The Design of a Single Funding Point Charging Architecture

Christos Tsiaras, Martin Waldburger, Guilherme Sperb Machado, Andrei Vancea, and Burkhard Stiller

University of Zürich, Communication Systems Group CSG, Switzerland
{tsiaras,waldburger,machado,vancea,stiller}@ifi.uzh.ch

Abstract. Most federations across the world apply Single Sign-On (SSO) Authentication and Authorization Infrastructure (AAI) platforms. Thus, access to services offered by organizations, which belong to such a federation, can be granted to their users independent of their current location. The increasing demand to charge users for those service usages lead organizations to establish various charging mechanisms. However, until today the majority of organizations is using service-dependent solutions to perform charging. This policy absorbs the utility of an SSO system, since users still have to monitor and control each credit account separately. Therefore, the approach proposed defines an extension to SSO platforms, which is consolidated, non dispersed and service-independent. A Single Funding Point Charging Architecture (SFP-CA) allows users to settle payments using funds from the same credit account, for any type of service they use inside their federation.

Keywords: Accounting, Authorization, Single Funding Point, Charging Architecture.

1 Introduction

An outstanding example of organizations belong to a federation is universities that usually are monitored by a governmental federation [4], [10], [17]. End users, who are either students or employers of universities, are granted access to services offered by their institution via Authentication and Authorization Infrastructure (AAI) platforms. Services like printing, Short Message Service (SMS), or Voice over IP (VoIP), lead to high bandwidth demands and costs. A reckless usage causes an increment in related expenses. Thus, nowadays charging of end users is adopted by the majority of institutions [5], [7]. However, in most cases each institution has a separate service-dependent charging solution [18]. Each of these solutions would demand from a user to have multiple credit accounts which are used to pay for services consumed, across a federation, as well as inside the same institution. The existence of multiple funding points absorbs the utility of a Single Sign-On (SSO) system, because users have to monitor, control and learn how to use each credit account separately. Additionally, institution's Information Technology (IT) administrators are forced to maintain separate infrastructure in order to support each credit account type per user. Thus, the amount of

R. Szabó and A. Vidács (Eds.): EUNICE 2012, LNCS 7479, pp. 148–160, 2012.

working hours spent by organizations due to multiple funding points grows accordingly to the size of their user base. Furthermore, specific services, such as SMS, may be offered only by selected institutions in a federation. However, with a federation-wide charging in place, it will be possible to provide this set of services to other federation members, using the available infrastructure. Thus, the need for "replicated hardware investments", like an SMS gateway, will be minimized, since federations demand for this service is probably already covered by existing infrastructure.

An important lack of today institution's charging architectures features, is the ability of a real-time service access decision making, based on funds availability while users are consuming resources. For example, on [18] if the user has any non-negative account balance, the system will allow a printing-job up to hundred pages. As the total cost of each printing-job is calculated after its finalization, a user may print a significant amount of pages without having the necessary funds. The ability of taking the decision to interrupt a service due to lack of available funds is a powerful tool, when the minimization of free-riding is attempted. Furthermore, having multiple funding points for different services inside a federation/organization is like having multiple wallets to pay when buy different goods at the same mall/store. Therefore, the design decision for a dedicated support of a charging functionality in federations has been taken.

The newly designed "Single Funding Point Charging Architecture" (SFP-CA) handles the problem of charging event and session-based services offered by multiple organizations, which belong to the same federation; irrespective users charging method, home organization, current location, and with the use of a single funding point, while the decision to grant access is taken beyond the authentication and authorization criteria, considering the available amount of user funds in real-time. Due to the presumed existence of a security layer and a trusted federation, which ensures a full transmission data integrity and an overall system availability (e.g., SWITCH WAYF Service [16]), no security issues will be examined through out the design.

The remainder of this paper is structured as follows. Related work is discussed in Section 2, followed in Section 3 by the charging architecture of the SFP-CA. A detailed analysis of requirements as well as fundamental components are discussed within the same section. Furthermore, Section 4 is focused on the charging procedure for local and remote users, where the exact procedure is presented. Finally, this work is concluded in Section 5.

