Capgemini

TRANSITIONING PUBLIC SAFETY CRITICAL COMMUNICATIONS TOWARD LTE/5G MCX: **A GROWING MOMENTUM**

1

THE SHIFT TO BROADBAND MCX FOR PUBLIC SAFETY IS ACCELERATING AMID THE RISE OF EXTREME EVENTS

The availability of highly reliable and secure communications systems is integral to the mission of Public Safety and Security teams (police, fire brigades, ambulances, etc.) engaged in critical situations. It is a true lifeline for the first responders on the ground and the public they serve.

Public Safety Mission-Critical are at a turning point: around the globe, they are progressively migrating from legacy professional mobile radio (PMR) technologies to LTE/5G solutions with MCX (Mission-Critical voice, data, video) to both support **legacy** and new **advanced multimedia services** and enhance **situational awareness** during crisis situations.

This evolution is driven by multiple factors:

- The **increasing number and magnitude of crises** (climate-related events such as fires and floods, social demonstrations, riots, terrorist attacks) which stresses the resources and capabilities of Public Safety organizations
- The correlated growing imperative for first responders and command centers to have **more advanced communications systems** leveraging data, video, and real-time geolocation in addition to voice to increase situational awareness and operational efficiency
- The **limitations of existing PMR solutions** (TETRA, P25, etc.) in terms of service evolution and supplier concentration
- The **growing readiness and maturity of the 3GPP and MCX ecosystem** for Mission-Critical communications in terms of suppliers (network, device, application), standards, and solutions.

Capgemini interactions with **Public Safety authorities (PSAU)** around the world highlight a growing consensus toward mobile broadband LTE/5G solutions with MCX. The last 12 months show a massive acceleration, with more and more governments and authorities either planning or launching large-scale transformations. Alongside well-known early adopters (FirstNet in the US, SafeNet in South Korea, Virve2.0 in Finland, to name a few), and the RRF program in France[1], we see numerous RFIs/RFPs being launched in Europe and beyond (e.g., ESN/Lot3 in the UK, ASTRID in Belgium, NOOVA in the Netherlands, MSB in Sweden, etc.). Even the TCCA Broadband roadmap published in January 2019[2] recommends governments and operators start the process of transition as early as possible.

1. With its consortium partner Airbus SLC, Capgemini is the integrator of Lot 2 "E2E Integrator, Core Network, MCX and Terminal" of the Réseau Radio du Futur (RRF) program *https://www.capgemini.com/news/press-releases/consortium-led-by-airbus-and-capgemini-selected-by-the-french-ministry-of-the-interior-for-the-radio-network-of-the-future-rrf/*

