Providing Identity Assured User Generated Services Using IMS

Seppo Heikkinen

Tampere University of Technology
P.O.BOX 553
FIN-33101 Tampere, Finland
seppo.heikkinen@tut.fi

Abstract. The advent of ubiquitous computing will increase the dynamism in the relationships of the entities. This is especially true, if the visions about the proliferation of the amount of small operators become reality. Also, even though the operators would like to tightly control the service provisioning landscape, it is more likely that the innovative concepts come from external parties. The user themselves might be the service creators as they already have become content generators. However, the service providers still should be compensated for their efforts as this can lead to better quality services. Naturally, some try to fraudulently get services without paying. Thus, non-repudiable solutions are needed that ensure that the services are provided and paid for. In this paper we investigate an architecture that uses IP Multimedia Subsystem (IMS) as service platform to provide user generated services in an assured and secured way.

Keywords: Accounting, hash chains, HIP, IMS, service provisioning

1 Introduction

The current mobile operator landscape is dominated by static relationships between incumbent operators. Operators have created tight agreements about their interaction with the interest in retaining the control of their subscribers. But when we consider IP based services available in the Internet, there is less subscriber control and innovative service concepts can be provided. It has been claimed, though, that some operators try to intervene by, for instance, blocking or degrading the quality of Voice over IP (VoIP) traffic, i.e., in order to prevent the users circumventing the competing call services provided by the operator.

However, operators have also taken steps to provide service platforms of their own in order to compete against the innovative service providers of the Internet. One such architectural initiative has lead to the development of IP Multimedia Subsystems (IMS), which could allow the operators to provide rich services in a flexible and quality assured manner. Even though the architecture is envisaged to provide many different kind of services, even ones provided by external parties, the deployment still relies on the existence of “well known” partners, who provide reliable user and accounting information without any strong protective measures. This does not promote flexible and dynamic interaction models, especially considering that the research on ubiquitous technologies and ambient networking suggests an increase in the dynamic relationships between various entities. These visions provide enablers that could change the operator landscape in such a way that also small players, even individuals, could act as operators and provide, for instance, access services in easy manner. Naturally, when the dynamism increases, the security issues become even more important, because you no longer can rely on the “good behaviour” of a known and well established operator.

The operators also need to consider flexible service provisioning models. Thus, they should support innovative ideas coming outside their walled gardens. Social media has shown that ordinary users can be content creators, so they might as well excel in service creation. This is already starting to show in the creation of service mashups using simple tools, such as Yahoo Pipes. Additional incentive is given, if the users can be compensated for their efforts.

In this paper we discuss the potential of employing IMS in such an ambient networking environment, where the relationships are based on dynamic interaction and more assurance is needed for the actions taken. We investigate how it would be possible to provide user generated services using the available service infrastructure. Such services could be, for instance, related to streaming media or one could envisage enhancements to the current peer-to-peer interaction (like the piecewise approach of BitTorrent) to ensure fair sharing ratios. Also, VPN like tunnelling services could be provided. Thus, the idea is to sketch enhancement for IMS to allow the users provide services in a flexible way, but also take into account the liability aspects, so that the compensation from the provision of resources can be guaranteed giving more incentive to create attractive services. The operator is included in the initialisation of the service, hence taking into account the interests of operators to retain certain level of control of the actions of their customers, for which they have accepted liability (to a certain limit).

From a technical viewpoint, the solution is based on the idea of running Host Identity Protocol (HIP) on top of Session Initiation Protocol (SIP) and using the IMS home operators to ensure the identity of the communicating end points. The user providing the service receives non-repudiative evidence of the service usage in the form of hash chain tokens, which are strongly bound to the identity of the service consumer. Thus, emphasis is on the secure naming of the entities, so that every party of the transaction, i.e. payers and payees, can be reliably identified.

This paper is organised as follows. In the next section we briefly discuss the related work and technologies employed in our solution concept. The third section sketches the proposed solution on high level. In the fourth section we discuss the characteristics of the system and the fifth section concludes the paper.

2 Related work

Host Identity Protocol is an experimental proposal for introducing an additional identity layer to the Internet stack [1]. This "3.5 layer" enables decoupling the dual nature of IP addresses, so that the end point identity and locator roles can be separated into two distinct concepts. Thus, better mobility and multihoming solutions can be provided. As the identifiers in this model have cryptographic properties they are able to implement secure naming of entities. HIP functionality is based on a handshake procedure, which uses four messages to authenticate the end point identities and create keying material with the help of Diffie-Hellman exchange for protecting the association between the communicating entities. This base exchange also includes puzzle mechanism to mitigate denial of service concerns.

