Roaming Security in 5G Systems*

No Author Given

No Institute Given

Abstract. The Next Generation Critical Communication (NGCC) system in Norway ("Nødnet") will be using mobile systems as its basis. In particular, it appears that Nødnett will be realized as a Home Environment (HE) with its own network functions, but it will not feature the serving network (SN) functions or the radio access network (RAN) part. Thus, the Nødnett system will rely on a roaming agreement with one or multiple existing operators. However, "national roaming" will also be permitted for Nødnett, which means that Nødnett users will be permitted to use other networks if the preferred one is unavailable. Altogether, this means that roaming and roaming security are very important for Nødnett. In this paper, we investigate and evaluate the state of the art of 5G roaming security, and its application to Nødnett. Roaming, in 5G, is conducted over the N32 interface. Thus, we investigate the security of the "Protocol for N32 INterconnect Security" (PRINS) and the use of TLS over the N32 interface. The PRINS protocol also permits so-called IPX operators (roaming brokers) to be part of the exchange, which potentially creates additional problems for the Nødnett use cases.

Keywords: Nødnett · 5G roaming · Security · PRINS · TLS · NGCC · SEPP · N32 interface · IPX

1 Introduction

Public Safety (PS) agencies and organizations including police, fire department, and health services traditionally used long-established closed networks, such as TErrestrial Trunked RAdio (TETRA) which can provide a narrow-band for voice and text-based communications. However, these traditional networks are unable to meet the new requirements of the PS networks, such as picture and video transmission, high-definition video and audio for surveillance, wireless and wearable sensors, and high-speed internet access, not only in the case of the home networks but also in the context of national roaming and especially neighboring countries roaming scenarios. PS providers are focusing on finding ways to implement such infrastructure in collaboration with multiple existing commercial networks to enable maximum availability in case of any public emergency.

As the need for PS has now changed, Fifth Generation Networks (5G) have been

* Research financed by the Norwegian Research Council (NRC). See `sintef.no/en/projects/2021/raksha-5g-security-for-critical-communications`

identified as the enabling technology to fulfill the specific requirements of the PS Networks. The 5G systems incorporate a REST API based "Service Based Architecture (SBA)" as the main core network system signalling scheme. SBA is a web-centric technology, featuring HTTP, JSON, TLS, and OAuth 2.0 in the signaling process[1]. Moreover, in scenarios involving roaming, the N32 interface acts as a bridge between SEPPs (Security Edge Protection Proxy) across diverse PLMNs (Public Land Mobile Network) i.e., also based on the above-mentioned technologies. The main focus of this research is to investigate 5G roaming security challenges in NGCC system. In particular, we investigated the roaming security of TLS and PRINS (Protocol for N32 Interconnect Security) which provides roaming Value Added Services(VAS). Furthermore, we argued that no single roaming method is ideal for Next Generation Nødnett (NGN) scenarios, such as National or global roaming (e.g., with Sweden, Finland). Thus, the choice of roaming techniques should be contingent on the unique requirements of each scenario.

1.1 Motivation - The Norwegian Nødnett Context

In Norway, the public safety network is, as mentioned above, based on TETRA. However, the TETRA-based network was scheduled to be decommissioned in 2026 (there will likely be extensions). It has been decided that the new PS network will be based on the commercial mobile network [1]. That is, it will be using 4G/5G technologies. The Nødnett organization will own and operate the PS-specific services/nodes; the rest of the network is to be provided by agreements with the 4G/5G telecom providers. It is still not known if the Nødnett subscribers will have their own unique Mobile Network Code (MNC) (part if the subscriber identifier) or if Nødnett will have separate HE network functions. If so, the Nødnett subscribers would technically be roaming in the hosting (serving) network.

There will be a main provider, which will be hosting the Nødnett subscribers. Additionally, one will permit, with restrictions, that Nødnett subscribers be roaming onto the other 4G/5G networks if needed. This is called "national roaming", and it is not normally permitted due to commercial competition reasons.

In conclusion, the Nødnett subscribers will depend on roaming functionality. Nødnett subscriber generally need subscriber identity privacy and subscriber location privacy, in addition to data confidentiality. During roaming, these security/privacy services will critically depend on secure roaming data exchange. For 5G, this means that the so-called N32 interface must be properly secured.

