Open Location-Based Service Using Secure Middleware Infrastructure in Web Services

Namje Park[1], Howon Kim[1], Seungjoo Kim[2], and Dongho Won[2]

[1] Information Security Research Division, ETRI,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{namejepark,khw}@etri.re.kr
[2] School of Information and Communication Engineering, Sungkyunkwan University,
300 Chunchun-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea
skim@ece.skku.ac.kr,dhwon@dosan.skku.ac.kr

Abstract. Location-based services or LBS refers to value-added service by processing information utilizing mobile user location. For this kind of LBS, the role of security service is very important in the LBS that store and manage the location information of mobile devices and support various application services using those location information. And in all phases of these functions that include acquisition of location information, storage and management of location information, user management including authentication and information security, and management of the large-capacity location information database, safe security service must be provided. We show the security methods for open LBS in this paper.

1 Introduction

Given the recent advancement of mobile telecommunications technology and rapid diffusion of mobile devices, the importance of wired and wireless Internet services utilizing the past and present location information of users carrying mobile terminals with location tracking function is growing. LBS refer to value-added services that detect the location of the users using location detection technology and related applications. LBS is expected to play an essential role in creating value-added that utilizes wired and wireless Internet applications and location information, since these are very useful in various fields.

In view of the current controversy on the information-collecting practices of certain online sites concerning their members particularly with regard to the disclosure of personal information, it is only natural that there is heightened concern on the disclosure of personal information regarding the user's present location, given the unique characteristics of LBS. Easily disclosed information through certain online sites include member information, i.e., name, resident registration number, and address. Moreover, there is a growing concern that such personal information are leaked for purposes other than what has been originally intended. Such concern is even more serious since location information on customers and possibility of tracking their movements can constitute a direct encroachment of other people's privacy by them-

O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481, pp. 1146 – 1155, 2005.

selves. Hence, there is a growing need to conduct research on LBS security both in korea and abroad to prevent disclosure of personal information of individuals especially in the areas of authentication and security.

Furthermore, an open LBS service infrastructure will extend the use of the LBS technology or services to business areas using web service technology. Therefore, differential resource access is a necessary operation for users to enable them to share their resources securely and willingly.

This paper describes a novel security approach to open LBS to validate certificates based on the current LBS environment using the web services security mechanism, presents a location-based platform that can block information leak and provide safe LBS, and analyzes authentication and security service between service systems and presents relevant application methods.

2 Framework Model for Providing Secure Services

2.1 Security Service Framework

Web services can be used to provide mobile security solutions by standardizing and integrating leading security solutions using XML messaging. XML messaging is considered the leading choice for a wireless communication protocol. In fact, there are security protocols for mobile applications that are based on XML messaging. Some of these include SAML, which is a protocol for transporting authentication and authorization information in an XML message. It can be used to provide single sign-on web services. On the other hand, XML signatures define how to sign part or all of an XML document digitally to guarantee data integrity. The public key distributed with XML signatures can be wrapped in XKMS (XML Key Management Specification) formats. In addition, XML encryption enables applications to encrypt part or all of an XML document using references to pre-agreed symmetric keys. Endorsed by IBM and microsoft, WS-security is a complete solution to providing security to web services. It is based on XML signatures, XML encryption, and same authentication and authorization scheme as SAML (Security Assertion Markup Language).

