Secure and Seamless Session Management in Mobile and Heterogeneous Environment

Ali Hammami and Noëmie Simoni
Telecom ParisTech, LTCI, UMR 5141 CNRS, 46 Rue Barrault, F75634 Paris Cedex13, France

Keywords: Security as a Service, Device as a Service, Mobility and Heterogeneity, Secure and Unique Session, Security Continuity, Token, SIP+, Virtual Private Device Network.

Abstract: The Next Generation Network and Services (NGN/NGS) environment becomes more and more heterogeneous and mobile. Furthermore, today user seeks to access his services within a secured session ensuring the continuity and the quality of service. This rapid evolution and requirements raise the issue of guarantying the continuity of user-centric session in an advanced mobility context. This work targets particularly access control and security aspects based on Service Oriented Architecture in mobile and heterogeneous environments. To address the aforementioned challenges, we propose a secure and seamless session management solution that is based on several concepts and mechanisms. First, this solution ensures security management that overcomes session security and uniqueness challenges by gathering ubiquitous, mutualisable, autonomous and stateless service components. Second, we present a multiple and heterogeneous terminal composition by proposing a Virtual Private Device Network (VPDN) concept that is based on secure and auto-managed components. Finally, in addition to these proposed architecture components and concepts, we introduce SIP+ in order to ensure the security continuity within a seamless session during user mobility.

1 INTRODUCTION

The emergence and evolution of Next Generation Networks (NGN) have raised several challenges mainly in terms of heterogeneity, mobility and security. In fact, the user is able, in such environment, to have access to many networks, via multiple devices, with a vast choice of services offered by different providers. Furthermore, end-users claim to be constantly connected anywhere, anytime and anyhow. Besides, they want to have a secure access to their services through a dynamic, seamless and continuous session according to their preferences.

In order to meet these challenges, a new vision of services called Next Generation Services (NGS), which addresses heterogeneity, mobility and user-centric issues, should be adopted. This approach based on Service Oriented Architecture conceives each resource (terminal, access network and service) as a service that intervenes in a dynamic service session. In addition, it provides many advantages in terms of reusability, dynamicity, flexibility, interoperability and mutualization.

However, security is still a crucial issue in such open mobile environment and dynamic session that involves multiple services. Indeed, in order to integrate security aspects to this novel service architecture, security should not be ensured in a static and centralized way, it should be provided as a service. Thus, we aim through our proposal based on security as a service approach to ensure a secure service access and to guard security continuity within a seamless session.

To achieve this objective, we have to consider mobility aspects involved in our NGN/NGS context. In fact, in a user-centric vision, the user wants to access his personalized services that are provided by various service providers (service mobility), while switching between different terminals (user mobility) or access networks (terminal mobility). All these mobility types must be ensured while preserving a continuous user session (session mobility). In this paper, we focus particularly on combining security and user mobility aspects. This type of mobility consists of the fact that a user can change his terminal during the same session according to his preferences. To ensure a secure usage and change of the different user terminal, we introduce the device-as-a-service approach that consists of considering each user terminal as a service component belonging to Virtual Private Device Network (VPDN). In this way, we show how the user can use and change his terminal within a secure

Hammami A. and Simoni N..
Secure and Seamless Session Management in Mobile and Heterogeneous Environment.
DOI: 10.5220/0004071602820289
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 282-289
ISBN: 978-989-8565-24-2

and continuous session.

In this paper, we propose then a secure and seamless session management solution applied in mobile and heterogeneous environment. This solution permits to answer principally the following questions: How to guarantee a secure service access within a continuous session? How to manage user terminals and ensure secure usage of these terminals during his session? And how to ensure security continuity during user mobility?

The remainder of the paper is organized as follows. In section 2, we present an overview of existing approaches that invoke security and mobility aspects and use the Session Initiation Protocol (SIP)(Rosenberg et al., 2002) to support these aspects. In section 3, we describe our proposition. In this section, we define first our security management solution based on security service components and a token used for single sign seamless session. Then, we introduce the VPDN concept. Next, we address user mobility aspect by proposing a token based SIP+ protocol to ensure the continuity of security. Section 4 shows the feasibility of our proposition. Finally, section 5 presents the conclusion and perspectives for future work.

