**3GPP TSG-CT WG1 Meeting #146C1-240224**

**E-meeting, 22 – 26 January 2024**

**Source: Xiaomi**

**Title: Message definition and information elements coding for SLP key request procedure**

**Spec: 3GPP TS 24.514 v0.5.0**

**Agenda item: 18.2.23**

**Document for: Agreement**

**1. Introduction**

This p-CR provides the message definition and information elements coding for SLP key request procedure.

**2. Reason for Change**

The procedures for SLP key request procedure are defined in clause 8.3.1.1.3 3GPP TS 24.514, the corresponding "Message functional definition and contents" and "Information elements coding" should be defined.

**3. Proposal**

It is proposed to agree the following changes to 3GPP TS 24.514 v0.5.0.

\* \* \* First Change \* \* \* \*

## 10.x Security for ranging and sidelink positioning messages

### 10.x.1 General

This clause defines the XML schema and MIME type related to 5G Prose security messages for ranging and sidelink positioning.

### 10.x.2 application/vnd.3gpp-prose-pc8+xml

The MIME type is used to carry information related to the 5G ProSe security operation for ranging and sidelink positioning. It shall be coded as an XML document containing one of the following 5G ProSe security messages for ranging and sidelink positioning:

a) a PROSE\_SLPK\_REQUEST message; and

b) a PROSE\_SLPK\_RESPONSE message.

Each of those messages is presented in the XML document as an XML element named after the corresponding message.

### 10.x.3 XML schema

Implementations in compliance with the present document shall implement the XML schema defined below for messages used in 5G ProSe security procedures for ranging and sidelink positioning over PC8\* interface.

<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"

 xmlns="urn:3GPP:ns:Ranging\_SL:Security:2024"

 elementFormDefault="qualified"

 targetNamespace="urn:3GPP:ns:Ranging\_SL:Security:2024">

 <xs:annotation>

 <xs:documentation>

 Info for Ranging\_SL Security Control Messages Syntax

 </xs:documentation>

 </xs:annotation>

 <xs:complexType name="empty-type"/>

<!-- Complex types defined for transaction-level -->

 <xs:complexType name="SLPK-request-type">

 <xs:sequence>

 <xs:element name="transaction-ID" type="xs:integer"/>

 <xs:element name="SERVICE-ID" type="xs:integer"/>

 <xs:element name="SLPK-ID" type="xs:string" minOccurs="0" />

 <xs:element name="Kslp-freshness-parameter-1" type="xs:hexBinary"/>

 <xs:element name="HPLMN-ID" type="xs:hexBinary"/>

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <xs:complexType name="SLPK-accept-type">

 <xs:sequence>

 <xs:element name="transaction-ID" type="xs:integer"/>

 <xs:element name="SLPK-ID" type="xs:string"/>

 <xs:element name="Kslp" type="xs:hexBinary"/>

 <xs:element name="Kslp-freshness-parameter-2" type="xs:hexBinary"/>

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <xs:complexType name="SLPK-reject-type">

 <xs:sequence>

 <xs:element name="transaction-ID" type="xs:integer"/>

 <xs:element name="SLPK-ID" type="xs:string"/>

 <xs:element name="SLPK" type="xs:hexBinary"/>

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <!-- Complex types defined for Message-level -->

 <xs:complexType name="PROSE\_SLPK\_REQUEST-type">

 <xs:sequence>

 <xs:element name="SLPK-request" type="SLPK-request-type" minOccurs="0" maxOccurs="unbounded"/>

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <xs:complexType name="PROSE\_SLPK\_RESPONSE-type">

 <xs:sequence>

 <xs:element name="SLPK-accept" type="SLPK-accept-type" minOccurs="0" maxOccurs="unbounded"/>

 <xs:element name="SLPK-reject" type="SLPK-reject-type" minOccurs="0" maxOccurs="unbounded"/>

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

 <xs:element name="anyExt" type="anyExtType" minOccurs="0"/>

 <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>

 </xs:sequence>

 <xs:anyAttribute namespace="##any" processContents="lax"/>

 </xs:complexType>

<!-- Top level Security Message definition -->

 <xs:element name="rangingsl-security-message">

 <xs:complexType>

 <xs:choice>

 <xs:element name="PROSE\_SLPK\_REQUEST" type="PROSE\_SLPK\_REQUEST-type"/>

 <xs:element name="PROSE\_SLPK\_RESPONSE" type="PROSE\_SLPK\_RESPONSE-type"/>

 <xs:any namespace="##other" processContents="lax"/>

 </xs:choice>

 </xs:complexType>

 </xs:element>

</xs:schema>

### 10.x.4 Semantics

#### 10.x.4.1 General

The <rangingsl-security-message> element is the root element of this XML document and it can be one of the following elements:

1. <PROSE\_SLPK\_REQUEST>

b) <PROSE\_SLPK\_RESPONSE>

#### 10.x.4.2 Semantics of <PROSE\_SLPK\_REQUEST> element

The <PROSE\_SLPK\_REQUEST> element contains:

a) zero or more < SLPK-request> elements which contain transactions sent from the UE to the SLPKMF;

b) zero or one <anyExt> element containing elements defined in future releases;

c) zero or more elements from other namespaces defined in future releases; and

d) zero or more attributes defined in future releases.

