Formal Verification of the PRINS: Secure Application Layer Protection for 5G Roaming*

Taeho Won, Bonam Kim, and Ilsun You†

Kookmin University, Seoul, Republic of Korea
{xoghdnjs12,kimbona,isyou}@kookmin.ac.kr

Abstract

The rapid expansion of 5G roaming highlights the importance of secure authentication and data protection across inter-PLMN communications. This study formally verifies PRINS (PRotocol for N32 INterconnect Security), which introduces a policy-based layer above TLS in the N32-c interface to strengthen application-layer security. Using ProVerif, we analyzed PRINS with respect to secrecy, integrity, and correspondence properties. The model abstracts key cryptographic functions, including JWE, JWS, and the TLS exporter. The verification results confirm confidentiality, consistent key derivation between SEPP entities, and message integrity across IPX nodes. One correspondence query returned false due to intentional message ordering rather than a security flaw. Overall, PRINS satisfies core security properties but still relies on TLS, suggesting further analysis in 6G roaming environments. Future work should also quantify how misuse of the TLS exporter may impact PRINS's upper-layer security.

Keywords: Formal Verification, 5G, Roaming, ProVerif

1 Introduction

The fifth-generation (5G) mobile network, characterized by ultra-low latency, ultra-high throughput, and massive connectivity, has rapidly expanded across diverse industrial domains such as smart factories, autonomous driving, and remote healthcare, all of which require real-time and reliable data transmission[1]. In such environments, seamless service continuity through roaming among different Public Land Mobile Networks (PLMNs) has become indispensable[2]. However, during the roaming process, signaling and data exchanges between operators are routed through external networks, where conventional Transport Layer Security (TLS) encryption alone is insufficient to fully mitigate threats such as policy violations, message tampering, and replay attacks at the application layer.

According to 3GPP TS 33.501[3], the Security Edge Protection Proxy (SEPP) is responsible for securing inter-PLMN communications over the N32 interface by establishing mutually authenticated TLS sessions. Nevertheless, this protection remains confined to the transport layer. TLS ensures confidentiality of transmitted data but does not guarantee that inter-PLMN signaling messages are policy-compliant or verifiable by higher-layer entities.

To address these limitations, this study introduces the Protocol for N32 Interconnect Security (PRINS), which enhances application-layer protection by adding a policy-driven layer above the TLS session within the N32-c interface. PRINS employs JSON Web Signature (JWS)[4] and JSON Web Encryption (JWE)[5] to ensure message-level authentication, integrity, and confidentiality. To verify its security, we formally analyze PRINS using the ProVerif[6] tool, focusing on the properties of secrecy, integrity, and freshness.

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. W2, December 16-18, 2025, Sapporo , Japan.

†Corresponding author

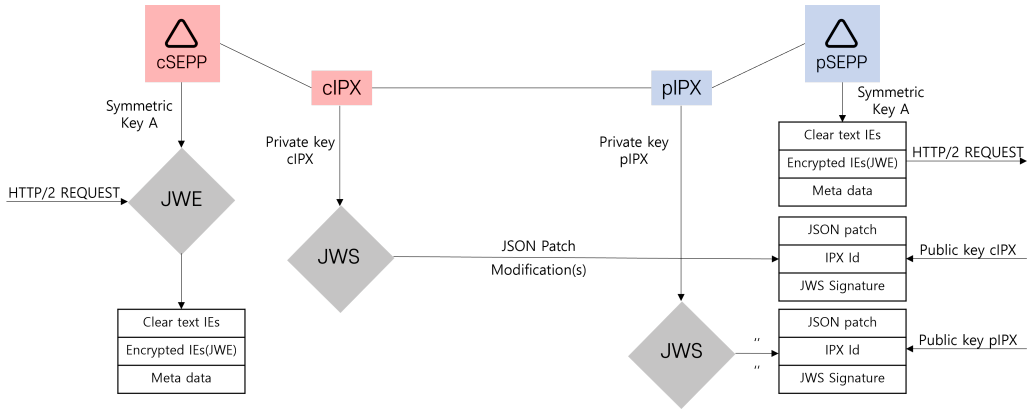

Figure 1: Architecture and Operational Flow of PRINS

2 Background

2.1 5G Roaming

In 5G roaming, communication between operators is handled by the SEPP, a network function defined by 3GPP to secure inter-PLMN signaling through the N32 interface. During roaming, home and visited SEPPs exchange authentication and policy information over secure channels established by TLS[7].

