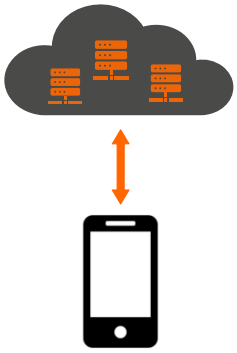
DESCRIPTION R0 TEST PROGRAM

	R0* *Security Quick Scan*	R1 *Security Quick Check*	R2 *Security Best Practices*
ETSI EN 303645 & NISTIR 8259A Coverage	**Questionnaire & Document Review**	**Selective Testing**	**Selective Testing**
Testing Focus	Evidence Review	Frequent Attacks	Security Best Practices
Testing Type	No testing on this level	Black-Box	Black-Box
Example Use Case	Part of procurement process	Batch sample test / quick filter	Dedicated test
Cycle Time	1 week	1 week	2 weeks
Man. Support	Full support	None	None

Full coverage
Partial coverage

*) R0 provides a complete conformity assessment including conformity verdict

App & Cloud included



R0 is a test program tailored towards retailers. Retailers usually neither have access to implementation/design details nor to test environments.

R0 is a review-based conformity assessment where no independent 3rd party tests are performed. This allows a cost-effective approach whenever independent testing is not required or for products with low risk exposure. The outcome of this activity is a conformity assessment report.

R0 is conducted in three steps:

1. Customer, in this case a retailer, is sent a basic questionnaire to determine the functionality and capabilities of the device, the related mobile application and cloud services and how the cybersecurity case has been considered. Within the R0 program, the retailer forwards the questionnaire to the manufacturer requesting all relevant data, documents and evidence from the manufacturer, which is then forwarded by the retailer to SGS.
2. Security experts from SGS review the provided information evaluating whether all applicable requirements of the security standard(s) in scope are covered. During this process, the provided information and evidence needs to be complete and consistent demonstrating
    a. how the requirements are functionally fulfilled and
    b. how the requirements have been tested on manufacturer side.
3. Based on the review process, presented evidence and an analysis of any further provided documents, SGS is preparing a conformity report.

The process in step 2 contains one feedback round, allowing the retailer to provide missing or updated documents and evidence, in case documents and evidence provided originally were not enough.

BASELINE REQUIREMENTS FOR DEVICES

The baseline requirements we review and test against for IoT devices are based on public international standards, recommendations, and expertise. For example. the security standard EN 303 645 "*Cyber Security for Consumer Internet of Things: Baseline Requirements*"[1]

[1] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

published by ETSI or the recommendations NISTIR 8259A "*IoT Device Cybersecurity Capability Core Baseline*"[2] published by NIST.

Those standards and recommendations specify high-level security and data protection requirements for consumer IoT devices and their interactions with associated cloud services.

BASELINE REQUIREMENTS FOR MOBILE APPLICATIONS

The baseline requirements we review or test against for mobile applications used to interact with an IoT device are based on public international standards, recommendations, and expertise. For example, the security standard Mobile Application Security Verification Standard (MASVS)[3] published by OWASP provides specific requirements for mobile applications in general. They adhere to mobile application security best practices and cover requirements in terms of code quality, handling of sensitive data, and interaction with the mobile environment.

BASELINE REQUIREMENTS FOR CLOUD SERVICES

The baseline requirements we review or test against for cloud services used to interact with an IoT device are based on public international standards, recommendations, and expertise. For example, security guidelines like OWASP's Top 10 for Web Applications[4] and similar provide requirements around relevant cloud services. Note that the scope is limited to the device's context, i.e., only functionality which is relevant to and/or used by the device is within scope of the interview.

HISTORY

Version	Date	Author	Changes
1.1	Jun 11, 2021	SGS Cybersecurity Services, Graz	Update illustration
1.0	Mar 2, 2021	SGS Cybersecurity Services, Graz	Release

[2] https://csrc.nist.gov/publications/detail/nistir/8259a/final
[3] https://mobile-security.gitbook.io/masvs/
[4] https://owasp.org/www-project-top-ten/