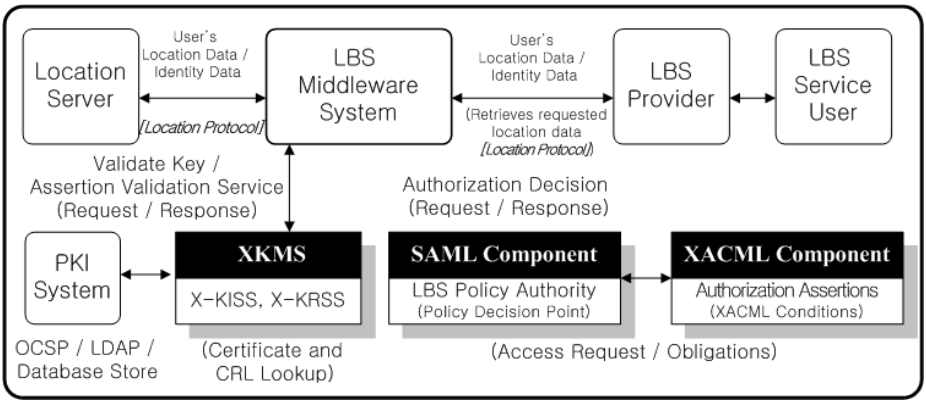

Fig. 1. Proposed secure LBS middleware service model

When a LBS-mobile device client requests access to a back-end application, it sends authentication information to the issuing authority. Depending on the credentials presented by the LBS-mobile device client, the issuing authority can then send a positive or negative authentication assertion. While the user still has a session with the mobile applications, the issuing authority can use the earlier reference to send an authentication assertion stating that the user was in fact authenticated by a particular method at a specific time. As mentioned earlier, location-based authentication can be done at regular time intervals. This means that the issuing authority gives location-based assertions periodically as long as the user credentials enable positive authentication.

Security technology for LBS is currently based on KLP (Korea Location Protocol). Communication between the LBS platform and Application Service Providers should be examined from the safety viewpoint vis-à-vis XML security technology. As shown in the security service model of the LBS platform in figure 1, the platform should have an internal interface module that carries out authentication and security functions to provide the LBS application service safely to the users[2].

2.2 Structure of Mobile Location Protocol in Korea

The protocol used for data exchange between the LBS server and terminals operates based on the MLP (Mobile Location Protocol) protocol established by LIF (Location Inter-Operability Forum). KLP is korea location protocol. The application of the authentication and security factors to KLP should be configured considering the following points:

The KLP is an application-level protocol for querying the position of mobile stations independent of underlying network technology. The KLP serves as the interface between a location server and a location-based application. The details of the location information security structure between the location information providers and the LBS providers should be defined in terms of confidentiality, integrity, and authentication and access control element as shown in figure 2.

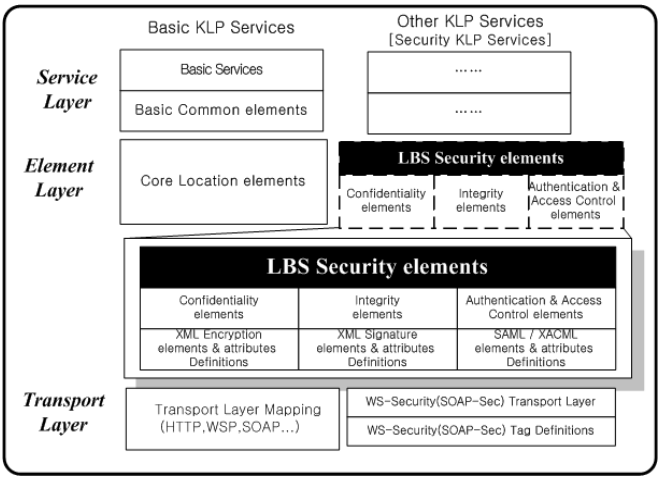

Fig. 2. Security protocol for secure open LBS services

These elements should be configured into a standard reference system for LBS security and authentication on WS-security-based transport layers. Based on this structure, the LBS security service transmits location information safely between the LBS platform and the Service Providers in accordance with the XML-based request and response model.

2.3 Standard Element Layer Definition for LBS Security

For LBS provided on the service layers of KLP, KLP service protocols can be divided into five different services, whereas message transmission can be defined in three types as request, answer, and report messages.

