Chapter 21

# INTER-ORGANIZATIONAL E-SERVICES ACCOUNTING MANAGEMENT ON COMPUTATIONAL GRIDS

Franco Arcieri[1], Fabio Fioravanti[2], Enrico Nardelli[1,3] and Maurizio Talamo[1]
*(1) NESTOR - Laboratorio Sperimentale per la Sicurezza e la Certificazione di Servizi Telematici Multimediali - Università di Roma "Tor Vergata"*
*(2) Dipartimento di Informatica - Università dell'Aquila*
*(3) Istituto di Analisi dei Sistemi ed Informatica "Antonio Ruberti" - Roma, CNR*

Abstract: Accounting management is of strategic importance for a successful uptake of computational Grid technology within the user community. Computational Grid is one the most important paradigms for distributed computing and high-performance e-service provision. In this paper we present an architecture for accounting management of e-services on computational Grids which fully meets both the reliability and security requirements for accounting management architectures defined by the Internet Engineering Task Force (IETF). The presented solution, based on previous work successfully deployed in many italian public administrations, nicely fits with the overall Grid architectures and features a clear separation between management of the service and its control.

Key words: Certification of E-Services, Accounting Management, Grid Accounting.

## 1. INTRODUCTION

Grid-aware accounting management is concerned with the generation, communication and processing of data related to the consumption of resources used during a computation requested by a Virtual Organization on a Computational Grid. Resources which can be considered for accounting can be very heterogeneous, ranging from physical devices (like mass-storage devices or CPUs) to network bandwidth and process activity. Furthermore, security and reliability requirements of accounting management protocols

greatly vary depending on the intended use of collected resource consumption data. Indeed, accounting data can be used for performing activities which are inherently imperfect, like capacity and trend analysis, or activities requiring a higher degree of precision, like charging users for resources usage *(billing)* or verifying the correctness of a procedure *(auditing)*. For example, moderate packet loss can be tolerated when predicting future trends in resource usage, while it becomes unacceptable in usage-sensitive billing where it may cause revenue loss. Moreover, given that Computational Grids naturally span over multiple domains, and accounting data are exchanged between different organizations, reliability and security requirements must be stronger than in the intra-domain setting. Accounting management is of strategic importance for the development of computational Grids ([Foster et al., 2001]), where members of autonomous and independently operated organizations join to form a Virtual Organization (VO). In this scenario, members of a VO share a common set of resources and applications which cooperate in order to provide a complex service resulting from the composition of several component subservices. Of course, these interactions take place in a strictly controlled way , and one of the most important requirements is to be able to certify the actual provision of a component subservice to the requesting client, both for billing purposes and for conformance to service level agreements. Since component subservices are usually already existing and based on legacy IT systems, any solution to this certification problem should feature low invasiveness and strong independence from the application level.

Unfortunately, approaches to accounting management which have been presented in the literature (see, for example, [Aboba et al., 2000] and [Rigney, 1997,Case et al., 2002,Carrel and Grant, 1997]) propose solutions which require agreement on a common set of standards and protocols. Therefore, they are not suitable to be easily adopted in Grid environment because they require that all involved organizations modify their legacy IT systems, thus raising a serious organizational problem, not to mention additional setup and maintenance costs. On the contrary, our solution is based on the analysis of network traffic and the reconstruction of information flows related to e-service provision. In particular, by aggregating and correlating requests and replies related to the same service invocation, our architecture allows one both to monitor the performance of the whole system or of some of its nodes, and to certify service supplying, thus providing invaluable support in case of legal disputes.

We show that our solution satisfies the reliability and security requirements for accounting management defined by the Internet Engineering Task Force (IETF) in [Aboba et al., 2000] while featuring low invasiveness. Thus, it can be rapidly and effectively deployed on very large

networks with no changes in the software infrastructure, as it is being demonstrated by its successful use in the realization of a number of inter-organizational e-services in the Italian Public Administration (PA) (see [Arcieri et al., 1999,Arcieri et al., 2002,Arcieri et al., 2001a,Talamo et al., 1999] for details).