When SEPPs communicate directly, TLS provides confidentiality and integrity at the transport layer. However, inter-operator connections often traverse one or more intermediate IP Exchange (IPX) providers that relay signaling data between SEPPs. In a conventional end-to-end TLS configuration, IPX nodes can only forward encrypted data and cannot access or modify its contents.

In some cases, IPX providers may need limited visibility into certain non-sensitive message fields for routing optimization, traffic prioritization, or policy enforcement. Because full end-to-end TLS prevents such operations, an additional mechanism is required to allow controlled access while maintaining end-to-end security. To address this, the PRINS protocol was introduced to operate above TLS, enabling selective visibility and policy-based integrity verification. The detailed mechanisms of PRINS are described in the following subsection.

2.2 PRINS

PRINS provides enhanced application-layer protection for signaling exchanges between SEPPs in 5G roaming environments. While TLS secures data transmission at the transport layer, PRINS introduces a policy-based protection layer above TLS that ensures message integrity, authenticity, and verifiability across multiple network domains.

The overall parameter exchange and key derivation flow of PRINS is illustrated in Figure 2. The core structure of PRINS combines JWS and JWE to secure signaling messages exchanged over the N32-c interface. Each SEPP converts signaling data into JSON format, applies a digital signature using JWS, and then encrypts the signed payload using JWE. This layered protection guarantees authenticity, integrity, and confidentiality simultaneously.

For message authentication, PRINS uses the Edwards-curve Digital Signature Algorithm (Ed25519) to sign outgoing messages. Depending on configured policies, an intermediate IPX node may be authorized to verify JWS signatures for specific fields while encrypted payloads

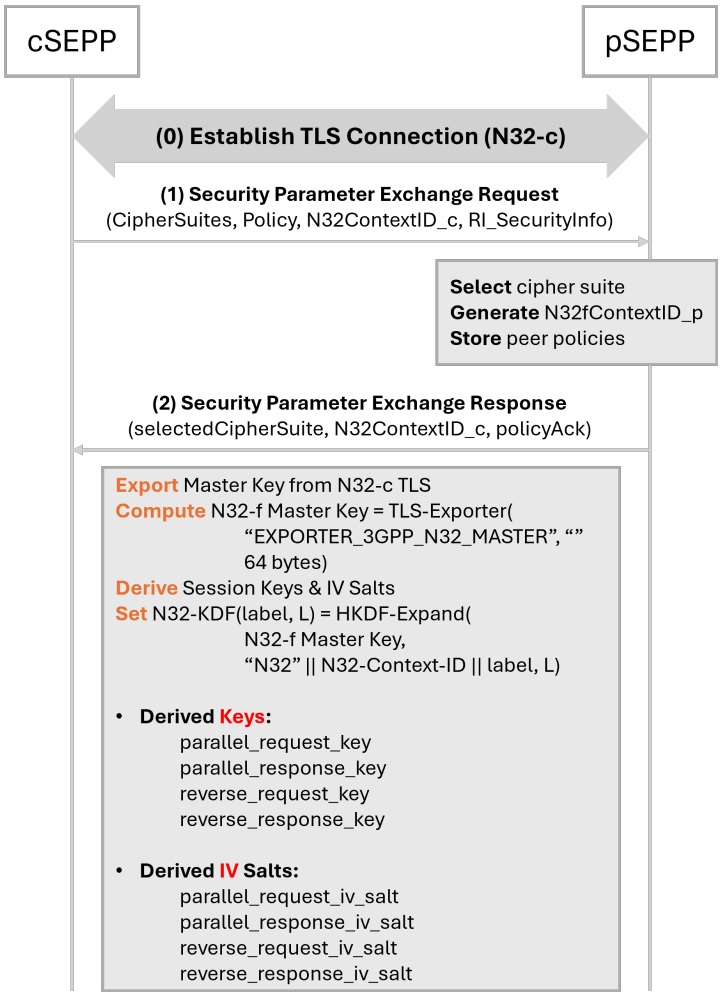

Figure 2: Parameter Exchange and Key Derivation Procedure for PRINS

remain hidden. For encryption, PRINS applies the Advanced Encryption Standard in Galois/-Counter Mode (AES-GCM) with either 128-bit or 256-bit keys, derived from the N32-c TLS exporter. The GCM mode provides authenticated encryption by generating an integrity tag that enables immediate detection of any message tampering.

