3GPP TSG SA WG3 Security — S3#12 **S3-000272**

11-14 April, 2000

Stockholm, Sweden

Source: TIA TR-45.2 Security Focus Group Chair

To: TSG SA WG3

Title: Global Challenge for Initial Registration

Agenda Item: Joint TR-45/S3 Meeting

Contact: Terry Jacobson, Chair TIA TR-45.2 Enhanced Security Focus Group
email: terryjacobson@lucent.com
phone: 1-630-713-1665

---

1 INTRODUCTION

TR-45.2 and the TR-45 AHAG are currently deliberating the use of Global Challenge for Enhanced Subscriber Authentication (ESA) on initial registrations of the mobile station in the Serving System. The issues are speeding up access processing and minimizing system loading on TR-45 traffic channels. This discussion is ongoing.

This contribution provides background on the need for high speed access processing and concerns about radio resource utilization.

2 HIGH SPEED ACCESS PROCESSING

The use of Global Challenge for initial registration enables the Home System to authenticate the MS using the authentication signature provided by the MS in its initial system access. This speeds up the access process by avoiding intersystem operations and air interface messages required for 3GPP AKA.

2.1 Background

When wireless service providers first deployed supplementary services (e.g., Intelligent Network based services) that are provided by the Home System, subscribers occasionally experienced unacceptable delays in accessing supplementary services. The delays occurred when the initial mobile station (MS) access in the Serving Network was an MS origination and the access invoked a supplementary service. The delay was due to the time needed to authenticate the MS before the subscriber profile was transferred to the Serving Network. The subscriber profile identified the trigger detection points used by the Serving MSC to query the Home System for instructions to process the MS access.

TR-45.2 published *IS-778* in January 1999 to provide *Wireless Authentication Enhancements*. A major change enabled the Serving Network to obtain the subscriber profile in parallel with authentication of the MS upon initial access in a system. This change enabled the Serving MSC to obtain subscriber profile information and expedite access processing during the intervening authentication and registration period.

2.2 High Speed Authentication

Subcommittee TR-45.2 developed a requirement for High Speed Authentication in preparation for evaluating Enhanced Subscriber Authentication (ESA) proposals.

Requirement

ESA should minimize the length of time needed to authenticate the user upon initial access in a new Serving System (and upon any service access) subject to the minimum security requirements for ESA.

This requirement was intended to ensure that an ESA proposal did not further delay the time needed for MS access processing. In comparison to a Global Challenge authentication procedure, 3GPP AKA requires more intersystem operations and the exchange of additional air interface messages when an MS initially access the Serving Network.

When Global Challenge is used, the MS authentication signature is sent to the Home System in the initial Authentication Request message.

In comparison, 3GPP AKA requires the Serving System to send an Authentication Data Request to the Home System. The Home System responds with the Authentication Data Response. The Serving System pages the MS and assigns the MS to a dedicated channel. The Serving System send an Authentication Request to the MS and the MS responds with the Authentication Data Response. When the MS response is validated, the Serving System sends a Location Update Request to the Home System.

The additional delay introduced by AKA could aggravate a service affecting problem that has already been experienced by wireless service providers.

3 TRAFFIC CHANNEL UTILIZATION

3GP AKA-based mutual authentication and key agreement procedures are conducted on a dedicated radio channels. The impact on radio resources in the case of initial MS registration when Global Challenge is not available is being studied.

3.1 3GPP AKA Impact on Capacity

When the Serving System receives a Registration access from an MS and determines that this is a new registration, the Serving Network requests a fresh AKA Vector from the Home System. When the Vector is received, the MS is paged and assigned to a dedicated channel. The AKA authentication and key agreement procedure is conducted. The dedicated channel is released upon completion of the procedure.

Initial studies conclude that there is a reduction of available traffic channel capacity when Global Challenge is not available. This will be especially important in high density areas that experience a large number of initial registrations (e.g., airports).