Bittium, Athonet, Nemergent and MCOP Successfully Tested Multi-vendor e2e Ciphered Mission Critical Push-To-Talk Calls

Successful Multi-Vendor test demonstrates during the Fourth MCX Plugtest End-to-End Ciphered Mission Critical Push-To-Talk Calls.

BILBAO, SPAIN, November 21, 2019 /EINPresswire.com/ -- Bittium, Athonet, Nemergent and the Mission Critical Open Platform (MCOP) project have successfully tested multi-vendor end-to-end ciphered Mission Critical Push-To-Talk (MCPTT) call. Secure multi-vendor communications are one of the keystones in open standards, enabling mission-critical communications over private and public networks. The test took place during the fourth MCX (collectively for MCPTT, MCVideo and MCData services) Plugtests™ that were organised by the European Telecommunications Standards Institute (ETSI) in Kuopio, Finland. The Plugtest series is the first independent testing of public safety and other mission critical LTE, and the tests are essential to ensure seamless access to mission critical services over 4G networks across different vendors' products and implementation. The tests also provide essential feedback to 3GPP Working Groups on mission critical communication specifications.

The test for end-to-end multi-vendor secured MCPTT calls over mission critical grade LTE included MCOP's SIM-based authentication, setting up security associations using IPSec between Bittium Tough Mobile 2 as the user equipment and Athonet's IP Multimedia System (IMS) core, and Nemergent's MCPTT standardised key exchange, authentication, service authorisation, and ciphering mechanisms. In order to have a fully end-to-end secure solution, the different vendors demonstrated interoperability at all the nodes involved in the communications chain (UE, LTE, IMS, KMS, IdMS, CMS, GMS, AS) and at the different 3GPP-defined message exchange protocols.

By using fully 3GPP Release 14/15 compliant mechanisms, the MCX user initially exchanged keying information and certificates with the Key Management System (KMS). Then the client logged in and retrieved access token from the IMS to later obtain fully secure authenticated access to the MCX Application Server (AS). The MIKEY-SAKKE protocol allowed proper sharing of keying information between the participants in the call to secure both MCX specific signaling and voice communications.

The test is a milestone that once again demonstrates the maturity of the MCX solutions and shows that customers already have access to fully secure MCX solutions.

"This is a great achievement considering the whole mission critical communication community and we are proud to have been part of the test with our secure Bittium Tough Mobile 2 smartphone. It is good to see that cyber security issues are gaining more and more importance also in the public safety area", said Jari Sankala, Senior Vice President, Defence and Security at Bittium

"We are pleased to partner such visionary companies with our products and enable such an important milestone for MCPTT functionality" said Daniele Munaretto, Public Safety Manager. "Athonet has supported all the ETSI MCPTT and MCX plugtests since inception with EPC, IMS and eMBMS solutions and is pleased to enable this important "first-time" activity"

Dr. Jose Oscar Fajardo , CEO from Nemergent claimed that “We are proud of partnering once again with these pioneering companies; all together, we managed to show multi-vendor carrier-grade solutions going beyond niche interpretations of the 3GPP procedures”.

Dr. Fidel Liberal, MCOP coordinator stated “Once again the use of open APIs has been proven as the best way to foster the deployment of pioneer standardised multivendor mission critical communications ecosystems”.

Bittium - Defense & Security
Bittium is a trusted Finnish company with over 30 years of experience in advanced radio communication technologies and biosignal processing. For the Defense & Security market, Bittium provides the most modern products and solutions for tactical and secure communications. The products and solutions for tactical communications bring broadband data and voice to all troops across the battlefield. For secure communications, Bittium offers proven mobile devices and cyber security solutions certified up to the CONFIDENTIAL level. Net sales in 2018 were EUR 62.8 million and operating profit was EUR 2.8 million. Bittium is listed on the Nasdaq Helsinki Exchange. www.bittium.com

Athonet
Athonet provides a complete in-house LTE/5G Connectivity Platform for Hybrid, Edge and Private networks. Our platform allows customers to break free from the restrictive, expensive, proprietary and centralised architecture of legacy solutions and embrace the true potential of wireless networks – capturing new sources of revenue whilst also massively reducing CapEx and OpEx. From deploying the world's first LTE Smartgrid and first LTE solution in an earthquake zone in 2011/2012 to the award of Lot 1 of the French PCSTORM tender for the Gendarmerie in 2019, Athonet's solution has led the development of Private LTE and become its gold standard. Athonet is a four times winner of the Global Mobile Awards at Mobile World Congress 2019 and the International Critical Communications Awards in 2018 and 2019. Athonet’s solution is being used by network operators, governments and enterprises across the world.

Nemergent
Nemergent Solutions SL is a Spanish SME with full focus on 3GPP standards-based MCX implementations. Nemergent software products are fully developed in the EU and include the main functional nodes both at client and server sides. Nemergent software stacks are being used worldwide for commercial deployments in the Public Safety and Public Transport verticals, and for early prototyping and testing of the standard solutions.

MCOP
The Mission Critical Open Platform (MCOP) is a collaborative project initially funded by the U.S. Department of Commerce, National Institute of Standards and Technology through the Public Safety Innovation Acceleration Program (PSIAP). MCOP aims to face the challenges of the emerging and complex MCPTT clients. The project has already defined, developed and validated a set of Open APIs for easy integration of MCPTT clients on different Mission Critical devices.

Further information:

Leire Eguia
Nemergent Solutions SL
+34 944 98 74 82
email us here
Visit us on social media:
LinkedIn