Security functions that should be provided to LBS service layers should be defined as LBS security elements. For element layers, there are seven main definitions: subscriber identification element, functional element, location element, configuration element, location accuracy element, network element, and context element. For the seven types of element definition DTD (Data Type Definition), the attribute parameters requiring security are displayed in bold font.

① Subscriber Identification Elements Definitions

Among subscriber identification elements, there are three elements requiring security: 'msid', which represents the identification information of mobile telecommunications subscribers; 'codeword', which is the access code defined in each subscriber terminal, and; 'session', which is the information on the session of the LBS client with the subscriber terminal. There is a need to encrypt data using XML encryption tag elements.

② Functional Element Definitions

As an element requiring security among functional elements, the 'url' represents the necessary address information to send an answer to the report. 'url' is part of the 'pushaddr' item that can contain the ID and password. Thus, it is necessary to encrypt data using XML encryption tag elements.

③ Location Element Definitions

As the element requiring security among location elements, 'time' represents the time when the service was carried out upon the request for location information. It is therefore necessary to encrypt data using XML encryption tag elements.

④ Shape Elements Definitions

'X', 'Y', and 'Z' are elements requiring security among configuration elements. As coordinate values, 'X', 'Y', and 'Z' are the basic units of location information. Thus, these data have to be encrypted using XML encryption tag elements.

⑤ Quality of Position Definitions

Since location accuracy elements represent accuracy based on the location information for which security has already been dealt with, there is no need for separate security. Nonetheless, it is necessary to examine security elements that can be applied to the necessary attribute parameters for enhancing the quality of the future LBS service.

⑥ Network Parameter Element Definitions

CDMA (Code Division Multiple Access), GSM (Group Special Mobile), CDMA-2000, and WCDMA (Wideband CDMA) are defined in network elements. As such, transport layer security should be dealt with on the transport layer of KLP. Likewise, the security function depending on the network infrastructure should be examined separately.

⑦ Context Element Definitions

As an element requiring security among context elements, an identifier can be used in an element for the provisioning of the privacy structure. This includes ID that allows the use of location information service, 'sessionid' that can substitute for 'pwd', 'pwd' as the password for a registered user implementing the location service, and 'serviceid' as an identifier for distinguishing services and applications that access the network. For 'sessionid' and 'pwd', it is necessary to encrypt data using XML encryption tag elements. In addition, since 'serviceid' requires security to access service, such security should be based on authentication using the PKI (Public Key Infrastructure) interface.

3 Security Protocol for Secure Open LBS Middleware Services

Three types of principals are involved in the proposed protocol: LBS application (server/client), SAML processor, and XKMS server (including PKI). The proposed invocation process for the secure LBS security service consists of two parts: initialization protocol and invocation protocol.

The initialization protocol is a prerequisite for invoking LBS web services securely. Through the initialization protocol, all principals in the proposed protocol set the security environments for their web services (Fig. 3). The following is the flow of setting the security environments:

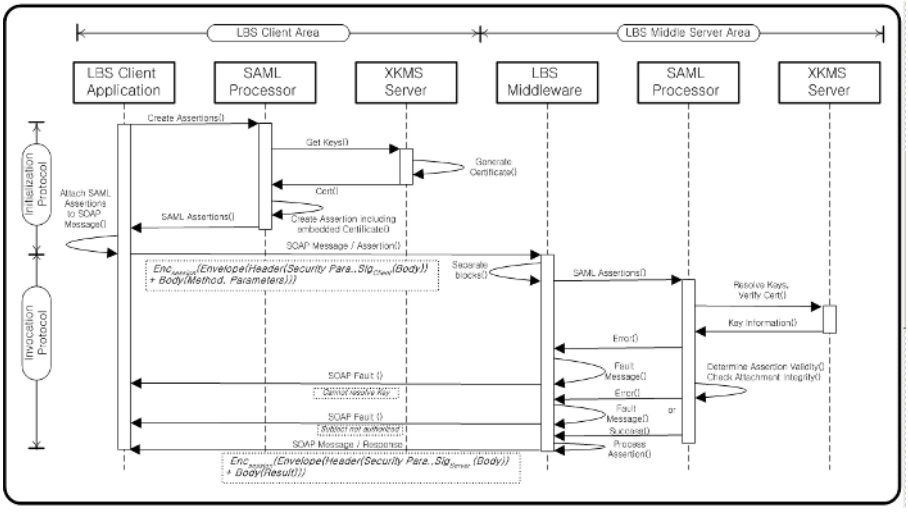

Fig. 3. Security protocol for secure open LBS services

The client first registers information for using web services. It then gets its id/password, which will be used for verifying its identity when it calls web services via a secure channel. The client gets SAML assertions and installs a security module to configure its security environments and to make a secure SOAP message. It then generates a key pair for digital signature and registers its public key to a CA.

The client creates a SOAP message containing authentication information, method information, and XML signature. XML then encrypts and sends to a server such message. The message is in the following form: $Enc_{session}(Envelope\ (Header\ (SecurityParameters, Sig_{client}(Body))+Body(Method,\ Parameters))))$, where $Sig_x(y)$ denotes the result of applying x' s private key function (i.e., the signature generation function) to y. The protocol shown in Fig. 3 shows the use of end-to-end bulk encryption [3,7,9]. Security handlers in the server receive, decrypt, and translate the message by referencing security parameters in the SOAP header. To verify the validity of the SOAP message and authenticity of the client, the server first examines the validity of the client's public key using XKMS. If the public key is valid, the server receives it from a CA and verifies the signature. The server invokes web services upon completion of the assessment of the security of the SOAP message. It then creates a SOAP message that contains the result, signature, and other security parameters. The server encrypts the message using a session key and sends it back to the client. Finally, the client evaluates the validity of the SOAP message and server and receives the result.