IP Multimedia Subsystem (IMS) is an architecture designed by 3GPP to facilitate the provision of multimedia services over IP packet networks [2]. Thus, it aims at being a service platform for the next generation networks (and current ones as well), which allows delivering rich services to users with assured quality of service (QoS). It should be noted that even though these services are generally expected to be telecom centric, IMS has the potential of becoming a more general platform for service provisioning integrating various application domains, i.e., in the fashion of service oriented architecture. Another, a more cynical viewpoint might argue that it is just a desperate attempt of telecom operators to retain their walled garden thinking against innovative (and sometimes anarchistic) Internet originated service development. Nevertheless, the decision to allow interaction between operator IMS infrastructure and external service providers is political, as well.

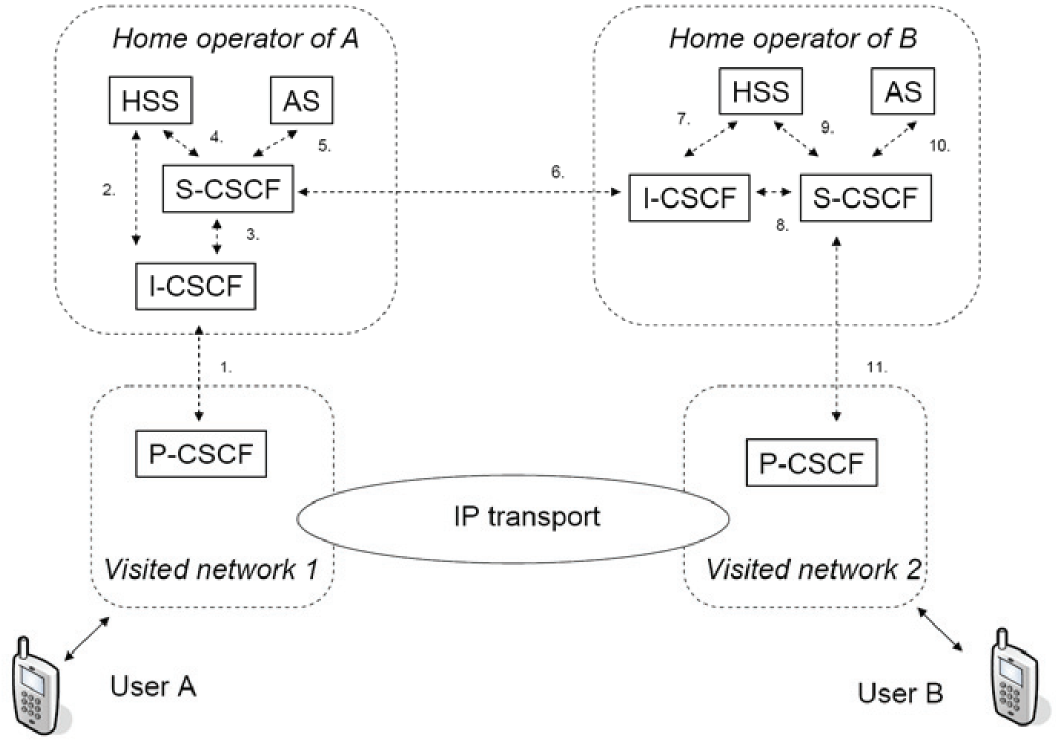

Fig. 1. A simplified view on IMS architecture in terms of session establishment

At the heart of IMS is Session Initiation Protocol, which works as a signalling protocol for setting up and managing the sessions between the parties. Even though IMS is supposed to support variety of different kind of service models, it currently very much relies on the static interaction with the known partners. In other words, the interacting operators are expected to be trustworthy without any strong technical measures to ensure the data integrity, and application services are tightly connected to the home operator domain. A simplified IMS architecture is presented in Fig. 1 in terms of session establishment, emphasising the hop by hop nature of SIP signalling (different kind of topologies are also possible). It includes different proxy elements (Call State Control Function, CSCF), subscription management (Home Subscriber Server, HSS), and application servers (AS). A detailed presentation of IMS can be found in [2].

