УДК 621.391

А. С. Луцишин[1]
І.А. Самолюк[1]

ОСОБЛИВОСТІ ПЕРВИННОЇ АУТЕНТИФІКАЦІЇ У МЕРЕЖАХ СТАНДАРТУ 5G-NR FR2

[1]Вінницький національний технічний університет

Анотація

Розглянуто первинну аутентифікацію у мобільній мережі стандарту 5G-NR FR2, як один із видів захисту особистих абонентів та ресурсів мережі від несанкціонованих втручань. Проаналізовано алгоритми проходження сигнального обміну через елементи мережі та фунціональні особливості даної процедури.

Ключові слова: 5G, безпека 5G, QoS, первинна аутентифікація.

Abstract

Primary authentication in the mobile network of the 5G-NR FR2 standard is considered, as one of the types of protection of personal subscribers and network resources from unauthorized interference. Algorithms of signal exchange passing through network elements and functional features of this procedure are analyzed.

Keywords: 5G, 5G security, primary authentication, QoS.

Вступ

У мережах 5G введено декілька нових функцій для підвищення безпеки, щоб зробити мобільну систему ще більш захищеною та надійною порівняно з системами попереднього покоління. Оновлена процедура аутентифікації є одним з таких нововведень. Первинна аутентифікація пропонує два механізми: (1) Аутентицікація з обміном ключами (5G AKA) та (2) Розширений протокол аутентифікації (EAP-AKA). Вони вирішують існуючі проблеми безпеки в попередніх системах поколінь. Зокрема, введення процедури «Домашній контроль» коли аутентифікація відбувається в домашній мережі, та концепція прихованого ідентифікатора підписки (SUCI). Найбільш поширеним методом первинної аутентифікації є EAP-AKA, що використовується у більшості сучасних зразків обладнання [1].

Результати дослідження

Процедура первинної аутентифікації на основі EAP-AKA, що включає операції служб AUSF та UDM для доступу 3GPP, показана на рис. 1 [2].

Алгоритм проходження сигнального обміну через елементи мережі:

1) Користувачське обладнання (UE) надсилає повідомлення реєстрації (Registration Request NAS) до служби аутентифікації (SEAF), що містить або SUCI, або ідентифікатор UE 5G (5G-GUTI).

2) Отримавши запит на реєстрацію, SEAF викликає первинну аутентифікацію, відправивши запит на до AUSF. Якщо SEAF має дійсний 5G-GUTI, він відправляє SUPI та повторно аутентифікує UE.

3-4) AUSF перевіряє SNN у запиті. Якщо перевірка успішна, AUSF відправляє запит на отримання аутентифікаційних даних до UDM зі значеннями SUCI та SNN.

5-6) Отримавши SUCI, UDM викликає SIDF для розшифрування її у SUPI. На основі SUPI, UDM/ARPF вибирає метод аутентифікації (5G-AKA або EAP-AKA) і генерує вектор аутентифікації (AV). Для EAP-AKA створюється трансформований AV (AV' [RAND, AUTN, XRES, CK', IK']), відповідь на дані аутентифікації надсилається до AUSF.

7-8) AUSF надсилає виклик аутентифікації (RAND та AUTN) до SEAF. SEAF передає цей виклик до UE разом з ідентифікатором набору ключів (ngKSI) та Anti-Bidding down.

9-10) UE перевіряє свіжість AV. Якщо AUTN дійсний, UE обчислює відповідь (RES) та ключі (CK/IK або CK'/IK'), і відправляє відповідь SEAF у повідомленні Authentication Response NAS з RES.

11) SEAF надсилає відповідь на виклик до AUSF у повідомленні Authentication Request [3].

12–14) AUSF перевіряє відповідь на виклик, і якщо перевірка успішна, AUSF повідомляє UDM про результат аутентифікації як "Успіх".