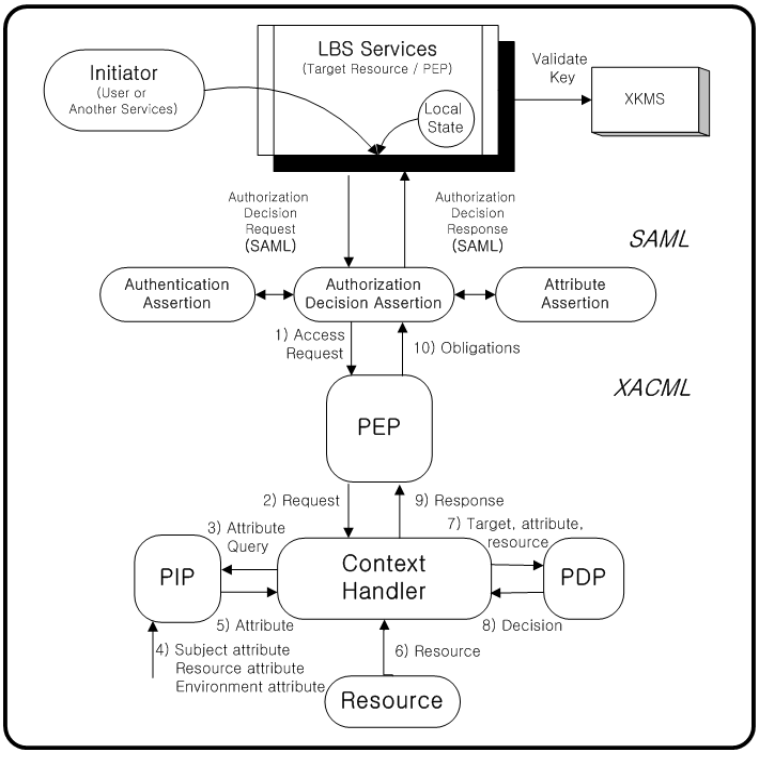

Fig. 4. SAML/XACML message flow using XKMS in open LBS

In the existing LBS service, there is no mechanism for differential resource access. To establish such security system, a standardized policy mechanism is required. The XACML specification is employed to establish the resource policy mechanism that assigns a differential policy to each resource (or service)[2,3]. SAML also has such policy mechanism, whereas XACML provides a very flexible policy mechanism that is applicable to any resource type. For the proposed implementing model, SAML provides a standardized method of exchanging authentication and authorization information securely by creating assertions from the output of XKMS (e.g., assertion validation service in XKMS). XACML replaces the policy part of SAML (Fig. 4). Once the three assertions are created and sent to the protected resource, verification of authentication and authorization at the visiting site is no longer necessary. SSO (Single Sign-On) is a main contribution of SAML in distributed security systems[1].

Figure 4 shows the flow of SAML and XACML integration for differential resource access. Once assertions are created from the secure identification of the PKI-trusted service, the access request is sent to the policy enforcement point (PEP) server (or agent) and to the context handler. The context handler then parses and sends to the PIP (policy information point) agent the attribute query. The PIP gathers subject, resource, and environment attributes from the local policy file, with the context handler giving the required target resource value, attribute, and resource value to the PDP (policy decision point) agent. Finally, the PDP determines and sends to the context handler the access possibility to enable the PEP agent to allow or deny the request [4].

4 Simulations

We have modeled our architecture as a closed queuing system as in figure 5, and we analyzed of approximate Mean Value Analysis (MVA) as described in [5,6,8]. In the scenario of figure 5, the secure LBS procedure has two job classes, initial secure location update step and secure LBS roaming step. $r_{im,jn}$ means the probability that a class *m* job moves to class *n* at node *j* after completing service at node *i*. And *ratio* represents a ratio of total users to secure LBS roaming users[8]. Analyze steps of class switching closed queuing system are following.

Step1: Calculate the number of visits in original network by using (1)

$$e_{ir} = \sum_{j=1}^{K} \sum_{s=1}^{C} e_{js} r_{js,ir} \tag{1}$$

where K = total number of queues, C = total number of classes.

Step 2: Transform the queuing system to chain.

Step 3: Calculate the number of visits e^{*}_{iq} for each chain by using (2)

$$e^{*}_{iq} = \frac{\sum_{r \in \pi_q} e_{ir}}{\sum_{r \in \pi_q} e_{1r}} \tag{2}$$

where r = queue number in chain q, q □ = total queue number

Step 4: Calculate the scale factor α_{ir} and service times s_{iq} by using (3) with (1).

$$s_{iq} = \sum_{r \in \pi_q} s_{ir}\alpha_{ir}\ ,\ \alpha_{ir} = \frac{e_{ir}}{\sum_{s \in \pi_q} e_{is}} \tag{3}$$

Step 5: Calculate the performance parameters for each chain using MVA.

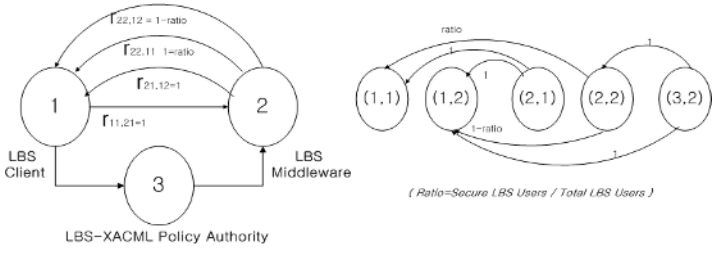

Fig. 5. Multiple class queuing system in the Secure LBS push scenario

XKMS has been implemented based on the design described in previous section. Package library architecture of XKMS based on CAPI (Cryptographic Application Programming Interface) is illustrated in figure 6. Components of the XKMS are xml security library, service components api, application program. Although XKMS service component is intended to support xml applications, it can also be used in order environments where the same management and deployment benefits are achievable. XKMS has been implemented in java and it runs on JDK ver. 1.4 or more.

