Open Ecosystems in Public Safety Communications: MCOP Lessons Learned and Future Steps

Bittium ENENSYS EXPWAY TCCA Universidad del País Vasco Euskal Herriko Unibertsitatea CAMPUS OF INTERNATIONAL EXCELLENCE

Dr. Fidel Liberal
fidel.liberal@ehu.eus

DISCLAIMER

This presentation was produced by guest speaker(s) and presented at the National Institute of Standards and Technology's 2019 Public Safety Broadband Stakeholder Meeting. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government.

Posted with permission

Outline

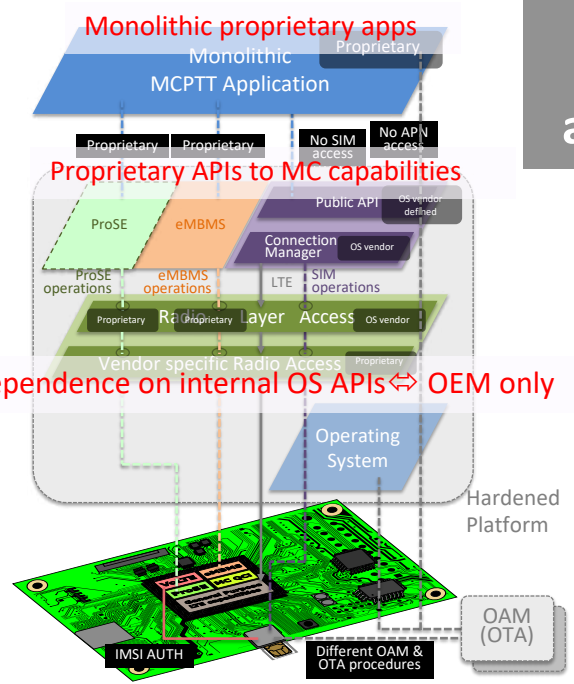
- Problem addressed
- MCOP Approach
- Main expected outcomes
  - Technical
  - Others
    - Foster innovation…
      - Company interest mainly
    - Build a community

Problems addressed

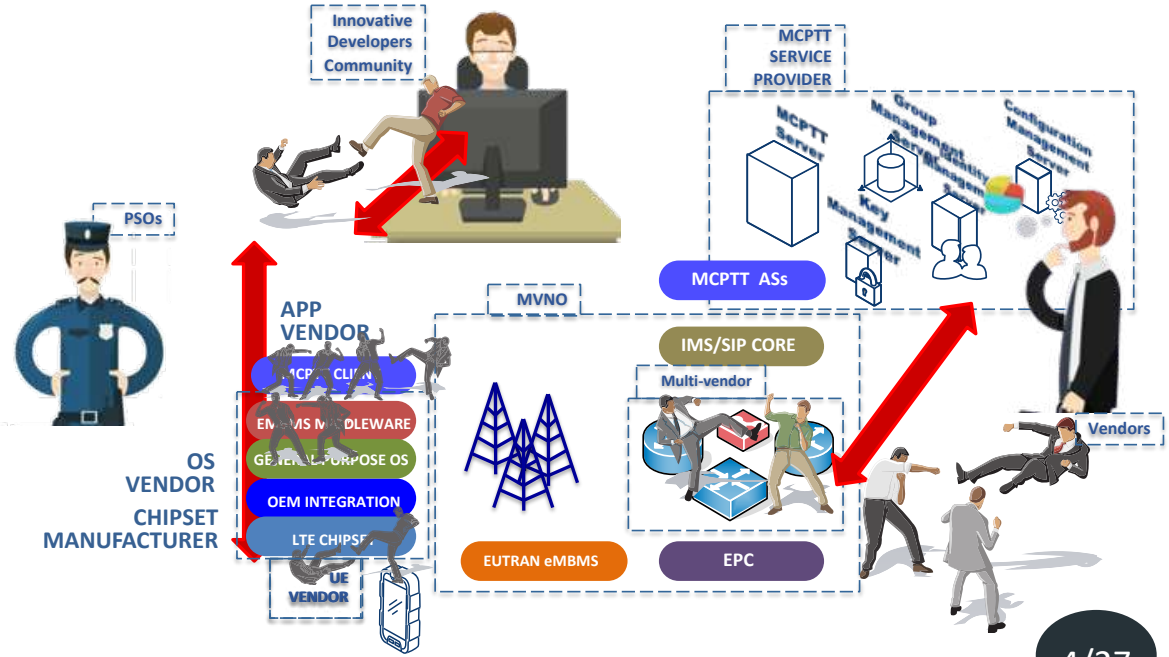
vs.

