

---

**Title:** Proposed WID: NDS Authentication Framework Extension for TLS  
**Source:** Nokia  
**Document for:** Discussion and decision  
**Agenda Item:** 6.4

---

### **Work Item Description**

**Title:** NDS Authentication Framework Extension for TLS

**1 3GPP Work Area**

	Radio Access
X	Core Network
	Services

**2 Linked work items**

*Network Domain Security; Authentication Framework*

**3 Justification**

In release 6 the Authentication Framework (NDS/AF) was specified to provide entity authentication for the 3GPP network nodes that are using NDS/IP. The authentication was developed to replace the (not so scaleable) default IPSEC/IKE use of pre-shared secrets to authenticate the network elements.

In release 6, SA3 has specified that TLS may be used to protect the SIP signalling between IMS CSCF and a SIP proxy located in a foreign network (non-IMS network). Extending NDS Authentication Framework for TLS connections provides an option for non-IMS networks to establish secure connections for SIP traffic to IMS network.

Generic Bootstrapping Architecture (GBA) includes a diameter proxy (D-Proxy) that functions as a proxy between the visited NAF, and the subscriber's home BSF. If the BSF and the NAF are located in different operators' networks, the Zn' reference point between the D-Proxy and the BSF is secured using TLS. As an authentication framework as available for IPSEC provided by NDS/AF is not available for TLS certificates, the authentication has to be solved by manual configuration of the involved operators.

**4 Objective**

The objective is to study security requirements and solutions how NDS Authentication Framework specified for nodes that are using NDS/IP can be extended to provide entity authentication for the nodes that are using TLS.

**5 Service Aspects**

*None identified*

**6** **MMI-Aspects**

*None identified*

**7** **Charging Aspects**

*None identified*

**8** **Security Aspects**

*The work item is a security item.*

**9** **Impacts**

<b>Affects:</b>	<b>UICC apps</b>	<b>ME</b>	<b>AN</b>	<b>CN</b>	<b>Others</b>
<b>Yes</b>				X	
<b>No</b>	X	X	X		
<b>Don't know</b>					X

**10** **Expected Output and Time scale (to be updated at each plenary)**

<b>New specifications</b>						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
<b>Affected existing specifications</b>						
Spec No.	CR	Subject		Approved at plenary#	Comments	
33.310		Network Domain Security, Authentication framework		SA#30 (December 2005)		

**11** **Work item rapporteur(s)**

Tiina Koskinen, Nokia

**12** **Work item leadership**

SA3

**13** **Supporting Companies**

Nokia,...

**14** **Classification of the WI (if known)**

	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)