The manner in which the various XKMS service builds upon each other and consumes each other's services is shown in the following diagram.

The figure for representing testbed architecture of XKMS service component is as follows figure 6.

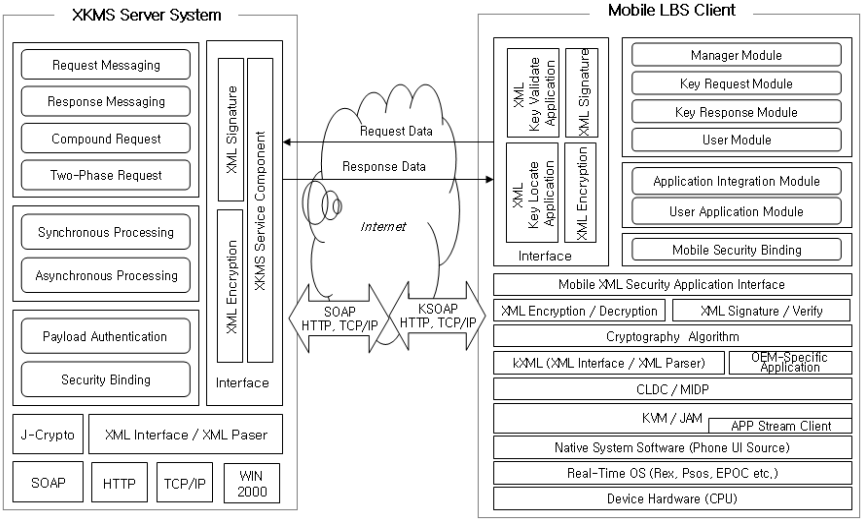

Fig. 6. Testbed Architecture of XKMS component for Open LBS

Figure 7 showed difference for 0.2 seconds that compare average transfer time between client and server of XML encryption &decryption by XML Signature base on XML security library. According as increase client number on the whole, showed phenomenon that increase until 0.3 seconds.

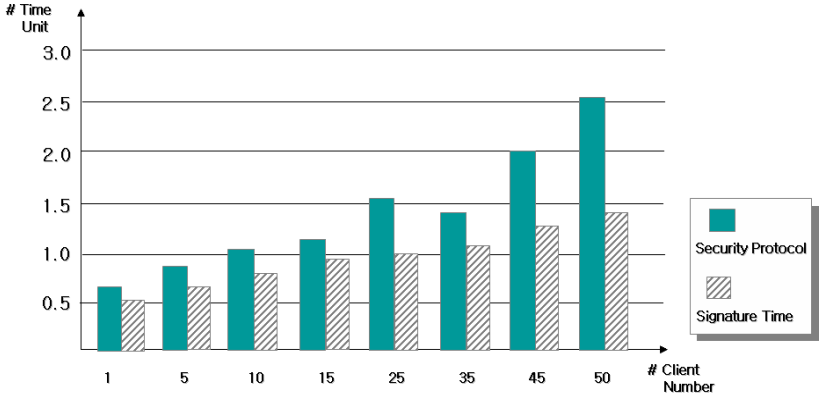

Fig. 7. Simulation Result of XKMS Protocol

Figure 7 is change of average transmission time according as increase client number in whole protocol environment. If client number increases, we can see that average transfer time increases on the whole. And average transfer time increases rapidly in case of client number is more than 45. Therefore, client number that can process stably in computer on testbed environment grasped about 40(At the same time). When compare difference of signature time and protocol time, time of xml signature module is occupying and shows the importance of signature module about 60% of whole protocol time.

5 Conclusion

This paper sought to present a location-based platform that can block information leak and provide safe LBS as well as to establish methods for authentication and security application between service systems for presentation. Toward this end, LBS security requirements were examined and analyzed. In particular, the trend of technology and standard was analyzed to provide safe LBS. To formulate an authentication method as well as a security technology application method for LBS on MLP, MLP security elements were identified based on LBS security requirements by defining the MLP security structure, which serves as the basis for KLP.