The <SLPK-request> element contains:

a) a <transaction-ID> element containing the parameter defined in clause 11.x.1;

b) a <SERVICE-ID> element containing the parameter defined in clause 11.x.x4;

c) a <SLPK-ID> element containing the parameter defined in clause 11.x.3;

e) a <Kslp-freshness-parameter-1> element containing the parameter defined in clause 11.x.x2;

f) zero or one <HPLMN-ID> element;

i) zero or one <anyExt> element containing elements defined in future releases;

j) zero or more elements from other namespaces defined in future releases; and

k) zero or more attributes defined in future releases.

#### 10.x.4.3 Semantics of <PROSE\_SLPK\_RESPONSE> element

The <PROSE\_SLPK\_RESPONSE> element contains:

a) zero or more <SLPK-accept> elements which contain the accepted transactions;

b) zero or more <SLPK-reject> elements which contain the rejected transactions;

c) zero or one <anyExt> element containing elements defined in future releases;

d) zero or more elements from other namespaces defined in future releases; and

e) zero or more attributes defined in future releases.

The <SLPK-accept> element contains:

a) a <transaction-ID> element containing the parameter defined in clause 11.x.1;

b) a <SLPK-ID> element containing the parameter defined in clause 11.x.3;

c) a <Kslp> element containing the parameter defined in clause 11.x.x1;

d) a <Kslp-freshness-parameter-2> element containing the parameter defined in clause 11.x.x3;

f) zero or one <anyExt> element containing elements defined in future releases;

g) zero or more elements from other namespaces defined in future releases; and

h) zero or more attributes defined in future releases.

The <SLPK-reject> element contains:

a) a <transaction-ID> element containing the parameter defined in clause 11.x.1;

b) a <PC8\*-control-protocol-cause-value> element containing the parameter defined in clause 11.x.4;

c) zero or one <anyExt> element containing elements defined in future releases;

d) zero or more elements from other namespaces defined in future releases; and

e) zero or more attributes defined in future releases.

\* \* \* Next Change \* \* \* \*

## 11.x Security for ranging and sidelink positioning message formats

### 11.x.x1 KSLP

This parameter is used to provide a 256-bit KSLP as specified in 3GPP TS 33.533 [5].

### 11.x.x2 KSLP freshness parameter 1

This parameter is used to indicate 128-bit long KSLP freshness parameter 1 as specified in 3GPP TS 33.533 [5].

### 11.x.x3 KSLP freshness parameter 2

This parameter is used to indicate 128-bit long KSLP freshness parameter 2 as specified in 3GPP TS 33.533 [5].

### 11.x.x4 SERVICE-ID

This parameter is used to identify the particular application that triggers the security operation for ranging and sidelink positioning. This information element is coded as the ProSe identifier specified in clause 11.3.3 of 3GPP TS 24.554 [6].

### 11.x.1 Transition ID

This parameter is used to uniquely identify a PC8\* control protocol for Ranging\_SL security transaction when it is combined with other PC8\* control protocol for Ranging\_SL security transactions in the same transport message. The UE shall set this parameter to a new number for each outgoing new key request. The transaction ID is an integer in the 0-255 range.

### 11.x.2 SLPK

This parameter is used to indicate the SLPK allocated by the SLPKMF. The calculation of the SLPK is defined in 3GPP TS 33.533 [5].

### 11.x.3 SLPK-ID

This parameter is used to indicate the identifier of the UE stored SLPK.

### 11.x.4 PC8\* control protocol cause value

This parameter is used to indicate the particular reason why a PROSE\_UE\_SLPK\_REQUEST message from the UE has been rejected by the SLPKMF. It is an integer in the 0-255 range encoded in Table 11.x.4.

Table 11.x.4: PC8\* control protocol cause value

|  |
| --- |
| 0 Reserved |
| 3 UE authorization failure |
| 1, 2, 4-255 Unused |

\* \* \* End of Changes \* \* \* \*