2 Related Work

Shibboleth [12] is a well known AAI platform used by many federations across the world. It designs a single SSO service across, as well as within the boundaries of an organization. A federated identity management concept is used in order to grant user access to different resources. Each user belongs to a single Identity Provider (IdP), which is responsible for user authentication. However, the Shibboleth AAI is very limited in accounting and monitoring tasks. The goal of the AMAAIS project [2] (Accounting and Monitoring of AAI Services) is to extend Shibboleth's functionality in that direction. The AMAAIS project initiated from the need of the SWITCH Federation [15] to monitor the use of resources of higher education institutions in Switzerland. This work goes beyond the AMAAIS accounting and monitoring extensions. It proposes the respective SFP-CA on top of AMAAIS extensions.

The charging solution proposed in this paper adopts the ideas proposed in [8] and [9] in order to achieve a larger variety of services support and the inter-domain charging functionality between higher education institutions. For example, SFP-CA is fully compatible with services like A^4-Mesh [1]. However, since it relies only on the existence of an AAI platform, it can be adopted by federations beyond the higher education institutions boarders.

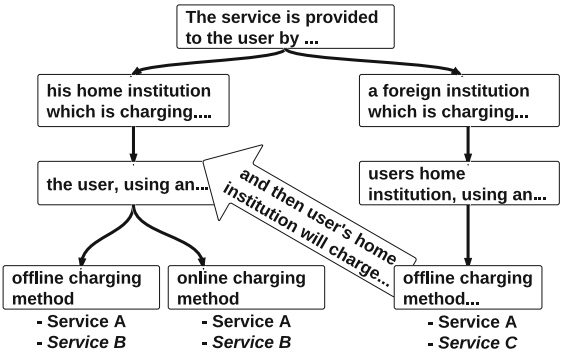

Fig. 1. Charging procedure

3 Charging Architecture

SFP-CA's challenge is that it equally supports event and session-based services, offline and online charging mechanisms (which are quoted in literature [11] as also postpaid and prepaid charging mechanisms), and that it handles price discrimination between users based on their relationship with the institution. This becomes even a larger challenge, when an accounting, monitoring and AAI architecture orchestration is targeted. SFP-CA handles to charge any user belonging to a federation no matter where his Identity Provider (IdP), or the Service Provider (SP) are located. Furthermore, users don't need a service or currency dependent funding method. Thus, inter-domain Charging Data Records (CDRs) will be created and exchanged if needed. The high level charging procedure of every possible scenario is outlined in Fig. 1.

In this scenario set, payments between institutions are shown. In order to minimize the overhead at the logistic department of institutions, minimal real money flow between them is required. Thus, the offline payment method is always used for payments between institutions. In order to support this broad scenario set a list of requirements which are part of this architecture is introduced in Section 3.1.

3.1 Requirements

Several requirements are mandatory in order to overcome significant limitations and introduce a universal charging architecture across a federation. First of all a funding source at the user side, if not there, is needed as a charging point for the resources that has been used. Additionally, a similar to user's funding point at the organization side is needed, so payments between organizations will be settled. Furthermore, in order to charge any service it is mandatory to have a service tariff map. An important feature

which increase the flexibility of a charging system, is the ability to apply a discrete charging policy for each user. Finally, a mechanism that interrupts a service, when needed, should be in place. Thus, the following list summarizes the requirements that has been just introduced (detailed in the following subsections):

1. User Virtual Funds Account (uVFA)
2. Organization Virtual Funds Account (oVFA)
3. Service Tariff Map (STM)
4. Service Usage Constraints and Limits (SUCL)
5. Interruption Service Trigger (IST)

These five requirements listed above ensure the fulfillment of the following four significant key features of a federation charging mechanism. Access to a service is subject to sufficient amount of available credits in case no constraints or usage limits forbid that. Services consumption will be charged according to the latest tariff provided by the SP. Service interruption supported in case circumstances dictate that. Finally, capability of inter-domain charging is supported through two different types of credit accounts which are mentioned above and described in more detail right after.