1.2 Evolution of Roaming from 1G to 5G

The First Generation (1G) of mobile wireless technology was introduced in 1980s and it was based on analog communication technology and only provided voice services. In the Nordic countries one had the Nordic Mobile Telephone (NMT) 1G

[1] See (In Norwegian) `https://www.nodnett.no/aktuelt/nytt-nodnett/` for details.

system. This system provided analogue speech/audio and digital signalling (Fast Frequency Shift Keying). Interestingly, roaming was included from the inception of the system (it was agreed by the Nordic national incumbent telecom providers in Kabelvåg/Lofoton (Norway) in 1969[2]. Roaming signalling was by means of an SS7 protocol called Mobile User Part (MUP). There were no security measures for either SS7 as such or MUP itself. The NMT system, while permitting use of modems, did not natively support data transmission.

The all-digital 2G system Global Systems for Communication (GSM) was designed form the onset to support data. GSM also introduced the Mobile Application Part (MAP) system signalling protocol, which provided system signaling (including roaming services). Most importantly, the GSM roaming standard introduced the SIM card and the International Mobile Subscriber Identity (IMSI) numbers which still play a critical role in enabling roaming including 2G/3G/4G and 5G technologies. Table 1. presents the protocols and technologies used for roaming from 1G to 5G.

Table 1. Roaming technology evolution[3]

2G	3G	4G	5G
1. SS7-MAP Protocol; No security in SS7.	1. SS7-MAP Protocol or Diameter Protocol for PS;	1. Diameter Protocol	1. Transport Protocol: HTTP/2 2. Serialization Protocol: JSON and JOSE 3. Security Protocol: PRINS, IPsec / TLS

1.3 A Historical Account of Roaming Security

Back in the early times of 2G/GSM, GSM was predominantly an European-only system. At the time, there were commonly very few operators per country. Typically, one have the incumbent operator (mobile and fixed network) and one or two competitor (mobile network). Thus, the overall number of operators were fairly small. This gradually changed, and the number of networks rose with GSM being adopted outside Europe and with with the introduction of virtual home operators (these does not own or operate a serving network).

Initially, handling roaming contracts were therefore quite manageable, but as the number of operators grew it soon became logistically complex. Most operators therefore tend to only have direct roaming agreements with a few select operators. The rest are handled by a roaming broker. A roaming broker is then an intermediate network which mediates the roaming process. When data us-

age became more common, the roaming broker also provided the data roaming services[2].

Originally, the GSM Association (GSMA) defined the GPRS Roaming Exchange (GRX) functionality for the 2G GPRS data network technology. Subsequently, this became the IP Exchange (IPX). The GSM Association has published various guidelines for GRX/IPX, which also includes security advise [4]. Despite this, the track record concerning security for GRX/IPX has not been very good.

A big part of this has to do with the total lack of security for SS7-based protocols [5,6]. Technically, it is therefore very challenging to "fix" the security for SS7-based protocols like the MAP protocol. It is also in practice impossible to enforce requirements to invest in dedicated systems that to provide bump-in-the-wire across nation-state boundaries (and thus jurisdictional and legal boundaries). There would be few business incentives to do so, and one would face problems satisfying lawful interception (LI) requirements, etc.

In theory, using Diameter as the roaming protocol framework, would facilitate a technical solution. That is, one may easily deploy IPsec as the security for Diameter-based applications [7][3], and this was a solution outlined in the Diameter specifications. However, the arrangement of IPX brokers as intermediates, are at odds with providing end-to-end security. One may have had hop-by-hop security, but there is little evidence to suggest that this has been attractive to operators. Thus, in reality, one cannot ensure or assume the Diameter-based roaming application have credible security protection in place for roaming cases. Consequently, it is to be expected that vulnerabilities have been reported [8,9,10].

1.4 The SEPP and N32 Interface for 5G Roaming

5G architecture integrated SEPP to secure outgoing HTTP/2 signaling at the edge of the PLMN, ensuring authentication, integrity, and confidentiality of HTTP/2 signaling over the N32 interface [11]. Consequently, to facilitate national and international roaming the N32 interface connects SEPP servers of different PLMNs [12]. One other responsibility SEPP has is to filter out malicious incoming HTTP/2 messages. The N32 interface consists of 2 different interfaces i.e., N32-c and N32-f where N32-c is a control plane interface and N32-f is a forwarding interface between the SEPPs. N32-f interface is responsible for forwarding the HTTP/2 messages between Network Functions (NF) services after applying for application-level security protection. Although Application layer security protection offered by N32-f is applicable only in the presence of negotiated PRINS between operators, TS 29.573 section 4.2 [13]. Such forwarding can help to secure the communication where IPXs are involved. Thus, PRINS allows certain field modifications to the intermediary operators which poses high

[2] It has been common to route traffic back to the home network. Thus, with data roaming, there was a need to facilitate this in an efficient way.