Challenge 1 UE architecture

Monolithic proprietary apps

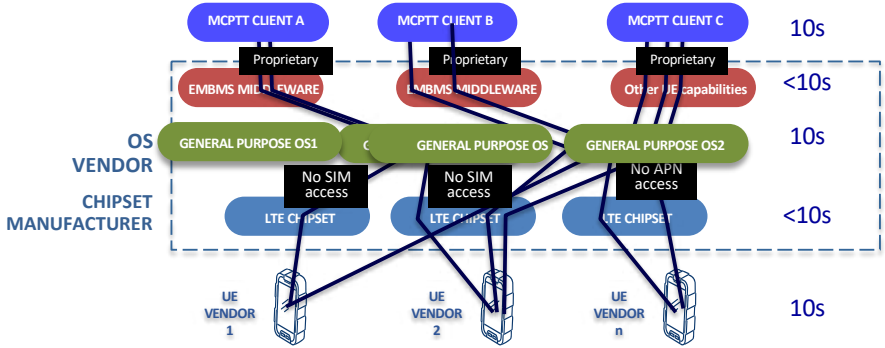


Challenge 2 complex ecosystem

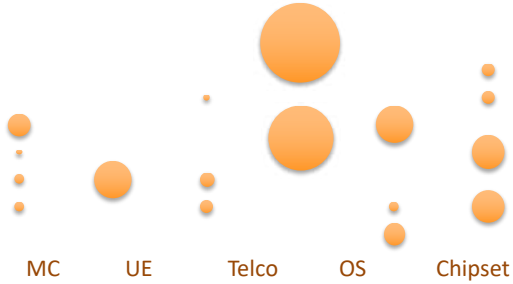


Summary: UE Integration burden

Hundreds of combinations (different release cycles)