The paper is organized as follows. In Section 2 we discuss requirements for accounting management in an inter-organizational framework for e-service provision. Our architectural solution is described in Section 3 and its possible extension to certification of web services is briefly discussed in Section 4.

## 2. REQUIREMENTS FOR INTER-ORGANIZATIONAL E-SERVICES ACCOUNTING MANAGEMENT FOR GRIDS

In an inter-organizational decentralized model, like that used on computational Grids, autonomous organizations exchange information over the network in order to provide a complex service to the end-user. The overall service thus results from the cooperation among several component subserservices, each supplied by a (partially) independent organization which autonomously manages its legacy information systems and its policies about information security and dissemination.

Each subservice provider must then both carry out assigned institutional activities in an effective and efficient way and cooperate with *service providers,* which are in charge of providing the overall service to the end-user. A service provider is an organization which is distinct from the organizations providing the component subservices, and is the unique responsible for provision of a specific service. In terms of the architecture of a computational Grid, subservices are resources and service providers are members of a VO. Additionally, from a different perspective, we may also consider service providers as resources and end-users as members of another VO.

An example from the Italian PA is the support that Ministries of Health and of Labour and the National Institute for Social Welfare have to provide, in a scenario where relevant changes are introduced in the national welfare system, both to the Government (in evaluating various options for changes) and to citizens (to keep them up-to-date with their rights and duties according to their pension scheme).

In this scenario, we can identify additional requirements which have not been considered in the IETF Reference Architecture proposed in [Aboba et al., 2000]. An ideal solution to the inter-organizational certification

problem would require the involved organizations to agree on a common set of protocols and standards like those being developed by the IETF, or proposed by the Open Grid Services Architecture (OGSA) research group in [Foster et al., 2002] and to modify their IT systems accordingly.

Unfortunately, in the inter-organizational scenario presented above this approach is unfeasible for the following reasons. Agreement on a common set of standards is typically not scalable: each organization naturally tends to use a different set of protocols for communication with each other cooperating organization, thus leading to a clearly unmanageable proliferation of "standards". Also, the adoption of a unique standard cannot be imposed by a hierarchically superior organization in a scenario in which involved organizations are financially and operationally autonomous.

Indeed, as we have already mentioned, component subservices are provided by existing legacy IT systems which are very difficult or impossible to modify, and are thus regarded as black-boxes. Even if existing IT systems can actually be modified, this practice is not economically profitable because of the additional financial resources required both for implementation and for maintenance.

## 3. AN ACCOUNTING MANAGEMENT ARCHITECTURE FOR E-SERVICES IN AN INTER-ORGANIZATIONAL SCENARIO

We now illustrate our reference architecture and we show that:

(i) it can be regarded as an instance of the IETF Reference Architecture presented in [Aboba et al., 2000] for accounting management,

(ii) it meets the requirements for auditing applications as they have been defined in [Aboba et al., 2000], and

(iii) it meets the additional requirements for accounting management in an inter-organizational framework.

The architecture we propose for certification of e-services provision is based on the following main entities: *network probes, the probes controller* and the *certification server* (see Figure 1).