3.1.1 User Virtual Funds Account (uVFA)

At least one uVFA is required on each user account regardless its home institution. The credits on this account will be used so the user will pay for the resources he requested from the SP. If the user is charged with a postpaid method, the uVFA balance allowed to get negative values. With respect to a decentralized design, each user's IdP is responsible to create and maintain uVFAs. The SP is not responsible for the funding source. The funds will be absorbed directly from user's uVFA. One fundamental characteristic is that uVFA's balance is not expressed in real monetary units. SFP-CA is currency independent so Virtual Units (VUs) which are later translated in monetary units are used.

3.1.2 Organization Virtual Funds Account (oVFA)

The oVFA is the equivalent to the uVFA element on the organization side. The key difference between uVFAs and oVFAs is that each organization has one oVFA "paired" with every other organization in the Federation. It may seem inefficient and hard to maintain. However, this approach ensures the timely handling of potential errors. Furthermore, as the number of the organizations inside a federation does not change often, creating new oVFAs after all will be in place the first time, will be rare.

Similar to the uVFA VUs, which can be converted given a rate to monetary units, are used to express oVFA's balance. An organization *B* will add funds to his account, when a user who belongs to organization *A* will use some resources at *B*. At the same time the organization *A* will decrease his account's balance by the same value. This value represents the service cost. Thus, by the end of a given period each organization will know how much should pay, or receive, to every other organization without the overhead of the detailed transactions examination. When a payment between organization *A* and *B* is settled, both accounts are set to zero. Finally, as the aggregation of two "symmetric" oVFAs produces always zero, often checks in order to handle potential errors that occurred during the transfer of CDRs are highly recommended.

```
<?xml version="1.0"?>
<stm>
   <startup>2</startup>
   <termination>0</termination>
   <event>0</event>
   <rate>
      <value>2</value>
      <sec>20</sec>
   </rate>
   <minbalance>22</minbalance>
</stm>
```

Fig. 2. STM example

3.2 Service Tariff Map (STM)

The STM is the next requirement of the universal charging architecture, which is provided by each SP. It is a detailed description of every type of cost, such as the start up cost of a service (*e.g.*, the set up cost of a call), the rate of charging of a session based service (*e.g.*, a video conference or a call), the charging amount per event of an event based service (*e.g.*, an SMS), and the minimum available uVFA amount needed so the user will be allowed to access the service (`minbalance`). The `minbalance` tag is very important and should be carefully chosen when creating the STM. A value that covers the startup, termination plus five to ten times the rate or event/rate cost is recommended, `minbalance` importance will become more clear in Section 3.3.3.

Those information will be used properly by the SFP-CA to perform charging. STMs are available inside the federation, more details about the availability of STMs mentioned in Section 3.3.1. An example of a VoIP call STM presented on Fig. 2. For each call there is a two VUs start up cost as well as an additional charge of two VUs per twenty seconds. Thus, the `minbalance` in this case will allow a user to speak for two hundred seconds, which is a typical phone call duration in many countries [6].

3.2.1 Service Usage Constraints and Limits (SUCL)

The SUCL contains the knowledge of any service usage constraints and limits concerning the maximum number of consumed VUs per user, which is predefined by the user's home organization. The SUCL contains constraints of the maximum number of units that a user is allowed to spend, either in a specific period of time, and/or per session/event. The amount of VUs spent from the beginning of the period is included.

The SUCL can also contain discount information per domain and per type of service. User discounts are considered only during the uVFA but not during the oVFA balance update. Each organization need to pay the full price for any resources used by its users, at another organization of the federation, irrespective the discount that might offered to the end users by their home organization. In more detail, if user's organization is offering 50% discount to any type of service offered on every organization, user's organization will still pay 100% of service value when the service is offered by another organization.

