Key Considerations for User Management and Roaming in Military Private 5G[*]

Juseoung Lee[*], Donghyun Kum, and Jihoon Choi

Telecommunications Technology Association, Republic of Korea
{jslee, kdh0313, jihoonchoi}@tta.or.kr

Abstract

Globally, defense sectors are increasingly adopting Private 5G (P5G). These networks provide tactical advantages, such as high speed, ultra-low latency, and massive connectivity. However, their deployment scale can result in coverage limitations, which pose challenges for broad-area operations and allied interoperability. This paper proposes 'Roaming' as a key strategy to address these limitations. It analyzes the distinct characteristics of military networks and the resulting technical and policy considerations for user and subscription management.

1 Introduction

Private 5G (P5G) is increasingly utilized in the defense sector to provide secure, customized communication environments within defined areas, such as military bases and operational zones. However, modern warfare is conducted across broad geographical regions under unpredictable conditions. The localized deployment model of P5G makes connecting an entire theatre of operations impractical. To address this gap, this paper first analyzes the distinct characteristics of military networks in terms of connectivity and subscription management. Based on this analysis, it presents key considerations for implementing roaming between P5G networks and onto public networks.

2 Core Military Requirements and Architectural Considerations

Understanding the unique user management characteristics of military networks is a prerequisite for designing a P5G architecture.

1. Identity, Credential, and Access Management (ICAM) Systems: Military forces possess proprietary ICAM frameworks, including unique PKI certificates and identity verification systems[1].
2. Dynamic, Mission-Centric Authorization: Unlike static commercial service plans, military network access rights must be dynamically granted or revoked based on mission parameters, such as time, location, or authorized services.

This fundamental mismatch between said military requirements and the commercial ecosystem necessitates a discrete architectural approach, rather than the mere application of standard technologies. This imperative manifests as the following three key considerations:

[*] Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-39, December 16-18, 2025, Sapporo, Japan.

- **A Sovereign Provisioning System (for subscription management):** The commercial GSMA eSIM ecosystem cannot adequately address stringent military security requirements or proprietary ICAM integration. Therefore, a core consideration must be the establishment of a 'sovereign provisioning system (Non-GSMA)' which places the entire eSIM profile lifecycle under military standards and control. This approach is essential to ensure complete ICAM integration and maximum security sovereignty.

- **Mission-Centric Dynamic Authorization Methods:** Based on this sovereign subscription system, the implementation of 'mission-centric dynamic authorization' must differ by P5G deployment model. In a public network integrated (PNI)-P5G environment, which shares public unified data management (UDM) functions, the military ICAM system can dynamically modify the UDM subscriber profile. Conversely, in a Standalone-P5G environment with an independent 5G Core, a policy control function (PCF)-based policy approach is more suitable and secure: the UDM profile remains static, while the PCF interfaces with the military ICAM to control the access and mobility function and session management function in real-time.

- **The Need for a Military Roaming Hub (MRH):** P5G roaming is essential for wide-area and allied operations, but using commercial IP exchange (IPX) providers as mediators presents distinct limitations. Using commercial IPX risks compromising 'Data Sovereignty' and 'Operational Security' by exposing sensitive military information, such as network identifiers and traffic patterns. Furthermore, commercial IPX cannot validate or enforce the heterogeneous military security requirements specific to each nation. This necessitates a MRH architecture. This MRH must perform both 'a-priori policy verification' of each force's SEPP compliance and 'real-time technical verification' of certificates and algorithms.

3 Conclusion

This paper presented three key considerations for implementing dynamic user management and wide-area roaming in military P5G. First, **eSIM subscription management** must be addressed via a 'Sovereign Provisioning System (non-GSMA)' to ensure full ICAM integration and security sovereignty. Second, **dynamic authorization** demands an evaluation of the trade-offs between UDM profile modification and PCF policy control, based on the P5G deployment model (PNI-P5G vs. standalone-P5G). Third, **the roaming architecture** must consider the establishment of MRH to ensure compliance with and validation of nation-specific security requirements. These considerations provide a foundation for technical and policy decisions in future military P5G architecture planning.

4 Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MIST) (No. R S-2024-00441484, Development of Open Roaming Technology for Private 5G Networks).

References

[1] Department of Defense. Identity, credential, and access management federation framework. Technical Report Version 1.0, Department of Defense, November 2024.