3GPP TSG SA WG3 Security — S3#18 **S3-010166**
21 - 24 May, 2001
Phoenix, USA

3GPP T3 Meeting #19 ***Tdoc T3-010323***
St John, US VI, 8 - 11 May, 2001

Source: **TSG- T WG3**

To: **TSG-SA WG3**

Cc: **TSG-SA WG1**

Title: **Response to LS (S3-010128) on the Elaboration of KEY IDENTIFICATION EVENT**

Contact: Yael Baruch
Email: yael.baruch@Celltick.com
Tel: +972-9-9710200
Mobile: +972-54-386-744
Fax: +972-9-9710-242

T3 thank S3 for their LS on the above subject (attached).

The feature KEY IDENTIFICATION EVENT is still under study in T3 as a Release 5 topic, it has not been introduced to the Release 4 versions of TS 31.111 (T3) and TS 22.038 (S1).

T3 have, for Release 4, added additional parameters to existing commands in TS 31.111 (USAT) that partially solve the KEY EVENT requirement and are believed not to have any security implications. T3 are discussing whether the feature as originally conceived is still needed.

For this reason no activities by S3 are required for the time being. T3 will inform S3 once a conclusion has been reached, and if further assistance is required.

3GPP TSG SA WG3 Security — S3#17 **S3-010128**
27 February - 02 March, 2001
Gothenburg, Sweden

Source: **TSG-SA WG3**

To: **TSG-SA WG1, TSG-T WG3**

Cc:

Title: **Response to LS (S1-010200) on the Elaboration of KEY IDENTIFICATION EVENT**

Contact: Peter Howard

Email: peter.howard@vf.vodafone.co.uk

Tel: +44 1635 676206

S3#17 has briefly reviewed the new USAT event for key identification. S3 agrees with S1 that this feature must be provided in a secure manner to minimise risks due to malicious USAT applications intercepting keystrokes. S3 would welcome the opportunity to review this feature in more detail and to assist T3 in the specification of appropriate control mechanisms.

S3 would also like to know whether the feature is intended for R4 as indicated in the LS or for R5 as indicated in the attached CR. S3 doubt that sufficient review could be undertaken in time for R4.

TSG-SA WG 1 (Services) meeting #11 **TSG S1 (01) 0200**
Capetown, SA 6th to 9th February 2001 **Agenda Item: 5.3.2**

Source: **TSG-SA WG1**

To: **TSG-T WG3, TSG-SA WG3**

Cc:

Title: **Response to LS (T3-010xxx) from T3 chairman on the Elaboration of KEY IDENTIFICATION EVENT**

Contact: Yael Baruch

Email: yael.baruch@celltick.com

Tel: +972-9-9710-200

Mobile: +972-54-386-744

Fax: +972-9-9710-242

S1 has reviewed the both LS from the T3 chairman (S1-010144) and the explanatory background information (S1-010186) for the proposed new USAT "event" for key identification.

S1 agrees that the proposed functionality does have potential value in the support of new multimedia services on the condition that this functionality can be provided in a secure manner. This secure manner should provide the capability to deactivate of this functionality during some selected MMI activities (e.g., PIN entry).

S1 agrees that this new functionality is desirable for Release 4 if possible. If this functionality cannot be included within the timeframe of Release 4, this functionality should be included in Release 5.

S1 has approved a Release 4 CR to 22.038 (S1-010196) on the definition of this functionality.

Attached documents: S1-010144, S1-010186, and S1-010196.

TSG-SA WG 1 (Services) meeting #11 **TSG S1 (01) 0144**
Cape Town, SA 6th to 9th February 2001 **Agenda Item: 5.3.2**

Liaison Statement

To: TSG-S1, TSG-S3

Source: TSG-T3 chairman

(Note this LS is sourced from the T3 chairman because, due to a shortage of time at the end of the last T3 meeting to fully discuss the document, the LS was not able to be approved.)

Title: Elaboration of KEY IDENTIFICATION EVENT

Contact: Yael Baruch, (yael.baruch@celltick.com)

This liaison to inform S1 and S3 about a new release-4 feature discussed at the last T3 meeting regarding a new USAT "event" KEY IDENTIFICATION.

The goal and background of this feature and some questions raised at the recent T3 #17meeting in Berlin, Germany are described in more detail in document T3-010093 (attached).

This feature introduces a new "event" that indicates that a key on the MMI has been pressed and includes the key identification, in accordance with the “Get Inkey” command.

This proposal puts the onus of detecting a key being pressed on the mobile, whilst "freeing up" the USAT to perform other activities. Currently, for example, if the USAT wishes to detect a key being pressed, it has to issue the Get Inkey command to the ME and wait for the key to be pressed, and thus cannot carry on with other activities, such as updating or scrolling the display.