[3] This was the baseline when 3GPP introduced Diameter. Today, with RFC 6733, the advice is for TLS (or DTLS/SCTP).

risk for NGCC security. While ensuring application layer protection, in roaming scenarios involving IPXs, certain modifications are necessary for efficient routing and VAS which could only be achieved by utilizing the PRINS protocol. Consequently, if the TLS is the selected security policy between the SEPPs, the N32-f role is limited to forwarding HTTP/2 messages. By implementing the HTTP/2 protocol the N32 interfaces employ JSON as the application layer serialization protocol, TS 29.573 section 4.3 [13].
TLS enables end-to-end protection and prevents modifications at IPXs while roaming. However, this can lead to a loss of flexibility and control in roaming scenarios due to the increased number of roaming connections and IPXs. Nevertheless, TLS implementation is less complex and require minimal efforts for mobile operators as compared to PRINS. In addition, TLS could also fulfil the security requirements of Nødnett due to it's fully encrypted security mechanism. TLS deployment has been illustrated in Fig.1.

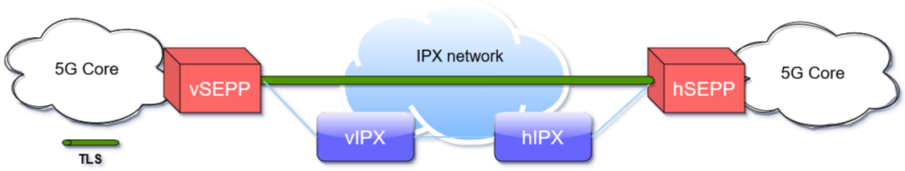

Fig. 1. Direct TLS deployment modal for 5G roaming

2 Protocol for N32 Interconnect Security (PRINS)

The Primary objective of the PRINS model is to provide confidentiality and integrity of sensitive information during their roaming via multiple IPXs. Secondly, it should allow signaling modifications between PLMNs. In addition, it should ensure traceability of any potential change or modifications of signalling between multiple PLMNs. PRINS combines N32-c and N32-f to provide Transport and application-level protection. According to 3GPP TS 33.501, Fig.2. illustrates the PRINS model, which facilitates 5G roaming.
N32-f requires implementation of Direct TLS for end-to-end roaming without IPXs, while PRINS should employ where traffic has to pass via IPXs. By utilizing PRINS, end-to-end security could be achieved at the application layer on top of TLS, ensuring hop-by-hop security for IPXs at the transport layer, as demonstrated in Fig.3. In contrast, PRINS utilizes Java Web Encryption (JWE) with Java Web Signatures (JWS) for application layer protection. However, giving more control to IPXs over PRINS may introduce multiple challenges for Next generation Nødnett :

– Each MNO may have distinct protection policies.

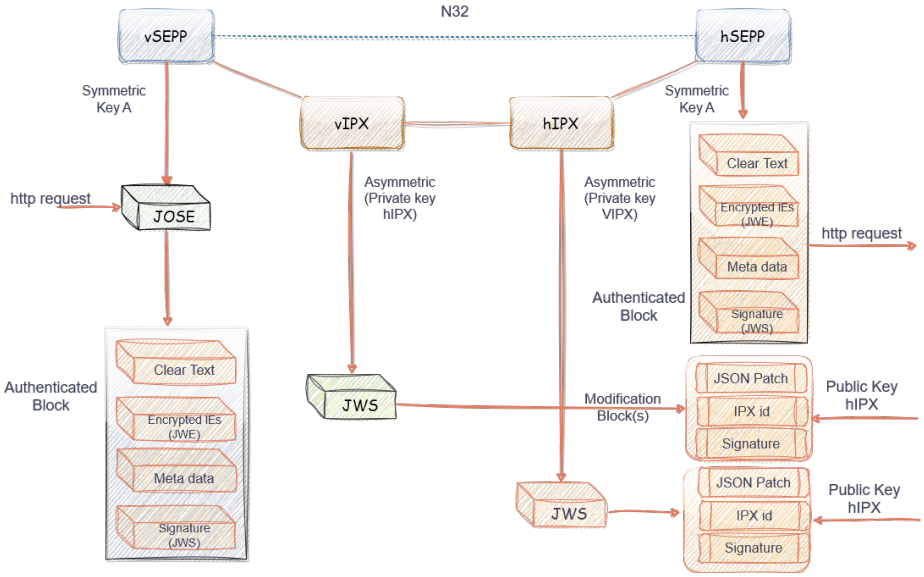

Fig. 2. PRINS modal for 5G roaming[14]