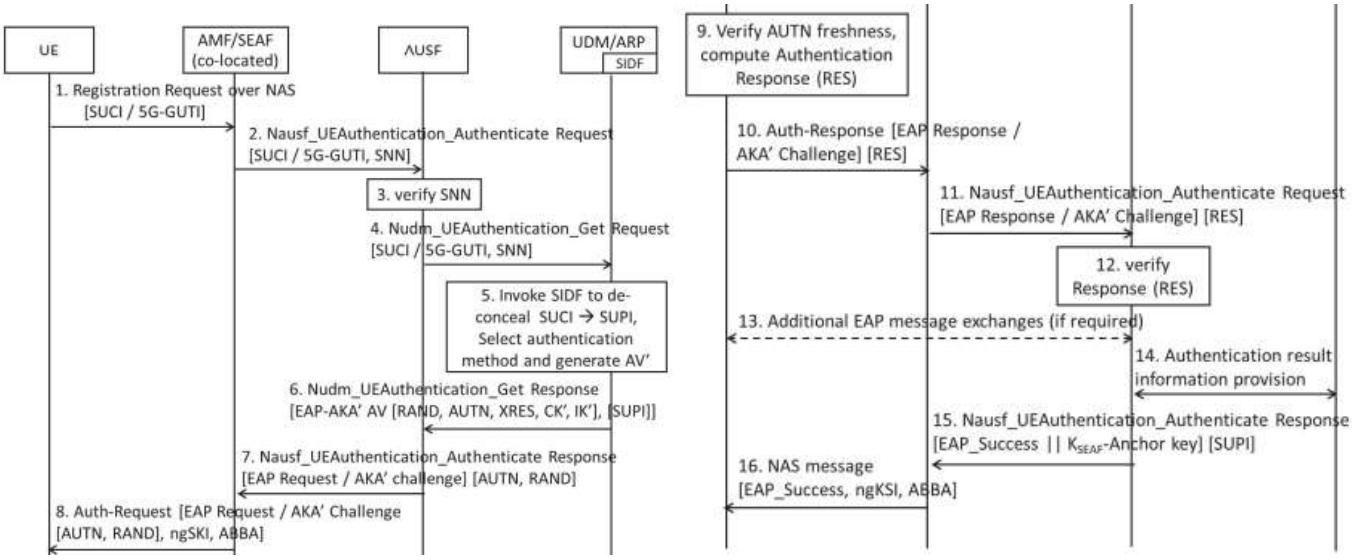

Рисунок 1 – Сигнальний обмін при первинній аутентифікації в 5G-NR FR2

15) AUSF отримує розширений майстер-ключ месії (EMSK) з CK' та IK' (згідно з RFC 5448) та використовує 256 найбільш значущих бітів EMSK як ключ KAUSF, а потім розраховує ключ KSEAF (основний ключ, з якого походять ключі захисту AS та NAS) з KAUSF.

16) SEAF далі генерує KAMF з KSEAF, отриманого від AUSF. Якщо AUSF та SEAF підтверджують успішну аутентифікацію, SEAF надає ngKSI та KAMF AMF. SEAF також надсилає повідомлення EAP Success до UE разом з ngKSI та параметрами ABBA [1].

Висновок

Проведено аналіз процедури первинної ідентифікації в мобільній мережі стандарту 5G-NR FR2 з метою забезпечення безпеки особистих даних абонентів та ресурсів мережі від несанкціонованого доступу. Детально досліджено алгоритми обміну сигналами між складовими елементами мережі та розглянуто функціональні аспекти даної процедури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1) X. Huang, T. Yoshizawa, and S. B. M. Baskaran, "Authentication Mechanisms in the 5G System", JICTS, vol. 9, no. 2, pp. 61–78, May 2021.
2) A. R..Prasad, S. Arumugam, S. B. M. . Baskaran, and A. Zugenmaier, "3GPP 5G Security", JICTS, vol. 6, no. 1-2, pp. 137–158, May 2018.
3) IETF RFC 5448, May 2009, Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)

Луцишин Андрій Станіславович — аспірант, спеціальності 172 - Телекомунікації та радіотехніка, факультет інформаційних електронних систем, ВНТУ, Вінниця, e-mail: lutsishin07@gmail.com

Самолюк Ірина Анатоліївна – аспірант, спеціальності 172 - Телекомунікації та радіотехніка, факультет інформаційних електронних систем, , ВНТУ, Вінниця, e-mail: tkp15b.samoliuk@gmail.com.

Науковий керівник: ***Барась Святослав Тадіонович —*** канд. техн. наук, професор кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, Вінниця, e-mail: barasst03@gmail.com.

Lutsyshyn Andrii S. – postgraduate student, majoring in 172-telecommunications and radio engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: lutsishin07@gmail.com

Samoliuk Iryna A. – postgraduate student, majoring in 172-telecommunications and radio engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: tkp15b.samoliuk@gmail.com.

Supervisor***: Baras Sviatoslav T.*** **—** candidate. Sc., Professor of the Department of Infocommunication Systems and Technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: barasst03@gmail.com.