As set forth in the T3 documents this enhancement "KEY IDENTIFICATION" opens new user interaction and application possibilities. It adds a useful feature for future advanced services. such as new user-friendly, interactive and fast mobile applications requiring a minimal number of keystrokes. Some

of these applications require continuous actions, even if the user does not respond to them.

If S1 agree that this is a useful new feature which should be standardised, T3 believe that the USAT Stage 1 document may need to be updated to reflect this.

T3 would like to point out that concerns were raised regarding user awareness of the activation of this feature, giving the USAT the possibility to intercept key strokes in a standardised manner. T3 seek the opinion of S1 and S3 on this issue, as it raises a potential security threat.

One way of reducing the potential security threat is to offer the user the possibility of disabling this feature.

3GPP T3 (USIM) Meeting #17
Berlin, Germany, 15 - 17 January, 2001

Tdoc T3-010093
(Updated version of T3-010029)

Background information for T3-010093
(CR 31.111: A new event Key Identification)

Source: Celltick Technologies

The proposed CR is the document T3-010066 and it is related to 3GPP 31.111. It adds the necessary knowledge for future advanced services - the identification of the pushed key by event.

Please note that in the following: when I mention “application” I mean “USAT application.

The kinds of services we are talking about

The services we related to in our CR are services with new user-friendly, interactive and fast (seconds) mobile applications requiring a minimal number of keystrokes.

Some of these applications require continuous actions, even if the user does not respond to them. For example with games: i.e. “Who wants to be a millionaire” where the user is choosing the correct answer from a running set of answers, or in addition - rolling screens, waiting for the user to choose one of them. The application can react differently according to what the user does or does not do, and acts according to different internal time outs.

The services needed to have semi real time (ASAP) and online services, from the point of view of the user (semi “real time” from the user’s point of view is just a few seconds).

When the service is active, it is important to have the possibility to change the text on the screen while waiting for the user to respond.

Why Get Inkey and Get Input are not enough nor suitable for these services

The new event differs from the Get Inkey and Get input commands.

The Get Inkey and the Get Inputs commands are used by an application’s menus and need user response or a Timeout to continue to its next step.
On the other hand, applications which use the suggested event can react and show Display Text/ Image, Play Tone, or any other stage in the application, without the need for user response.

Therefore, only those applications which use an event can implement the games we talked about before (i.e. “Who wants to be a millionaire”).

Why we chose not used the User Activity event

The User Activity event is normally used during idle mode, we did not want to mix the two stages (idle and runtime).

The necessity of getting all the requested pushed keys

It might seem that there is no sense to send all requested pushed keys to the SIM. Moreover it could cause a lot of traffic on the interface.

This first impression is not precise. The event will be set only when the service starts working; not during the whole time while the user uses his/her phone. Therefore we assume that each received pushed key is important to the application, otherwise the application will not set the event again (the application needs to set the event after each received key).

If the user is occupied with other actions not related to the service (i.e. dialing a number), it is logical that the service application stops running the service at that moment. Then the service application will not ask for the pushed key identification (it is not necessary, but maybe there is an exception, and the first digit of the dialed number may be received).

User confidentiality

One of the concerns of using event with key identification is the user confidentiality problem. In the case that the application gets the key identification by event, it could perform illegal actions on the received user information. Moreover it could do it without the user's knowledge and thus cause a user confidentiality problem.

We agreed that if the operator or the application providers would like to perform illegal actions, they can do it, with or without the new proposed event.
This is true no matter where the service is implemented (Terminal and/or SIM), and it can occur as well in existing services today.

We are going to eliminate the User Confidentiality problem by notifying the user about the usage of this kind of event, or other solutions if will be founds (T3 is still working on that).

Conclusions

There is a need to create a USIM/SIM that can work with new advanced services. As we all know, the advanced services are one of the most important features for the future. Therefore, the main point is that the T3 group should change the standard to insure that the terminal and the USIM could control advanced and future services and
we should find the way to do this.

However, the Get Inkey, the Get Input, and the User Activity commands cannot be the solution.

TSG-SA WG 1 (Services) meeting #11 **TSG S1 (01) 0186**
Cape Town, SA 6th to 9th February 2001 **Agenda Item: 5.3.2**

Background information for a new feature on STK (A new event Key Identification)

Source: Celltick Technologies

The kinds of services that required identification of the user activity by event

The services we related to are services with new user-friendly, interactive and fast (seconds) mobile applications requiring a minimal number of keystrokes.

