From: Muller, F. (Frank)
Sent: Monday, November 24, 2008 1:58 PM
To: 'lia.gerritse-vanbavel@kpn.com' <lia.gerritse-vanbavel@kpn.com>
Cc: Laarakkers, J. (Jeroen) <jeroen.laarakkers@tno.nl>; E.Visscher@dvme.nl
Subject: RE: service-based authentication

RE: service based authentication
Outlook item

Hi Lia,

The application for service-based authentication should be finished by now. See attached the email from Erik from last week.

Regards,

Frank

From: lia.gerritse-vanbavel@kpn.com [mailto:lia.gerritse-vanbavel@kpn.com]
Sent: Monday November 24, 2008 9:45 AM
To: Muller, F. (Frank); E.Visscher@dvme.nl
Cc: Laarakkers, J. (Jeroen)
Subject: RE: service-based authentication

Gentlemen,
How are things progressing with this? I would like to submit this one soon, and, if possible, another one from the RadioCards project in December. Will that work?
Regards,
Lia

From: Muller, F. (Frank) [mailto:frank.muller@tno.nl]
Sent: Monday November 10, 2008 7:56 PM
To: Erik Visscher
CC: Laarakkers, J. (Jeroen); Gerritse, C.J. (Lia) (KPNCC L&R CIPO Intellectual Property)
Subject: RE: service-based authentication

Hi Erik,

Your text is very good basic material, but as I already wrote, it made me think a lot, which resulted in a number of new insights.

First, just a quick comment on the current text. Here is a version of the Word document modified with Track Changes and slightly modified figures. I have made changes to figures 1, 3, and 4.

The following points of attention with regard to the figures:

- Numbers 130 and 132 from Figure 1 do not appear in the text. Does that mean that they can be removed, or that an entity (e.g., the AC manager) should have been given that number, or should they actually have had a different number? For example, number 128 from the text does not appear in Figure 1, while that may have been the intention.
- 312 and 314 are not yet correctly included in Figure 3.

As I wrote in my previous email, it will be difficult to pass an eXpected Service Code to the AuC or to have it determined by the Service Identification Unit in the AuC. There are even more practical objections to the

EX. 2022
Samsung v KPN
IPR2025-00512

implementation examples as they are now. However, I would leave them as they are, after all, they are examples.

Below, the whole idea is now examined more fundamentally:

First, the requirements for the solution:

- An attacker must not be able to change the Service Code (SC); it must therefore be firmly embedded in the response.
- The HLR/AuC must not need to know the value of the SC. In the interface to the HLR/AuC, there are no options to pass this on; the HLR only receives the IMSI (International Mobile Subscriber Identity) of the user.
- The HLR/AuC only provides one value for XRES to the MSC/VLR, not a series of outcomes to try out. (The interface does not offer any options for this.)
- Backwards compatibility: the solution must also work with 'old' Mobile Stations and MSC/VLRs that do not include the SC in the calculation of the response.
- No changes to the (U)SIM. We do not see changes to the SIM or USIM specs as a realistic option.

These requirements lead to a solution in which it is not the HLR/AuC that makes an adjustment to the response, but the MSC/VLR. The AuC and the (U)SIM can simply continue to work as before.

This does mean that the customer's secret key cannot be involved in this, because they are only known to the AuC and the (U)SIM.

Then, I conclude that the mobile with the SC must modify the response RES and with a one-way function, so that it cannot be undone by the attacker. The MSC/VLR can release the same one-way function on the XRES and SC to check the RES'. I have put this (rough sketch) in an added Figure 5. Actually, this solution is already described in broad terms on page 5, line 30 to page 6, line 18, but it should be added as a preferred implementation example, at the top of (the current) page 16. This solution also provides the desired backwards compatibility: if the mobile is not equipped with the option to take the SC with it, the MSC/VLR will not do this either, or vice versa.

In my opinion, this new event still corresponds exactly with Claim 1 and Claim 2. Claim 3 and 4 are tailored to the implementation example you described and do not match the new insights. So, I think that additional claims are needed. The old Claims 3 and 4 should remain, I think. Claims 5, 6, 7, 8, and 9 also fit the new insights. Claim 10 does not. Claims 11 to 15 do.

Furthermore, there should be a Service Identification Unit (or Trusted Module, or Authentication Manager, or something like that) in the mobile that securely determines via which interface the challenge has arrived and processes the correct Service Code in the RES'. This module should also be the only module that receives the RES value from the UICC; see my Figure 6. The 3G radio card could play this role, but it does not have to.

The only thing that is not yet fully secured, and for which I do not yet have a ready-made solution, is that the attacker could make the network or the mobile appear more stupid than it is (namely not able to include the SC in the response), and, in this way, abuse the backwards compatibility. But I don't need to have solved that already to be able to patent the idea so far?

I wanted to leave it at that for now. Can you call me if you have any questions about it, which I can well imagine, if I need to provide more detailed input, or if you want to discuss how we will proceed with this?

Regards,

Frank

From: Erik Visscher [mailto:E.Visscher@dvme.nl]
Sent: Wednesday October 8, 2008 3:40 PM
To: Laarakkers, J. (Jeroen)
Cc: Muller, F. (Frank); Hartog, T. (Tim); Fransen, F. (Frank); lia.gerritse-vanbavel@kpn.com
Subject: service-based authentication

Dear all,

Attached is the draft regarding the above application. Please let me have your critical comments and additions where necessary. I also have a question (see p.13 description).

Kind regards,

De Vries & Metman
Erik Visscher

Overschiestraat 180
1062 XK Amsterdam
The Netherlands
Tel: +31 20 5110930
Fax: +31 20 5110931
E-mail general: mail@dvme.nl
Website: www.dvme.nl

This e-mail and the information it contains is for the use of the addressee(s) and may be confidential or privileged. Unauthorised use, disclosure or copying is strictly prohibited. If you are not the/an addressee and are in possession of this e-mail, please notify us immediately.

De Vries & Metman is a partnership consisting of professional corporations. The general terms and conditions of de Vries & Metman, which stipulate a limitation of liability, the applicability of Dutch law and the exclusive jurisdiction of the District Court of Amsterdam, are applicable to all work performed. A copy of the general terms and conditions is available on request or at www.dvme.nl.

This e-mail and its contents are subject to the DISCLAIMER at http://www.tno.nl/disclaimer/email.html

TRANSLATOR'S CERTIFICATE OF TRANSLATION

Questel-Orbit, Incorporated
2331 Mill Road, Suite 600
Alexandria, VA 22314, U.S.A.
www.questel.com

Questel Project Number: [ ]
Date: 05/07/2025

To whom it may concern:

I, Hugh T. Robinson, a translator fluent in the Dutch and English languages, on behalf of Questel, do solemnly and sincerely declare that the following is, to the best of my knowledge and belief, a true and correct translation of the document(s) listed below in a form that best reflects the intention and meaning of the original text.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true. I further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Original Document Identifier:	[2008.11.24 RE_ service based authentication-1.msg]
Translated Document Identifier:	[ ]

Signed this 7th day of May, 2025

Hugh Robinson

Signature

Hugh T. Robinson

Name