Subscriber Authentication in Cellular Networks with Trusted Virtual SIMs

Conference Paper · March 2008

DOI: 10.1109/ICACT.2008.4493913 · Source: IEEE Xplore

3 authors:

Michael Kasper
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.
18 PUBLICATIONS **210** CITATIONS
SEE PROFILE

Nicolai Kuntze
Hochschule Mainz
95 PUBLICATIONS **483** CITATIONS
SEE PROFILE

Andreas U. Schmidt
Institute of Electrical and Electronics Engineers
86 PUBLICATIONS **519** CITATIONS
SEE PROFILE

Subscriber Authentication in Cellular Networks with Trusted Virtual SIMs

Michael Kasper, Nicolai Kuntze, Dr. Andreas U. Schmidt
Fraunhofer-Institute for Secure Information Technology SIT
Rheinstrasse 75, 64295 Darmstadt, Germany
Email: {michael.kasper,nicolai.kuntze,andreas.u.schmidt}@sit.fraunhofer.de

***Abstract*—The primary goal of this paper is to design a software replacement for a Subscriber Identity Module (SIM) based on the *TCG MPWG Reference Architecture* in order to access a mobile cellular network and its offered services. Therefor, we introduce a *virtual software SIM (vSIM)* with comparable usage and security characteristics like the traditional smartcard-based solution. Additionally, running a virtual SIM as a trusted and protected software on a mobile device allow significant expansion of services by introducing new usage scenarios and business models, cost reduction and more flexibility. Our approach demonstrates the substitutability of a SIM card with an adequate trusted software module supported and protected by a trustworthy operating system. In particular we propose several methods for authentication and enrollment of a subscriber.**

I. Introduction

In its *TCG Mobile Reference Architecture*, the Mobile Phone Work Group of the Trusted Computing Group (TCG MPWG) specifies a new concept to enable trust into future mobile devices. It offers new potentials for implementing trust in mobile computing platforms by introducing multiple trusted engines on behalf of different stakeholders supported by a hardware-based trust anchor [1], [2]. Due to the capabilities of a mobile trusted platform (MTP) to support multiple trusted engines with protected storage, strong isolation and secure communication within a defined security perimeter, the MTP is able to take over the SIM functionality.

This paper is organized as follows. In Section II, we give an overview of the vSIM architecture. The following Section III is the core of this paper. Here we present conceptual models for subscriber enrollment and authentication in mobile cellular networks using trusted computing. Furthermore, we discuss the benefits in context to existing proposals. In Section IV we conclude on our work and point out further research.

II. Architectural Overview of a vSIM Platform

The TCG MPWG has developed an architecture on a high level of abstraction for trusted mobile platforms. In this section, we familiarize the reader with significant components and services of a vSIM platform. For a better understanding, we recommend to [1] and [3]. In particular, the paper [3] of the authors introduce to essential parts of the *TCG MPWG Reference Architecture* and give an overview of significant platform components in terms of our objective. Figure 1 schematically shows the layout of such a MTP. It holds an

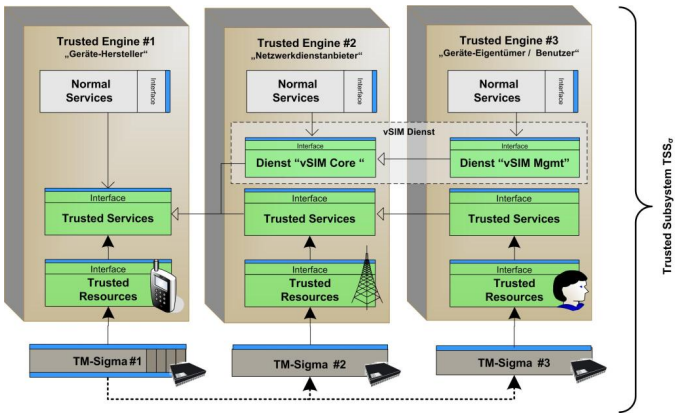

Fig. 1. Trusted vSIM Architecture

(abstract) virtual software SIM service which substitutes the traditional smartcard and its functionality.

In general, a MTP supports a set of trusted engines (TE). Each engine represents a protected domain associated with a specific stakeholder. In our purpose, we consider a minimal set of four different stakeholders: the Device Manufacturer (DM), the Mobile Network Operator (MNO), the Device Owner (DO) and the Device User (DU). For the sake of simplicity, we assume that the device owner is equal to a user of a mobile device, and therefore we set $DO = DU$.