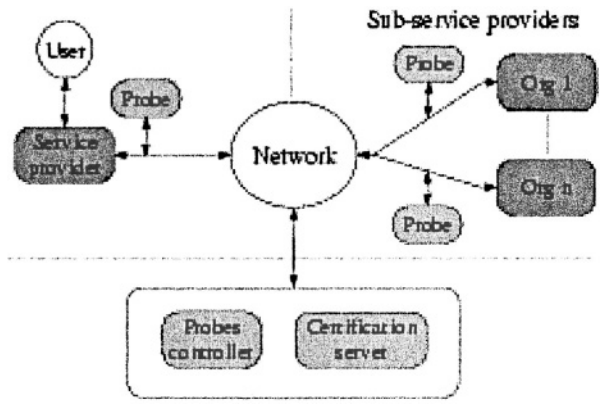


***Figure 1: The architecture for certification of e-services in an inter-organizational scenario.***

*Network probes* (or *probes,* for short) are devices installed at service and subservice providers which monitor and analyze network traffic related to a specific service for which they have been configured. Probes reconstruct information flows from acknowledged TCP segments related to the same service request and send reconstructed application-level data (e.g. XML) to the probes controller for further processing. Probes are equipped with an UPS (Uninterruptable Power Supply) unit, self-diagnosis tools and largely redundant disk space, thus providing support for archival accounting and increasing robustness of the accounting management process against data loss and hardware failures. They are fully scalable because only service specific traffic is monitored. Probes have no terminal devices which can be used to access their internal resources, but they are fully configurable from remote by using SNMP and a proprietary protocol based on UDP.

With respect to the context of the IETF Reference Architecture ([Aboba et al., 2000]), network probes play the role of network devices: they are located at organizations sites and send accounting data to a central server. From a functional point of view, however, they are also similar to accounting servers because they aggregate accounting information and generate session records, although also the architecture presented in [Aboba et al., 2000] provides for this eventuality.

Network traffic generated by network probes is not very high because only synthetic information, possibly compressed, is transmitted over the network, thus reducing resource consumption. This approach also feature high scalability in terms of computing power because accounting data processing is spread among several probes and the load on the probes controller is reduced. Notice that no change in existing IT systems is needed

for probes to function properly and thus our architectural solution features low invasiveness.

In order to better understand how network probes reconstruct application level messages exchanged by two hosts on the Internet we will now shortly review the behaviour of the TCP/IP protocol. When a process running at the application level (e.g. an HTTP client or HTTP server) wants to send a message (e.g. an HTTP request or response) to a process running on a different host, it passes the application message to the underlying transport protocol along with the destination host address and port number. In the TCP/IP protocol suite there are two choices for the transport protocol: (*i*) TCP which is a reliable and connection-oriented protocol, and (*ii*) UDP which is unreliable and connectionless. In the following we will focus on TCP because it is the transport protocol adopted by most application level protocols (e.g. HTTP, SMTP, FTP, etc.). The case for UDP is even simpler. The TCP layer, on receiving an application message, splits it in smaller parts whose size depends on a TCP parameter called MSS (Maximum Segment Size). Each of this smaller parts, together with an header containing checksums, acknowledgments and information about congestion control, constitutes a TCP *segment.* TCP segments are delivered to the underlying IP layer which is in charge of delivering them to destination, possibly over multiple IP *packets.*

Network probes intercepts IP packets travelling on the network, recognize acknowledged TCP segments and reconstruct application messages. Recall that TCP is a reliable protocol, that is, parties involved in a TCP communication notify each other about the correct receival of data. In summary, the activity of network probes is similar to that of the TCP and IP protocol implementations running at the host they are installed at. For example, a network probe installed at host A and configured for monitoring the traffic between A and a different host B, processes network traffic from B to A as if it was the intended recipient of the application message.

The *probes controller* aggregates and correlates data about sub-services provision related to the same service request in different organizations. Correlation of exchanged information flows also guarantees protection against replay attacks: for example, the probes will ignore a provider claiming to have provided a service which was not requested by any user. Confidentiality can also be ensured by encrypting local storage, if desired. Correlated data are then forwarded to the certification server. The probes controller is thus, in the IETF architectural framework, playing the role of the accounting server both from the architectural and the functional points of view.

Communication between network probes and the probes controller is based on TCP and features data object integrity. Authentication and

confidentiality are also guaranteed by use of public-key cryptography. The data collection model is event-driven with support for batching and scheduling thus featuring high reliability and scalability, and is fully programmable.

The *certification server* receives correlated data from the probes controller and stores them in a relational DBMS. Correlated data can then be used for monitoring the performance of the system, locating bottlenecks, generating detailed reports and statistics, and, most importantly, for generating certificates of service provision. Therefore the certification server plays, both functionally and architecturally, the role of the billing server in the IETF reference architecture.