- Operators are required to keep track of which intermediary IPX is permitted to modify the messages and public keys of these IPXs.
- The terms of the roaming agreement could be different from partner to partner.

3 Next Generation Nødnett(NGN) Roaming Requirements

When it comes to NGN implementation, there are several questions that should be investigated, notably the allocation of responsibilities between governmental bodies and commercial operators. Following are the certain requirements in context of roaming and its security that should be investigated before implementing NGN:

- Full spectrum coverage even within tunnels, air-to-ground connectivity (for helicopters), remote areas, ensuring availability during major incidents or weather circumstances.
- Ensuring data security and protection against malicious threats.
- The solution must ensure the security of signalling messages from any potential manipulation,tampering or intrusions by attackers. In addition, authenticity and integrity should be ensured.
- Verification of the source network's legitimacy, which transmitted the signalling message should be traceable.

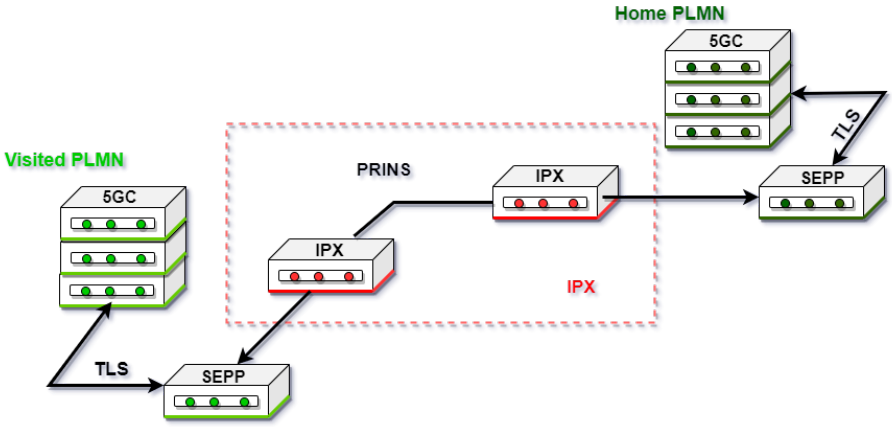

Fig. 3. Securing 5G control plane using PRINS

- It is important to consider operational aspects of key management especially where intermediaries are involved.
- Ensuring the secure management of cryptographic data, involving SEPP peers and IPX providers.
- All of the services should be revoked and all data should be removed once the assigned role of intermediary IPX has been fulfilled.
- Anonymity should be ensured for the user (Police, Ambulance etc.), and their actions should remain non-traceable from attackers. This non-traceability prevents adversaries from connecting a user's communication activities and forming fake user's profile.

4 Potential Security Challenges Impacting NGN Roaming Implementation

Before diving into the details of roaming security challenges we mentioned two roaming deployment models for the sake of simplicity, which will be referred to later as case 1 or case 2:
Case 1: NGN-PRINS deployment Modal: Where certain signaling modifications are allowed between PLMNs via multiple IPXs.
Case 2:NGN-TLS deployment Modal: Where modifications are not allowed in between IPXs to ensure end-to-end protection.

HTTPs/2 security SEPP enables authentication, confidentiality, and integrity by encrypting HTTP/2 messages in non-roaming and roaming scenarios. HTTP/2 facilitates concurrent requests and responses over a single TCP connection for both client and server[1]. Hence, the adoption of HTTP/2 introduced a set of security challenges inherited from its architecture.

