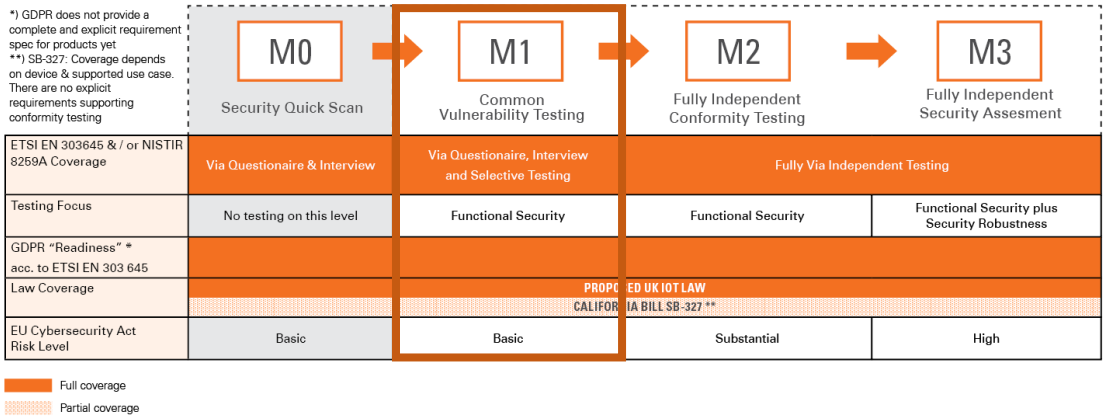
# DESCRIPTION M1 TEST PROGRAM




M1 is an interview and review-based assessment approach supported by a partial vulnerability scanning and testing campaign for products with low risk exposure.

The purpose of this test program is to provide an efficient way to provide an independent test of the most common vulnerabilities for the type of device which even an adversary with only proficient expertise could exploit and hence results in a comparable lower effort of testing. These common vulnerabilities usually include password security, secure updates, or authentication mechanisms. The type of vulnerabilities depends on the type of device. An IoT device running a web application with a configuration interface is subject to different attacks compared to a smart light switch communicating over Zigbee and Wi-Fi. The requirements in scope are manually tested and combined with automated vulnerability scanning tools. The remaining security requirements of the standards in scope are assessed via an interview process.

M1 is conducted in four steps:

1. The customer is sent a basic questionnaire to determine the functionality and capabilities of the device and the related mobile application and cloud services.
2. Security experts from SGS and the customer go through a detailed interview process where every applicable requirement of security standards in scope are covered. During this process, the customer needs to present evidence which demonstrates
    a. how the requirements are functionally fulfilled and
    b. how the requirements are tested internally.
3. A selected number of requirements is independently tested by security experts from SGS in one of the cyber security labs.
4. Based on the interview process, presented evidence and independent tests, SGS is preparing a conformity report.

The independent tests in M1 are conducted in a black-box test setting. In black-box testing, the evaluator is placed in the role of an external adversary with no internal knowledge of the target system. Testers are only provided with information that is publicly available.

To conduct the tests in a time efficient manner, the customer shall provide 3 samples and a testing environment for the mobile application and cloud backend.


© SGS Société Générale de Surveillance SA – 2020

## 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/