Charging in IMS does not contain any strong security mechanisms, as it just uses SIP headers and Diameter parameters to convey information about the relevant events. Thus, no non-repudiation, for instance, is offered and the user is at the mercy of the operator. There is, however, considerable amount of work in the field of micropayments about using hash chains to provide granular payment solution in various contexts. One such is presented in [3], which used KeyNote credentials along with hash chains to implement One-Time Password (OTP) coins, without any strong bindings to the actual traffic, though. Hash chains themselves were already presented by Lamport in 1981 as one-time password mechanism [4]. Our approach is based on the ideas presented with OTP coins, but uses SPKI certificates as an assertion mechanism to provide non-repudiation. [5] already discussed the details of using such system integrated with HIP. In [6] hash chains were used to provide authentication and non-repudiation solution to a system integrating the use of WLAN and 3G network with the help of EAP.

Many other key management solutions are also available, such as IKEv2 [7], but perhaps the closest one for the purposes of this paper would be Multimedia Internet Keying (MIKEY) [8], which is especially suited for SIP scenarios. However, the intention of our solution is also provide identity association establishment and possibility to negotiate additional associations. While MIKEY could be extended to include such functionality, the choice was to go for more identity oriented approach.

2 Scenario overview

The presented scenario builds on the premise of entity identities. In other words, it is expected that every entity, even networks, is in possession of an identifier, for which it is able to provide proof of possession. One such example, used in HIP, is Host Identity Tag (HIT), which is a hashed representation of the public key and has the benefit of providing a concise representation of the identity. Additionally, it is assumed that the operator relationships are dynamic. This follows the line of ambient networking thinking, which suggests that technical development makes it feasible also for the small players to assume the operator role. So, current assumptions of pre-existing static roaming agreements are no longer valid and there is more uncertainty about the trustworthiness of the received data.

The idea of the scenario is to provide user generated services to other users in such a fashion that non-repudiable accounting records can be generated. The previously unknown user identities are vouched for by their respective home operators. With the employment of the principles of HIP, the users are able to secure their connections and ensure that the service is provided to the correct entity. Note that the users are in possession of both identity layer idenfiers, e.g., HITs and typical SIP layer identifiers.

2.1 Service registration

User B, who wishes to provide services of her own, has basically two options in the architecture we are envisaging: the service is provided directly by the user or it is provided through an external provider, i.e., it acts as a service proxy. In the latter case one can see two further options depending on the association between the user and the proxy. It could be an application server provided by the home operator of B, but it also could be totally independent entity with no direct administrative connection with the home operator, e.g., YouTube kind of entity in the case of streaming service.

In any case, the user is responsible of contacting her home operator in order to update the initial Filter Criteria (iFC), which will dictate the processing of the SIP messages directed to or originating from the user. This way S-CSCF, a central routing entity in IMS, knows how to route the message directed to the service identifier of the service of the user. Service identifier is a typical SIP URI, which is either assigned by the home operator or suggested by the user in accordance with any previous agreements she has with the operator. The home operator should provide a separate registration service for its users that has the possibility of updating iFC accordingly, be it a redirection to a service provided by the user or a proxy server.

In case of an external proxy provider, the user also is responsible of providing the usage offer terms and a delegation certificate, which authorises the provider to act on behalf of the user. The home operator might have a policy that dictates that it has to receive such assertion at the time of the registration, but it is not entirely necessary as the authorisation is more crucial at the time of the negotiation of the service usage. Proper authorisation ensures, though, that no illegitimate redirection requests take place. SPKI certificate naming the HITs of the parties of delegation is used.

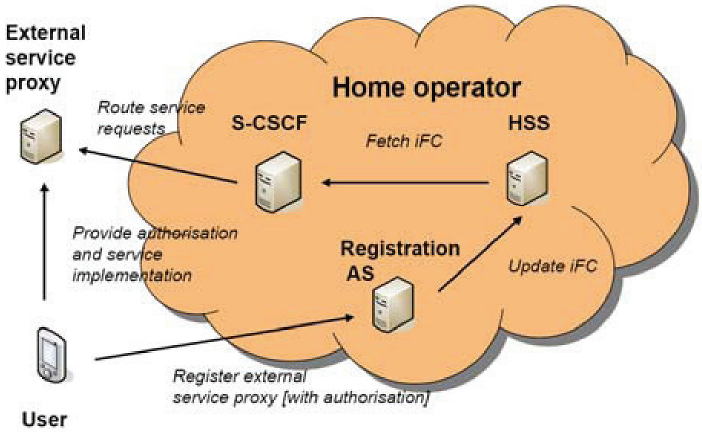

Fig. 2. Interaction of service elements within the context of user generated services

Tasks for the different elements are summarised in Fig. 2. It gives a general idea how different entities interact within the envisaged scenario, which includes the use of proxy service provider. Within the operator network the elements can use Diameter, whereas subsequent message routing is done with SIP as usual. The registration and interaction with the service proxy can use other protocols, in simplest case it could be HTTP. The user interface for them can be dependant on the implementation, as well.