2. *https://tcca.info/documents/january-2019-ppdr-broadband-roadmap.pdf/*

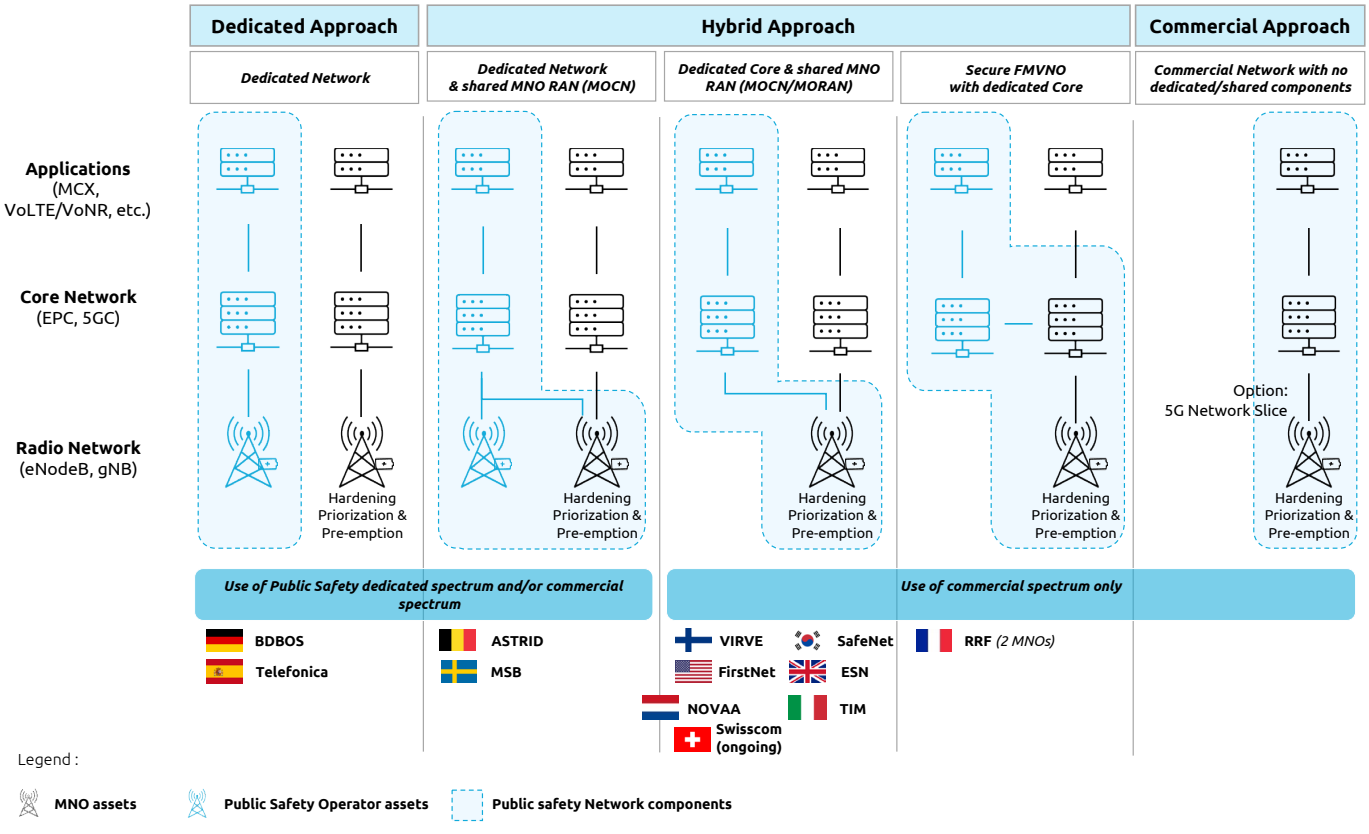
2

AMONG THE AVAILABLE DEPLOYMENT MODELS, THE MOCN MODEL SEEMS TO BE PREFERRED BY PUBLIC SAFETY AUTHORITIES

To implement mission-critical communications over LTE/5G radio networks, PSAUs can choose from multiple networks and operating models. The right choice is very much dependent on local strategy, investment capacity, time-to-market imperative and specific requirements, among which are the availability and amount of PPDR spectrum and legacy national PMR assets and teams.

Most countries are selecting a **hybrid model** based on (i) a dedicated and secured Core Network with MCX controlled by the PSAU, and (ii) leveraging the radio coverage provided by one or several public Mobile Network Operator(s). **The Multi-Operators Core Network (MOCN)** model is the most frequently used; providing close control and monitoring of over-the-radio network features and KPIs. FirstNet in the US, SafeNet in South Korea, or Virve in Finland are examples of MOCN deployments and other European states are planning to select this model (e.g., ASTRID in Belgium, ESN in the UK, NOOVA in the Netherlands, or