For each environment, we define a trusted subsystem $\mathcal{TSS}_\sigma$ as a logical unit of a trusted engine together with its interrelated hardware compartment of a stakeholder σ. It is used for security-critical functionality and consists of a Mobile Trusted Module (MTM_σ) with its associated trusted engine TE_σ. All sensitive data required by the trusted subsystems is protected by their dedicated MTM_σ, either directly or indirectly.

Device Manufacturer Subsystem: The $\mathcal{TSS}_{DM}$ is responsible for the integrity and configuration of a device. It typically controls all internal and external communications and provides all security-critical hardware resources of a device. For this reason, all protocol messages of an embedded TSS_σ are routed through resources of $\mathcal{TSS}_{DM}$ to its destination.

Mobile Network Operator Subsystem: All cellular services of a platform are assigned to $\mathcal{TSS}_{MNO}$. It is responsible for administration and protection of the *vSIM Credential* ($Cred_{vSIM}$) and implements the network authentication mechanisms. Therefor, it provides a *vSIM Core Service*

($vSIM_{CORE}$) to the device owner, which implements the fundamental SIM functionality.

Device Owner Subsystem: In context of the vSIM service, the $\mathcal{TSS}_{DO}$ protect all personal information and corresponding user credentials ($Cred_U$). Moreover, it holds a *vSIM User Management Service* ($vSIM_{MGMT}$) and is responsible for administration and authentication of local users. In particular, $vSIM_{MGMT}$ offers an internal authentication oracle to the $vSIM_{CORE}$ service, to provide evidence of a local user's identity.

III. Subscriber Authentication with Trusted virtual SIMs

In this section, we will give an informal description of the scenario and identify the essential components of an idealized protocol. Based on this scenario, we design two intergraded conceptual models for subscriber authentication in mobile cellular networks using trusted computing. Furthermore, we discuss how user enrollment and key delivery mechanisms are carried out efficiently.

A. Base Scenario

The use-case under consideration is illustrated in Figure 2 and involves four significant entities: the local user (U), the trusted mobile platform (MTP), the Mobile Network Operator (MNO), and the Point-of-Sale/Point-of-Presence (POS).

In this scenario, U wants to establish a long-time relationship with the MNO (Step 1), in order to use the mobile network infrastructure and its offered services (e.g. GSM, UMTS or Location Based Services). Instead of purchasing a physical SIM card, the MNO supplies the $vSIM_{CORE}$ service inside $\mathcal{TSS}_{MNO}$ with a virtual software SIM credential (Step 3). Every time a user wants to access the mobile network, he/she authenticates to the vSIM service (Step 4), which uses the vSIM credential to perform network authentication (Step 5,6).

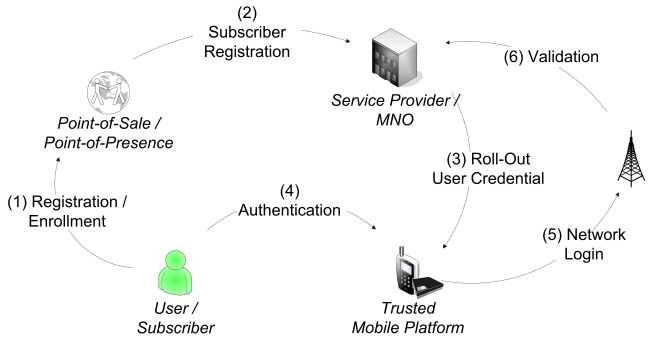

Fig. 2. Generic Trusted Mobile Scenario

B. Subscriber Enrollment and vSIM Credential Roll-Off

A user of a MTP wants to acquire an vSIM credential to use with the $vSIM_{CORE}$ service. The subscriber credentials are pre-generated by the MNO, derived from an initial secret, or generated by the MNO during the acquisition. This protocol is used to

- request a vSIM credential,
- authenticate the involved entities, and
- download and install the requested vSIM credential.

Because the vSIM services are completely implemented as a trusted software application, it implies that the respective vSIM credentials has to be transferred from the MNO to the vSIM service in a secure manner. In traditional SIM-based systems, the subscriber gets a security token after his/her enrollment. Contrary to a vSIM, this security token physically exists and can be pre-delivered with an included key, to the respective Point-of-Sale.