2 RELATED WORK

Mobility management, within a seamless session while ensuring a secured access in continuous and simplified way, is still a major research issue. We present and discuss, in this part, some research works related to the different aspects involved in this context and that are based on SIP the most popular signalling protocol for this issue.

(Schulzrinne and Wedlund, 2000), is the very initial paper that shows how mobility management can be supported by SIP in order to provide all common forms of mobility, including terminal, session, personal and service mobility for SIP-based applications. Particularly, we are interested to session, and personal mobility. As it is defined by authors, session mobility allows a user to maintain a media session even while changing.terminals. They describe the way when it is supported by SIP using REFER and INVITE messages. Personal mobility, as it is defined in this paper, allows to address a single user located at different terminals by the same logical address. This type of mobility is ensured by a SIP forking proxies making the user reached at any of his devices. These different types of mobility are addressed without taking into account security aspects.

(Zhang et al., 2009), propose SIP security mechanisms that support seamless mobility only during the handover of mobile terminals among different access networks (terminal mobility). This solution does not address user mobility that consists of changing terminal with ensuring service continuity. Moreover, authors focus on security aspects for network and transport layer to secure SIP signaling and data transmission of SIP services. But, they do not consider non-functional security aspects such as identification, authentication and authorization.

As defined in (ETSI, 2010), IMS is an Overlay Session/ Control Architecture that acts as a session middleware in NGN. IMS uses basically SIP for controlling sessions. This protocol supports terminal and user mobility. However, when dealing with user mobility, a new session is established with the second terminal and services offered by the prime terminal become inaccessible.

In (Vim et al., 2010), authors deal with session mobility which allows user to maintain his session and ensures service continuity even while changing terminals. They discuss two ways for supporting session mobility: network- and user equipment- based approach. In network based approach, network initiates a session transfer while user equipment initiates a session transfer in user equipment based approach. They show the feasibility of session mobility control according to the former approach in IMS. This work focuses only on continuity of media services, and does not consider continuity of security services that ensures a secure and simplified access to any service during a seamless session.

None of the cited work has treated mobility impact on security aspects, namely, access control. Most of these recent work deal only with functional aspect of mobility independently of security aspects. Even there is some work that introduce security to mobile environment, they consider this aspect only on network level. Therefore, a new solution that integrates security to service, equipment (terminal) and user levels, while supporting mobility, is needed. Thus, we propose, through this paper, an innovative security management approach that guarantees a secure terminal and service access for each end-user. Moreover, our proposal supports mobility, particularly, user mobility, in a seamless way while keeping all user resources, namely his terminals considered as service platforms, accessible in a secured way during his session. So, for example, when a user wants to continue a session begun on his mobile phone on his laptop, he can remain using the GPS service offered by his mobile phone after he changes the terminal. For this purpose, we introduce the VPDN concept. Finally, we propose mechanisms to ensure security continuity

within a secure and seamless session.

3 PROPOSITION

In this section, we describe our proposal that is composed of three complementary parts. First, we present our security management solution that is based on security service components and security token that is exchanged between these different components. Second, we introduce our VPDN concept that permits to manage the set of user terminals and to provide a secure usage and change of these terminals. Finally, we treat security continuity within a seamless session during user mobility. Therefore, we propose an extension of the signalling protocol SIP+ that supports the token transfer.

3.1 Security Management

3.1.1 Security Service Components

As NGN users require continuity of service in a heterogeneous, mobile and open environment, security as a service concept can be an efficient approach to facilitate this requirement. In fact, in order to ensure security, continuity and uniqueness of the session, and to meet the needs of mobility (terminal, user, session and service mobility), security should not be seen with its classic image. It must be provided as a service ensured by a set of security components offering the user a secured and simplified access to his services.

Therefore, we adopt in our architecture design a Service Oriented Architecture (SOA). This SOA approach provides many advantages in terms of reusability, dynamicity, flexibility, interoperability and evolution of services. Nevertheless, according to our NGN/ NGS context, our proposition of security services is not limited to the aforementioned SOA service characteristics.

Indeed, our approach consists of further architectural aspects. First, we consider the mutualization aspect that reflects ability of a service to be not only reusable, but also shareable. To satisfy this aspect, SEs (Service Elements) should be stateless such that they can be used and shared among multiple sessions. Second, SEs should be autonomous that implies independence between the different SEs. This means that SE should not need other SEs to ensure its functionalities. Finally, we consider the Self-management aspect that represents the Self-monitoring of the QoS contract.