The charging component utilizes this information in order to terminate a running, or deny access to a service and consider any possible discount. SUCL is the only non mandatory requirement of the SFP-CA. Every user account without an SUCL is considered to be a condition free user. Users missing an SUCL are limited only by the

```
<?xml version="1.0"?>
<sucl>
   <service>all</service>
   <maxunit>
      <session>1000</session>
      <event>100</event>
      <period>
         <days>365</days>
         <limit>999999</limit>
         <used>12345</used>
      </period>
   </maxunit>
   <discount>
      <domain>home</domain>
      <tos>all</tos>
      <percent>50</percent>
   </discount>
   <negative>yes
      <domain>home
         <amount>-1000</amount>
      </domain>
   </negative>
</sucl>
```

Fig. 3. SUCL example

available credits on their uVFA. However, due to safety reasons it is highly recommended that IdPs create an SUCL for each of their users, or group of users. An example of an SUCL can be seen on Fig. 3.

3.2.2 Interruption Service Trigger (IST)

The IST is responsible for urgent termination of a service, due to insufficient funds, or in case a maximum usage limit has been reached. Each SP should provide the IST which will send the termination signal to the SP.

In case of a printing job IST could execute printer's *cancelJob(jobID)* method, or if the service is a VoIP call the *soft hangup <channel>* command execution on an Asterisk VoIP server [3] will drop the call.

3.3 Components

There are four "managers" listed below orchestrating the charging procedure on SFP-CA. Those managers handle four basic procedures, host and retrieve STM per type of service, host and retrieve STM per SP, update uVFA's and oVFA's balance and last but not least accept and handle local and remote user's requests to access a service after authentication and authorization procedure is finished.

1. Service Provider Manager (SPM)
2. Charging Rate Manager (CRM)
3. Account Balance Manager (ABM)
4. Charging Manager (CM)

The major interactions of those elements are outlined in Fig. 4. Two way action arrows represent decision making as well as attribute update procedures. In more

detail, CMs and ABMs take decisions concerning user access to a service and update uVFA/oVFA balance. One way actions arrows represent the cost related information retrieval by the CRM and the SPM, and processes which does not involve any attribute updates like pulling the IST when is needed. However, detailed interactions, like the update of the oVFA and the retrieval of the SUCL, will be explained in more detail in Section 4.1 to Section 4.2, as it is mandatory to have a prior knowledge of all participating elements on those procedures to better understand them.

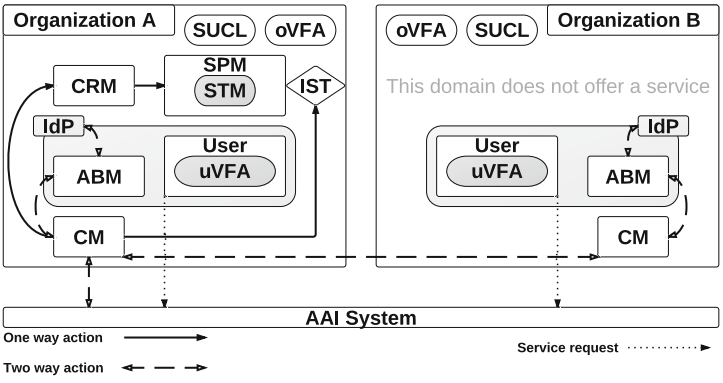

Fig. 4. SFP-CA elements interaction

3.3.1 Service Provider Manager (SPM)

If at least one SP exists inside an organization, it should also exist at least one SPM. Each SP is assigned to a SPM, which has prior knowledge of every available STMs offered by the SP. For example if one service, like SMS, has different tariff for domestic and international sent messages, then the SPM has a prior knowledge of which STM should be applied. When the SMS request will reach the SPM, the appropriate STM will be returned. This manager is service and location dependent. It is recommended that there is one SPM for each type of service and premises inside the organization. The SPM could be interpreted as a service request parser and a STM index. SPM is responsible to complete the matching procedure between the service request and the STM to be applied.