Some of these applications require combination of content depend on time with different display abilities. Moreover they require continuous actions, even if the user does not respond to them. For example with games: i.e. "Who wants to be a millionaire" where the user is choosing the correct answer from a running set of answers, or in addition - rolling screens, waiting for the user to choose one of them. The application can react differently according to what the user does or does not do, and acts according to different internal time outs.

The services needed to have semi real time (ASAP) and online services, from the point of view of the user (semi "real time" from the user's point of view is just a few seconds).

When the service is active, it is important to have the possibility to change the text on the screen while waiting for the user to respond.

Today the commands that enable the USIM to get the user activity identification are from the type of commands that are usually used by an application's menus. These applications need user response or a long TO (approximately 1.5 min) to continue to its next step. During this time the application cannot set any other proactive command (i.e. Display Text), unless the user responds, or the TO passed. The inability to do anything during this TO is not acceptable for these kinds of services.

What is required from S1

- To approve / disapproved this feature.
- LS to T3 and S3 notify them about the decision.
    - Suggestion in the case that S1 approves the feature: S1 approves the key identification event feature on condition that the security issue shall be resolved in T3 and S3 informed.
- Defined the feature
    - Suggestion: The definition of a new USAT "event" that indicates that a key on the MMI has been pressed and includes the key identification. This new feature has the possibility to get the user activity identification while another proactive command is

performed (such as display text). This feature allows continuous actions, even if the user does not respond to them.

- Add text to 22.038 suggestion:
-

6.2 SAT/USAT proactive capability

The SAT/USAT proactive capability is a mechanism whereby the USIM/SIM can request specific actions to be taken by the ME by issuing "proactive commands" thus establishing and maintaining an interactive dialogue with the user and/or communicating with the network..
The ME shall inform the USIM/SIM of the success or otherwise of each command issued to it by the USIM/SIM, and also indicate the command details and if applicable add more specific information.
The proactive command set allows the SAT/USAT to instruct the ME to:

1 display text supplied by the USAT/SAT on the ME's display, with an indication of priority (normal or high), and a defined action (user activity, user activity identification (in a secure manner) or timeout) to terminate the text display.

2 display a text string and obtain the response in the form of a single user keystroke or a string of keys entered by the user and pass the response to the USIM/SIM. If the response is designated as private by the USIM/SIM the ME shall not display the users response on the screen.

CR-Form-v

CHANGE REQUEST

⌘ **TS 22.038** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Indication of Key identification
Source:	⌘	Celltick Technologies
Work item code:	⌘	***Date:*** ⌘ 07/02/01
Category:	⌘	**B** ***Release:*** ⌘ R5

Use one of the following categories:
- ***F*** *(essential 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:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	The entire industry is now looking for new user friendly, interactive mobile applications requiring a minimal number of keystrokes so as not to deter non-technological savvy users from using the applications. Some of the new service applications require continuous actions, even if the user does not respond to them – (for example the user is choosing the correct answer from a running set of answers). The application can react differently according to what the user does or does not do, and acts according to different internal time outs. This functionality provides a simple solution for implementing interactive applications such as games, messaging, polls, etc, and it is suitable for GSM, GPRS, and 3G. It will benefit all the players as follows: The operators will enjoy increased usage of services. The SIM and ME vendors will be able to improve the services that they can jointly support. For the service application providers, it opens up a whole range of future sophisticated service applications.
Summary of change:	⌘	This Change Request proposes a new event that indicates that a key has been pressed and includes the key identifcation in a secure manner.
Consequences if not approved:	⌘	If this CR is not accepted, then the result will be limiting the functionality of future applications, and their adoption by less technological savvy users. There is a need to create a USIM/SIM that can work with new advance services. As we all know, the advanced services are one of the most important features for the future. Therefore, if the USIM has limited service support, it will also limit the user's usage.

Clauses affected:	⌘	6.2
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] 31.111, 11.14

Other comments: ⌘

6.2 SAT/USAT proactive capability

[…]
The proactive command set allows the SAT/USAT to instruct the ME to:

1 display text supplied by the USAT/SAT on the ME's display, with an indication of priority (normal or high), and a defined action (user activity or timeout) to terminate the text display.

2 display a text string and obtain the response in the form of a single user keystroke or a string of keys entered by the user and pass the response to the USIM/SIM. If the response is designated as private by the USIM/SIM the ME shall not display the users response on the screen.

[…]

19. allow the ME to display help information with the commands, by providing the associated text, related to the user action (e.g. menu selection).

20. Provide indication from the ME to the USAT when a key on the MMI has been pressed in a “menu” (response to prompt) or and event (independent action) methods, with key identification. This indication should be done in a secure manner.

TSG-SA WG 1 (Services) meeting #11 **TSG S1 (01) 0196**
Cape Town, South Africa, 6th to 9th February 2001 **Agenda Item: 5.3.2**