Taking into account these different aspects and characteristics, our proposed security management is based on three main components: Securityware, Security Agent and Security Data store.

The Security Service Provider (Securityware), shown in Figure 1, is responsible of the security management and control. Thus, our Security Service Provider proposition gathers all the security components as following:

- **Identification Service:** it enables the recognition of a user by the system . User can have one or more identifier types (e.g. login/password, One Time Password, smart card, biometry, or certificate);
- **Authentication Service:** it determines if an identity is actually what it claims to be. It aims to authenticate user only one time per session (unique authentication) for all requested services;
- **Authorization Service:** it occurs at the opening session time, when a user requests a set of services, to allow (or deny) him to use each service component. Indeed, authorization service evaluates the effective rights. Permission is granted according to rights associated to the user role;
- **Token Service:** it generates and updates the token;
- **Session Service:** it ensures the session creation and activation and the session identifier (Session_ID) generation (upon successful authentication). This service is responsible for managing and maintaining a secure end-to-end session;
- **VPDN Service:** it manages the set of user terminals (VPDN) and it generates the VPDN identifier (VPDN_ID).

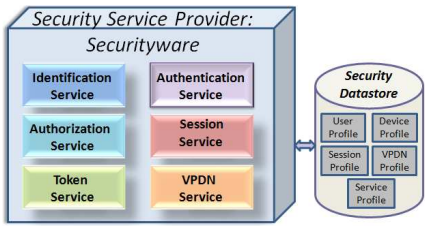

Figure 1: Securityware Architecture Components.

In order to facilitate and simplify the management of security and access control, we propose also a Security Agent that is deployed in each service platform or terminal which is considered simultaneously as a service platform and as a service. The Security Agent intercepts requests for the protected resource (service or terminal). It sends then a request to the Securityware asking for decisions regarding the required services. So, the Security Agent secures access to service platforms by checking authorizations due to the Securityware.

Finally, the Security Datastore contains all the information needed by the Securityware, namely, user profile, device profile, VPDN profile, session profile and service profile.

3.1.2 Token Role and Structure

In our proposed security management solution, the token is used for access control, namely, authentication and for maintaining a seamless session. It is created and updated by the Token Service during the session and VPDN creation.

Within the Securityware, the unique authentication is based on the token. It is considered as a flexible and powerful mechanism for exchanging security context between different service platforms or terminals (domains). This token represents a small collection of information that is transmitted to user (i.e. terminal security agent) when the session is first created. As user visits different service platforms that are protected by security agents, the token is propagated to these platforms and is used to retrieve the User_ID. Indeed, this token is retrieved at each subsequent request from the terminal such that the service platform (which may be the terminal itself) can recognize requests from the same user. Thus, the unique session is maintained automatically due to the token exchange.

The proposed token structure and data model are illustrated in Figure 2. Despite the fact that tokens have common structure, they can be different in usage and in the way they are generated.

Some tokens can also contain optional values. The common token structure of different tokens contains the following attributes and elements:

- **Token Type:** is an optional attribute;
- **Token_ID:** is a token attribute that represents its unique identifier;
- **Token_Value:** is an optional element that can be used for authentication.

  Session information:
- **Session_ID:** is the unique end-to-end session identifier. It is an attribute of the token that is exchanged between the Security Agent in the terminal and the Securityware;
- **Session_Name:** is a local value attribute in our Securityware that differentiates between sessions of the same user;
- **Session_Duration:** indicates the session validity period.

  User information:
- **User _ID:** is the user identifier in the current session. This attribute can be a random value generated by the Securityware. It can be a value chosen from the user characteristics such as IP address or login.

  VPDN information:
- **VPDN_ID:** is the identifier of the set of terminals deployed by the user during his session. This identifier remains unique even when the token is regenerated for a long duration session.
- **Domain:** is an element that identifies the domain that the generated token is related.
- **secure:** is a boolean value that indicates if the transport channel secure.