2.2 Service usage negotiation

In this work it is assumed that the interested user, i.e., user A, is aware of the service identifier. In other words, it is expected that the identity of the service is learnt some out of band means. This could be an entry in an external directory or an advertisement received during interaction with another service, like a related web service.

User A initiates the connection to the service using SIP INVITE semantics. However, this is enhanced with similar functionality as described in [9]. Basically, this means adding HIP related data to the message. Thus, A sends a SIP message, which also has similar content as in HIP R1 message, i.e., identity of the user and cryptographic parameter suggestions for the session. Puzzle mechanism is not included as it is assumed that the home operators are able to protect their own customers from the flood of signalling messages. In a sense, one can view IMS infrastructure as an indirection architecture providing rendezvous between the end entities. Note that if the service provider, i.e., B, would rather assume the responder role and require puzzle solving, it could use provisional response (PRACK message) to switch the roles and send its own R1 instead. We do not, however, consider this case further here.

The home operators are responsible for attaching their own assertions, which ensure the validity of the used identifiers, i.e., SIP URIs and HITs. This includes providing a signature in SIP headers, but could also include an additional certificate in SIP body to restrict the rights of the subscriber. Assertions are needed to ensure the liability of the parties, i.e., end users know that the operators are willing to vouch for the previously unknown identities and the operators know that the other operator is willing to accept the liability of behalf of its own subscribers. Another option would be that the user is in possession of a certificate, which has been previously issued by the home operator and assures the subscriber status of the given user identity. While it provides some performance benefits as the home operator does not need to sign every message, it cannot ensure the authenticity of the other SIP headers and is subject to possible revocation considerations and checks.

In addition to the mechanisms described in [9], user B attaches an offer statement to the "I2" message, which tells what sort of compensation she expects. In essence, this tells the hash chain token release frequency she expects to receive as a proof of the service usage, e.g., per kilobytes or per minute. In case of service proxy, the proxy is responsible of doing this, but it also has to include the delegation certificate issued by the user B as the service offer is bound to the identity of B. "I2" also contains identity and session specific parameters as in typical HIP message. The offer can be an SPKI certificate, much like in [5].

User A binds itself to the service offer by calculating a hash over the request and signing it. Additionally, A creates a hash chain of suitable length by recursive hash operations and includes the anchor value of this chain, i.e. the lastly generated one, to the signed statement. This is sent back to B (or proxy) in the "R2" message, which concludes the negotiation phase. After this the parties are in possession of each others identities and parameters, which they can use to secure a data traffic session between themselves. The flow of messages is depicted in Fig. 3.

