**3GPP TSG-SA3 Meeting #118 S3-242xxx**

Hyderabad, India 14 - 18 October 2024

**Source: Nokia, Nokia Shanghai Bell**

**Title: Discussion paper for KI#2.1**

**Document for: Information**

**Agenda Item: 5.14**

# 1 Decision/action requested

***In this box give a very clear / short /concise statement of what is wanted.***

# 2 References

<Examples of references, please delete when you have inserted your actual references:

[1]

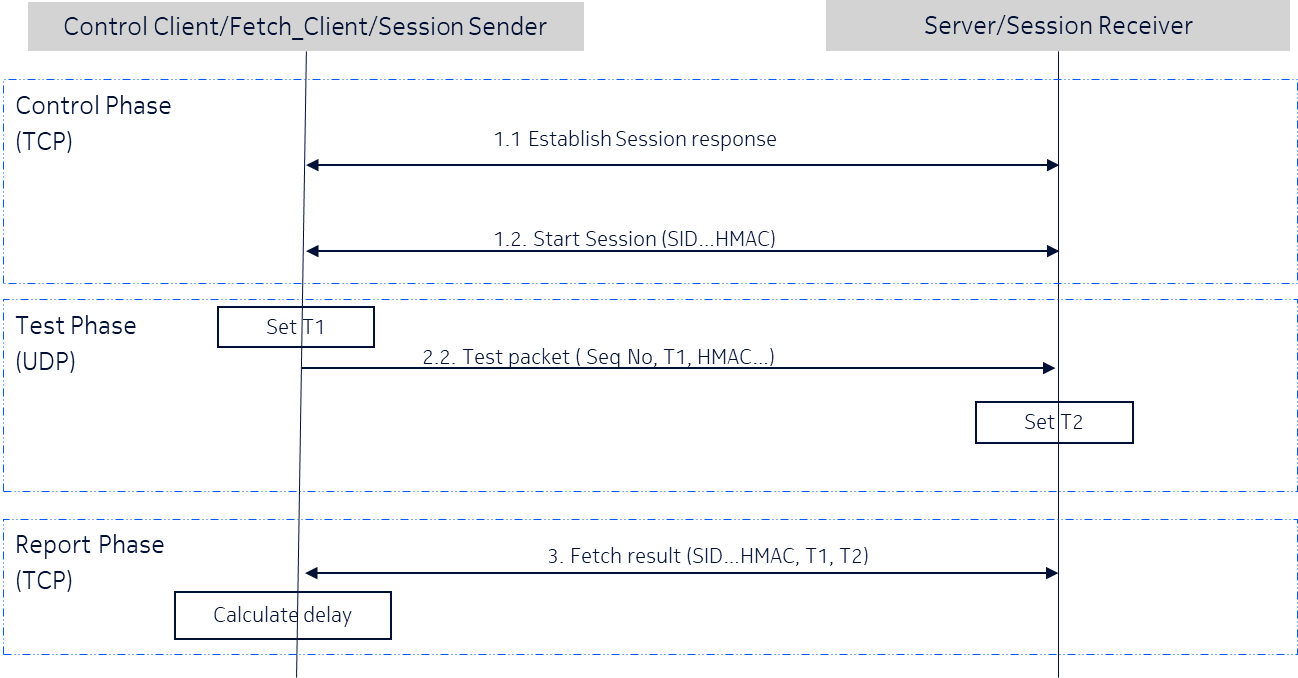
# 3 Rationale

SA2 concluded KI#2 of TR 23.700-49 (Study on Enhancement of support for Edge Computing in 5G Core network - Phase 3) that SMF can collect N6 delay measurement from candidate UPF(s) based on the measurement protocol supported by UPF and application side. The IETF RFCs corresponding to the IP Performance Metrics (IPPM) defined protocols, such as OWAMP (RFC 4656), TWAMP (RFC 5357) or STAMP (RFC 8762), etc., are leveraged for N6 delay measurement. ICMP (RFC 792) is also not excluded in SA2 study, although it is considered an unsecure protocol. Security considerations should be taken into account when those protocols are in use.