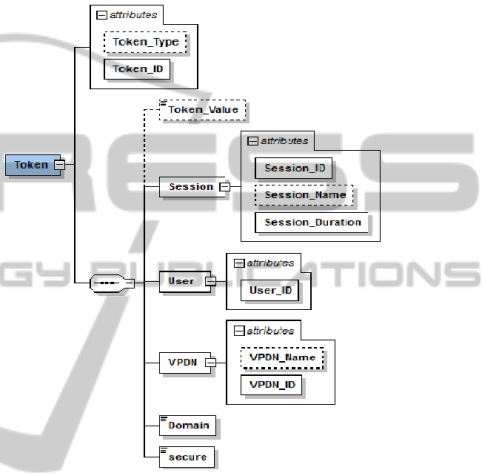

Figure 2: Token structure and format.

In our context, we define two types of token that have a common data structure and contain different profiles and different creation processes:

- **Authentication Token:** In this type of token, the Token_Value element contains a value that can be used as an authentication value. It is calculated by applying, as an example, HMAC function to user credentials.
- **VPDN Token:** this token extends the authentication token and contains the VPDN_ID in addition to session and user information.

3.2 The Virtual Private Device Network

3.2.1 What is the VPDN?

The VPDN (Virtual Private Device Network) represents a network of terminals which are present in the PAN (Personal Area Network) of the user and used during his service session. It permits to aggregate and manage this set of terminals in order to facilitate terminal change while preserving service continuity.

Within the VPDN, each terminal is considered as

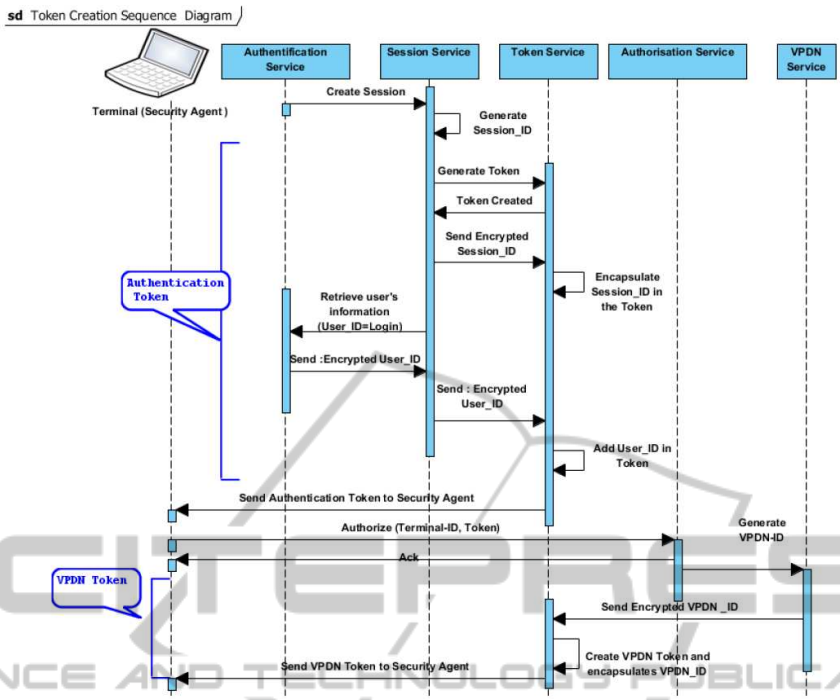

Figure 3: Token Creation.

a service component that defines a set of personalization and adaptation features and uses the real time user profile to manage his sessions based on his preferences and mobility. Moreover, each terminal accommodates a range of services that it can also be considered as a service platform or a service provider. In fact, it offers a set of terminal services (e.g. display service, keypad service, touch screen service) and it permits to deploy other services such as applicative services (e.g. location service).

Consequently, the terminal plays two roles: it is a service component managed by the VPDN (device as a service) and it represents a service platform.

3.2.2 VPDN Creation

In this part, we explain the way that a VPDN is created and a terminal can be added to it. This process invokes, principally, the three major security functions: identification, authentication and authorization. It implies also the Token Creation (Figure 3).

Hence, we describe the overall process involving security aspects.

We consider particularly login/password identification type. After user registration, the Identification Service creates a login and a password. When using the terminal, the user should be identified. Then, the Identification Service checks if his login exists already in the Security Data-store. If the response is positive, the terminal security agent receives from the Securityware a response meaning that the user already has an identifier.