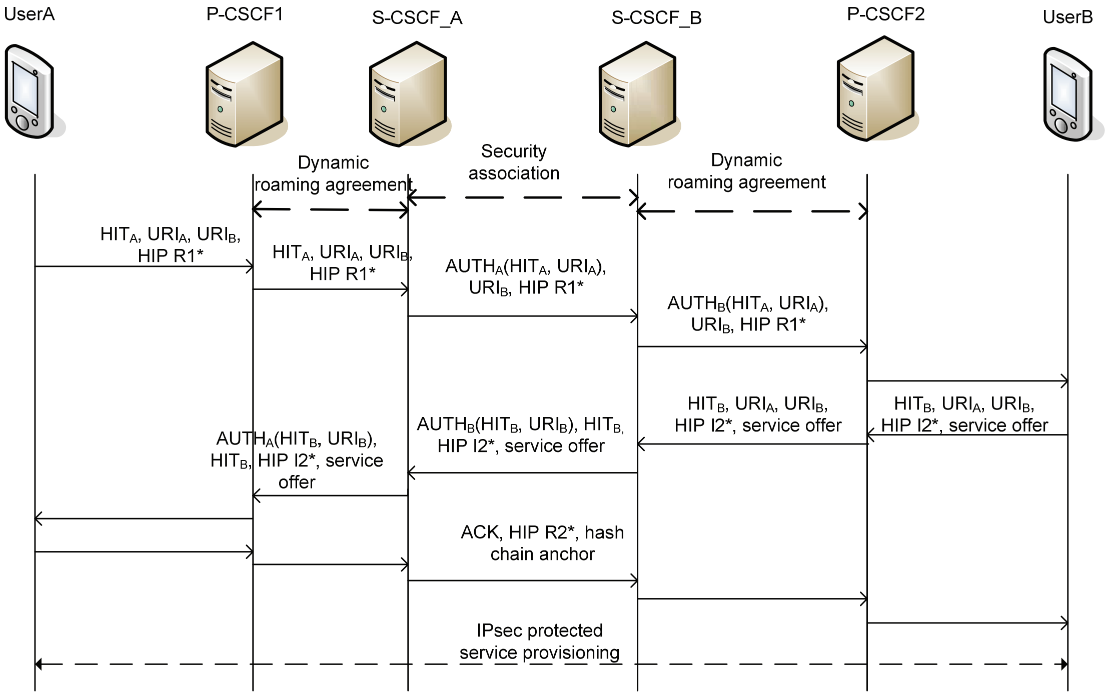
UserA
P-CSCF1
S-CSCF_A
S-CSCF_B
P-CSCF2
UserB
Dynamic roaming agreement
Security association
Dynamic roaming agreement
HIT$_A$, URI$_A$, URI$_B$, HIP R1*
HIT$_A$, URI$_A$, URI$_B$, HIP R1*
AUTH$_A$(HIT$_A$, URI$_A$), URI$_B$, HIP R1*
AUTH$_B$(HIT$_A$, URI$_A$), URI$_B$, HIP R1*
HIT$_B$, URI$_A$, URI$_B$, HIP I2*, service offer
HIT$_B$, URI$_A$, URI$_B$, HIP I2*, service offer
AUTH$_B$(HIT$_B$, URI$_B$), HIT$_B$, HIP I2*, service offer
AUTH$_A$(HIT$_B$, URI$_B$), HIT$_B$, HIP I2*, service offer
ACK, HIP R2*, hash chain anchor
IPsec protected service provisioning

Fig. 3. Signalling flows for establishing an identity association and service usage terms

2.3 Connection establishment

The parties A and B or, in case of proxied service, service proxy and A establish IP connectivity using an association they negotiated. This could be a connection protected by IPsec as in [10] or it could be a stream protected with SRTP [11]. An important thing is that the session keys are derived from the keying material that was created during the negotiation phase using the HIP mechanisms. This way the traffic is bound to the used identities and unauthorised parties do not have access to the provided service.

2.4 Association update

The association needs to be "refreshed" according to the frequency agreed upon during the negotiation phase. In essence, this means sending hash chain tokens, which ascertain to the service provider that the client is still willing to pay for the service. In practise chain values are conveyed using SIP messages using a suitable header extension. While it would be possible to do this directly between the communicating end points, in our approach this is done through the operator infrastructure. This is not more effective, but it gives the operators a chance to record the accounting information as well. Otherwise they might have less incentive to approve the use of this kind of architecture. This way the external proxy provider has less incentive to cheat, i.e., report faulty usage figures, because the home operator is aware of the amount of tokens used. While the service provider, be it a user or a proxy, keeps receiving hash tokens, it continues to provide the service. If not, then the provision of service is terminated. Similarly, if the service is not received, the consuming user does not provide any additional tokens. SIP flows for providing hash values are depicted in Fig. 4.