Stream multiplexing The stream multiplexing feature in HTTP/2 enables multiple streams to be transmitted over a single TCP connection, which can help in reducing network overhead. Over the N32 interface where PRINS is used (case 1), HTTP/2 protocol's SETTINGS-MAX-CONCURRENT-STREAMS allows control of overactive streams, with a suggested minimum of 100 for optimal multiplexing benefits. There's no upper limit, but it can be set up to 2,147,483,647 Streams [15]. However, the attacker can take advantage of this and can exploit the stream multitasking feature by sending computationally intensive requests over the N32 interface, such as APIs, by creating up to 2,147,483,647 streams to the NFp. The attackers can then launch the DOS attack by replicating it across multiple TCP connections, which may potentially disrupt availability of NGN while roaming. Conversely, in case 2 signaling over N32 is fully encrypted via TLS, therefore, it becomes hard for an attacker to make changes over the N32 interface. Meanwhile, when multiple IPXs are involved in national and global roaming, successful signaling transmissions cannot be guaranteed due to the lack of necessary modifications.

Flow control Flow control aimed to avoid interfacing between streams sharing same TCP connections. This feature uses various parameters including WINDOW-UPDATE frame and the SETTINGS frame, this feature determines the data limit that a sender can transmit to the receiver. However, this flexibility can be exploited by malicious receivers in case 1, such as NFC in 5G to launch on the NFP. The attackers can achieve this goal by sending tiny data transmissions using the WINDOW-UPDATE frame on the NFp, which keeps its resources occupied [16]. To prevent such attacks in 5G network, it is important to impose time restrictions for each NFP request. However, in case 2, due to encrypted signalling feature it will become even harder for the attacker to compromise flow control field.

Enforcing TLS upgraded versions TLS deployment modal could be adopted for providing integrity, confidentiality and replay protection while roaming[12]. Enforcing TLS could be most optimal solution for providing protection, however, upgraded versions of TLS (TLS 1.2, TLS 1.3) have not been enforced by the standard and it has been left for the operators to decide TLS version (TLS 1.2, TLS 1.3) based on their security requirements and the compatibility of their network infrastructure. As of today, TLS version 1.3, has been implemented, effectively mitigating critical vulnerabilities that were present in TLS 1.2 such as MITM attack, downgrades attacks[17]. To this end, TLS 1.3 provided a mechanism to protect against downgrade attacks. Consequently, it becomes crucial to enforce the adoption of TLS 1.3 by all the mobile operators involved, ensuring the security of Nødnett over N32 interface while roaming.

Complex PKI infrastructure The standard method for internetwork is really not specified by Specs but it can be used for Ncom it will be ok to use Oauth and agreement with roaming partners.

JSON Object Signing and Encryption (JOSE) JOSE comprises a set of JSON Web algorithms (JWA), JSON Web Encryption (JWE), JSON Web Signatures (JWS), and JSON Web Token (JWT), forming a set of standards that employ JSON-based data structures for data signing and encryption. JWE is used by SEPPs to protect messages on the N32-f interface, while JWS,are utilized by IPX providers to sign the necessary modifications for their mediation services. In the context of case 1 (PRINS deployment modal) the N32-f interface facilitates the exchange of JOSE protected HTTP/2 messages between two SEPPs. However, identified protection policy may necessitate message reformatting and some field alteration, particularly in cases involving PLMNs and IPX providers [18]. Attackers may take advantage of this reformatting/field alteration feature and can manipulate message as per their desire to launch attacks.
Conversely, forwarding of the HTTP/2 messages between SEPPs could be done without any reformatting or message alteration, when TLS deployment modal is the negotiated security measure. However, we can loose flexibility when there are too many IPXs are involved.

Policy handling by SEPP The SEPPs are responsible for enforcing protection policies to provide integrity and confidentiality at the application layer. However, The utilization of PRINS permits VAS and IPX providers to intervene at the application layer and do modifications based on the security policy of the roaming agreement[13]. Therefore, if a security policy has not been properly designed and agreed upon between roaming partners, IPXs may become able to modify the content of messages. This can result in message tempering, which can have serious outcomes for the integrity and authenticity of the transmitted data.

Too complex PRINS requirements When diving into the real-time implementation of PRINS protocols there could be multiple problems that MNOs can face. Hence, making it too complex for the implementation. Challenges that MNOs can face during PRINS implementation are as follows:

- Verifying modifications made by IPX carriers could be very complex for the terminating operators. In addition, multiple IPX carriers can do modifications in their own way which could become even more complex for the terminal operators to verify these modifications.
- hSEPP has no control over modifications and their perpetrators. As a result, PRINS opens up possibilities for attacks like Man-In-The-Middle (MITM).
- The negotiating process of protection policy contracts between MNOs and roaming partners is a considerable challenge, particularly when it comes to subsequent policy updates.
- As TLS and PRINS are non-compatible roaming deployment strategies and hPLMN and vPLMN should be on the same page for smooth roaming [19]. This selection process introduces considerable intricacies into the negotiation and operational establishment of global roaming.

