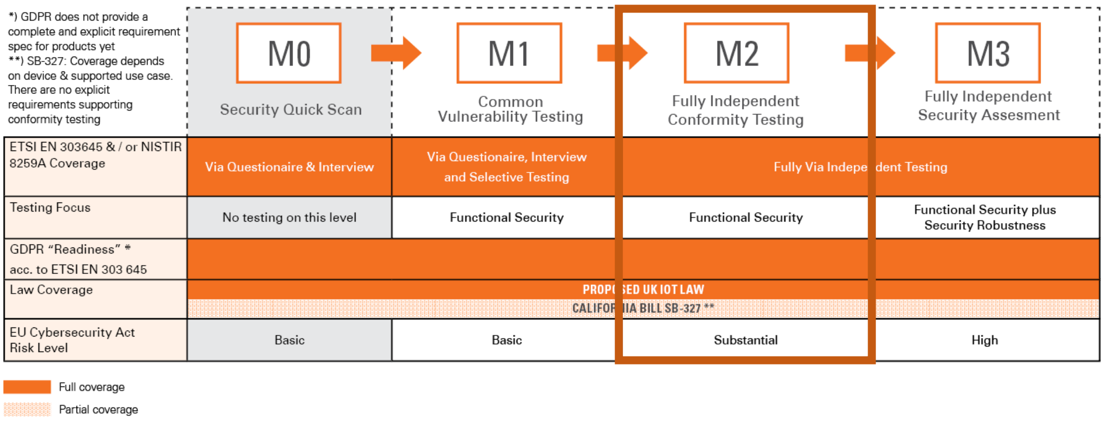
DESCRIPTION M2 TEST PROGRAM



	M0 Security Quick Scan	M1 Common Vulnerability Testing	M2 Fully Independent Conformity Testing	M3 Fully Independent Security Assesment
ETSI EN 303645 & / or NISTIR 8259A Coverage	Via Questionaire & Interview	Via Questionaire, Interview and Selective Testing	Fully Via Independent Testing	
Testing Focus	No testing on this level	Functional Security	Functional Security	Functional Security plus Security Robustness
GDPR “Readiness” * acc. to ETSI EN 303 645	■	■	■	■
Law Coverage	PROPOSED UK IOT LAW CALIFORNIA BILL SB-327 **			
EU Cybersecurity Act Risk Level	Basic	Basic	Substantial	High

*) GDPR does not provide a complete and explicit requirement spec for products yet
**) SB-327: Coverage depends on device & supported use case. There are no explicit requirements supporting conformity testing

■ Full coverage
░ Partial coverage

M2 is a fully independent conformity testing campaign for products with medium risk exposure.

The purpose of this test program is to independently test all applicable security requirements for a device. The security requirements are usually provided by a security standard, like EN 303 645. If all tests are passed successfully, the test program confirms the conformity to the standard in scope.

M2 is conducted in 3 steps:

1. Customer is sent a basic questionnaire to determine the functionality and capabilities of the device and the related mobile application and cloud services.
2. Customer provides appropriate test samples and all necessary information. Security experts from SGS independently test each security requirement in scope.
3. Based on the test results SGS is preparing a conformity report.

M2 is conducted in a grey-box test setting. Grey-box testers have some knowledge of the product which is not publicly available. A typical example is when vendors provide a firmware in binary format when it is otherwise not available in an unprotected format. Another example is when debug interfaces are provided to the evaluator to examine some internal functionality. The purpose of grey-box testing is to provide a more focused and efficient assessment of a product’s security. Furthermore, certain security requirements can only be tested with additional information and/or special interfaces.

In order to conduct the tests in a time efficient manner, the customer shall provide 5 samples and a testing environment for the mobile application and cloud backend.

BASELINE REQUIREMENTS FOR DEVICES

The baseline requirements we 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] 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 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 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.

DISCLAIMER

SGS does not warrant that, even in the case there have been no findings during SGS's security assessments and security tests, the test object as described above has no security flaws.

The test results were found at the time of initial testing and or market surveillance and are indicative to products with the listed Version Number and model identifier. The test results are subject to change should there be any change in the manufacturing processes and bill of material used (Hardware and Software).

SGS is not a manufacturer, supplier or distributor of products and makes no warranty, representation, or guarantee regarding the suitability of the products for any particular purpose, nor does SGS assume any liability whatsoever arising out of the use of the product. Buyers shall not rely solely on any data and performance specifications or parameters provided by SGS. Information provided in this document is proprietary to SGS, and SGS reserves the right to make any changes to the information in this document at any time without notice.

HISTORY

Version	Date	Author	Changes
1.0	Nov 10, 2020	SGS Cybersecurity Services, Graz	Release

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