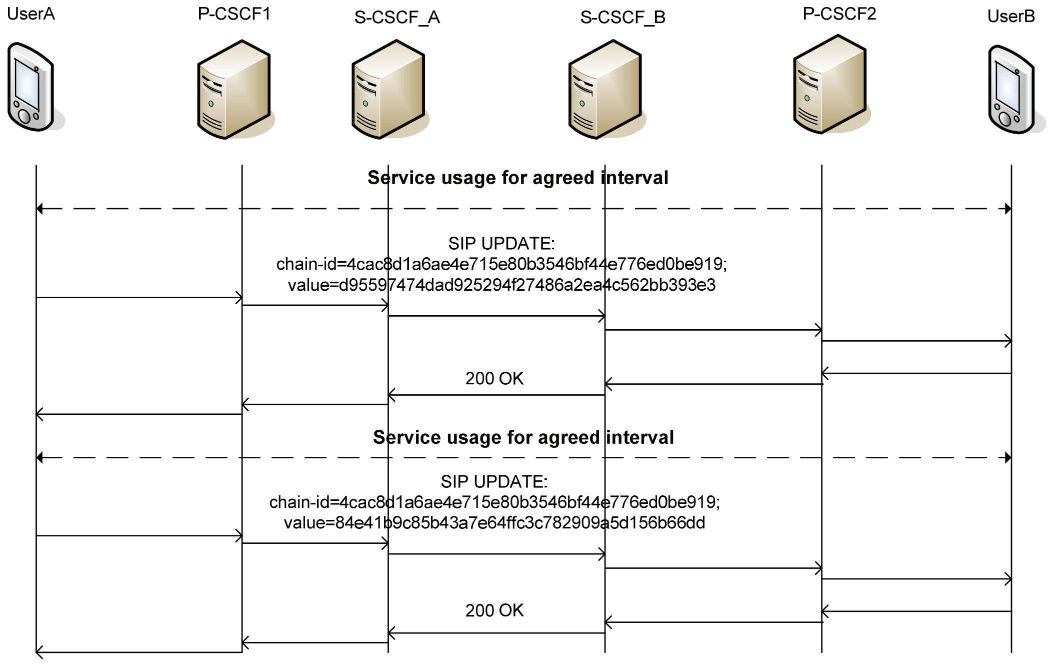
UserA
P-CSCF1
S-CSCF_A
S-CSCF_B
P-CSCF2
UserB
Service usage for agreed interval
SIP UPDATE:
chain-id=4cac8d1a6ae4e715e80b3546bf44e776ed0be919;
value=d95597474dad925294f27486a2ea4c562bb393e3
200 OK
Service usage for agreed interval
SIP UPDATE:
chain-id=4cac8d1a6ae4e715e80b3546bf44e776ed0be919;
value=84e41b9c85b43a7e64ffc3c782909a5d156b66dd
200 OK

Fig. 4. Submission of new hash chain values

2.5. Compensation

After termination of the service, the service provider needs to be compensated for the provision of its resources. The received hash values (or rather, just the last value and the total amount is sufficient) along with agreement certificates are presented to the home operator and it will compensate its user accordingly. It is assumed that the home operators have agreed on clearing procedures between themselves. Naturally there can be some flat rate agreements, but the accounting can be based on the hash chains, which provide non-repudiable evidence of the service usage. The home operator of A should use this information to bill its subscriber. In case proxy service provider is used, the clearing is done between it and the home operator of B. The delegation provided to the proxy can provide additional information regarding the revenue sharing between the proxy and B or this can have been provided separately during the registration of the service with relevant authorisation.

Accounting is based on the frequency of the hash chain values and they do not exhibit any value as such, but there could be a general agreement about the monetary value of a single unit. This information should be available during the offer and corresponding response phase as it will tell the implication in real world terms. Again, there might be some flat rate agreements, which allow the user to use certain kind of services for a certain amount (cf. maximum call minutes in certain flat rate subscription plans). However, it is also possible to provide Advice of Charge type of functionality as specified in 3GPP [12]. In practise this would mean providing XML documents to the user specifying the value of a single hash chain value. This will result in lengthy SIP messages, though. One option is also to make the hash chain tokens to correspond to the debit units specified for the IMS online charging [13].

3 Discussion

3.1 Trust and liability

The assumption is that the user trusts her home operator and they have exchanged identities, so the home operator is aware of the user identifiers both on application and identity layers. Such registration could be included, for instance, to the Authentication and Key Agreeement (AKA) procedure, when they both authenticate each other. Note that the user could be using a short term identifier in order to protect her privacy when interacting with external entities. Thus, every statement and assertion is bound to secure identifiers, for which is it possible to provide proof of possession.

As described in [9], the identity needs to be bound to the relevant SIP headers and message content. This takes place with the SIP Identity mechanism described in [14], although with the modification that an additional pair of identity headers is created for expressing the end entity identity as well as the corresponding signature. Additionally, the SIP level identity needs to be explicitly expressed with an additional header value, so that the both parties get the notion of each others identity, which they plan on using. An example of the relevant headers is given in Table 1.