Figure 1: network models for delivering mobile broadband critical communications

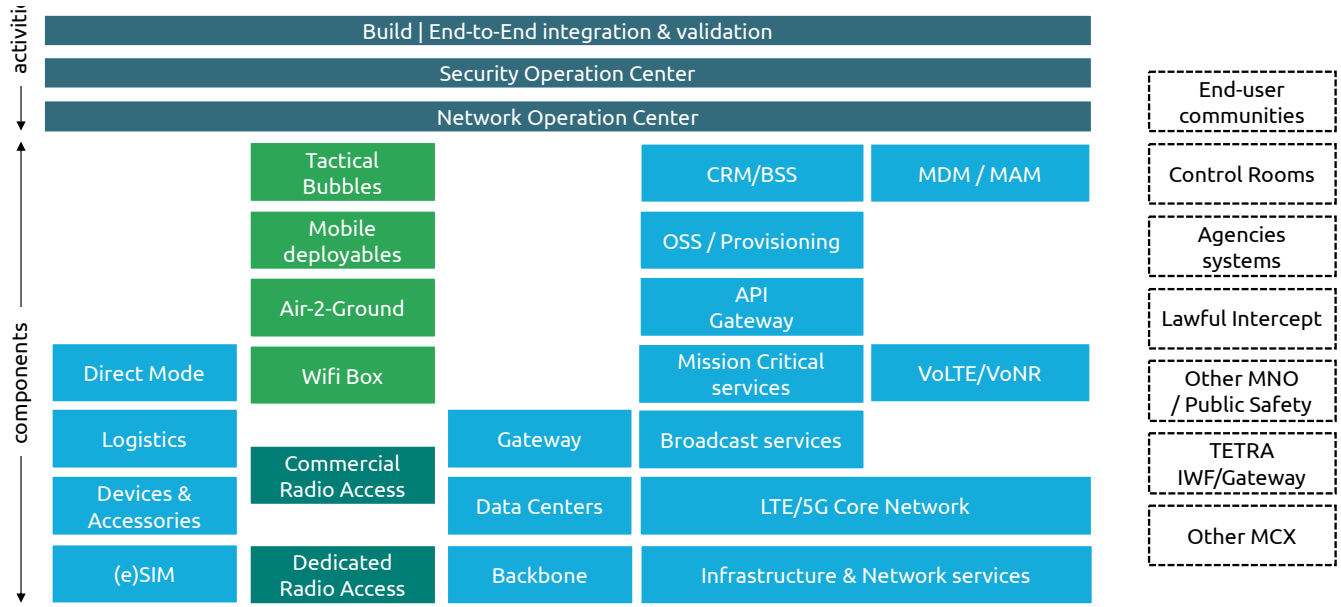


MSB in Sweden). In addition, we observe a sub-variant of the MOCN architecture, which combines the MNO's public radio network with a dedicated radio network using the PPDR spectrum. The **Full MVNO** model, which is being deployed in the RRF program in France with two host MNOs, provides a similar architecture to the MOCN model, albeit without the direct access to MNOs' radio networks. For RRF, investments and radio skills are entirely managed by the operators, with strict obligations in terms of radio network availability, coverage, prioritization, and pre-emption.

Aside from the hybrid models, other options exist. On the one hand, the **commercial model**, and on the other hand, the **private model**, which is the option preferred by the Spanish and German authorities. The commercial model would allow the PSAU to rely fully on the existing infrastructure of an MNO (in a 5G architecture, this could be based on a dedicated network slice). However, this implies full dependence on the MNO and therefore carries potential security risks. The slicing model is not mature yet, but it is an interesting architecture to investigate in the future with 5G SA. The private model relies on a dedicated radio network infrastructure, independent of any public mobile network: the PSAU becomes a fully-fledged telecom mobile operator with end-to-end control over wireless communications. This option requires substantial investment in the deployment of the core systems, in the nationwide radio network, as well as in network and services operation. The availability of sufficient PPDR spectrum is a key prerequisite.

While the model varies, the implementation of a mobile broadband mission-critical network does include a set of common functional and technical elements, as well as common build-and-run activities (Figure 2). Aside from the **core network** and the **MCX platform** – a key building block to replacing legacy PMR technologies – other functional and technical elements are also critical to the overall architecture and need to be carefully considered for a successful evolution. Those elements include the support of **non-mission-critical voice (VoLTE)** and **location services**, the provisioning and billing of users (**OSS/BSS)**, the mobile device/ application management for enrollment **(MDM/ MAM)**, the **eSIM platform** and network, and security operations and maintenance **(NOC and SOC)**.