Since the communication model between network probes and the probes controller can be programmed, it is also possible to improve resilience against faults:

(i) by making network probes contact failover probes controllers in case that the attempt to contact the primary controller fails, and

(ii) by implementing scheduling algorithms which are more suitable for use in some applications, like those with strict constraints on processing delay.

Of course, the same arguments also apply to communication between the probes controller and the certification server.

An additional advantage of our solution is that its neutrality both from a technical and from an organizational point of view allows a trusted third party on the same network to carry out the monitoring and certification tasks, thus providing a clear separation between *management* of the service and its *control,* and thus avoiding risks and conflict associated with cases where a same organizations plays a multiplicity of roles. Notice that the organizational issues presented above have not been addressed in [Aboba et al., 2000], which just requires stronger confidentiality of information exchanged by inter-domain accounting applications.

The architecture here presented has been deployed for certifying e-service provision in the following systems in the Italian Public Administration e-Government initiative ([Arcieri et al., 2001b,Mecella and Batini, 2001]):

1. SICC (Sistema di Interscambio Catasto Comuni) ([Arcieri et al., 1999,Talamo et al., 1999]) is a system for exchanging cadastral data between the following entities: Ministry of Finance, Municipalities, Notaries and Certified Land Surveyors. The system is accessible nation-wide through a Web-based interface since September 1998. The effectiveness of its use is demonstrated by the number of administrative transactions successfully completed through the system in year 2001: they are 800.000 per month, corresponding to 60% of the overall transactions related to cadastral services

accomplished every year in Italy. Note that certificates related to ownership, location, geometry and value of real estates, are mandatory in estate's selling transactions and their issue is subject to a fee, paid for by the buyer. In the month of September 2001 the total value of Ministry of Finance's income deriving from certificates issued through this system corresponds, on a yearly basis, to the 20% of the overall sum cashed by the Ministry for cadastral services, which is estimated for the year 2001 to amount to 78 million euros (roughly 70 million US dollars[1]).

2. SIM (Sistema Informativo della Montagna) ([Arcieri et al., 2001a]) is a system for providing services in various fields (cadaster, labour, pensions, public registry of personal data) to Italian citizens living in mountain areas. Its design started in 1998 and the overall financial effort has been, until now, of about 52 million euros (roughly 47 million US dollars). Nowadays it is currently being used as a fully operational system in about one thousand operating centers, all over Italy, serving more than 10 million inhabitants, more than 4000 of the about 8000 municipalities and covering more than 54% of the Italian territory. Its extension to the whole country is currently under implementation.

## 4. MONITORING AND CERTIFICATION OF WEB SERVICES

The problem of enabling interoperability between e-business applications on the World Wide Web is currently being addressed by using XML-based ([Bray et al., 2000]) standards like the Web Service Definition Language (WSDL) ([Christensen et al., 2001]) and the Simple Object Access Protocol (SOAP) ([Box et al., 2000]). These technologies provide a framework within which it is possible to expose existing network applications in a uniform and elegant manner.

A WSDL document contains the definition of the message exchange pattern between a service requester and a service provider (one-way, request/response, or publish/subscribe), together with the definition of the structure of the messages, the message data types and the bindings to concrete network protocols (HTTP GET/POST, SOAP, MIME) to be used for invoking the service itself. Messages exchanged by the service requester and provider are typically formatted according to the SOAP protocol. SOAP messages are XML documents consisting of three parts: (*i*) an envelope

[1]at the exchange rate of about 0.9 US dollars per 1 euro

describing the message content and the rules for processing it, (*ii*) an optional header for extending a message with new features like authentication and transaction management, and (*iii*) a body containing data related to service requests or responses. Although HTTP is used as the main network protocol, SOAP can potentially be used in combination with a variety of other protocols, like FTP, SMTP or RPC.