Table 1. SIP header values used for conveying identity information

Header	Example value	Explanation
P-End-Pub-Identity	<sip:userA_public@home.net>	Public SIP identity of the message sender
P-End-Identity	"Ccp+C2..<clipped>..zmJp CB7rBXGe+DnutU="	Signature created by sender (base64)
P-End-Identity-Info	<urn:hit:8dc49622d9be6fca7f1ecb8f3e6738e2>; alg=rsa-sha1	User identity used for signature creation
Identity	"ZYNBbHC..<clipped>..PKb fU/pryhVn9Yc6U="	Signature created by the operator (base64)
Identity-Info	<urn:net:homeA: aad1d9518a9bde5b8f3b5c6b59b6970e>; alg=rsa-sha1	Operator identity used for signature creation

In our scenario it is also assumed that the home operators have established an association. This entails securing their connectivity, but it also has established an agreement about the liability constraints. In other words, they are willing to guarantee the costs generated by their own subscribers in interaction with the entities of the other home operator. This creates the basis of trust the home operators have to each other's assertions. Thus, if home operator A asserts that user A is its subscriber, it also states that the costs of user A will be guaranteed to the negotiated limit. As the user B trusts her home operator B, she knows that the operator B will be liable for any actions of the entities it has asserted.

The agreement between operators A and B can be pre-established like nowadays or it can be created on the fly. The latter one requires dynamic roaming agreement procedures, which are discussed, for instance, in [15]. However, trust based on liability is in effect here as well. Unless an operator has some other knowledge about the identity and behaviour of the other operator, additional evidence is required. This could be based on an assertion of a financial institution or an operator organisation, like GSM Association.

3.2 Non-repudiation and accounting

The non-repudiation property of the proposed architecture comes from the combination of the used identities and the hash chains. When the service provider has bound its identity through signature to the service offer, it cannot claim larger compensation at later point. The user of the service binds her identity to the offer and the hash chain anchor, which is a first value of the chain she uses to provide evidence of the service usage. Due the assumption of a secure hash function, the user is the only one, who is able to create such a chain, i.e., hash function is irreversible (preimage resistance). Because the respective home operators have expressed their trust on the used identities, the end entities have a notion of trustworthiness of their communicating partner.

Use of incremental payment in the form of hash chains also allows the parties to react to any discrepancies in the service provisioning and usage. If the service provider does not keep receiving hash chain values at agreed intervals, it can stop providing service. On the other hand, if the service is not provided as agreed, the user can stop providing additional values. Thus, if there is evidence of service usage in the form of hash token, the service has been undeniably used.

Incremental solution also allows the home operator to keep track of the costs generated by the user. If the user exceeds her credit limit, the operator can terminate the service usage by preventing additional tokens and notifying the parties accordingly. Additionally, the home operator gets assured accounting information, which it can relate to the charging information coming from the visited operator. This can be beneficial in a case, where, for instance, the IP connectivity of the user is provided directly by the GGSN of the visited operator instead of tunneling the traffic first to home operator (as currently often can be the case). This way visited GGSN can more reliably charge for changed quality of service of the visiting user, e.g., because certain service requires better QoS. IMS originally is intended for this kind of service dependant QoS treatment, but operators have been reluctant to let go of the tight control of their customers. It should be noted, though, that colluding users can bypass the operator and provide no accounting figures from their service usage, but then they have some external notion of each others trustworthiness and it would be hard to prevent anyway. They do not enjoy the potential QoS benefits, though.

3.3. Challenges

While we envisage more dynamic networking and operator landscape, the suggested solution still has some assumptions about the parties and their network topologies. Denial of service can be one major concern, if external parties are able to inject or modify traffic without restrictions. Even though we suggest use of HIP, we have stripped off the puzzle mechanism in favour of not introducing additional roundtrips to the typical SIP INVITE flows. The service provider needs to do signature validation and setup a state for service negotiation. Thus, operator assistance is needed in order to prevent message floods targeted at crippling the end entity. However, as it is also expected that the entities have already registered with their home operators and relevant signalling associations have been created, there is already some security present to secure the connections, e.g., secure attachment solution discussed in [16].

The proposal also sets additional performance requirements for the home operators as they have to create signatures in order to authorise identities. In high volume traffic signing every message would be quite unacceptable. There is the option of using pre-issued certificates as mentioned above, but not all the messages need this kind of service, only the initial service negotiation invocation. Those transactions that need to use assured accounting can be directed to an application server that can take care of the message processing. In other words, S-CSCF does not need to concern itself with signing operations. Using additional application server also allows parallel processing in the case, where the operators have to first create a dynamic roaming agreement, before any further interaction can take place. This negotiation actually is likely to dominate the performance impact over signature generation.

