

GSMA 5G TRANSFORMATION HUB

The world's most innovative 5G solutions



Helping Public and Private 5G to Work Together

China Telecom deploys a new function to secure the interface to more than 1,000 private networks


China Telecom has developed the customized-interworking function (C-IWF) to secure the interface between its public network and private cellular networks. By reducing the risk of security breaches and enabling interoperability between equipment from different vendors, the C-IWF is designed to fuel greater adoption of private 5G networks.




Helping Public and Private 5G to **Work Together**

CASE STUDY LEAD: CHINA TELECOM

+ CHALLENGE

 Mobile operators need to secure the interface between their public networks and the growing number of private 5G networks, as an unsecured connection could be utilised to launch an attack through equipment that isn't being monitored by the network operator.

+ SOLUTION

 China Telecom's new customized-interworking function (C-IWF) is designed to provide a secure interface between its public network and private networks employed by enterprises.

Deployed in the operator's 5G core network, the C-IWF employs multiple security mechanisms to reduce the risk of breaches and ensures equipment from different vendors will work together. China Telecom is deploying the C-IWF in 18 provinces to interface with more than 1,000 private networks.


+ IMPACT & STATISTICS

 China Telecom says the C-IWF has greatly reduced the security risk from 5G private network devices. At the same time, the C-IWF's authentication function and message monitoring capabilities improve the operator's ability to manage and control network devices.

+ WIDER IMPLICATIONS

 Ultimately, China Telecom expects every private network's NFs (network functions) to connect to a C-IWF. It also anticipates that the solution will be adopted by other operators both inside and outside China, accelerating the growth of the 5G private network market. By some estimates¹, private networks could be deployed in up to 15 million locations, many of which will be factories or warehouses in China, India, Vietnam and other industrialising Asian countries.

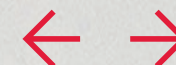
+ STAKEHOLDERS

 China Telecom

SOURCES & FURTHER INFORMATION

 Sihan Li, China Telecom:
lish9@chinatelecom.cn

¹ "European Private Wireless Market Astonishing Growth", PrivateLTEand5G.com, January 2022



Meeting the demand for private 5G networks

Across much of the world, there is rising demand for so-called private 5G networks. Enterprises are using these dedicated networks to support very specific use cases, such as the automation of a manufacturing plant or the management of a logistics hub.

As of September 2022, some 955 organisations globally had deployed private networks, according to data collated by the GSA². While the true number of private networks will be higher given that a number of deployments are not publicly announced, there is a big gap between the current reality and the theoretical potential. By some estimates³, private networks could be deployed in up to 15 million locations, many of which will be factories or warehouses in China, India, Vietnam and other industrialising Asian countries.

But the rising demand for these private networks can create challenges for mobile operators. Enterprises deploying their own 5G connectivity typically need to co-operate with operators both for regulatory reasons, such as a license to use the spectrum, and to enable interoperability with the public cellular networks. But a direct connection between the network functions deployed in an industry campus and the public network can raise security issues.

“These problems have seriously restricted the development of 5G networks in vertical industries,” according to the China Telecom Corporation Research Institute. “One of the issues is the contradiction between the operation model adopted by operators for the network and the demands of vertical industry customers for 5G networks.” In particular, enterprises usually want to be able to

control the devices and resources in their own networks, while operators need to monitor network resources.

Another problem can be connecting the interfaces between devices of different vendors. For example, the China Telecom Corporation Research Institute highlights the “unclear contents” in the N4 interface connection between the session management function (SMF) and user plane function (UPF) in a 5G core network. As a result, each equipment vendor has developed its own customised private fields to realise the related functions, making it difficult for mobile operators to ensure an interface connection between devices of different vendors.

At the same time, operators must ensure the security of their own network and information and the stable operation of their networks. Yet an operator can't fully supervise equipment deployed in a private network of an enterprise, raising the risk of a network attack being launched through this equipment and utilising the direct connection with the operator network.

² Private-Mobile-Networks December-2022 Summary Report, GSA, 2022

³ “European Private Wireless Market Astonishing Growth”, PrivateLTEand5G.com, January 2022

New function secures the interface to the public network

To secure the interface between public 5G networks and private 5G networks, China Telecom has developed the customized-interworking function (C-IWF). Deployed in the operator's 5G core network, the C-IWF communicates with the dedicated network functions deployed in an industry campus. The C-IWF supports multiple security mechanisms, network isolation and signalling aggregation. To ensure the C-IWF is robust, China Telecom has incorporated a load balancing and redundancy mechanism.

China Telecom says the C-IWF can be used in conjunction with various types of private 5G network, including those that have all the 5G core network functions, those that have all the core network functions, except the AUSF (the access and mobility management function); those that have all the core network functions, except AUSF and UDM (unified data management) and those that only have the UPF.

A C-IWF is not required in cases where a 5G private network is realised as a dedicated virtual slice of the existing public cellular network.