In a Web Service architecture ([Boot et al., 2002]), if a service requester wants to use a web service, it must first obtain the WSDL document containing the service description, either from the service provider itself or from a discovery agency, that is a network-accessible catalog where service providers publish their service descriptions, like the Universal Description, Discovery and Integration of Web Services (UDDI) ([Bellwood et al., 2002]). In order to successfully complete the service invocation, interaction between requester and provider must obey to the specifications contained in the WSDL document which describes the service. As long as the parties involved in service provision adhere to the same service description, the software systems actually providing the Web services can be implemented by using any technical solution, ranging from Java Servlets to Application Server Pages.

In order to certify web services provision by using the architectural solution presented in Section 3, network probes must be installed both at the service requester and at the service provider sites, and configured for analyzing and reconstructing exchanged messages as specified in the WSDL document describing the service. Furthermore, since a service can be invoked several times between the same requester and provider, even during a short time interval, exchanged data should also contain information allowing one to exactly identify the service invocation (like timestamps or sequence numbers), thus allowing the probes controller to reconstruct the message exchange pattern related to the same service provision. For example, if SOAP is used as the underlying network protocol, session information can be included in the header of all SOAP messages exchanged by the service requester and provider in a service provision.

Since our solution is based on reconstruction of application-level data, different technical solutions must be used for allowing it to operate on encrypted communication channels. However, our solution can be deployed even in case that exchanged information is partially encrypted. Indeed, in most cases by analyzing only the high-level structure of messages one is able to provide a certificate of service provision. Selective encryption of messages is also preferable from a computational point of view because encryption and decryption require additional computational power, and current specifications for Web services security ([Atkinson et al., 2002]) are following this direction, by requiring that an encrypted SOAP message is still a valid SOAP message.

## 5. CONCLUSIONS AND FUTURE WORK

In this paper we have described a specific system architecture (and its implementation) which:

(i) fully meets the reliability and security requirements for accounting management architectures defined in [Aboba et al., 2000] by the Internet Engineering Task Force (IETF),

(ii) satisfies additional requirements related to specific organizational constraints deriving from an inter-organizational distributed framework for e-service provision, and

(iii) can be used for monitoring resource usage on computational Grids both for billing and certification purposes.

Using the terminology of [Aboba et al., 2000], certification of e-service provision is an auditing application, since certifying e-service provision consists in the verification of the correctness of a procedure.

All IETF requirements are met, since network probes and the probes controller support archival accounting, data integrity is ensured both at packet and object level, authentication and confidentiality are guaranteed by use of public-key based technology, protection against replay attacks is provided by the correlation of requests and service provisions performed by the probes controller. Our architecture features both physical and functional independence from the application level and is thus a non-invasive solution for monitoring and certifying e-services supplying in an inter-organizational setting.

The neutrality of the proposed solution both from a technical and from an organizational point of view allows a trusted third party on the same network to carry out the monitoring and certification tasks, providing a clear separation between *management* of the service and its *control,* and thus avoiding the risky multiplicity of roles played by the organizations.

As a development of the solution presented in this paper, we plan to address in more detail the following issues: (*i*) how to extend the proposed solution for certifying web services provision, and (*ii*) how to expose the certification process itself as a web service.

## REFERENCES

[Aboba et al., 2000] Aboba, B., Arkko, J., and Harrington, D. (2000). Introduction to accounting management. RFC 2975.

[Arcieri et al., 1999] Arcieri, F., Cammino, C., Nardelli, E., Talamo, M., and Venza, A. (1999). The italian cadastral information system: a real-life spatio-temporal DBMS. In Bölhen, M., Jensen, C., and Scholl, M., editors, *Workshop on Spatio-Temporal Database*

*Management (STDBM'99),* pages 79–99, Edinburgh, Scotland, U.K. Lecture Notes in Computer Science vol.1678, Springer-Verlag.

[Arcieri et al., 2002] Arcieri, F., Cappadozzi, E., Naggar, P., Nardelli, E., and Talamo, M. (2002). Coherence maintainance in cooperative information systems: the Access Key Warehouse approach. *International Journal of Cooperative Information Systems,* 11(1–2): 175–200. A preliminary version was published in the Proceedings of the 4th International Conference on Cooperative Information Systems (CoopIS'99).

