**3GPP TSG SA WG3 Security — S3#25** **S3-020523**
**8 - 11 October 2002**
**Munich, Germany**

**Source**: Ericsson

**Title**: 3G-WLAN – Trust Model

**Document for**: Discussion and approval

**Date**: 20-09-02

# 1 Introduction

This contribution shows a 3G-WLAN system model, describing the key players and their trust relationships. It is proposed that the existing business and trust relations between GSM/UMTS operators and their customers are used to provide quick and convenient WLAN access for the current trusted customer base.

# 2 Trust Model

## 2.1 Trust model entities

Although any real implementation of a trusted access solution will depend on the exact system architecture, for the high-level concepts presented in this contribution we restrict attention to the three key players: the user/customer, the cellular operator, and the WLAN access provider.

Figure 1 shows a simplified system model showing only the three roles and their trust relationships.

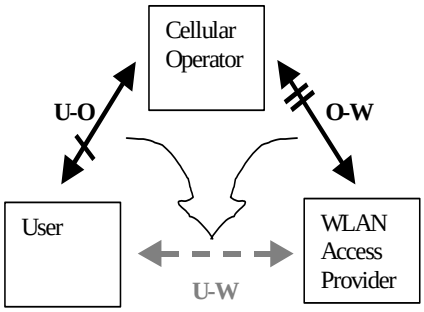


**Figure 1 Trust model**

The cellular operator offers GSM/GPRS/UMTS services. Architecture-wise, the "cellular operator" box represents the complete cellular network (including radio access network, core network, service network), and also extends to partners in a roaming consortium.

The WLAN access provider offers public Wireless LAN access as a service. The "WLAN Access Provider" box in the figure groups the WLAN access network and its possible supporting nodes. The WLAN access provider may be "part of" (owned by) the cellular operator or a cellular roaming partner, or it could be a WLAN-only access provider or Wireless ISP.

The user in this model is assumed to be a subscriber/customer of the cellular operator who wishes to use both the traditional cellular services and the complementary (but not complimentary) WLAN access, when available. As such, the user is assumed to operate equipment capable of both GPRS/UMTS and WLAN access. This could be some

combination of a phone (handset or PC-card) and a laptop / PDA, or possibly a combined WLAN/GPRS terminal. The collection of a user's devices acting on behalf of the user will often be called a client.

Legally, the user-operator trust relation, labelled "U-O" in Figure 1, is based on the service agreement between these two parties. From a technological perspective, this trust is embodied in a shared secret stored securely both on the user's (U)SIM and at the operator's Authentication Centre, and allows for an authenticated secure connection between the user's terminal and the cellular network.

If the cellular operator and the WLAN access provider are part of the same legal entity their trust relation is self-evident, and results in an intra-domain security solution. In the more general case, the operator-WLAN trust, labelled O-W in Figure 1, is based on roaming agreements or other partnerships (such as a Single Sign-On federation). Physically, this trust can translate to a security solution for roaming, AAA, trusted or semi-trusted servers in the context of WAP, or SMS-gateway access.

## 2.2 Trust relations

To design or evaluate a security solution, the trust relations between the participants must be identified. In a public WLAN access scenario, we have one or more operators and (possibly independent) access providers, and several subscribers.

The subscribers cannot trust each other. Someone else accessing the network from the same WLAN access network as the user, may be trying to perform DoS attacks targeted at the user, or eavesdrop on his traffic, steal his credentials to gain access at a later time etc.

An operator cannot trust any mobile terminal that tries to connect to the network. Before authentication, the mobile station could belong to anyone, with or without a subscription. Even after a mobile station has been authenticated, the device may act maliciously. The user himself may be performing fiendish activities, or someone else may have hijacked his session.

The operators and/or access providers may choose to trust each other. Such trust relations normally rely on (legally binding) roaming agreements. If such an agreement is in place, a user may use another operator's access network, and will be authenticated by the "home operator". Depending on which solution is chosen, the user may have to put trust in other, visited operators, as well as in his home operator.

It is probable that the cellular operators will provide the WLAN access in the future, and that small WLAN-only operators will be few or non-existent. It is, however, not impossible that there will be important WLAN-only operators on the market. These could team up with one or more cellular operators. The trust relations that are induced by access through such an operator are the same as the ones considered in the case of roaming between two cellular operators.

# 3 Proposal

It is proposed that the Trust Model described in section 2 is adopted by SA3, and incorporated to Annex B of Technical Specification 33.cde "WLAN Interworking Security".