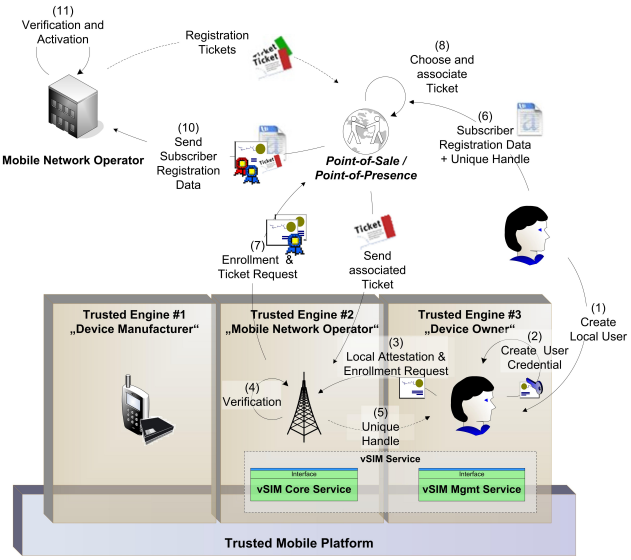

Fig. 3. Model "Subscriber Registration and Enrollment"

The Point-of-Sale POS orders a set of (pre-generated) registration tickets $Ticket_i$ from the MNO. A registration ticket consists of a triple: $Ticket_i := \{IMSI_i, RAND_i, AUTH_i\}$. The $IMSI_i$ identifies an *International Mobile Subscriber Identity* as described in [4]. In other scenarios, it may be a unique credential ID that is assigned by the network operator. The term $RAND_i$ denotes a random value, which is needed to challenge TSS_{MNO} in the course of the protocol. Finally, with the $AUTH_i$ the MTP is able to check the integrity and authenticity of $Ticket_i$.

Phase 1 : "Subscriber Registration and Enrollment": The following protocol sequence is depicted in Figure 3 describes the user enrollment and registration for services, offered by the MNO.

The user starts to request a new user credential for a local user, which is generated by TSS_U. For this, the local user enters a unique personal identifier ID_U, personal registration data $REGDATA_U$ and an authorization password CHV_U to the trusted service $vSIM_{MGMT}$ (Step 1).

Afterward, $vSIM_{MGMT}$ generates a asymmetric signature key-pair K_U and creates a certificate, which includes all relevant information, like the $REGDATA_U$ and the public

portion of K_U (Step 2). The $vSIM_{MGMT}$ pass this certificate $CERT_U$ to the $vSIM_{CORE}$ service (Step 3).

Within this step, $vSIM_{MGMT}$ requests a enrollment procedure and reports its current state and configuration to the local verifier of $vSIM_{CORE}$. The TSS_{MNO} validates the given data (e.g. against Reference Integrity Metrics (RIM)) and checks, whether the present engine's state is in a acceptable condition (Step 4). Once the $vSIM_{CORE}$ is convinced about trustworthiness of the device, generates a unique handle PID of this process and sends this value to the $vSIM_{MGMT}$ (Step 5).

Now, the user starts to communicate its registration data $REGDATA_U$ (e.g. name, address, accounting information, passport ID) and the PID to the Point-of-Sale (Step 6). $vSIM_{CORE}$ requests an enrollment procedure for U. Therefor, it signs the PID, its own certificate and the obtained user certificate and sends this package to the POS (Step 7).

After having received the request, POS chooses a $Ticket_i$, bind it to the key $K^{pub}_{TSS_{MNO}}$ (Step 8) and sends it to TSS_{MNO} (Step 9). In this case the POS could be an arbitrary point-of-sale or internet portal, which is accredited by the MNO.

Once the POS is convinced about trustworthiness of both, user and device, it attaches $CERT_U$ and the $IMSI_i$ (of the chosen ticket) to the given $REGDATA_U$, signs all gathered information with its private portion of its signature key K_{POS} and sends the signed data (online or offline) to the MNO (Step 10). Optionally, the POS encrypt the data with the public portion of K_{MNO}.

The MNO verifies the data and generates the $Cred_{vSIM}$ with the $IMSI_i$, the shared key K_i and the certificate $CERT_U$ and signs this bundle with the private signature key K_{MNO}. Finally, the MNO activates the signed $Cred_{vSIM}$ and the corresponding nonces in its authentication center (Step 11). Now, the mobile device is able to access the registration service provided by MNO over some kind of channel. For instance, this service is implementable as a network teleservice or internet download service.