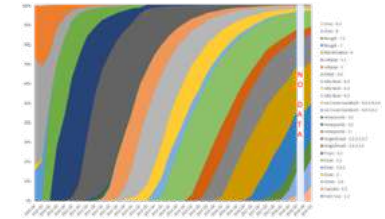


Unbalanced relationship

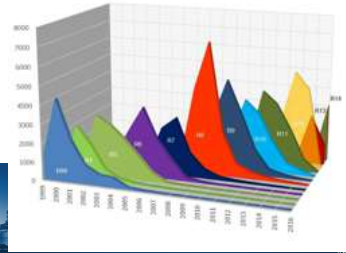


Relative size of MC and commercial industries

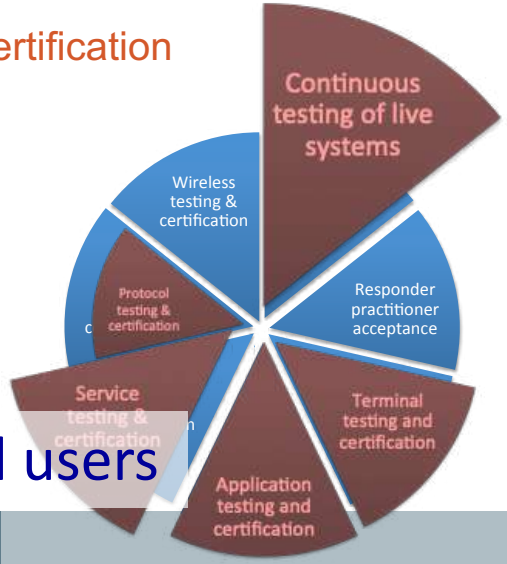
Never-ending expensive effort



X

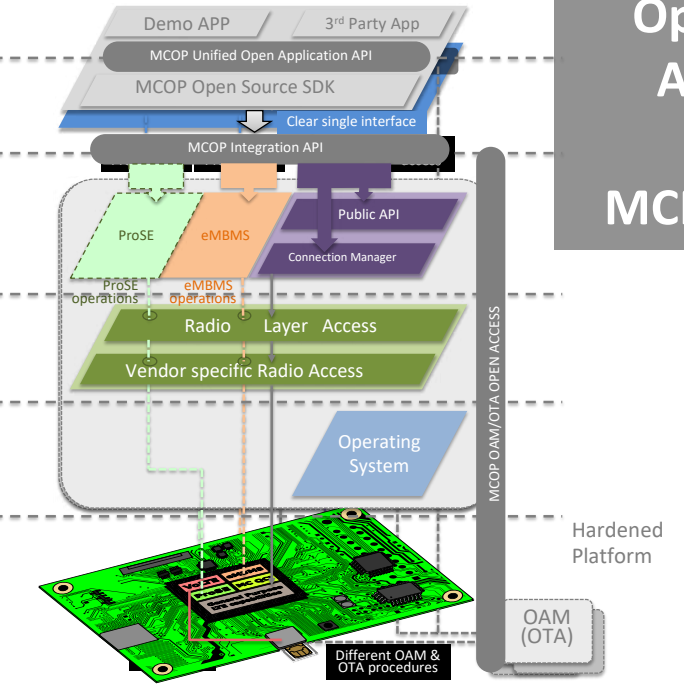


Cross (re)certification



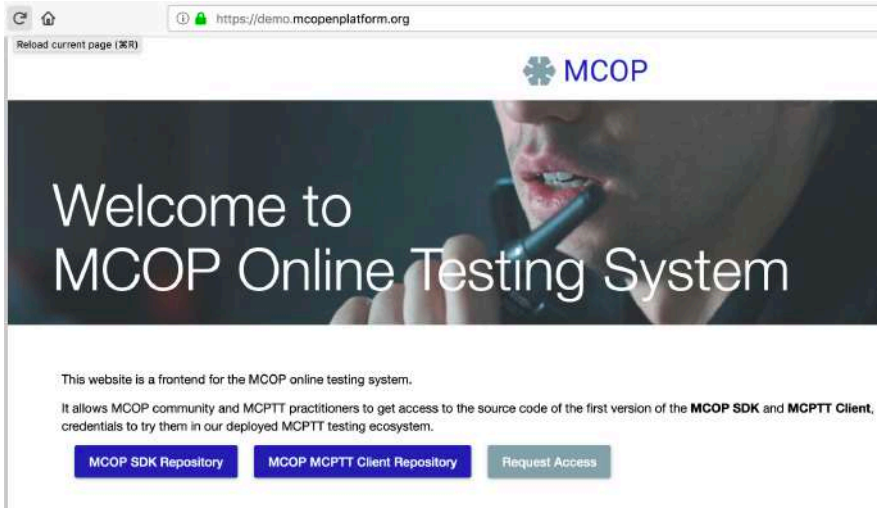
Lose-Lose for MC industry and users

MCOP approach



Open APIs
Apache 2 License
MCPTT SDK

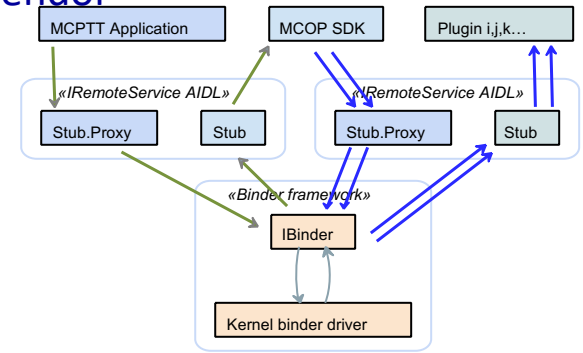
Free/Open Online Testing System



How it works

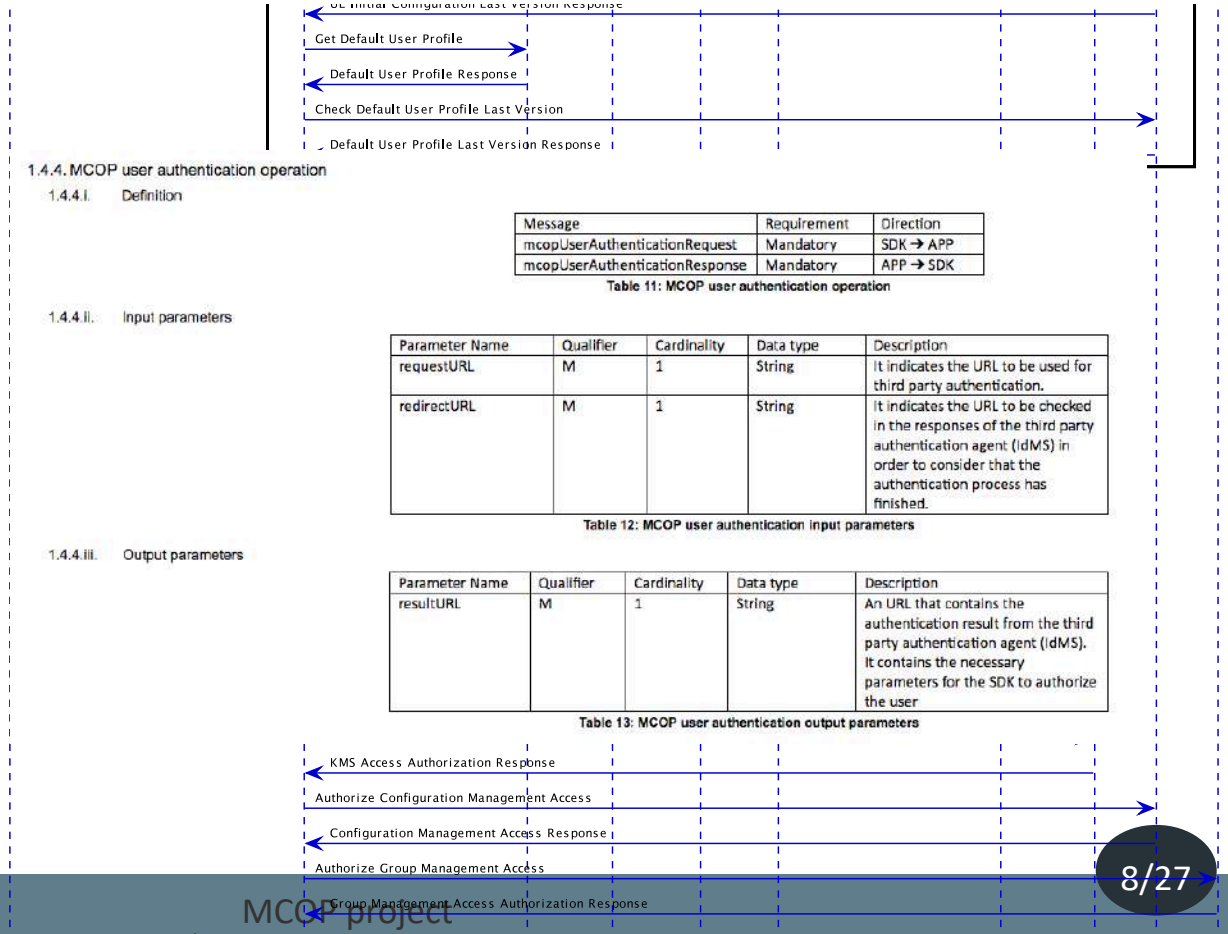
- Technology neutral API definition OPEN, for ANY platform
- De-coupling/isolation for different business models
  - Every component seamlessly provided by a different vendor
  - Licensing and release cycles
    - No constraint
- Access to prioritized resources
  - OEM only if needed
  - Mutual authentication framework
- Alignment with Android and under-standardization APIs
  - Future-proof

OAM Certificate Whitelist provisioning



MCOP APIs

- Open & free
  - Apache 2
- Technology Neutral



1.4.4. MCOP user authentication operation

1.4.4.i. Definition

Message	Requirement	Direction
mcopUserAuthenticationRequest	Mandatory	SDK → APP
mcopUserAuthenticationResponse	Mandatory	APP → SDK

Table 11: MCOP user authentication operation

1.4.4.ii. Input parameters

Parameter Name	Qualifier	Cardinality	Data type	Description