Figure 2: building blocks and key activities for a mobile broadband critical communications network

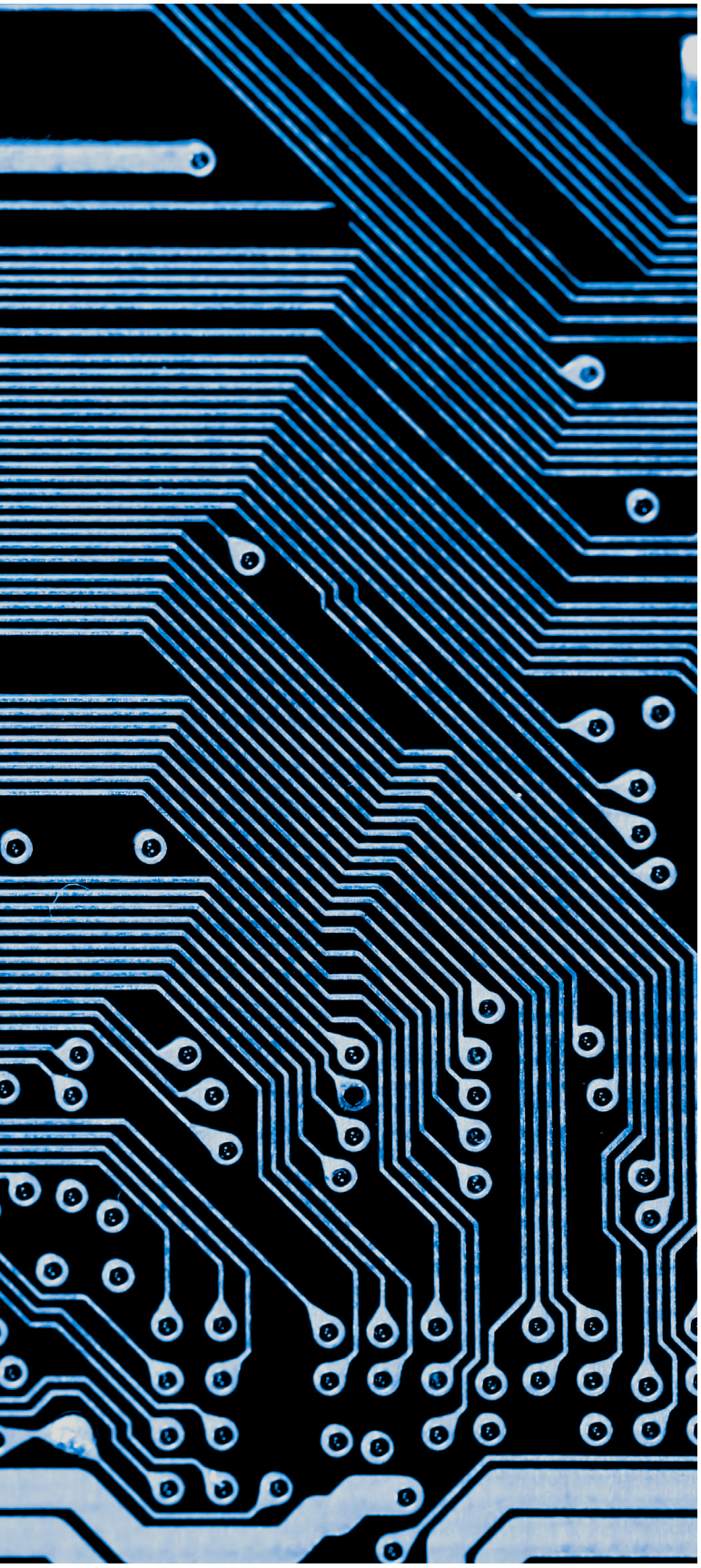


On the MCX side, we see the **growing maturity of market solutions** from key players, such as Airbus SLC, Frequentis, Leonardo, Motorola, Hytera, Samsung, Streamwide, and many others. Significant progress has been made on MCX interoperability, in part driven by the European BroadWay and BroadNet initiatives.

The **interworking between MCX and TETRA remains**, however, **a challenge** – standardization is still a work in progress and interworking also depends on how "open" TETRA systems are (e.g., with APIs). The experience of PSAU early adopters demonstrates that the interworking implementation is simplified when legacy TETRA and MCX providers are the same but proves more complex when different TETRA and MCX solution providers are involved. Close coordination of the migration across multiple Public Safety agencies is therefore required to limit interworking challenges. To mitigate risk and avoid vendor lock-in, some PSAU are considering a dual MCX solution.