Phase 2: "Secure vSIM Roll-Out and Installation": In the second phase of the protocol details the secure vSIM roll-out and installation as illustrated in Figure 4.

In order to obtain a $Cred_{vSIM}$, the user performs a log-in sequence and sends a unique id ID_U with a proper password CHV_U to the $vSIM_{MGMT}$ service, which loads the associated user key-pair K_U from protected storage (Step 1). In a next step, the $vSIM_{MGMT}$ initializes a *vSIM Roll-Out Procedure* and sends a request the the $vSIM_{CORE}$ service (Step 2). After having received this message, it unbinds the corresponding $Ticket_i$ and verifies the authenticity and integrity of the $Ticket_i$ (Step 3). Next, $vSIM_{CORE}$ extracts the $NONCE_U$ from the $Ticket_i$ and challenge U with this value.

$vSIM_{MGMT}$ signs the $NONCE_U$ together with its ID_U in order to prove its identity to the MNO. This bundle is sent back to $vSIM_{CORE}$.

After $vSIM_{CORE}$ has received the message, it composes a vSIM credential request and submits it to the assigned MNO registration service via some channel, mentioned above (Step 4). Therefor, $vSIM_{CORE}$ extracts $NONCE_{MNO}$ from the $Ticket_i$ and signs it together with the $IMSI_i$. Afterwards, the $vSIM_{CORE}$ sends its own signature and the obtained user signature to MNO.

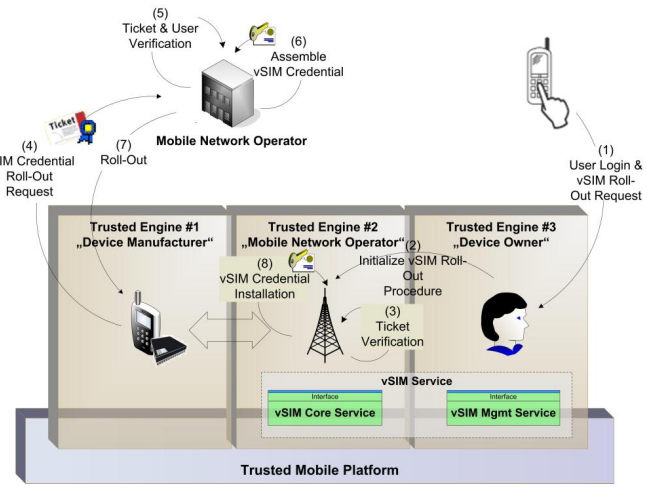

Fig. 4. Model "vSIM Credential Roll-Out"

Having received $vSIM_{CORE}$'s request, MNO verifies the messages and obtain $CERT_U$ and $Cert_{TSS_{MNO}}$ (either from the request or from local storage) (Step 5). If revoked, it replies with an error message and halts the protocol. Otherwise the request is approved by the MNO. Next, MNO prepares $Cred_{vSIM}$ for transfer to $vSIM_{CORE}$, and generates a randomly chosen session key K_S. Afterwards, the key K_S is bound with to corresponding binding key of TSS_{MNO} to the destination platform (Step 6). The MNO encrypt $Cred_{vSIM}$ with this session key and sends both to the TSS_{MNO} (Step 7).

Finally, TSS_{MNO} unbinds K_S. With this key it decrypts the vSIM credential and checks the enclosed signature (Step 8). If the decryption is correctly processed and the signature is verified, $vSIM_{CORE}$ seals the obtained $Cred_{vSIM}$ to valid platform configurations and finishes its installation.

C. Model "One" - Subscriber Authentication with compatibility to GSM - Authentication

Our proposal for model "One" is straightforward to actual GSM standard. It is implementable in conventional GSM clients without any technological changes at the GSM infrastructure and at the GSM authentication protocol. The main task of the vSIM service is to take over the functional range of the SIM card, with no additional duties and responsibilities regarding to the GSM 11.11 SIM specification [4]. The cryptographic algorithms A3 and A5, responsible for user authentication and key generation are implemented within the $vSIM_{CORE}$ service. [1]

[1]We note that the specified GSM algorithms is substitutable by any other authentication algorithm, which requires provisioning of symmetric keys (e.g. one-time-password hashes or symmetric cryptographic keys) and associated attributes in form of a subscriber credential.