After the identification phase, the system asks the user to be authenticated. Then, the user types his password. The request is directed to the Securityware. Afterward, the Authentication Service verifies the credentials (login/password) provided by the user compared with information stored in the Security Data-store.

Once the user is successfully authenticated, session initialization is performed by the Session Service. It generates the current session attributes namely the ”Session_ID” and the ”Session_Duration”. Then, a token is generated by the Token Service. It contains the necessary session and user information. In fact, it encapsulates the ”Session_ID”, ”Session_Duration” and ”User_ID” attributes. This latter attribute is retrieved from the Authentication Service. Afterward, the token is transmitted by the Securityware to the Security Agent in the terminal. This transmission takes place in a secure channel.

Due to this token, the user will be able then to use, depending on his rights, any service from different service platforms without being asked, in this unique session, to enter his credentials again.

Next, we have to verify that the user is authorized to use this terminal and to create a VPDN. So, an authorization request related to the use of terminal is sent by the Security Agent to the Securityware. The

Authorization Service generates a positive or negative response based on user rights associated to his role and on privileges related to the resource (terminal). Then, the response is sent to the Security Agent.

Once the user is authorized, the VPDN Service generates the "VPDN_ID" which is the identifier of the set of terminals deployed by the user during his session forming the VPDN.

The Token Service retrieves the VPDN identifier and updates the token. The terminal is registered in the VPDN profile.

3.3 Security Continuity: Token based SIP+

Due to NGN evolution, end users claim to access his services while using multiple terminals. They desire to have a dynamic session while considering their preferences and their QoS requirements. In addition, they want to maintain their sessions continuous and unique despite their mobility.

To reach these objectives and to guarantee the security, continuity and end-to-end QoS requirements in the user session, we propose token based SIP+ (Soulimani et al., 2011) that should overcomes these challenges regarding user mobility. It is an extended protocol from Session Initiation Protocol (SIP) that considers the terminal as a service platform. This protocol permits the user session creation, modification and termination based on service composition including the terminal.

To satisfy the user requirements when he needs to change his terminal (user mobility), SIP+ is able to maintain an end-to-end session continuity and to ensure QoS management and security continuity. Therefore, we should extend information carried by SIP methods to add the necessary information related to security aspects and QoS management for each service component involved in the session. This information is carried by REFER SIP+ and INVITE SIP+ messages. The user mobility process begins by sending a REFER message that informs the Securityware that the user wants to transfer his session to another terminal. Then, the Securityware send an INVITE SIP+ message to the second terminal. This message is composed of a header and a body that contains the security token and requested QoS criteria such as reliability, availability, delay and capacity. All added information are in XML format.

4 FEASABILITY

In this section, we describe first a user mobility scenario that invokes all the concepts and mechanisms that we have defined previously. Then we describe the implementation of our different security management components.

4.1 Scenario: User Mobility

In this subsection, we explain how the aforementioned security components, concepts and models are able to maintain a seamless, continuous and secure user session despite possible variations in user preferences and locations, and different mobility modes such as user mobility. The user mobility represents user ability to switch between terminals during his session and to access his services from anywhere at anytime.

For more clarity, we describe a user mobility scenario (Figure 4) on which we apply our proposed security components and SIP+ Invite and Refer messages. Thus, we consider the following use case.

Alice is at home, she wants to use her laptop. After the VPDN creation (initiation) process which consists of identification, authentication, authorization and Token generation phases, Alice can use her laptop (terminal1), open her session and compose her services after she is authorized.

The laptop plays two roles. First, it is considered as a service platform (SP1) that provides a set of services protected by a Security Agent. We consider in this scenario the display service (SE11) and the mail service (SE12). The former is a terminal service but the latter is an applicative service deployed in laptop. Second, this laptop represents a service component belonging to the VPDN.

Alice uses her laptop with its display component (SE11). She can then receive her mails (SE12) through this terminal. In this case, the VPDN of Alice is formed only by her laptop:

VPDN (Alice) = Laptop

We suppose that Alice leaves her house to go to the birthday ceremony of her friend by car. She desires to switch her session from her laptop to her Smartphone while keeping it continuous and secure. Then, the Security Agent1 (laptop) sends a "Sip+ Refer" request to the Securityware. The Securityware inspects and verifies whether terminal2 (Smartphone) belongs to the PAN of Alice, which is considered as her trusted devices (terminals), and opens a secure channel between two terminals.(figure4 , (1), (2) and (3)).