requestURL	M	1	String	It indicates the URL to be used for third party authentication.
redirectURL	M	1	String	It indicates the URL to be checked in the responses of the third party authentication agent (IdMS) in order to consider that the authentication process has finished.

Table 12: MCOP user authentication input parameters

1.4.4.iii. Output parameters

Parameter Name	Qualifier	Cardinality	Data type	Description
resultURL	M	1	String	An URL that contains the authentication result from the third party authentication agent (IdMS). It contains the necessary parameters for the SDK to authorize the user

Table 13: MCOP user authentication output parameters

MCOP project, Objectives

Mission
Critical
Open
Platform

Fostering innovation by targeting common needs of the industry
Traditional telco
Former OTT PTT solutions providers
Small integrators
PSOs' IT departments
Newcomers

- O1. Gather and agree on common requirements for the platform from industry fora
- O2. Analyze architecture problems.
- O3. Define an open platform including different level APIs.
- O4. Validate the architecture and intermediate APIs
- O5. Deploy and maintain a sustainable live on-site and online testbed
- O6. Disseminate the results

Possible enhancements

Current status

- Comprehensive 3GPP MCPTT Rel14 support
  - 4th ETSI MCX Plugtest
- Multivendor
  - Different GUIs
  - Different SDKs
  - Different eMBMS/Connectivity/Configuration