Phase 1: "Initialization of vSIM Credentials": First, the user initialize the vSIM services and performs a log-in sequence. He/she sends a unique id ID_U with a proper password CHV_U to the $vSIM_{MGMT}$ service (Step 1), which loads the associated user credential from protected storage (Step 2).

Afterward, the $vSIM_{MGMT}$ service connects to the trusted interface layer of the $vSIM_{CORE}$ service and sends a vSIM credential initialization request to the $vSIM_{CORE}$ service (Step 3). After having received this request message, $vSIM_{CORE}$ generates a number $RAND_{AUTH}$, randomly chosen from a suitable range and sends this value as an authentication challenge to $vSIM_{MGMT}$, which holds the actual signature keys of U.

Now, the $vSIM_{MGMT}$ takes the corresponding private portion of the user signature key, signs the challenge $RAND_U$ and sends this value back to the $vSIM_{CORE}$ service (Step 4).

Once, the $vSIM_{CORE}$ has received the signed message, it verifies its status. Finally, the $vSIM_{CORE}$ unseals $Cred_{vSIM}$ and initializes the SIM functionality using the $IMSI_i$ and K_i (Step 5).

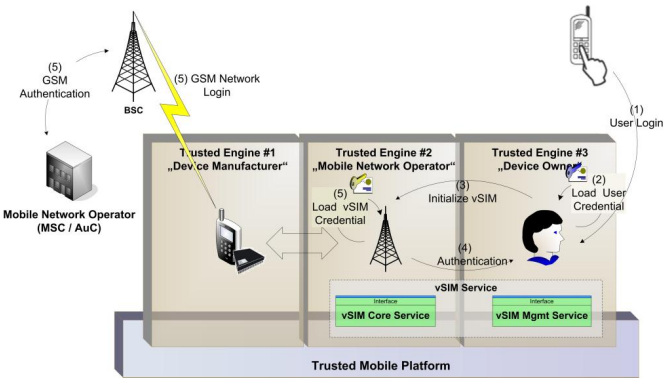

Fig. 5. Subscriber Authentication Figure - Model "One"

Phase 2: "Subscriber Authentication": The GSM standard defines its own authentication protocol based on SIM credentials. Since the SIM_{CORE} indirectly talks to the MNO, $\mathcal{TSS}_{DM}$ must provide a means to relay these messages between the $vSIM_{CORE}$ service and the MNO, this communication should be transparent to this protocol. All relevant communication mechanisms, like cryptographic algorithms A3 and A5, responsible for user authentication and key generation are implemented within the $vSIM_{CORE}$ module.

Following protocol sequence outline the authentication process in GSM networks (Step 5, Step 6): First, the MTP initializes the authentication process and sends the $GSMAuthAlgorithm$ command to the $vSIM_{CORE}$ service of TE_{MNO}. In the next step, the MTP requests for authentication at the GSM network. Therefor, TSS_{DM} relays $IMSI_i$ from $vSIM_{CORE}$ to MNO. The MNO generates internally a set of authentication triplets. It contains a authentication challenge $RAND_i$, a corresponding session key K_c and a $SRES$. The MNO replies to TE_{MNO} by sending the challenge $RAND_i$. This $RAND_i$ is passed to the $vSIM_{CORE}$ service. Next, it also uses the A3 algorithm together with the key K_i. The output of the algorithm is the challenge response message $SRES^*$. The $vSIM_{CORE}$ sends this $SRES^*$ message to the MNO. Finally, the MNO compares the $SRES$ with $SRES^*$. If they are equal, the subscriber is authenticated and $vSIM_{CORE}$ also derives the shared session key K_c

D. Model "Two" - Subscriber Authentication with Remote Attestation for Basic Network Access

In this section, we present a more comprehensive model compared with the precedent one. Additionally to model "One", we integrate remote attestation for basic network access. A variant of this method has been described in [5]. Beside the main task of SIM substitution, it provides

- user-authenticated access to the subscriber subdomain,
- device-authenticated access to a generic domain,
- mutual authentication between the MNO and a trusted mobile device.
- finer-grained functional restriction (e.g. SIM-lock), and
- dynamic down-/upgrade of services

As illustrated in Figure 6, all devices inside a generic domain are able to use the generic services of the mobile communication network. A MTP which is located in the MNO domain has access to both specific subscriber-authenticated services and generic services. Such generic service, for instance are location-based information or WLAN-based internet services. In case of a mobile phone is located inside the generic domain,