Overall, the **complexity of this multi-vendor and multi-system architecture** highlights the fundamental role of the **end-to-end system integrator** leading a strong urbanization of the solution, technical alignment, as well as testing and validation to ensure the security and robustness of the mission-critical network. This transformation program is a multi-year roadmap for the design, build, operation, and migration. Another challenge faced by PSAU is the availability of technical resources and skills required for the deployment and run of such networks in the current geopolitical context of heightened security and sovereignty stakes.

Overall, the complexity of this multi-vendor and multi-system architecture highlights the fundamental role of the end-to-end system integrator leading a strong urbanization of the solution, technical alignment, as well as testing and validation to ensure the security and robustness of the mission-critical network.



3

DEVICES AND SERVICES: BASICS FIRST!

Today, we see a large and continuously **growing catalog of available devices and accessories** for LTE MCX solutions from a diverse list of suppliers (Crosscall, Hytera, Motorola, Ruggear, Samsung, Sonim, Zebra, etc.). This is less evident for 5G devices (Crosscall, Samsung mainly) as the 5G public safety device ecosystem is still in the early maturity phase. However, the global market momentum around mobile broadband for Public Safety is generating interest from chipset manufacturers – Qualcomm for instance – and we expect the 5G device and accessories public safety ecosystem to develop soon.

There is an exception to the **availability of device-to-device management** (direct mode operation - DMO) which is still in its standardization phase (Release 17 onwards), but great progress has been shown for Public Safety and V2X (vehicle-to-everything) use cases, further reinforcing chipset manufacturers' willingness to offer this feature. In the meantime, device makers have developed accessories using PMR technology to make the DMO feature available today in addition to LTE/5G devices.

On the service side, **group voice communications** is and will remain the **absolute priority** for public safety users. It is a basic lifeline that requires the highest level of quality of service, network availability, and robustness, as well as additional features (noise cancelling, recording, privacy mode, etc.). It is the baseline that will be compared to TETRA and other PMR legacy solutions: no regression can be accepted by end users and the quality of service will be of paramount importance to building trust in the next-generation mobile broadband network.