5 Considerations for NGN Implementation in Norway

Norwegian Directorate for Civil Protection (DSB) has initiated a dialogue with key players in the market, including MCX (Mission Critical Services) system suppliers, mobile operators, and various service providers, seeking their input regarding a potential MCX services solution within the emerging emergency network [20]. Therefore, it has been decided and announced by DSB that commercial mobile operators are responsible for delivering coverage and core networks. Furthermore, the implementation of NGN, will rely on 5G and its subsequent generations[21].
In the context of 5G, for a strong roaming security posture following measures should be considered before implementing NGN roaming functionality:

- As NGN is set to roll out in collaboration with a specific group of Norwegian mobile operators, TLS implementation could be mandated by the Norwegian government for providing end-to-end protection. This preference for TLS over PRINS could stem because it has become the de-facto standard protocol for secure communication in technologies such as HTTP, JSON, IPsec, OAUTH 2.0, web services and APIs. [13]. Despite PRINS, TLS deployment also prevent intermediary operators to do modifications, for that reason, with a limited number of operators it could be a better solution for roaming.
- Implementing TLS 1.3 (i.e., latest version as of today) should be mandated for mobile operators to provide maximum security for critical communications.
- In global roaming with multiple operators/IPXs, TLS may not be mandated. TLS implementation could impact the availability of the network and Nødnett may loose flexibility when roaming within neighbouring countries (Sweden, Finland). In addition, providing additional control to IPXs leads to increased attack vector due to it's complex requirements.
- Enforce industry approved and non-depreciated secure versions of protocols, APIs and key management mechanisms.
- Implement Zero Trust Architecture (ZTA) for authenticating intermediaries. Recommended security controls such as continuous monitoring and logging should be performed in addition to the risk-analysis.
- All of the related mobile operators should agree upon a single security policy that is desired by DSB, Ncom for NGCC roaming purpose.
- Authentication and Authorization mechanism should be strongly protected for the verification of the source network's legitimacy. For this reason, OAUTH 2.0 can also be utilized to add extra layer of protection over NGN N32 roaming interface, however, it has not been mandated in 3GPP standard.

6 Conclusion

The ever-expanding demand for video, voice and audio services for NGCC, means that only the 3GPP-based networks (4G/5G) can provide the services required.

However, NGN has multiple security requirements, including roaming security, that are different from the ordinary mobile phone provisions. This paper analyzed and investigated 5G roaming security requirements and considerations over N32 interface. N32 roaming could be provided by using TLS or PRINS protocol, however, each has it's own limitations.

While a PRINS solution probably can be made to be relatively secure, it is not a given thing.

The fact that it is designed to cater for IPX intermediates will make it challenging proposition to ensure that sufficient security is attained. Use of TLS is advised/required for SBA internally within the core network of a operator domain. It is also permitted for use over N32. From a security point of view, this is certainly a better and safer choice. And, whats more, it should be fully possible to have this for the national case. That is, the national regulatory and/or the NGCC network owner may require use of TLS for N32 for the main service provider. It should also be fully manageable to require this for the national roaming cases. There are few physical networks and thus the number of roaming agreement that must cater to a TLS-for-N32 will be low.

Along the national borders, the NGCC users will need support even when crossing the national borders. Neighboring countries, like Norway and Sweden, require a long traditions (and agreements) for allowing this. Thus, it would be beneficial if TLS could be used to these roaming cases as well.

What use of TLS by itself will not solve, is the policy/access control handling of the message exchange. It seems certainly the case that the NGCC SEPP must handled this. Technically, one may even provide SEPP base filtering (with it's own well-defined policy rules) or one could handle this by means of OAuth delegation. That would require additional agreements.

In the end, we recommend that TLS is used for N32 roaming for all national roaming and for international roaming if permitted. In particular we strongly advocate that it be required or all national cases. Security policies and access control must be fully defined for roaming cases. We have here only highlighted the problem, but suffice to say that this must be investigated further.