[Arcieri et al., 2001a] Arcieri, F., Cappadozzi, E., Nardelli, E., and Talamo, M. (200la). SIM: a working example of an e-government service infrastructure for mountain communities. In *Workshop Electronic Government (DEXA-eGov'01), associated to the 2001 Conference on Databases and Expert System Applications (DEXA'01),* pages 407–411, Munich, Germany. IEEE Computer Society Press.

[Arcieri et al., 2001b] Arcieri, F., Giaccio, R., Nardelli, E., and Talamo, M. (2001b). A framework for inter-organizational public administration network services. In *International Conference on Advances in Infrastructure for Electronic Business, Science, and Education on the Internet (SSGRR'01),* L'Aquila, Italy. IEEE Computer Society Press.

[Atkinson et al., 2002] Atkinson, B., Della Libera, G., Hada, S., Hondo, M., Hallam-Baker, P., Klein, J., LaMacchia, B., Leach, P., Manferdelli, J., Maruyama, H., Nadalin, A., Nagaratnam, N., Prafullchandra, H., Shewchuk, J., and Simon, D. (2002). Web services security (WS-Security).

[Bellwood et al., 2002] Bellwood, T., Clement, L., Ehnebuske, D., Hately, A., Hondo, M., Husband, Y., Januszewski, K., Lee, S., McKee, B., Munter, J., and von Riegen, C. (2002). Universal description, discovery and integration of web services (UDDI) version 3. http: //uddi.org/pubs/uddi_v3.htm.

[Boot et al., 2002] Boot, D., Champion, M., Ferris, C., McCabe, F., Newcomer, E., and Orchard, D. (2002). Web services architecture. http: //www.w3.org/TR/ws-arch.

[Box et al., 2000] Box, D., Ehnebuske, D., Kakivaya, G., Layman, A., Mendelsohn, N., Frystyk Nielsen, H., Thatte, S., and Winer, D. (2000). Simple object access protocol (soap) 1.1. http: //www.w3.org/TR/SOAP.

[Bray et al., 2000] Bray, T., Paoli, J., Sperberg-McQueen, C. M., and Maler, E. (2000). eXtensible Markup Language (XML) 1.0 (Second Edition). http: //www.w3.org/TR/REC-xml.

[Carrel and Grant, 1997] Carrel, D. and Grant, L. (1997). The TACACS+ protocol. Internet Draft draft-grant-tacacs-02.txt.

[Case et al., 2002] Case, J., Mundy, R., Partain, D., and Stewart, B. (2002). Introduction and applicability statements for internet standard management framework. RFC 3410.

[Christensen et al., 2001] Christensen, E., Curbera, F., Meredith, G., and Weerawarana, S. (2001). Web Services Description Language (WSDL) 1.1. http: //www.w3.org/TR/wsdl.

[Foster et al., 2002] Foster, I., Kesselman, C., Nick, J. M., and Tuecke, S. (2002). The physiology of the grid: An open grid services architecture for distributed systems integration, http: //www.globus.org/research/papers/ogsa.pdf.

[Foster et al., 2001] Foster, I., Kesselman, C., and Tuecke, S. (2001). The anatomy of the grid: Enabling scalable virtual organization. *International Journal of Supercomputer Applications,* 15(3): 200–222.

[Mecella and Batini, 2001] Mecella, M. and Batini, C. (2001). A review of the first cooperative projects in the italian e-government initiative. In *1st IFIP Conference on E-Commerce, E-Business, E-Government (I3E-01),* pages 831–844, Zurich, Switzerland. Kluwer.

[Rigney, 1997] Rigney, C. (1997). RADIUS accounting. RFC 2139.

[Talamo et al., 1999] Talamo, M., Arcieri, F., Conia, G., and Nardelli, E. (1999). SICC: An exchange system for cadastral information. In Güting, R. H., Papadias, D., and Lochovsky, F., editors, *6th International Symposium on Large Spatial Databases (SSD'99),* pages 360–364, Hong Kong, China. Lecture Notes in Computer Science vol.1651, Springer-Verlag.