As we consider the VPDN as a peer-to-peer network, each terminal is auto-managed and acts as a peer. Thus, the Security Agent1 is able to send an "Invite SIP+" request directly to terminal2 (Smartphone)

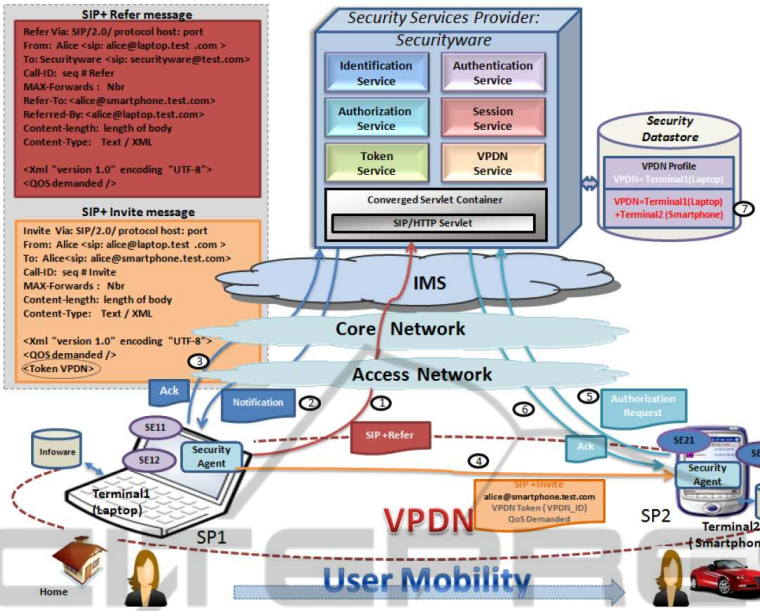

Figure 4: Security Continuity during User Mobility.

carrying the token that contains the VPDN identifier(figure4, (4)). The Security Agent2 intercepts the request to verify due to the Securityware if terminal2 is part of the VPDN of Alice and if she is authorized to access his session and compose services(figure4, (5)). The Securityware inspects the token and session validity. If the answer is positive, an acquittal is sent by the Securityware and the VPDN profile is updated. (figure4, (6) and (7)). For the VPDN profile update, see the two cases below.

Alice passes from her laptop to her Smartphone while maintaining her session (user mobility). The terminal change implies invocation of the component (SE21) which corresponds to the display service of the Smartphone.

Depending on her needs, Alice changes her service composition to build an application using a new logic of service.

She can then continue her communication with her friend all along her drive. Following the user mobility, we can consider two cases:

- **1st Case:**
  Terminal 1 (Laptop) remains active. In this case, terminal2 (Smartphone) could be seen as a service platform that provides (SE21) and (SE22) services. When switching his terminal, user actually preserves the same service composition with a set of services provided by terminal 2. For example, Alice used, with terminal1, the display service (SE11), and she needs, when using terminal 2, the service (SE21) which is functionally equivalent to (SE11). Thus, the Security Agent checks, with the Securityware, if Alice has the right or not to access this service considering his role. In this case, the VPDN becomes:
  $$VPDN(Alice) = \{Laptop, Smartphone\} \quad (1)$$
- **2nd Case:**
  Terminal 1 (Laptop) state becomes unavailable and it must send ”bye” to Securityware. In this case, terminal1 could be seen as a service component that is changed by terminal 2(Smartphone) in the VPDN. Thus, the Security Agent only checks token validity, and the VPDN becomes:
  $$VPDN(Alice) = \{Smartphone\} \quad (2)$$

4.2 Implementation

In order to prove the feasibility and to validate our proposition, we use the test-bed architecture of our UBIS project shown in figure 9. In the terminal level of this architecture, we found the service platform Userware, defined on the terminal and that contains applicative services and management services (e.g. the Security Agent). For the transport network, the VirtuOR solution is used. It permits to have different virtual entities such as IPv4 and IPv6 routers, access points, SIP servers, etc. Due to this solution, we can obtain a transport network platform. In the core network, we use an advanced version of Fokus Open IMS for the control layer to support SIP+ signaling messages. In the service level, a service platform named Serviceware that contains applicative services and management services developed by UBIS