References

1. Nathalie Wehbe, Hyame Assem Alameddine, Makan Pourzandi, Elias Bou-Harb, and Chadi Assi. A security assessment of http/2 usage in 5g service-based architecture. *IEEE Communications Magazine*, 61(1):48–54, 2022.
2. Heikki Ahava. The standardization of mobile systems from nmt to mobile internet. In *History of Nordic Computing 4: 4th IFIP WG 9.7 Conference, HiNC 4, Copenhagen, Denmark, August 13-15, 2014, Revised Selected Papers 4*, pages 171–180. Springer, 2015.
3. GSMA. 5GS Roaming Guidelines, Version 4.0,28 May 2021. `https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v4.0.pdf`.
4. GSM Association et al. Guidelines for ipx provider networks (previously inter-service provider ip backbone guidelines). *Version*, 9:13, 2013.
5. Sergey Puzankov. Stealthy ss7 attacks. *Journal of ICT Standardization*, pages 39–52, 2017.

6. Luiza Odete H de Carvalho Macedo and Miguel Elias M Campista. Attacks to mobile networks using ss7 vulnerabilities: a real traffic analysis. *Telecommunication Systems*, pages 1–13, 2023.
7. P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko. RFC 3588: Diamter Base Protocol. `https://www.rfc-editor.org/rfc/rfc3588`, 09 2003.
8. Isha Singh, Silke Holtmanns, and Raimo Kantola. Roaming interface signaling security for lte networks. In *International Conference on Security for Information Technology and Communications*, pages 204–217. Springer, 2018.
9. Silke Holtmanns, Siddharth Prakash Rao, and Ian Oliver. User location tracking attacks for lte networks using the interworking functionality. In *2016 IFIP Networking conference (IFIP Networking) and workshops*, pages 315–322. IEEE, 2016.
10. Silke Holtmanns, Yoan Miche, and Ian Oliver. Subscriber profile extraction and modification via diameter interconnection. In *Network and System Security: 11th International Conference, NSS 2017, Helsinki, Finland, August 21–23, 2017, Proceedings 11*, pages 585–594. Springer, 2017.
11. Sławomir Kukliński, Krzysztof Szczypiorski, Konrad Wrona, and Jedrzej Bieniasz. 5g-enabled defence-in-depth for multi-domain operations. In *MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM)*, pages 1024–1029. IEEE, 2022.
12. 3GPP TS 33.501. Security architecture and procedures for 5G system, Release 18. `https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/`, 2023. [Accessed 07-09-2023].
13. 3GPP TS 29.573. Technical specification group core network and terminals; 5g system; public land mobile network (plmn) interconnection; stage 3 (Release 18) — 3gpp.org. `https://www.3gpp.org/ftp/Specs/archive/29_series/29.573/`. [Accessed 07-09-2023].
14. GSMA. Report 5g mobile roaming revisited (5gmrr) phase 1, version 1.0. `https://www.gsma.com/newsroom/wp-content/uploads/NG.132-v2.0-1.pdf`. [Accessed 07-09-2023].
15. Mike Belshe, Roberto Peon, and Martin Thomson. Hypertext transfer protocol version 2 (HTTP/2). Technical report, 2015.
16. Amit Praseed and P Santhi Thilagam. Multiplexed asymmetric attacks: Next-generation ddos on HTTP/2 servers. *IEEE Transactions on Information Forensics and Security*, 15:1790–1800, 2019.
17. Hyunwoo Lee, Doowon Kim, and Yonghwi Kwon. Tls 1.3 in practice: How TLS 1.3 contributes to the internet. In *Proceedings of the Web Conference 2021*, pages 70–79, 2021.
18. 3GPP TS 29.573. 5G system; public land mobile network (plmn) interconnection (release 18). `https://www.3gpp.org/ftp/Specs/archive/29_series/29.573/`. [Accessed 07-09-2023].
19. Anushka Bishen. Security for 5g. 5g americas — 5gamericas.org. `https://www.5gamericas.org/security-for-5g/`. [Accessed 07-09-2023].
20. DSB Nødnett. Dsb ønsker markedsdialog om nytt nødnet. `https://www.nodnett.no/aktuelt/rfi/`.
21. DSB Nødnett. Viktig beslutning om nytt nødnett. `https://www.nodnett.no/aktuelt/nytt-nodnett/`.