This architecture allows PRINS to support secure and policy-aware message handling in multi-hop environments. IPX nodes can process only authorized metadata (such as routing headers) while sensitive information remains protected. Each PRINS message also includes a policy identifier and an integrity verification tag defining which entities can access or modify specific data fields. In this way, PRINS offers partial visibility and verifiable control that pure TLS cannot provide, achieving a balance between security assurance and operational efficiency.

2.3 ProVerif

ProVerif is an automated formal verification tool that evaluates the security of communication protocols within the symbolic model. It abstracts cryptographic operations as mathematical

functions and uses process algebra derived from the applied pi-calculus to simulate all possible message flows between honest entities and adversaries. This allows verification of whether a protocol preserves confidentiality, integrity, and authentication properties at a design level, without relying on implementation details.

A ProVerif model generally consists of three parts: declarations, processes, and queries. Declarations define cryptographic primitives such as symmetric and asymmetric encryption, hash functions, and digital signatures. The process section models the behavior of each protocol participant, including message exchange and key derivation. The query section specifies security goals to verify, such as:

- Secrecy: confirming that a key or message cannot be learned by an attacker.
- Integrity: ensuring that a received message originated from a legitimate participant.
- Correspondence: checking causal consistency between protocol events, for example `event(A) ==> event(B)`.

In the PRINS verification model, ProVerif abstracts key cryptographic components such as the TLS exporter, JWS signing, and JWE encryption. Events are used to record major protocol steps, including message generation, forwarding through the IPX node, and validation at the peer SEPP. Queries are defined to evaluate whether the derived session keys and message integrity are consistent and whether confidential data remains protected from adversarial disclosure.

Through this modeling approach, ProVerif enables systematic verification of the PRINS protocol under adversarial conditions in the N32-c interface, ensuring that the protocol's logical security guarantees hold beyond implementation-level assumptions.

3 Formal Verification of the PRINS

This section presents the formal verification of the PRINS protocol using the ProVerif tool. The goal of the verification is to prove that the proposed policy-based layer above TLS preserves confidentiality, integrity, and event correspondence in the N32-c interface even when intermediate IPX entities participate in message forwarding.

3.1 Overview of the Verification Model

The ProVerif model represents the PRINS protocol as a set of communicating processes that capture the essential message exchanges between the core entities: the client SEPP (cSEPP), two intermediate IPX nodes (cIPX and pIPX), and the peer SEPP (pSEPP). Each process abstracts the behavior of its counterpart in the actual protocol. The overall structure follows the secure handshake and data protection sequence as defined in 3GPP TS 33.501, but is simplified to focus on key derivation and message integrity verification.

- **cSEPP**: initiates the handshake, selects cipher suites and policy, derives the session key using HKDF functions and the TLS exporter, encrypts the payload with JWE, and transmits it to the IPX network.
- **cIPX / pIPX**: act as intermediate IPX relays. Each node adds its own signed forwarding block using JWS to ensure that message integrity is verifiable along the multi-hop path.

- **pSEPP**: receives the final message, verifies both JWS signatures, decrypts the JWE payload, and confirms session key derivation consistency.

The model includes event markers such as `csepp_payload`, `cipx_forward`, `pipx_forward`, `payload_delivered`, `derived_cSEPP`, and `derived_pSEPP` to record critical protocol stages. Each event corresponds to a significant security-relevant operation, enabling ProVerif to reason about correspondence and secrecy relationships.

The TLS handshake itself is abstracted by the function `tlsExporter(masterSessionKey, label, context)`, which yields the derived N32-f master key shared between both SEPPs. Cryptographic functions such as `hkdfExtract`, `hkdfExpand`, `jws_sign`, `jws_verify`, `jwe_enc`, and `jwe_dec` are modeled symbolically with their correctness defined through reduction rules. The Dolev-Yao attacker is assumed to have full control over public channels but not over the private TLS exporter or signing keys.

