

DESCRIPTION R2 TEST PROGRAM

**1) SB-327: Coverage depends on device & supported use case. There are no explicit requirements supporting conformity testing

	R1 Security Quick Scan	R2 Common Vulnerability Testing
ETSI EN 303645 & / or NISTIR 8259A Coverage	VIA SELECTIVE TESTING	VIA SELECTIVE TESTING (HIGHER COVERAGE THAN IN R1)
Testing Focus	Functional Security	Functional Security
GDPR "Readiness" * acc. to ETSI EN 303 645	not possible	not possible
Law Coverage	PROPOSAL CALIFORNIA	UK IOT LAW BILL SB-327 **
EU Cybersecurity Act Risk Level	Basic	Basic

Full coverage
 Partial coverage

Only black-box access to the product!

Therefore no higher levels defined.

In case retailer has according access to manufacturer information the packages M2 and M3 can be used.

R2 is a test program tailored towards retailers. Retailers usually neither have access to implementation/design details nor to test environments. Typically, they also require quick results of any form of testing done.

The R2 test program provides cyber security testing for batch samples in a black-box 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 public information. R2 provides a quick assessment of common vulnerabilities which are typical for the type of product. These common vulnerabilities usually include password security, secure updates, or authentication mechanisms. The tests are utilizing test automation and vulnerability scanning combined with manual testing. The results are analysed by SGS security experts and a technical report is provided.

R2 is conducted in 3 steps:

1. Retailer is providing SGS a spec sheet, user manual and the product.
2. Security experts from SGS conduct security tests.
3. The results are analysed and summarized in a technical report.

The device-relation to the mobile application and cloud services are also considered during testing.

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