- Quick prototyping: Tailored app
  - Head-up-display for firefighters
  - Quick prototyping

Expected Impact

Events, advocacy

NEM, SONIM

APIs vs. SDK

- PSOs
  - Improve **MCPTT Awareness** and encourage informed decisions/purchases
  - Easier and planned **product integration**
  - Avoid single **vendor dependence**
  - Hands on **trial and training**
- MC Apps developers & new pra
  - **Open** Community and standard troubleshooting platform
  - **Standardization**/normalization/certification/conformance testing
  - Shared knowledge, **reference implementation** and MC-grade **experimentation platform**
  - **Reduce production costs and open integration possibilities**
  - Un-tie APP level from specific HW platform

MCOP: Lessons Learned and Next Steps

Jani Lyrintzis - Bittium

Lessons Learned

- Bittium and other MCOP partners have already realized and leveraged tangible benefits achieved by using MCOP APIs and SDK in integrating and testing Mission Critical applications, the overall integration, testing and verification effort is significantly reduced and simplified.
- With MCOP the focus can be placed in optimization of value-added functions such as user experience and system reliability, rather than in creating and integrating proprietary APIs and other tedious tasks.

Next Steps

- Bittium is a strong proponent of open technologies such as MCOP, whose biggest (and perhaps the only) problem currently is wider industry adoption.
- We see that in the future open APIs for Mission Critical Communications could and should be integrated in the work of standardization and industry bodies such as 3GPP, TCCA and PSTA.
- Moreover, it should be adopted by certification bodies such as GCF and PTCRB, so that testing of the APIs would be part of the normal device certification process.
- Yet another way to promote open APIs and provide wider interoperability of mission critical applications could be BroadWay, a joint initiative between 11 European countries for pan-European PPDR (Public Protection and Disaster Relief) system.

MCOP Southbound API for MBMS

Bartolo Scanavino
ENENSYS/Expway Telecom Market Product Director

Situation Awareness with MC Data

Firemen can receive building layouts and floor plans on their devices including the live positions of their teammates.

eMBMS pushes maps and location updates continuously to the team in the field.

Managers can see in real-time which members of the team need assistance.

Enriched details with MC Video

When there is an accident the first responder arrives and few people go inside to check the situation and report back to the team.

The live camera stream is streamed via eMBMS in the surrounding area.

With the support of video the team can make a better assessment of the actual situation.

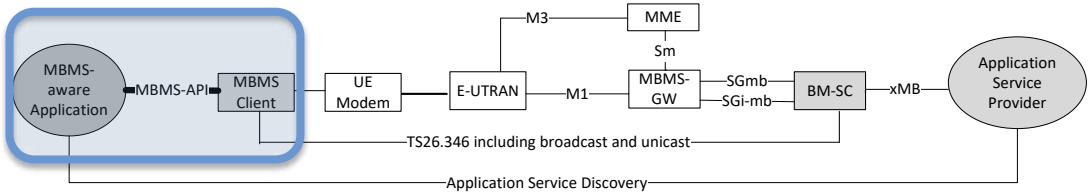
Mining communications with MC-PTT

A push-to-talk group is created between groups or all the people working in the mine.

MCPTT over eMBMS is activated to send the downlink audio stream.

Improved reception quality enhances the communication between teammates, with no network congestion

Southbound API for MBMS



- delivery of Public Safety services with MBMS is :
  - Congestion Free (MBMS spectrum is allocated and not subject to contention with Unicast traffic)
  - Highly Reliable (improved coverage thanks to SFN and NoACK)
  - Efficient (single bearer from the MBMBS server to all users of the group)
  - Synchronized (all UEs receive data at the same time)
- The MBMS Client exposes an API to the MCOP Open Source SDK, enabling MBMS reception and monitoring
- The MBMS Client runs as a standalone service in UE and can handle multiple applications

What the MBMS Client provides

- The MBMS Client monitors the MBMS reception quality and notifies it to the application
- It provides an API to get EGCI and list of MBMS SAI for location reporting, and notifies the application whenever there is a change
- It provides an asynchronous API to open/close MBMS bearers and access the embedded group communications
- The received IP packets are made available on a network interface

What's next?