A novel security approach to open LBS was proposed to validate certificates based on the current LBS security environment using XKMS and SAML and XACML in xml security. This service model allows a client to offload certificate handling to the server and to enable the central administration of XKMS polices. To obtain timely certificate status information, the server uses several methods such as CRL (Certificate Revocation List), OCSP, etc. The proposed approach is expected to be a model for the future security system that offers open LBS security.

References

1. M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC 2560 (1999)
2. Namje Park, et. Al.: The Security Consideration and Guideline for Open LBS using XML Security Mechanism, ASTAP 04/FR08/EG.IS/06. (2004)
3. M. Naor and K. Nissim: Certificate Revocation and Certificate Update, IEEE Journal on Selected Areas in Communications, 18 (4) (2000)
4. Chanho Lee , et. Al.: A Scalable Structure for a Multiplier and an Inversion Unit in GF(2m), ETRI Journal, V.25, No.5 (2003) 315-320
5. Yuichi Nakamur, et. Al.: Toward the Integration of web services security on enterprise environments, IEEE SAINT 02. (2002)
6. Boudewijn R. Haverkort John: Performance of Computer Communication Systems : A Model-Based Approach, Wiley & Sons (1999)
7. Sungmin Lee et. Al.: TY*SecureWS:An integrated Web Service Security Solution based on java, LNCS 2738 (2003) 186-195
8. Minsoo Lee, et. Al: A Secure Web Services for Location based Services in Wireless Networks. Networking2004 (2004)
9. Mi-Jung Choi, et. Al.: XML-Based Network Management for IP Networks, ETRI Journal, Vol.25, No.6 (2005) 445-463

ANNEX A. Security Elements & Attributes in DTD

```
<!--// Subscriber Identification Element Definitions //-->
        1 Line) <!ELEMENT  msid     (#PCDATA)>
        5 Line) <!ELEMENT  codeword  (#PCDATA)>
        10 Line) <!ELEMENT  session    (#PCDATA)>
        12 Line) <!ELEMENT  start_msid  (msid)>
        13 Line) <!ELEMENT  stop_msid  (msid)>
<!-- // Function Element Definitions // -->
         11 Line) <!ELEMENT  pushaddr  (url, id?, pwd?)>
         17 Line) <!ELEMENT  url  (#PCDATA)>
<!--// Shape Element Definitions //-->
         5 Line) <!ELEMENT  coord       (X, Y?, Z?)>
         6 Line) <!ELEMENT  X  (#PCDATA)>
         7 Line) <!ELEMENT  Y  (#PCDATA)>
         8 Line) <!ELEMENT  Z  (#PCDATA)>
<!--// Location Element Definitions //-->
         1 Line) <!ELEMENT  pos   (msid, (pd | poserr), net_param?)>
         2 Line) <!ELEMENT  eme_pos   (msid, (pd | poserr), esrd?, esrk?)>
         3 Line) <!ELEMENT  trl_pos   (msid, (pd | poserr))>
         5 Line) <!ELEMENT  pd   (time, shape, (alt, alt_acc?)?, speed?, direction?, lev_conf?)>
         10 Line )<!ELEMENT  time  (#PCDATA)>
<!--// Context Element Definitions //-->
         2 Line) <!ELEMENT  sessionid   (#PCDATA)>
         4 Line) <!ELEMENT  requestor   (id, serviceid?)>
         5 Line) <!ELEMENT  pwd   (#PCDATA)>
         6 Line) <!ELEMENT  serviceid   (#PCDATA)>
         9 Line) <!ELEMENT  subclient  (id, pwd?, serviceid?)>
<!--// Quality of Position Definitions //-->
         None
<!--// Network Parameter Element Definitions //-->
         None
```