The C-IWF is responsible for signaling forwarding between devices in the trusted area (the public network) and devices in an untrusted area (the private network). During the forwarding process, the C-IWF hides or replaces the confidential information of the devices in the trusted area, and forwards the processed signalling to the

correct network device, so as to avoid exposing the information of the devices in the trusted area to the untrusted area.

The C-IWF can also isolate devices in untrusted areas, and provide secure access capabilities and dynamic authorisation capabilities: Before the device in the untrusted area is authenticated, the communication channel with the public network is completely blocked by the C-IWF. For the devices in the untrusted area that have passed the verification, the C-IWF continuously monitors the security of the traffic. For the devices that violate the security policy, the C-IWF blocks the communication with the public network.

If the devices in the untrusted area and the devices in the trusted area belong to different vendors, the C-IWF is also able to adjust the interface between the devices of different vendors: It

adapts the content of the message sent by the sender, so that it can be received successfully. "With the continuous introduction of devices from new vendors, the operator only needs to iteratively upgrade the signalling interworking gateway (the C-IWF), instead of all the devices in the trusted area," explains the China Telecom Corporation Research Institute.

While some equipment vendors have now developed their own C-IWF, these solutions are only compatible with their own network equipment, according to China Telecom, which says its C-IWF is entirely vendor-neutral.



Supporting more than 1,000 private networks in China

China Telecom first tested the C-IWF in 2022, using it to secure the interface with a private 5G network operated by a Xiaomi factory in Beijing. By the end of 2023, China Telecom expects to have deployed the C-IWF in 18 provinces in China, by which time it will be securing the interface with more than 1,000 private 5G networks. Equipped with C-IWF, China Telecom says it is able to deploy private 5G networks on a large scale, accelerating their positive impact on the economy.

China Telecom says the C-IWF has greatly reduced the security risk from 5G private network devices. At the same

time, the C-IWF's authentication function and message monitoring capabilities improve the operator's ability to manage and control network devices. "Ultimately, this high flexibility, security and controllability [means a] 5G private network can meet the needs of both the operator [itself] and vertical industry customers," notes the China Telecom Corporation Research Institute. The telco plans to further expand the capabilities of the C-IWF in line with the ongoing advances in 5G technology.

In time, China Telecom expects every private network's UPF to connect to its C-IWF – it will become a default solution. It also anticipates that the solution will

be adopted by other operators both inside and outside China. "Supported by C-IWF, the 5G vertical industry security solution could enable mobile operators around the world to build a secure boundary to protect their public networks when connecting to a 5G private network," says Wang Qingyang, director of the Institute of Mobile and Terminal Technology in China Telecom Corporation Research Institute. "The mobile operators can then prevent the potential attacks from one private network and make the public network stable for other customers."

Supported by C-IWF, the 5G vertical industry security solution could enable mobile operators around the world to build a secure boundary to protect their public networks when connecting to a 5G private network

Wang Qingyang - Director of the Institute of Mobile and Terminal Technology in China Telecom Corporation Research Institute



By resolving many of the security and interoperability issues associated with private 5G networks, the C-IWF promises to accelerate the adoption of this technology by enterprises. “We have effectively removed one of the major obstacles holding back the wider deployment of private 5G and the private 5G market will be better developed,” adds Fu Zhiren, vice president of China Telecom Corporation Research Institute. “As a result, we believe that enterprise adoption will grow rapidly in 2024 and beyond.”

That could help mobile operators open up a major new B2B revenue stream. GSMA Intelligence estimates that global total revenue from 5G private network deployment will increase from less than US\$10 billion in 2023 to US\$109.4 billion in 2030⁴.

We have effectively removed one of the major obstacles holding back the wider deployment of private 5G and the private 5G market will be better developed

Fu Zhiren - Vice president of China Telecom Corporation Research Institute



⁴ Private 5G Industrial Networks - An analysis of Use Cases and Deployment, GSMA, June, 2023

About the GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

For more information, please visit the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: [@GSMA](https://twitter.com/GSMA).

GSMA 5G Transformation Hub

The GSMA 5G Transformation Hub is a source of information on some of the most innovative 5G solutions in the world. This portal contains case studies detailing design, benefits, key players, measured value and the future impact of scaling up these 5G solutions worldwide. The 5G Era is now firmly established and this family of standardised GSM technologies, including mmWave, are being rolled out successfully across the globe. The GSMA 5G Transformation Hub, launched at MWC Barcelona in 2022, provides details of how 5G is best placed to deliver real value for a range of key sectors including manufacturing, energy, transportation, media and live entertainment, smart cities and construction. Many more case studies will be added, in the coming months, covering even more industries and the GSMA is asking Members to nominate innovative 5G case studies to add to this global digital showcase. The 5G Transformation Hub and this particular Case Study are both sponsored by Qualcomm.

www.gsma.com/5GHub

About this case study

This case study is for information only and is provided as is. The GSM Association makes no representations and gives no warranties or undertakings (express or implied) with respect to the study and does not accept any responsibility for, and hereby disclaims any liability for the accuracy or completeness or timeliness of the information contained in this document. Any use of the study is at the users own risk and the user assumes liability for any third party claims associated with such use.