3.3.2 Charging Rate Manager (CRM)

The premises of an organization are usually distributed. Furthermore, the same type of service could be provided by multiple departments of an organization (*e.g.*, printing facilities). Thus, multiple SPMs for a given type of service coexist. The CRM forwards a request to the appropriate SPM. Due to the overall system fault tolerance, multiple CRMs will run in parallel. Synchronization between CRMs is performed either manually, every time a new SP is added, or in a daily basis.

3.3.3 Account Balance Manager (ABM)

The ABM is a multi threaded process that accept and apply charging requests from the CM and manages uVFA/oVFA balances. Each time a charging request received an

amount equal to the `minbalance` mentioned on Section 3.2 deducted from user's uVFA balance. When the cost of a service reach `minbalance`, a new deduction equal to it is taking place. At the end of a service any unused amount is aggregated to user's uVFA balance. If a user run out of the minimum VUs needed, the ABM notifies the CM and the service is interrupted. If the `minbalance` set to be less than a threshold equal with the startup, termination plus one time the rate or event cost, then the ABM will deduct this threshold from uVFA. However, in order to minimize uVFA balance updates, or prevent a user accessing a service due to high `minbalance` value; the `minbalance` value should be chosen carefully. During the online charging procedure, a similar mechanism to the six step credit reservation procedure proposed at [13] is used. The amount of VUs to be reserved each time needed is equal to `minbalance`.

3.3.4 Charging Manager (CM)

The heart of the SFP-CA is the CM. This is the decision maker component concerning the access to a service according to user's available funds. It also considers user's past resources usage and check if any usage limits are reached. Furthermore, "orders" the ABM to update uVFA and oVFA balance when needed.

The CM handles every charging issue thus, there are multiple CMs per domain. Each user is assigned to a single CM but multiple users can be handled by one CM. Last but not least, all the ISTs inside an organization are accessible by every CM of the same organization. All the CMs can communicate and exchange data between them, so charging requests can be addressed to any CM. For user assignment to a CM and the corresponding CM retrieval Chord lookup protocol is used [14].

Table 1 summarizes the component and requirement(s) association with each problems that the SFP-CA is solving.

Table 1. Components and requirements association with problems handled by SFP-CA

SFP-CA component	SFP-CA requirement(s)	Problem
CRM	STM	Support of event and session-based services
CM	--	Support of multiple organizations, which belong on the same federation
ABM	uVFA oVFA	Support of prepaid and postpaid payment method
ABM	oVFA	Inter-domain charging
SPM	--	SP's and user's location-independent charging
--	uVFA	Single funding point
CM ABM	uVFA	Access control based on available funds

4 Charging Procedure

The SFP-CA establishes a flexible solution, which handles every charging issue independent of the type of service (event- or session-based), the payment relationship between the user and the IdP (prepaid or postpaid), using a slightly differentiated procedure between local and remote users.

The reason that the charging procedure is divided into this two categories is that although a trustworthy environment inside a federation exist, it make sense that each organization need to maintain the control of charging for every service that is offered inside its boundaries. Furthermore, organizations in a federation are independent and maintain a degree of freedom concerning the technologies that they adopt. Thus, for back-ware compatibility purposes, and the ability to support multiple charging solutions if an organization is not compatible with the SFP-CA, the distinction between local and remote users charging policy has been chosen. In non compatible cases the remote user is charged, simply by forwarding the request to a non real-time available funds monitoring charging solution.

Section 4.1 describes the complete, error and deadlock free charging procedure for local users, when the SUCL or the uVFA available balance, does not prevent the resources usage. An example with no external failures, like server crashes and network/link unavailability is selected on purpose, in order to examine how the SFP-CA behaves. Each rectangle represents a task that, due to deadlock avoidance, should be completed within a certain time threshold, else access to the service is denied. Thus, access to services that can not be charged for some reason, is not granted. A similar example concerning the remote user charging procedure is part of Section 4.2. As the sequence diagrams in both local and remote user cases show, the service request is directed first to the AAI system. Thus, only authenticated and authorized users will be able to access a service. Finally, as Fig. 4 shows the IST can be triggered only by the CM and not by a malicious users. It is important to consider, as discussed, that security issues are not examined in detail in this case.