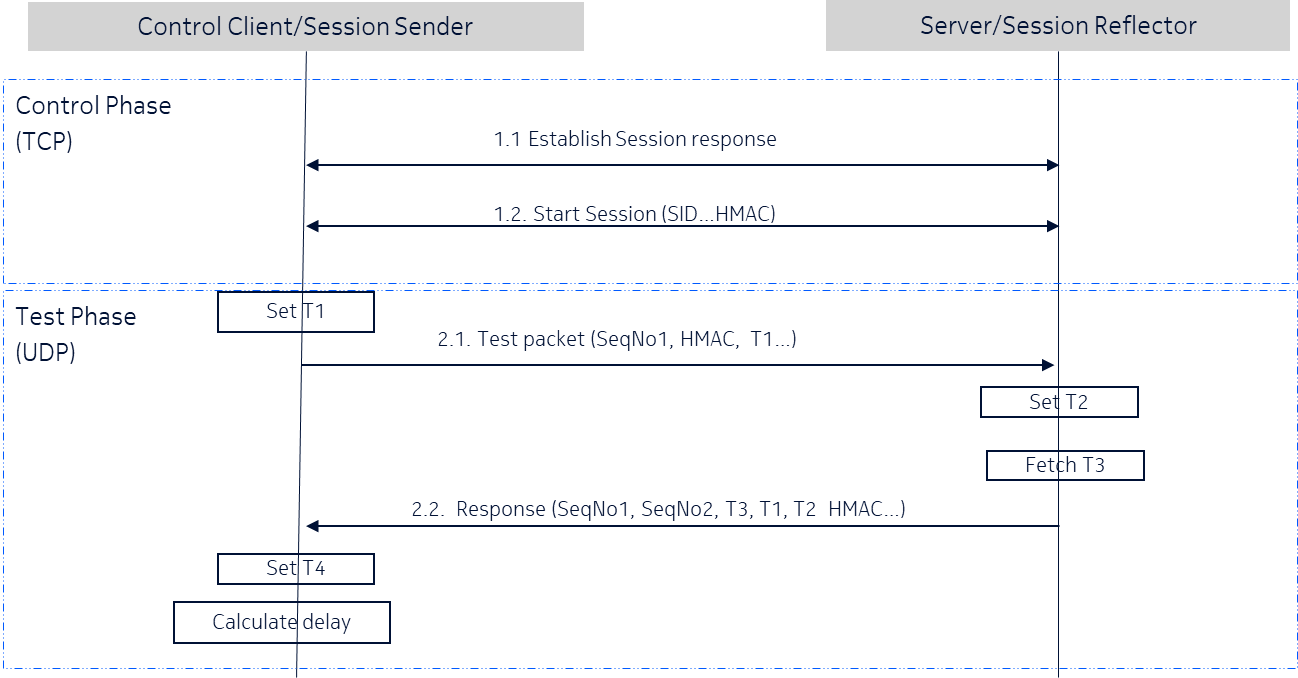
This paper is intended to illustrate the security mechanisms of those possible protocols to be used for the N6 delay measurements to support selecting secure protocols and facilitate configuration and enable security capabilities of each protocol. The description of the security mechanisms workflows per protocol have been added for further clarification.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Protocol** | **OWAMP**  **(RFC 4656)** | **TWAMP**  **(RFC 5357)** | **STAMP**  **(RFC 8762)** | **ICMP**  **(RFC 792)** |
| **Security Capability** |  |  |  |  |  |
| **Authentication** |  | HMAC | HMAC | HMAC | N/A |
| **Confidentiality** |  | AES | AES | Transport layer | N/A |
| **Integrity** |  | HMAC | HMAC | HMAC | N/A |
| **Replay Protection** |  | sequence numbers or timestamps | sequence numbers or timestamps | sequence numbers or timestamps | None |
| **DoS prevention** |  | With authentication | With authentication | With authentication | None |
| **TLS support** |  | TLS is not recommended in RFC | TLS is not recommended in RFC | DTLS/IPSec for encryption | None |
| **Exchange Parameters** |  | Security mode, KeyID, Session keys, Count, Salt, Challenge, IVs | Security mode, KeyID, Session keys, Count, Salt, Challenge, IVs | N/A | N/A |
| **Configuration Parameters** |  | Shared secret  Encryption Algorithm (AES).  HMAC Algorithm (SHA-256).  Security Policies to limit resource use, such as network capacity and memory | Shared secret  Encryption Algorithm (AES).  HMAC Algorithm (SHA-256).  Security Policies to limit resource use, such as network capacity and memory | Shared Secret  Security mode  KEM algorithm (e.g. DH)  HMAC Algorithm (SHA-256). | N/A |

