3GPP TSG SA WG3 Security — S3#37 **S3-050064**
21 - 25 February 2005
Sophia Antipolis, France

Agenda Item: IMS

Source: Ericsson

Title: Access Security Requirements

Document for: Discussion/Decision

1. Introduction

Today, IMS is also going to be deployed on wired environments. These wired environments impose somewhat different requirements to the access security solution than the wireless environments. ETSI TISPAN is one of these parties that are currently specifying how to use IMS with wired access networks. In this document, the term 'wired environment' is meant in a broad sense, e.g. it includes also the internet-based access environments. The purpose of this contribution is to examine some of the requirements that wired access networks pose to the access security solution.

2. Requirements

There are five major differences on the wireless and wired access networks that affect to the access security solution. Current situation in wired access networks is the following:

- Lot of NAT devices are deployed.
- UEs are very different from wireless devices used in RANs, e.g. PCs.
- Fixed UEs seldom contains smart card readers.
- Large number of subscribers can contact P-CSCF directly.
- There is a need to provide same services for both wireless and wired environment.

From these differences we can derive five requirements for the access security solution:

- NAT traversal has to be possible.
- Legacy UEs (including PCs) need to be supported with minimum changes.
- Use of IMS without smart cards should be possible.
- Support for fixed-mobile convergence.
- P-CSCF requires additional protection.

NAT traversal is a very important requirement. As IMS is going to be deployed in networks with NAT devices, a solution for NAT traversal is needed.

There is a clear requirement for supporting already deployed UEs with minimum changes. The most common UE in wired environments is currently a PC, while there of course are also other client devices. Access security solution should accommodate these legacy clients as well as possible.

With a term *fixed-mobile convergence* we mean that eventually the UEs in wireless and wired networks would need to be able to use the same services. The situation where one service network, namely IMS network, can provide services for all different networks and UEs, is desirable for all players in the telecom industry. In fact, this is one of the main reasons why TISPAN is founded in the first place.

- One other important requirement is that legacy UEs on the wired access networks seldom have smart card readers. In order to support these legacy UEs, we need to come up with novel ways to do subscriber authentication and key sharing. On wired environment, the most typical situation is that subscribers can connect P-CSCF more or less directly. Also this matter needs to be tackled on the security specifications.

Some other requirements have also come up. One of them is a support for seamless session mobility. *Seamless session mobility* means the procedure where UE changes its network layer address and still maintains active sessions. It still is not clear whether this is a requirement or not. It is not, for example, included in NGN R1, but it might become as a requirement in the future for many wired access network types.

One of the organizations standardizing the use of wired access network with IMS is ETSI TISPAN. The work in TISPAN is still in early stages. Nevertheless, some studies regarding the access security solution have already been made. For example, a feasibility study of IPsec and TLS for securing access networks [2] has been done.

3. Suggestions

We propose that the current access security solution needs to be expanded to accommodate these new requirements. Furthermore, this access security solution should be done in 3GPP, since it inherently has a lot of competence on IMS security related issues.

ETSI TISPAN and other parties that are standardizing the use of IMS with wired access network now and in the future will do their own studies on security requirements and solutions. These requirements and solutions should be used as an input for the 3GPP's specification process. The goal would be to find an access security solution that would satisfy all concerned parties. In other words, it would be desirable that only one specification would be produced.

We have attached a R7 CR to 33.203 that proposes some new access security requirements to IMS.

3. References

[1] S3-040990, "IMS security extensions", Ericsson's contribution, submitted to 3GPP SA3 #36.

[2] 05TD161, "Feasibility of IPsec and TLS to provide SIP signalling security on the access in NGN/IMS", Ericsson's and Alcatel's contribution, submitted to ETSI TISPAN#05.

3GPP TSG SA WG3 Security – S3#37 ***att_S3-050064***
21-25 February 2005, Sophia-Antipolis, France

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.203** **CR** **078** ⌘ **rev** **-** ⌘ Current version: **6.5.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Access Security Requirements
Source:	⌘	Ericsson
Work item code:	⌘	IMS
Date:	⌘	08/02/2005
Category:	⌘	**B**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	Requirements for access security are increasing, because IMS is going to be used also on the wireline side (e.g. from the internet and from the access network on NGN). These new requirements should be documented by 3GPP in order to avoid the birth of many separate specification by different standardization bodies.
Summary of change:	⌘	New requirements for the access security solution.
Consequences if not approved:	⌘	3GPP's access security solution cannot be used with wired access networks.

Clauses affected:	⌘	

Other specs affected:	⌘	Y	N		⌘
		☐	☐	Other core specifications	
		☐	☐	Test specifications	
		☐	☐	O&M Specifications	

Other comments:	⌘	

**** Begin of Change ****

5.5 Fixed-mobile convergence

In order to gain secure access to the IMS from the wired access networks, the IMS access security solution shall accommodate the following:

- NAT traversal: NAT devices are widely deployed.
- Legacy UEs: These are most typically PCs.
- The use of UEs, which do not contain smart card: PCs do not have smart cards.

P-CSCF shall be protected in secure manner, when it is used with wired access networks. This is due to a fact that P-CSCF is more vulnerable to external security threats on wired access networks, since subscribers typically have a direct IP connection to it.

**** End of Change ****