4.1 Local Users Charging Procedure

What first happens when a user requests access to some resources offered by a SP located in his home organization, is the authentication and authorization procedure by the AAI platform. Then the request is forwarded to the CM who is retrieving through the ABM all the necessary charging attributes, like uVFA's balance, user's charging method (online/offline) and the SUCL. Those information retrieved by user's IdP. This is the first decision point for the CM. If user's uVFA balance is not zero when online charging method should be applied, and there is no limit reached according to his SUCL, the CM proceed to the next decision point.

The STM is retrieved from the SPM and if the user has sufficient funds, like the minimum amount needed to grant access to the service, the CM notifies the ABM to begin charging the user. ABM notifies the CM that the charges are applied and then the CM grant user's access to the service. The procedure described above illustrated on the sequence diagram on Fig 5.

4.2 Remote Users Charging Procedure

In case that a user is trying to access a service offered by another organization inside the federation, the first three steps of the procedure described above, authentication, authorization, service request from the CM, are the same.

However, each CM is responsible only for users belong in his organization. Thus, the charging request is forwarded to the remote CM. The remote CM is following the same procedure like the service is offered by user's home organization. Furthermore, the remote ABM updates the oVFA balance. Right after, the remote CM notifies the local CM that all the charges will be applied so the local CM updates the respective oVFA balance and grant user's access to the service. The remote user's charging procedure presented on Fig. 6.