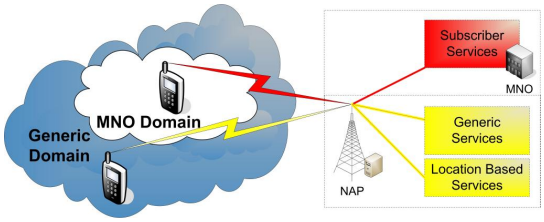

Fig. 6. Restricted Subdomain by Trust Credentials

it uses a generic credential $Cred_{BASE}$ based on remote attestation mechanisms, to gain basic network access. The assignment to the subscriber domain of MNO is then done by performing a user-specific authentication process using vSIM credentials.

Phase 1: "Basic Network Access": First, the MTP initialize the remote attestation and device authentication process. MTP requests the trusted engine TE_{DM} for a platform attestation and device authentication, addressed to the MNO. Then, TE_{DM} performs this request and connects to the corresponding network access point NAP_{MNO} (Step 1). Therefor, the TSS_{DM} generates a random value $RAND_{BASE}$ and and performs a platform attestation. Next, the base authentication service of TE_{DM} sends $RAND_{BASE}$, the attestation data and its certificate $Cert_{DM}$ to the network access point.

Having received this request, the NAP_{MNO} checks the state of the client machine. If the signed integrity metric of the client platform fails verification or no reference state is found,

the NAP_{MNO} aborts the protocol and replies with an error message. Otherwise, the platform passed authentication and is considered as trustworthy. Afterward, the NAP_{MNO} requests an accredited entity to generates a session key K_{BASE} and a network ticket (Step 2). Such an accredited entity may be an authentication center AUC_{MNO}, which belongs to the mobile network provider MNO. Substantially, the ticket contains the following information:

$$Ticket_{BASE} := \{ID_{MTP}, ID_{NAP}, K_{BASE}, REALM_{BASE}, LIFETIME_{BASE}\}.$$

Next, AUC_{MNO} encrypts $Ticket_{BASE}$ with the public (or shared) encryption key K_{NAP} and send both, $Ticket_{BASE}$ and K_{BASE} to the NAP_{MNO} (Step 3), which relays it to the client platform (Step 4). Therefor, the message is bound to the trusted subsystem TSS_{DM} with the corresponding public key $K_{TSS_{DM}}$ and a valid platform state.

Once, TSS_{DM} has received the signed message, it verifies the status of the signed $RAND_{BASE}$ (Step 5). If revoked, the subsystem replies with an error message and halts the protocol. Otherwise the AUC_{MNO} is authenticated by the challenge response.

Next, TSS_{DM} decrypts the session key K_{BASE} and sends $ENC_{K_{NAP}}(Ticket_{BASE})$ together with an authenticator A_{MTP} to the NAP_{MNO}. The authenticator A_{MTP} is composed of its platform identity ID_{MTP}, the current network address $ADDR$, and a timestamp $TIME$.

After, NAP_{MNO} has received the encrypted ticket, it verifies the embedded information. If the status is valid, the MTP is authenticated and access to the generic services is granted.

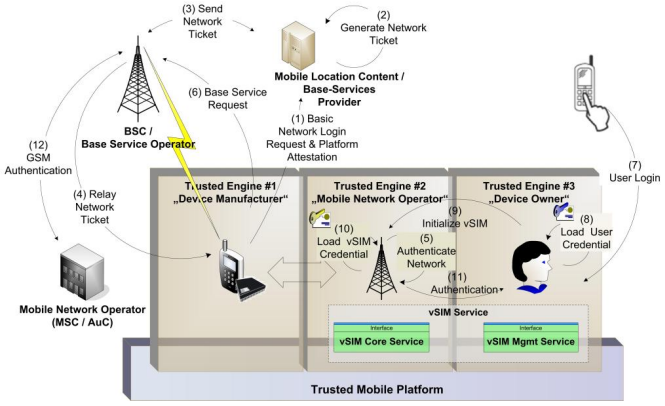

Fig. 7. Subscriber Authentication Figure - Model "Two"

Phase 2:"Initialization of vSIM Credentials": The initialization of a vSIM credential is performed in Steps 7 - 11 of Figure 7. This process is identical to model "One".

