3GPP TSG SA WG3 Security — S3#18 **S3-010280**

21 - 24 May, 2001

Phoenix, USA

Source: Stuart Ward, Colin Blanchard

Title: UE Split over several Devices Version 2

Document For Discussion at SA3#18

Agenda Item: 9.9

Introduction

There have been a number of LS and Papers discussing the case of establishing connections through a UE that consists of several separated components, connected by bluetooth, Infra Red, Cable, 802.11 or other technology. Here we present a few ideas for the establishment of a security structure for this type of connection.

References

23.227 V1.0.0 Application and User Interaction in the UE - Principles and Specific Requirements

T2-000793 Discussion document on UE functionality split over physical devices

S1-010166 LS from S1 to SA2, SA3, T2, TSG-T, T3, CN1, SA; Date: 9th February 2001

SP-010177 Response to LS (T2-000793) on discussion document on UE functionality split over physical devices

Principals

The security mechanisms should be as strong as that already established for the single component UE.

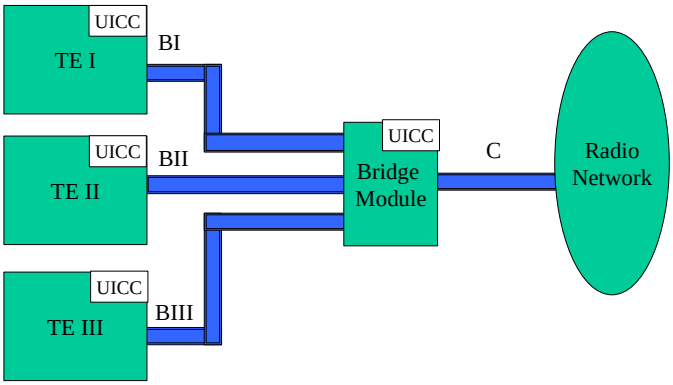
The services used must be clearly attributable to a USIM and associated subscription.

The confidentiality of any inter-linking system will be presumed to be insecure, but it may not be appropriate for us to standardise encryption protocols on these links.

Proposal

Each component should have a SIM or USIM and be capable of performing either GSM authentication or 3GPP AKA

A bridging component (one that is able to connect to a 3GPP network and offering connections to other devices) will allow those devices to use join a local network. Trust between the devices can be established mutually between the bridge device and component devices by treating this network as a roaming partner, and allowing the bridge device to get authentication vectors for each of the component modules and perform the AKA protocol with each device.



Network of UE components linked to the network via a bridge component

TE I would connect to the Bridge module and present and IMSI for verification. The Bridge module would then request an authentication vector over its established network connection and perform an AKA sequence with TE I. This would result in the generation of IK and CK which could then be used to encript the connection between these devices.

All billing would be attributed to the USIM account in the bridge device. This device would then need to keep account of services used if the component USIM is to be charged. For example if the bridge device is in a taxi then the customer would have the charges added to their fair.

Issues

A new UE message protocol is required to request and deliver the authentication vector to the bridge device. This can be modeled on the existing MAP messages that perform this between networks.

Network operators will need to provide customers with additional SIM or USIM cards for these components but there would be no need to link these to a subscription. As all charges would be attributed to the USIM in the bridge device.

These sort of devices currently do not have USIM / SIM slots incorporated in to them

Current authorisation is implicit, connecting the cable or enabling the IR port is all that is required. This implicit authorisation dose not happen with short range radio connections.

The component's USIM belongs to another network for which the network attached to the UE-Bridge component does not have a roaming agreement. This would most likely arise in a home area with competing networks. Unless the networks agreed to offer roaming agreements then this type of connection would fail.