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="Token">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Token_Value" minOccurs="0"/>
        <xs:element name="Session">
          <xs:complexType>
            <xs:attribute name="Session_ID" use="required"/>
            <xs:attribute name="Session_Name"/>
            <xs:attribute name="Session_Duration" use="required"/>
          </xs:complexType>
        </xs:element>
        <xs:element name="User">
          <xs:complexType>
            <xs:attribute name="User_ID" use="required"/>
          </xs:complexType>
        </xs:element>
        <xs:element name="VPDN">
          <xs:complexType>
            <xs:attribute name="VPDN_Name"/>
            <xs:attribute name="VPDN_ID" type="xs:string" use="required"/>
          </xs:complexType>
        </xs:element>
        <xs:element name="Domain"/>
        <xs:element name="secure" type="xs:boolean"/>
      </xs:sequence>
      <xs:attribute name="Token_Type"/>
      <xs:attribute name="Token_ID" use="required"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Figure 5: Token XML pseudo-code.

equip. This platform is implemented using GlassFish and Sailfin. We explain below how we implement and deploy our different security management components in this architecture.

First, we use Java language to write the proposed security architecture components, namely, Securityware and Security Agent. For our Securityware, we use EJB technology to develop autonomous, loosely connected and stateless services. These services are deployed in SailFin Application Server that supports various APIs such as JMS, JNDI, JDBC and Sip servlet. Our proposed Securityware extends actually some security parts involved in OpenSSO project. For our Security Agents, they are deployed in each terminal or service platform. In order to support SIP+, we deploy then Converged Application Container which is composed of SIP and HTTP servlets and will permits to switch from HTTP to SIP. We note that all transactions between different components are secured using SSL protocol.

Second, our Security Datastore is an LDAP directory (openDS) that contains our used information and is connected to the Securityware. Finally, we present, in Figure 10, the XML based pseudo-code of our proposed token.

5 CONCLUSIONS

In this paper, we have proposed a security as a service solution that ensures a secure and seamless session management in mobile and heterogeneous environment. This solution relies basically on security service components and token mechanism. We have introduced also VPDN concept that manages a secured access and usage of user terminals according to his preferences and locations.

In addition, we have proposed a SIP+ extension that supports token exchange between different components. Then, we have used this token-based SIP+ to ensure user mobility while keeping security continuity within a seamless session. Finally, we have proved the feasibility of our solution. As future work, we aim to secure SIP+ messages including the token and to evaluate the performance of our solution against possible attacks and vulnerabilities. Furthermore, our future work will not be limited to terminal level but we will consider also service level to ensure consequently session mobility.

ACKNOWLEDGEMENTS

The authors would like to thank Hassane AISSAOUI. They would also like to thank all the participants in the UBIS project, financed by the French ANR VERSO 2008 in which is situated this work.

REFERENCES

A.Hammami and N.Simoni (2010). Sécurité et mobilité :les nouveaux défis du contexte NGN. In *GRES Canada*.

ETSI (2010). IP Multimedia Subsystem (IMS), (Stage 2) 3GPP TS 23.228 version 8.6.0 Release 8 .

Kanneganti, R. and Chodavarapu, P. (2008). *Soa security*. Dreamtech Press.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and Schooler, E. (2002). Rfc 3261 sip: Session initiation protocol.

Schulzrinne, H. and Wedlund, E. (2000). Application-layer mobility using sip. In *Service Portability and Virtual Customer Environments, 2000 IEEE*, pages 29–36. IEEE.

Soulimani, H., Coude, P., and Simoni, N. (2011). User-centric and QoS-Based Service Session. In *Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific*, pages 267–274. IEEE.

Vim, J.-C., Kim, S.-K., and Lee, B.-S. (2010). Network Initiated Inter UE session transfer control in IMS. In *ETRI Korea*.

Zhang, L., Miyajima, H., and Hayashi, H. (2009). An innovative sip security mechanism with seamless mobility support. In *Wireless Communications and Networking Conference, 2009 IEEE*, pages 1–5. IEEE.