3.2 Security Properties and Queries

To evaluate the logical security of PRINS, six security queries were defined in the ProVerif model. They correspond to the main design goals: key agreement consistency, message integrity, path verification across IPX nodes, and secrecy of the SEPP internal value.

1. **Secrecy:** `query attacker(seppSecret)` tests whether the internal cSEPP secret is ever revealed to the attacker.
2. **Key Correspondence:** `event(derived_cSEPP(k, ctx)) ==> event(derived_pSEPP(k, ctx))` verifies that the key derived by cSEPP corresponds to that derived by pSEPP.
3. **Reverse Key Dependency:** `event(derived_pSEPP(k, ctx)) ==> event(derived_cSEPP(k, ctx))` confirms the causal order of key derivation events.
4. **IPX Forwarding Order:** `inj-event(pipx_forward(ctx)) ==> inj-event(cipx_forward(ctx))` checks whether pIPX forwarding occurs only after cIPX forwarding.
5. **Payload Delivery Integrity:** `inj-event(payload_delivered(payload, ctx)) ==> inj-event(csepp_payload(payload, ctx))` ensures that a payload decrypted at pSEPP was indeed generated by cSEPP.
6. **Multi-hop Validation:** `inj-event(payload_delivered(payload, ctx)) ==> inj-event(pipx_forward(ctx))` guarantees that all delivered messages passed through the final IPX node.

Each query targets a distinct aspect of PRINS: (1) secrecy, (2) and (3) key agreement correspondence, (4) forwarding order across IPX nodes, (5) end-to-end payload integrity and source authenticity, and (6) multi-hop path enforcement.

3.3 Verification Results

The ProVerif results are presented in Figure 3, and the corresponding detailed analysis is summarized in Table 1. All secrecy and correspondence queries were successfully verified except for one reverse key correspondence query, which returned `false` due to the intentional order of

```
Verification summary:
Query not attacker(seppSecret[]) is true.
Query event(derived_cSEPP(k,ctx_3)) ==> event(derived_pSEPP(k,ctx_3)) is true.
Query event(derived_pSEPP(k,ctx_3)) ==> event(derived_cSEPP(k,ctx_3)) is false.
Query inj-event(pipx_forward(ctx_3)) ==> inj-event(cipx_forward(ctx_3)) is true.
Query inj-event(payload_delivered(payload_2,ctx_3)) ==> inj-event(csepp_payload(payload_2,ctx_3)) is true.
Query inj-event(payload_delivered(payload_2,ctx_3)) ==> inj-event(pipx_forward(ctx_3)) is true.
```

Figure 3: Summary of ProVerif query results for PRINS.

operations between the client and peer SEPP. This behavior is not a flaw but rather a modeling artifact of sequential key derivation in the handshake design.

These results confirm that PRINS maintains confidentiality of its secret values, ensures correct sequencing of message forwarding through IPX nodes, and preserves the integrity of payloads exchanged between SEPPs. The single false result corresponds to the expected directionality of key derivation events, reflecting the client-initiated order rather than any security flaw.

3.4 Discussion

The formal verification demonstrates that PRINS satisfies the core security goals of confidentiality, integrity, and correspondence under the Dolev-Yao threat model. The message flow through multiple IPX nodes is authenticated and traceable, while the payload remains confidential due to AEAD-based encryption. The verified model further confirms that unauthorized modification attempts by IPX nodes would be detected through JWS signature validation at the peer SEPP.

However, several modeling limitations must be acknowledged. First, TLS internals and exporter misuse scenarios are abstracted, so potential vulnerabilities related to key reuse or exporter misconfiguration are not covered. Second, the model assumes secure key management and trusted public keys for SEPP and IPX entities. Finally, with the advancement of quantum computing, currently deployed public key algorithms such as Ed25519 and certain symmetric primitives may become vulnerable, potentially leading to the collapse of existing cryptographic