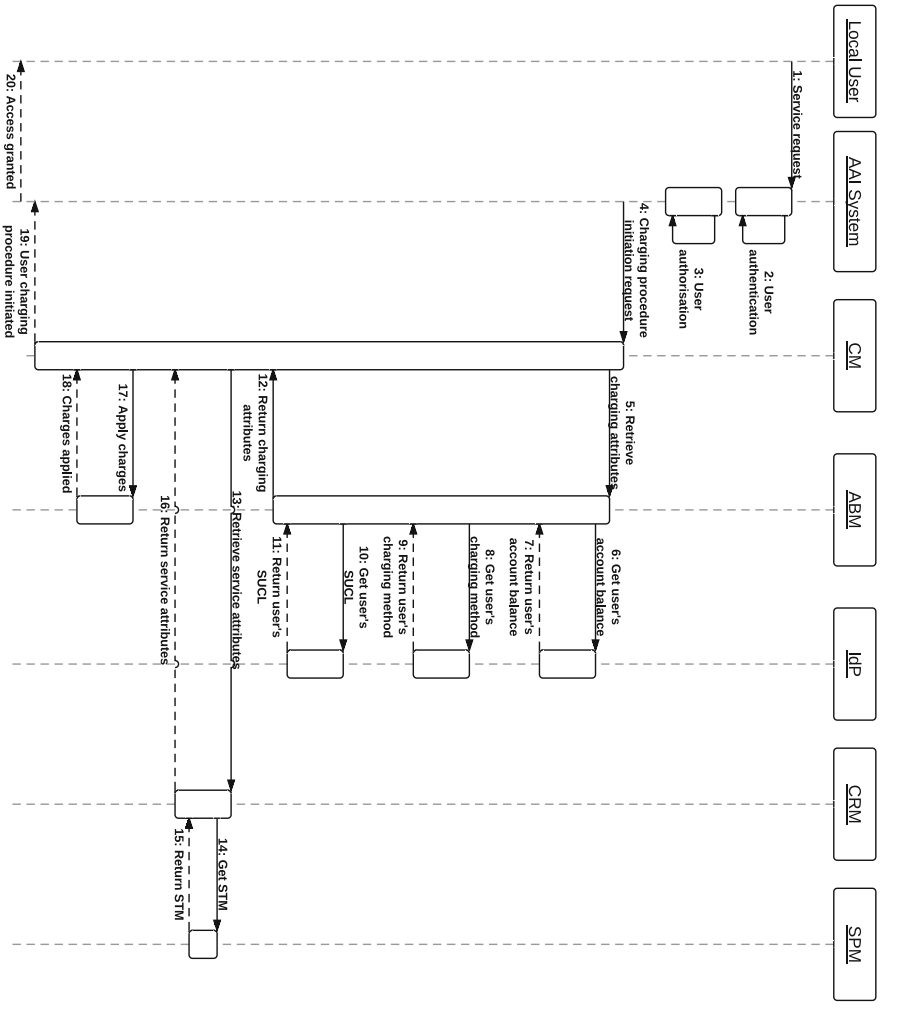

Fig. 5. Local user sequence diagram

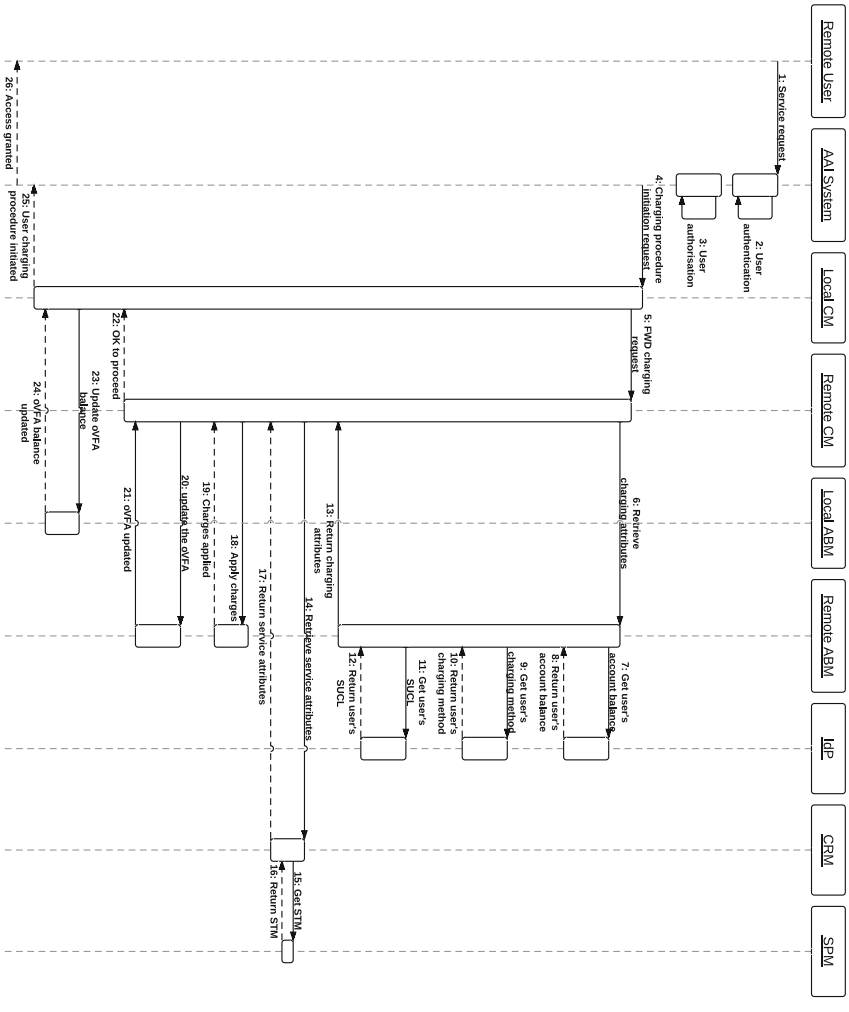

Fig. 6. Remote user sequence diagram

5 Summary and Preliminary Conclusions

In this work a charging architecture to support organizations across a federation has been proposed. The key features of this charging architecture are the ability to extend any AAI platform, and provide real time user access control based on the available fund amount. Furthermore, SFP-CA is service, payment method, and monetary unit independent. It introduces a single funding point inter/intra-domain charging, and last but not least, payments between the organizations are fully supported.

