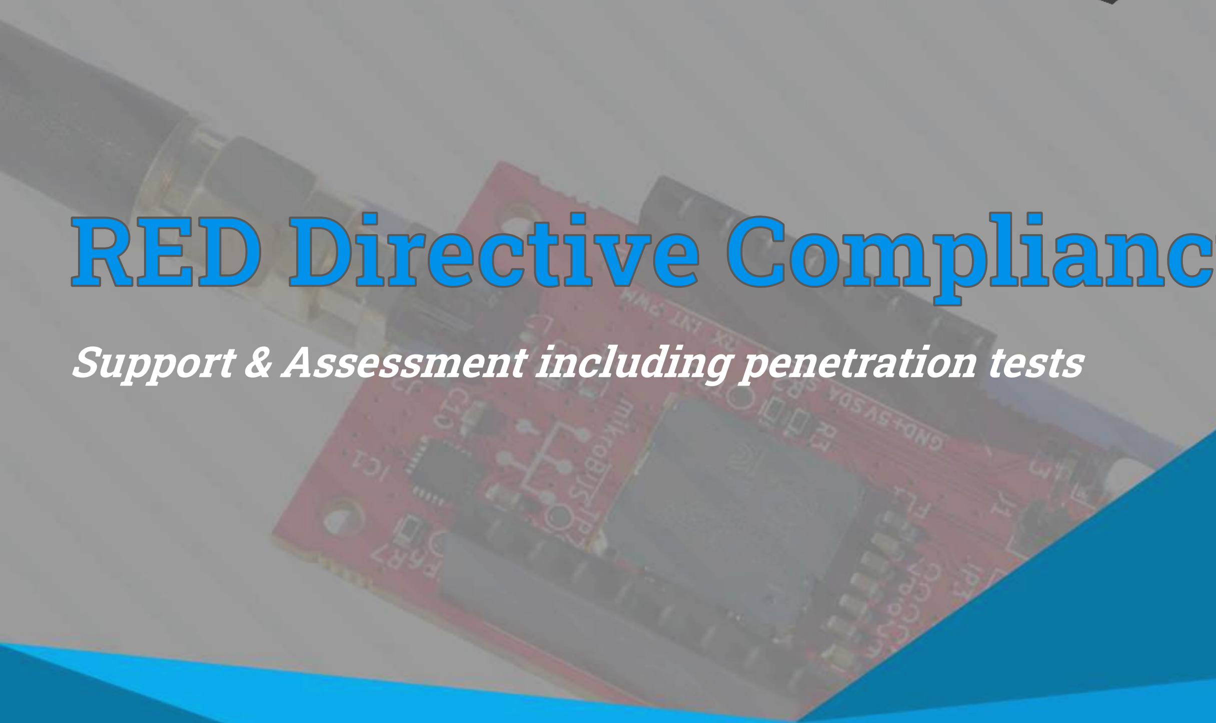
TrustnGo
Plug & Play Security



RED Directive Compliancy

Support & Assessment including penetration tests

In Brief

Securing an embedded device can be a challenge and demonstrating this security is another one.

During the past years, the EU has severely tightened cybersecurity requirements for IoT & embedded devices. In August 2025, the cybersecurity part of the 2014/53/UE RED directive will enter into force and vendors of wireless digital products will have to fulfill the requirements of the related EN 18031 standard.

TrustnGo provides consulting, assessment & testing services to tackle these challenges and allow you to meet the requirements of the EN 18031 standard the D-day.

Addressed Markets

- **Wireless devices connected to the internet**
  - ✓ Network devices
  - ✓ Gateway
  - ✓ Industrial IoT
  - ✓ Sensors, etc.
- **Wireless devices processing personal data**
  - ✓ Toys
  - ✓ Wearables
  - ✓ Smart Home
  - ✓ GPS, etc.

The EN 18031 standard

The RED directive introduces three essential requirements about device resilience as well as network, personal data or payment method protection. Each essential requirement is covered by one of the parts of the EN18031standard.

Being an harmonized standard, a conform product is presumed fulfilling the essential requirements of the directive. In most cases, there is **no need to involve a *notified body*** to demonstrate the conformity of your product against the standard.

How TrustnGo can help with the RED directive ?

TrustnGo offers its customers a streamlined, yet flexible, turn-key assessment process that should meet most of the customer's use cases. Three different pre-packaged offers are available.

Quick diagnostic

- Two-day workshop
- Preliminary risk & gap analysis
- Prioritized roadmap to handle deviations

For vendors that are still actively working on their product.

Pre-assessment

- Two-day workshop
- Full risk & gap analysis
- Writing of the technical documentation required by the standard

For vendors willing to derisk a certification done by a notified body.

Compliancy assessment

- Optionnal pre-assessment
- Assessment of the technical documentation
- Penetration tests required by the standard
- Writing of a complete report demonstrating the compliance with the standard

For vendors willing to do a self-assessment or fully derisk a certification done by a notified body.

What happen when deviations are found ?

When a deviation is found the customer can either fix it alone or **ask for some support** from TrustnGo. We provides consulting & development services to help customers to reach the requirements of the standard.

Why choose TrustnGo ?

✓ **Ten-year experience** in cybersecurity

✓ **Reduced costs & delay** compared to notified bodies

✓ **Technical support** to meet the requirements

Additional services

- **Integration of security features**
  - Secure bootloader
  - TrustZone & Secure Enclaves
  - Secure coms & Crypto. libraries
- **Secure Development Life-Cycle**
  - Code review & hardening
  - Review of the development process
  - Supply chain security
  - Monitoring of vulnerabilities
- **Cryptography & provisioning of secrets**
  - PKI management
  - Crypto. protocols analysis
  - Secure provisioning

Version 1.0

Ready-to-use security software stack

TrustnGo also offers **TrustnSafe SDK** a complete, portable & easy to use software stack designed to protect your microcontroller based products.

TrustnGo
Plug & Play Security

https://trustngo.tech
+33 781 765 448
sales@trustngo.tech

TrustnGo S.A.S
20 rue Paule Marrot
33300 Bordeaux