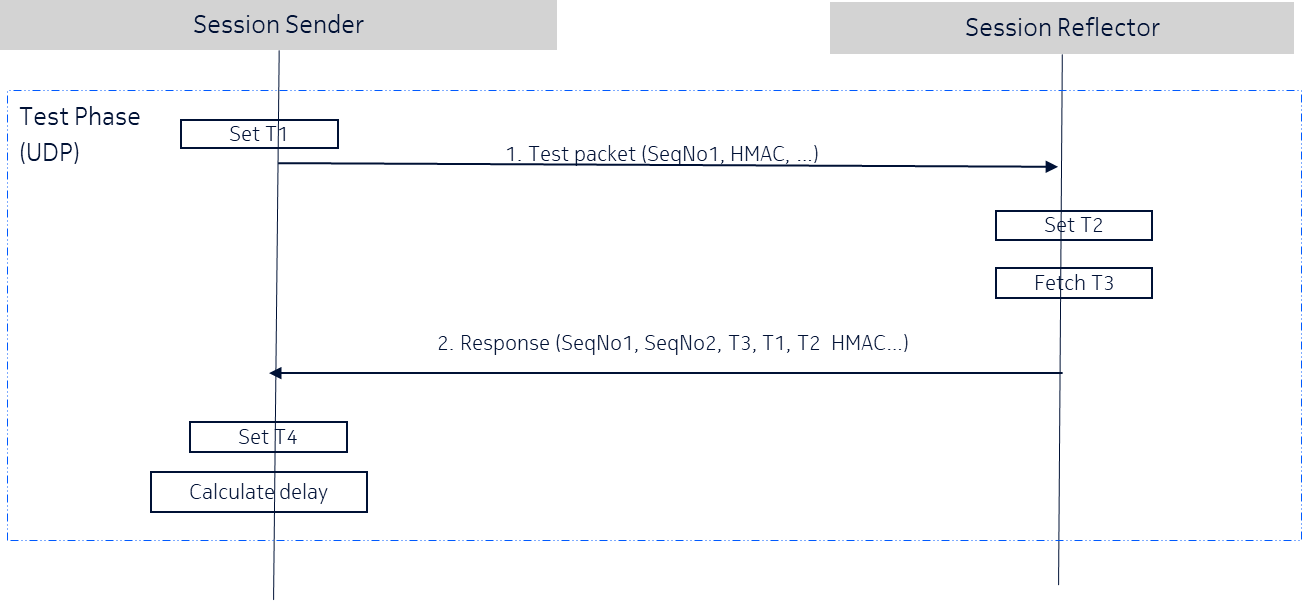
The security procedure for OWAMP is represented in the following figure:



The security procedure for TWAMP is represented in the following figure:



The security procedure for STAMP is represented in the following figure:



# 4 Detailed proposal

It is proposed that the security analysis of the possible protocols to be used in N6 delay measurement is part of the solution for KI #1.1.

It is also proposed that only protocols supporting security mechanisms are recommended and endorsed by SA3.