Phase 3: "Subscriber Authentication": Similar to Section III-C, this variant performs subscriber access with compatibility to regular GSM authentication. In an additional step, K_{BASE} is substituted by the session key K_c on both sides, the NAP_{MNO} and MTP (Step 12).

At this point a mutual authentication between the AUC_{MNO} and U has been performed. The AUC_{MNO} is authenticated by the signed challenge, obtained in step 4. On the other hand, the user has prooven its identity by $SRES$. The authentication between NAP and U is implicitly proven by a valid communication key K_c.

If an explicit authentication of these entities is required, some additional steps have to be carried out. The NAP authenticates itself to the platform by the following steps. First the NAP extracts the timestamp from the authenticator A_U. Next, NAP increments the value and encrypts it with the shared communication key K_c (or a derivation of it). Finally, it sends the message back to the trusted platform.

E. Classification of existing virtual SIM proposals

Since the term vSIM is not new, we clearly separate our invention from existing vSIM schemes. In general, the related approaches can be categorized into the following four classes

- a single-trust anchor architecture using SIM-CCs,
- a client-server architecture using SIM-CCs or vSIMs,
- a dual trust anchor architecture using SIMs-CCs, and finally
- a single trust-anchor architecture using vSIMs.

Single Trust-Anchor Architecture using SIM-CCs: This architecture is the established and proposed means for subscriber authentication in current used, mobile cellular networks, including the mobile communication systems GSM and UMTS. It holds one single physical SIM-CC (Circuit Card) as security ancor. In this case, the SIM-CC offers a protected environment and hold the subscriber credential as well as the required algorithms.

Client-Server Architecture using SIM-CCs or vSIMs: Another approach for subscriber authentication is based on a client-server architecture [6], [7]. The primarily idea behind this concept is to provide a backend for storage of any number of SIM-CCs or vSIMs. Each remote client is equipped with a SIM emulation which acts as a mediator. While performing network authentication, the client connects to the backend in order to relay the authentication messages.

Dual Trust-Anchor Architecture using conventional SIMs: This approach identifies an architectural direction with two coexisting hardware-based trust anchors, namely the SIM and the MTM. Each anchor is instructed to process different tasks. While the primarily task of the SIM is to identify and authenticate a local user in a secure manner, the MTM is mainly responsible for providing evidence of the trustworthiness of the device and its associated components. This approach represents the *State-of-the-Art* for next-generation mobile handhelds, according to major members of the Trusted Computing Group.

Single Trust-Anchor Architecture using virtual SIMs: A software-based vSIM (SW-vSIM), mentioned in [8]–[11], completely stores the subscriber information in form of a credential in addressable non-volatile memory. The computation algorithms (like A5/A3) are stored within that store as well. A HW-integrated virtual SIM (HW-vSIM) solution envisages a on-chip solution with multiple vSIMs [12]. Here, each HW-vSIM integrates the subscriber credential into an

individual vSIM module, which is stored and encrypted within nv-memory of a dedicated microcontroller.

All these solutions implicitly or explicitly demands a trusted environment in which the vSIM is executed. Unlike the precedent architecture, our approach identifies a hybrid solution. It is based on one hardware-based trust anchor, namely the MTM, and virtual SIMs as software protected by a secure compartment of a trustworthy operating system.

F. Benefits and Vantages of TC-based vSIMs

In order to envision the benefits and advantages, we will define the following benchmarks which are seen as crucial for development and production, as well as for market and user's requirements: (1) *Security and Trustworthiness*, (2) *Cost-effectiveness*, (3) *Flexibility and Scalability*, (4) *Portability and Mobility*, and (5) *Usability, Compatibility and Acceptance*.

Security and Trustworthiness: It is important, that our proposed vSIM services are at least as secure as traditional SIM-Cards. Therefore, the platform must satisfy some generic SIM security characteristics, namely *Protected Storage*, a tamper-resistant *Isolated Execution Environment*, *User Authentication* and *Secure Channel*. This includes, that an adversary is not able to read, modify or destroy security-sensitive data or circumvent the access control mechanisms. It also must prevent leakage of sensitive information and has to guarantee that all required services are availability and work as expected.

Cost-effectiveness: Our approach reduces the production as well as the logistical costs, regarding to the two-trust-anchor solution while keeping an adequate level of security and trustworthiness. First, the MNO is able to reduce the production costs, while using the already installed MTM for its purpose of subscriber authentication. Second, as the vSIM is completely implemented as a software object, it implies that a $Cred_{vSIM}$ can transferred from the MNO to the vSIM Container via an arbitrary network connection. A MNO can reduce and minimize effective costs of the logistic process.