- MCPTT and MCVideo can both be managed by current version of the APIs
- In release 15, FEC and ROHC were added, the MCOP APIs will be updated to support these important features
- In release 16 MBMS MCData was defined using the File Download delivery method, the MCOP APIs will be extended to control and monitor file reception

Lessons learned

- Technical entry barriers still exist
  - SIM storage
  - IPSEC
  - Need to involve UE vendors / SIM manufacturers
- Conveying the right message
  - Inmediate needs vs long time benefits
    - SDK vs. APIs
    - What is your business model?
- How to build a (Public Safety) real community
  - Open source…

Lessons learned

Open APIs message

DEs - Device eco-system Sub-objectives
(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)

DEs8 Peripheral Equipment Interfaces
Standard interfaces shall be used (physical as well as wireless) for connection to any peripheral equipment/external devices.

DEs9 Open APIs/SDKs for MC application development
Open APIs shall be used with availability of SDKs to support MC application development

AEs - Application Eco-system Sub-objectives
(All Tenders shall include sufficient information to describe how they will achieve each Sub-objective)

AEs1 Open APIs
The technology used in service provisioning shall provide open Application Programming Interfaces (APIs) and/or equivalent forms of intercommunication, and data formats for the technology used in the service provision. These APIs, etc. and data formats shall be available without delay, without licensing or confidentiality constraints, and royalty-free, to nominated Suppliers.

Ss1 Use of Open Common Standards
Pan-European broadband PPDR network, devices and services shall be based on open common standards (e.g. 3GPP, ETSI, IETF, IEEE, OMA). Open standards shall be made in a transparent and open process by organisations who's membership is open to all and who's standards are available to all.

Ss2 3GPP Mission Critical Services
3GPP standardised MCX services shall be offered. MCX 3GPP release 15 is considered as a recommendation. All other 3GPP components and services shall be interoperable to support MCX services.

What's next!!!!

- Next steps in MCOP
  - Focusing on API definition
  - Creating MCOP API steering committee
  - Evolution / convergence of MCOP APIs
    - MCData/MCVideo APIs COMING SOON
- Pushing supporter program

MCOP Supporter

Vendors

Nemergent Solutions

sonim. BUILT FOR LIFE™

TeloSystems

TD Tech

funkwerk

mintech

PSOs/Public Operators

MINISTÈRE DE L'INTÉRIEUR

ERILLISVERKOT

Coming soon

- Hackathon

Hosted by NIST PSCR

CONTEST 002//

No Need To Repeat: Delivering Mission Critical Communications

Strengthen voice communications with push-to-talk technology for mission-critical response.

Prizes

UP TO $2,200,000 IN PRIZES

Prizes available for online, in-person and National Contest winners to incentivize innovation and help emergency responders save lives

$350,000	$650,000	$1,200,000
Total prize purse for all codeathons	Total national prize purse for the Demonstration Round Contest	Total national prize purse for the Seed Round and Progress Round Contests

GET STARTED

ATTEND A CODEATHON NEAR YOU

10 Cities
September 27-29 &
November 1-2

PARTICIPATE IN PERSON

PARTICIPATE IN THE ONLINE CONTEST

June 1 through November 15

Develop and submit your prototype or solution to win up to $65,000 in prizes as a National Winner.

PARTICIPATE ONLINE

TCCA

Critical communications for all professional users

www.tcca.info

Contact: admin@tcca.info, +44 191 231 4328

The Critical Communications Association

Supporting **open and standardised** mobile critical communications technologies and complementary applications.

Catalysing competitive **multivendor markets** worldwide through open standards and harmonised spectrum.

Members are **end users, operators, industry** and other stakeholders globally sharing **knowledge** and **experience**.

Collaborative working across the critical communications **ecosystem** to develop and drive the most effective solutions for all.

Critical communications for all professional users

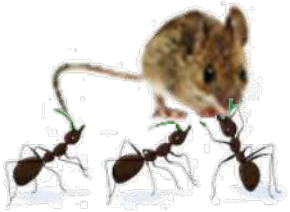
Public Safety Broadband Eco-System

Critical communications for all professional users

Growing the Eco-System

We can grow the eco-system by:

- Using Common Open Standards
- Using Common Open APIs



MAKE THE PUBLIC SAFTEY ECO-SYSTEM GREAT

MCOP Supporter

Critical communications for all professional users

NIST PSIAP
FEDERAL AWARD ID: 70NANB17H151

Mission Critical Open Platform

Bittium ENENSYS EXPWAY TCCA Universidad del País Vasco Euskal Herriko Unibertsitatea CAMPUS OF INTERNATIONAL EXCELLENCE

Dr. Fidel Liberal
fidel.liberal@ehu.eus