Table 1: Summary of ProVerif query results for PRINS

Property	Query	Result
Secrecy of seppSecret	query attacker(seppSecret)	True
Key correspondence (c⇒p)	event(derived_cSEPP(k,ctx)) ⇒ event(derived_pSEPP(k,ctx))	True
Key correspondence (p⇒c)	event(derived_pSEPP(k,ctx)) ⇒ event(derived_cSEPP(k,ctx))	False
IPX forwarding order	inj-event(pipx_forward(ctx)) ⇒ inj-event(cipx_forward(ctx))	True
Payload delivery integrity	inj-event(payload_delivered(payload,ctx)) ⇒ inj-event(csepp_payload(payload,ctx))	True
Multi-hop validation	inj-event(payload_delivered(payload,ctx)) ⇒ inj-event(pipx_forward(ctx))	True

assumptions.

Overall, the verification results establish the logical soundness of PRINS and its robustness against message replay or modification attacks in multi-hop N32-c communications. Further discussion on extended verification and experimental validation is included in the Conclusion section.

4 Conclusion

This study conducted a formal verification of PRINS, a policy-based application layer protection mechanism designed to enhance the security of the N32-c interface in 5G roaming environments. To overcome the limitations of conventional TLS protection, PRINS introduces a message-level signing and encryption structure based on JWS and JWE, thereby ensuring integrity and confidentiality even in multi-hop IPX forwarding scenarios.

The verification using ProVerif confirmed that PRINS satisfies its core security properties, including secrecy, integrity, and event correspondence. Furthermore, the protocol successfully detects message modification and replay attacks through signature verification across intermediate IPX nodes. A single false query observed in the reverse correspondence test was attributed to the intentional sequential order of key derivation events and does not indicate a security flaw. Overall, PRINS demonstrates logical completeness and structural soundness as an upper-layer protection protocol for inter-PLMN communications.

Nevertheless, the current model abstracts internal TLS operations and omits implementation-dependent aspects such as public-key management and exporter configuration errors. Additionally, with the advancement of quantum computing, the security of conventional public-key and symmetric algorithms may be compromised, necessitating the integration and verification of post-quantum cryptographic (PQC) schemes[8]. Future research will focus on extending PRINS with quantum-resistant primitives, evaluating its resilience against exporter misuse and key compromise scenarios, and exploring its adaptability to multi-operator security interworking in forthcoming 6G network architectures[9].

In conclusion, PRINS provides a logically verified, policy-driven framework that enhances application-layer trustworthiness in 5G roaming environments. Its modular design establishes a solid foundation for the evolution toward quantum-secure and interoperable protection mechanisms in next-generation mobile networks[10].

Acknowledgement: This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (RS-2024-00441484, Development of open roaming technology for Private 5G network).

References

[1] GSMA. 5g security guide, version 3.0. Permanent reference document: Fs.40, GSMA, July 2024.

[2] Ralf Keller, David Castellanos, Anki Sander, Amarisa Robison, and Afshin Abtin. Roaming in the 5g system: The 5gs roaming architecture. *Ericsson Technology Review*, 2021(6):2–11, 2021.

[3] 3GPP(3rd Generation Partnership Project). 5g; security architecture and procedures for 5g system (3gpp ts 33.501 version 18.10.0 release 18). Technical report, 3GPP, July 2025.

[4] Michael B. Jones, John Bradley, and Nat Sakimura. JSON Web Signature (JWS). RFC 7515, May 2015.

[5] Michael B. Jones and Joe Hildebrand. JSON Web Encryption (JWE). RFC 7516, May 2015.

[6] Bruno Blanchet. *Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif*, pages 54–87. Springer International Publishing, Cham, 2014.

[7] 3GPP(3rd Generation Partnership Project). 5g; 5g system; public land mobile network (plmn) interconnection; stage 3 (3gpp ts 29.573 version 18.11.0 release 18). Technical report, 3GPP, Sep 2025.

[8] Rongjie Zhou, Huaqun Guo, Francis E C Teo, and Spiridon Bakiras. A survey on post-quantum cryptography for 5g/6g communications. In *2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, pages 1–6, 2023.

[9] M. A. Rahman, M. Islam, et al. Security requirements and challenges of 6g technologies and applications. *Sensors*, 22(6):1–30, 2022.

[10] Ericsson. Impact of quantum computing on 5g and 6g security. Technical report, Ericsson, 2019.