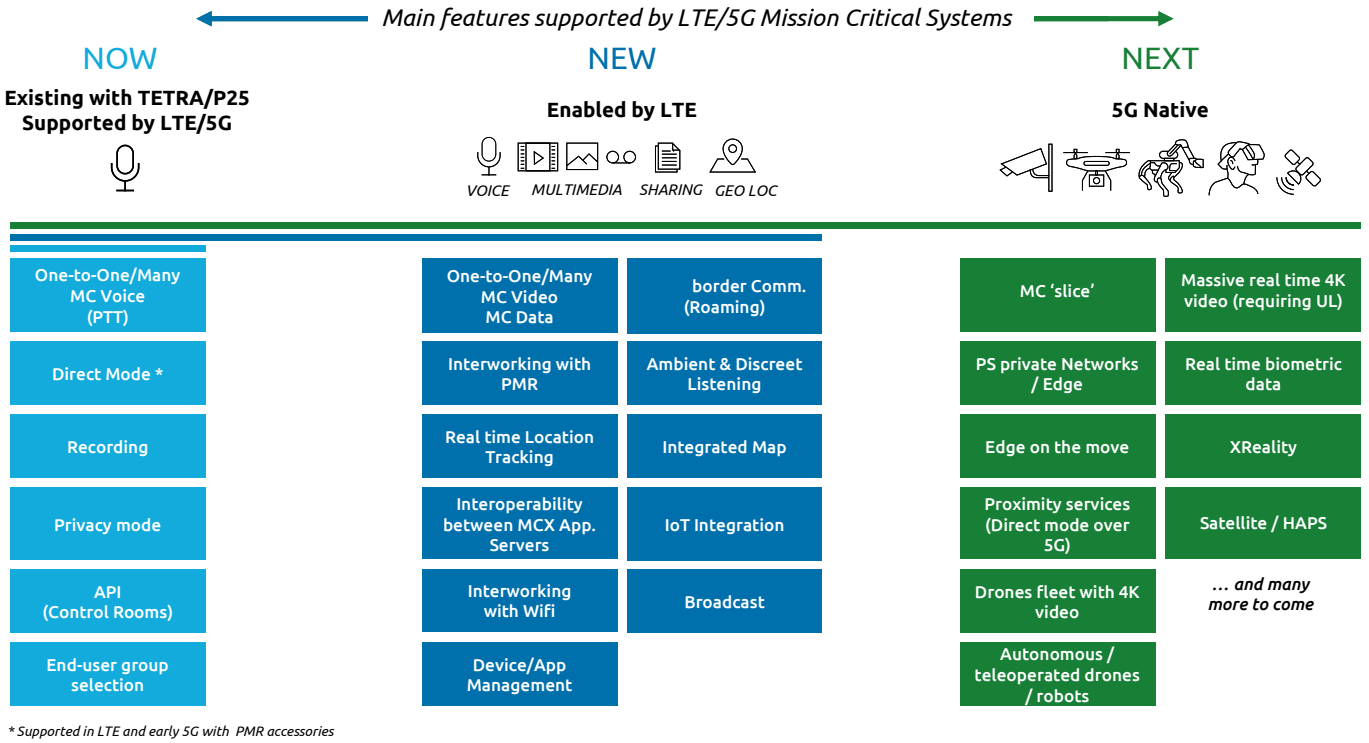
4

FUTURE EVOLUTIONS ARE IN SIGHT TO FURTHER ACCELERATE THE ADOPTION OF BROADBAND LTE/5G MCX FOR PSAU

The move towards mobile broadband Mission Critical (MC) communications will pave the way for an **expanding set of services**, which will **enhance situational awareness**:

- First, LTE MCX networks are driving the use of multimedia applications (via MC data and MC video sessions) such as the sharing of documents/photos, reports, video from Public Safety users on the ground broadcasted to the control room and vice-versa, **videos from street cameras/drones** sent to the users, **enhanced location tracking**, ambiance and/or discreet listening.
- Next, as mobile broadband networks increasingly use 5G, we expect **more mission-critical IoT use cases** with massive 4K video streams provided by a fleet of cameras or drones, remote/effective control of IoT devices such as drones, mobile robots or sensors, use of augmented reality services, potentially enhanced by future network slicing capabilities. 5G will also enable the deployment of MCX applications and AI use cases at the Edge (i.e., in dedicated areas such as prisons, or as part of tactical command centers in the event of a crisis). In addition, we see a growing number of initiatives around the integration of **5G NTN (non-terrestrial networks)** connectivity and direct-to-device LEO satellite communications, which end users will progressively benefit from in the future.

Figure 3: MCX services continuum, for public safety



** Supported in LTE and early 5G with PMR accessories*

5

CAPGEMINI POSITION IN THE PUBLIC SAFETY MARKET

Capgemini is a trusted transformation partner of Public Safety authorities and service providers in their journey from PMR to LTE/5G with MCX, from strategy to implementation. Together with our partner Airbus, we are the end-to-end integrator of RRF in France. We work with Public Safety authorities, government agencies, and telecom service providers on migration strategy as well as program design and build, relying on our extensive track record and know-how both in the telecom and public sectors. We leverage a strong ecosystem of technology partners as well as assets and accelerators, such as our 5GLab dedicated to Public Safety, where we continuously develop and test 5G MCX use cases. This experience, combined with close interactions with Public Safety authorities in most European countries and extensive research and interviews with end-user communities, technical providers, and telecom operators, has positioned Capgemini at the forefront of this transformation.

AUTHORS

Patrice Crutel
Technology and Platform Strategy Director
Capgemini Invent

Pierre Fortier
Vice President 5G Global Lead
Capgemini Invent

Pierre Nelson
Senior Consultant, Business Technology
Capgemini Invent

Nazirali Rajvani
Senior Director 5G & Edge Group Portfolio
Capgemini

Antoine Mercier
Enterprise Architect
Technology & Services Director
Capgemini Technology & Services

About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | www.capgemini.com

Copyright © 2023 Capgemini. All rights reserved.