Flexibility and Scalability: The vSIM service architecture for subscriber authentication offers flexibility and scalability to both, the user and the MNO. The following opportunities shortly sketch the benefits concerning this issue: (1) parallel vSIMs in a single Mobile Device, (2) Online Registration and Roll-Out of vSIM Credentials, (3) Network-based Migration of a vSIM Container and vSIM Credentials, (4) Remote Update of Services, Firmware and Applications and (5) Dynamic Up- and Downgrade of Network Services

Portability and Mobility: The vSIM architecture allows subscribers to use a $Cred_{vSIM}$ with arbitrary MTP. With the identified protocols for deployment and management in [3], a vSIM credential is removeable and portable to other devices. Hence, it enables a subscriber to use its credential with other devices, and vice versa.

Using two different vSIM compartments on behalf of the stakeholder MNO and U, the vSIM architecture enables explicitly to differentiate between device and subscriber identity. A MTP and a subscriber have their own identity with different intended usage characteristics.

Usability, Compatibility and Acceptance: Determining usability and compatibility of a system is an important part, since it finally leads to the acceptance of the proposed vSIM architecture. For this reason, we have designed the subscriber authentication protocols with a high level of compatibility to current GSM standards.

IV. Conclusion and Further Work

The present paper demonstrates the substitutability of a SIM card with an adequate trusted software module, supported and protected by a trustworthy operating system. In this regard, we have introduced vSIM Credentials as a means for subscriber authentication based on the TCG MPWG technology. It offers a real alternative to the other SIM-based solutions under consideration, while an sufficient degree of security and usage characteristics are reached. The prototypical implementation of the Trusted vSIM architecture and the specified services as an extension to an existing Trustworthy Computing Platform is currently under development.

Using a vSIM as a trusted and protected software allows expansion to a much wider field of authentication and identification management systems on Standard-PC platforms [13]. The realization of (mobile) trust credentials in user-centric scenarios by vSIM credentials or the support of online transactions are thinkable approaches.

References

[1] TCG. TCG MPWG Mobile Reference Architecture. Specification Version 1.0, 2007.

[2] TCG. TCG MPWG Mobile Trusted Module Specification, Version 0.9, 2006.

[3] Michael Kasper, Nicolai Kuntze, and Andreas U. Schmidt. On the Deployment of Mobile Trusted Modules. In *To appear in: Proceedings of the Wireless Communications and Networking Conference WCNC, Las Vegas, USA*, 31 March - 2 April 2008.

[4] GSM Recommendations GSM 11.11. Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface. Technical report, ETSI, 1997.

[5] Nicolai Kuntze and Andreas U. Schmidt. Trusted Computing in Mobile Action. In *Peer reviewed Proceedings of the ISSA 2006 From Insight to Foresight Conference*. Information Security South Africa (ISSA), 2006.

[6] Implementa GmbH. Virtual SIM System for Carrier Class GSM Gateways. http://www.implementa.com.

[7] Goldtwaite et al. System and Method for mobile transactions using the bearer independent protocol, Pat. No. US 7280847 B2. United States Patent, 2007.

[8] Kalavade et al. Method and apparatus for integrating billing and authentication functions in local area and wide area wireless data networks, Pat. No. US 2003/0051041 A1. United States Patent Application Publication, 2003.

[9] Zabawskyj et al. Method for implementing a wireless local area network (WLAN) gateway system, Pat. No. US 2003/0051041 A1, Pat. No. 2004/0258031 A1. United States Patent Application Publication, 2004.

[10] Waugh et al. Integration scheme for a mobile telephone, Pat. No. US 2003/0051041 A1, Pat. No. 2004/0258031 A1, Pat. No. US 6324402 B1. United States Patent, 2001.

[11] Jones et. Al. Use of Internet Web technology for wireless internet access, Pat. No. US 6873609 B1. United States Patent, 2005.

[12] Lindemann et al. Replacement of externally mounted user interface modules with software emulation of user interface module functions in embedded processor applications, Pat. No. US 6799155 B1. United States Patent, 2004.

[13] Jane Dashevsky, Edward C. Epp, Jose Puthenkulam, and Mrudula Yelamanchi. SIM Trust Parameters. *Intel Developer Update Magazine*, 2003.