Finally, the SFP-CA will be implemented on top of an AAI system and operate with an existing charging infrastructure. Thus, the migration of present charging solutions inside a federation can become with the minimum overhead. Organizations will benefit from a simple all-in-one charging solution. Any service offered by an organization can become available for all members of the federation without the need to create virtual/guest user accounts by the "host" organization. Unused resources will be available to other organizations, as well as the utility of the effort which is done by organizations to maintain a service will be maximized (SMS example).

Acknowledgment. Many thanks are addressed to all members of the AMAAIS project for their contributions and priceless discussions. This work was funded by the E-Infrastructures Program of the BBT, Berne, Switzerland.

References

1. A4-Mesh Project. Authentication, Authorization, Accounting and Auditing in Wireless Mesh Networks, https://a4-mesh.unibe.ch/ (visited in November 2011)
2. AMAAIS Project. Accounting and Monitoring of AAI Services, http://www.csg.uzh.ch/research/amaais (visited in March 2012)
3. Asterisk The Open Source Communication, http://www.asterisk.org/ (visited in March 2012)
4. Bundesministerium für Bildung und Forschung, http://www.bmbf.de/ (visited in March 2012)
5. Eidgenössische Technische Hochschule Zürich, http://www.ethz.ch/ (visited in March 2012)
6. Fernmeldestatistik 2010 (Provisorische Ergebnisse), p.14, http://www.bakom.admin.ch/dokumentation/zahlen/00744/00746/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDeoR8fmym162epYbg2c_JjKbNoKSn6A (visited in March 2012)
7. IT-Universitetet i København, http://www.itu.dk/ (visited in March 2012)
8. Lutz, D.J., Lamp, D., Mandic, P., Hecht, F., Stiller, B.: Charging of SAML-based Federated VoIP Services. In: International Conference on Internet Technology and Secured Transactions (ICITST), London, U.K, pp. 1–8 (December 2010)
9. Lutz, D.J., Stiller, B.: Combining identity federation with Payment: The SAML-based Payment Protocol. In: 12th Network Operations and Management Symposium (NOMS), Osaka, Japan, pp. 495–502 (April 2010)
10. Ministère de l'Éducation nationale, de la Jeunesse et de la Vie associative, http://www.education.gouv.fr/ (visited in March 2012)
11. Kurtansky, P., Stiller, B.: State of the Art Prepaid Charging for IP Services. In: Braun, T., Carle, G., Fahmy, S., Koucheryavy, Y. (eds.) WWIC 2006. LNCS, vol. 3970, pp. 143–154. Springer, Heidelberg (2006)
12. Shibboleth: An Internet 2 Project. Shibboleth in Use, http://shibboleth.internet2.edu/shib-in-use.html (visited in March 2012)
13. Sou, S.I., Hung, H.N., Lin, Y.B., Peng, N.F., Jeng, J.Y.: Modeling Credit Reservation Procedure for UMTS Online Charging System. IEEE Transactions on Wireless Communications 6(11), 4129–4135 (2007)

14. Stoica, I., Morris, R., Liben-Nowell, D., Karger, D.R., Kaashoek, M.F., Dabek, F., Balakrishnan, H.: Chord: A Scalable Peer-to-peer Lookup Protocol for Internet Applications. IEEE/ACM Transactions on Networking 11(1), 17–32 (2003)
15. SWITCH Federation, http://www.switch.ch/ (visited in March 2012)
16. SWITCH WAYF Service, http://www.switch.ch/aai/support/tools/wayf.html (visited in March 2012)
17. Utbildningsdepartementet, http://www.regeringen.se/ (visited in March 2012)
18. VPP – Versatile Printing and Plotting, https://www1.ethz.ch/id/services/list/vpp/index_EN (visited in March 2012)