A potential complication is also the length of the messages. As the negotiation procedure contains both SIP and HIP specific data, it is not possible to fit that to a single UDP datagram in every case. According to SIP specifications, the implementations then have to switch using TCP. This has a slight performance penalty [17], but can also be additional problem if Network Address Translation (NAT) is in place. Thus, NAT traversal techniques would be needed. However, if all network elements were HIP enabled, SIP layer could use HITs instead of IP addresses as contact points as done, for instance, in [18]. In large messages, SIP content redirection mechanism for fetching assertions might be one option, as well.

4 Conclusion

In this paper we have sketched an architecture for providing user generated services with the help of IMS. It employs the principles of HIP and expects every entity to be in possession of a secure identifier. This allows secure naming of participants and also presents an accounting solution, which can be used to provide non-repudiable evidence of the service usage. As it uses hash chains, it is able to provide granularity to the service provisioning so that in case of misuse service interaction can be terminated and further waste of resources prevented.

Because of all the assumptions it may not be realistic to expect this kind of solution to enjoy deployment anytime soon. Hence, it is targeted towards future networks, which exhibit more ubiquitous and dynamic characteristics. However, this does not mean that parts of this work, like allowing user generated services within IMS framework with appropriate authorisation, would not be a feasible approach for current development as well. The worth of IMS is, after all, dictated by the richness of the provided service portfolio.

5 References

1. Moskowitz, R., Nikander, P., Jokela, P. (Ed.), Henderson, T.: Host Identity Protocol. IETF RFC 5201. Apr 2008
2. 3GPP: IP Multimedia Subsystem (IMS). 3rd Generation Partnership Project Technical Specification. TS23.228 V8.1.0. June 2007
3. Blaze M. et al. TAPI: Transactions for Access Public Infrastructure. In: Personal Wireless Communications. Sep 2003
4. Lamport L.: Password authentication with insecure communication. In: Communications of the ACM, vol. 24, no. 11. 1981
5. Heikkinen S.: Non-repudiable service usage with host identities. In: Second International Conference on Internet Monitoring and Protection. Jul 2007
6. Yang, C., Yang, Y., Liu, W.: A Robust Authentication Protocol with Non-Repudiation Service for Integrating WLAN and 3G Network. In: Wireless Personal Communications, vol 39, no. 2. Oct 2006
7. Kaufman, C.: Internet Key Exhange (IKEv2) Protocol. IETF RFC 4306. Dec 2005
8. Arkko J., Carrara E., Lindholm F., Naslund M., Norrman K.: MIKEY: Multimedia Internet KEYing. IETF RFC 3830. Aug 2004
9. Heikkinen, S.: Establishing a Secure Peer Identity Association Using IMS Architecture. In: Third International Conference on Internet Monitoring and Protectionz. Jul 2008
10. Jokela, P., Moskowitz R., Nikander P.: Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP). IETF RFC 5202. Apr 2008
11. Tschofenig H., Shanmugam M., Muenz F.: Using SRTP transport format with HIP, IETF Internet-Draft draft-tschofenig-hiprg-hip-srtp-02, expired. Oct 2006
12. 3GPP: Advice Of Charge (AOC) using IP Multimedia (IM) Core Network (CN) subsystem. 3rd Generation Partnership Project Technical Specification TS24.647 V8.0.0. Sep 2008
13. 3GPP: Telecommunication Management; Charging Management; Diameter charging application. 3rd Generation Partnership Project Technical Specification TS32.229 V8.4.0. Sep 2008
14. Peterson, J., Jennigs, C.: Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP). IETF RFC 4474. Aug 2006
15. 3GPP. Network Composition Feasibility Study. 3rd Generation Partnership Project Technical Report. TR22.980 V8.1.0. June 2007.
16. Heikkinen S.: Security and Accounting Enhancements for Roaming in IMS. In: 6th International Conference on Wired / Wireless Internet Communications. May 2008
17. Nahum E.M., Tracey J., Wright C. P.: Evaluating SIP Proxy Server Performance. In: 17th International workshop on Network and Operating Systems Support for Digital Audio & Video. Jun 2007
18. So J.Y.H., Wang J., Jones D.: SHIP Mobility Management Hybrid SIP-HIP Scheme. In: Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. May 2005