



Mission Critical Testing as a Service Webinar 10 June 2020 Q&A

View the webinar recording [here](#)

This document sets out the questions and answers given after the webinar.

Q. Which LTE RF test platforms are compatible with the MCS-TaaSting solution?

A. Enensys, a partner in the project is providing the LTE capable platform that will be integrated in the solution although the TaaS paradigm allows incorporating other testing options. As mentioned, this is part of the IPCAN model, not a TTCN3 based RF tester (that would cover the whole UU model).

Q. Will this test or certify how an MCS Client interacts with other apps on a UE?

A. No, this is currently not in scope of the project. From our involvement in the MCOP initiative (www.mcopenplatform.org), we are fully aware that open APIs and clear interfaces in the UE are of outermost importance. However, in MCS TaaSting we focus on the official certification workflow (like GCF or PTCRB) explained in the talk, following 3GPP RAN5 test cases and resulting TTCN3 code. Since 3GPP focuses on UE to Server interface this will be the area covered at least on the short term. Later MCS-TaaSting products may incorporate new features. Any further feedback on tester requirements are welcome (contact info@mcstaasting.com).

Q. What specific certification you look from User Interface/User Experience on MCS Client and its test requirement/standards if any?

A. In the talk and slides we explained different kind of possible certifications being conformance and performance testing two of the most relevant for the questions. Since MCPTT is still the key feature demanded by the mission critical community, in terms of QoE, 3GPP has already identified the relevant KPIs (KPI1-4, including call setups and mouth-to-ear delay) and the target values. NIST PSCR has proposed some testing procedures but performance evaluation is not yet part of the 3GPP defined test cases. Therefore it will not be part of the initial deployment but will more than likely be considered for evolution of the MCS-TaaSting products.

Q. What security conformance certification is recommended on MCX client such as (OpenID auth), Key Management across cross security domain?

A. 3GPP TS 33.180 has defined the security mechanisms (i.e. OpenID connect, IMS-AKA, IPSEC, SRTP, TLS, Mikey-Sakke and KMS federation among others) and crypto suites to be used for MCX. They will therefore be evaluated with MCS-TaaSting as part of the different test cases including bootstrapping and securing of the different call types. You can check for example user authentication and authorization in the preamble 5.1 in 3GPP TS 36.579-2 for more information.



Q. What are the conformance certification on Group Management, CMS (Configuration Management)?

A. Similar to the previous question, the test cases in 3GPP RAN5 (current and future) TS 36.579 Technical Specification (parts 1-7) will be gradually included in the MCS-TaaSting portfolio. In terms of CMS, so far at least test cases 5.2 and 5.3 in 3GPP TS 36.579-2 consider explicitly CMS and test case 5.1 considers CMS.

Q. What are the certification conformance across MCX Servers (across carriers and also for Group Management enablement)?

A. So far we follow the status and priorities defined by 3GPP RAN5 test cases and TF160 resulting TTCN3 code and will focus on the user to server interface being the system under test the UE.

Q. Any certification for ProSe (Direct mode) test cases and its execution?

A. In order to verify and later validate any test cases the testing engine needs to be used with real implementations. Therefore, although off-network test cases have been defined in 3GPP RAN5 TS 36.759-2, Section 7, due to the apparent lack of implementations (widely justified by missing ProSe capable devices) we will initially focus on the On-Network test cases. When the situation changes and devices with ProSe support will become available, we will adapt MCS-TaaSting accordingly.

Q. Can you explain how this MCS - TaaSting is different from PTCRB evaluation from client perspective (MCX)?

A. MCS TaaSting aims to support the testing according to GCF or PTCRB MCS certification initiatives by providing both the required standard-based and validated testing tools. Part of the MCS-TaaSting project is the evaluation of certification programs like PTCRB or GCF certification and make sure MCS-TaaSting can be used for these certifications. This part of the project is done by PSTA and TCCA, who has experiences with mission critical testing and certification.

Q. What interfaces are expected to be tested for cross-cellular carrier situations (MCSMI, CAPIF, etc.)?

A. Core LTE/5G functionalities are not part of the MCS test cases defined by 3GPP in 3GPP TS 36.579 Technical Specification which, together with resulting TTCN3 rules, form the foundation of the MCS TaaSting tester. Therefore, initially only UE to Server interface will be considered.

Q. Are there going to be tests that involve separate security domains?

A. No, they are not part of the 3GPP defined conformance test cases yet.

For further information on the MCS-TaaSting project, please contact info@mcstaasting.com