IDIS (2009) 2:189–204
DOI 10.1007/s12394-009-0028-0

Information exchange in business collaboration using grid technologies

Fotis Aisopos · Konstantinos Tserpes · Magdalini Kardara · George Panousopoulos · Stephen Phillips · Spyridon Salamouras

Received: 20 January 2009 / Accepted: 2 September 2009 / Published online: 29 September 2009

Abstract With the emergence of service provisioning environments and new networking capabilities, antagonistic businesses have been able to collaborate securely by sharing information in order to have a beneficial result for all. This collaboration has sometimes been imposed by state legislation and sometimes been desirable by the firms themselves so as to resolve frequently occurring abnormalities. In any case, as information exchange takes place between antagonistic firms, security and privacy issues arise. In the context of this paper, a collaborative environment has been analyzed for enterprises that set out in the banking sector. A Grid-based Anti-Money Laundering (AML) system has been developed in an effort to take advantage of the Grid infrastructure, supporting the secure and trustful exchange of information between financial institutions and ensuring the confidentiality of the data transferred and the authentication of the users to whom they are available. Special emphasis is put on security mechanisms for supporting identity and privacy management as well as in Service Level Agreements (SLA) enforcement for enabling a trust enforcement platform in a collaboration business model.

Keywords Service provisioning · Grid · Money laundering · Business collaboration · Privacy management · SLA

F. Aisopos (✉) · K. Tserpes · M. Kardara
NTUA, Athens, Greece
e-mail: fotaisopos@telecom.ntua.gr

G. Panousopoulos
Exodus S.A., Athens, Greece

S. Phillips
IT Innovation Centre, Southampton, UK

S. Salamouras
University of the Aegean, Samos, Greece

Introduction

Collaboration that requires information exchange at a business level is a very sensitive area, especially when it is to be implemented within a competitive market frame. Competition is hindering the development of strategic partnerships and a complicated framework is required so as to maintain trust across all collaborating members whose activities can be cooperating or non-cooperating e.g. antagonistic, cheating or even malicious.

The benefit from building business partnerships is summarized in the mindset: By sharing we gain more. Strategic alliances enable businesses to gain competitive advantage through access to a partner's resources, including markets, technologies, capital and people. Fast growing companies rely heavily on alliances to extend their technical and operational resources. In the process, they save time and boost productivity by not having to develop their own, from scratch. Any such collaboration involves interactions, knowledge sharing and information exchange.

However, even though collaboration between the organizations that are involved in a supply chain has been studied (e.g. (lacovou et al. 1995; Cachón and Fisher 2000; Mukhopadhyay et al. 1995; Porterfield 2008)) and to some markets realized, little work has been done in the case where antagonistic firms are collaborating by sharing information so as to achieve a common goal (which is not to build trust with intent to monopolize business (Moody 1904), that is, to create a cartel). Even though it is unusual, cases where information exchange between antagonistic organizations is required exist. In general, there are two conditions that constitute prerequisites for this case to hold: a) the organizations of a specific sector are imposed to involve a specific business process in their existing ones that delivers no direct benefit to them but only loss, and b) the business process' performance is improved, the cost reduced and the organisations will have a long-term benefit in their reputation through collaboration. Of course, this is a very rare case and is the one that this paper studies.

On the downside, while organizations may choose to exchange information with their competing partners in order to improve performance and reduce costs, they must balance the risks associated with providing information that can be used against them. Access to corporate data or even sensitive data belonging to third parties (e.g. the customers), may lead not only to a competitive disadvantage but also to legal issues. Information exchange then becomes a double-edged sword where it is a source of efficiency in implementing the business process but can allow firms to act selfishly.

SOA and Grids allow the creation of trusted environments for information exchange between competitive organizations making sure not to compromise private information or corporate secrets, as well as, not to expose the business to competition hazards. More importantly, using this technology it is made possible to not compromise sensitive private data along with the identity of the owner, but to partly expose information and only in the case of a true positive, to expose identity.

This paper focuses on presenting a system that has been developed in order to enable to competitive organizations that set out in the banking sector to collaborate using Grid technologies. The principle behind its operation is the trust establishment through long term application SLAs that are agreed by the executives of each bank (e.g. Chief Compliance Officers). The claimed breakthrough is that the risk management details expressed in these long term SLAs are reflected along with other technical terms in

short/medium termed technical SLAs. Furthermore, we exploit the properties of Grids in order to establish a dynamic security framework, at all the levels of the information exchange process. Finally, the proposed system achieves to manage identity so as to not compromise it at any point. This system is named Anti-Money Laundering in Grids (AMONG) and it is a product of the BEinGRID IST project (Business Experiment in Grid (BEinGRID IST), www.beingrid.eu).

In what follows, the paper presents the market on which the problem of establishing trustful collaborations appears ("Background: anti-money laundering"), and it introduces the technical solution for the trust enforcement and the Grid security mechanisms for identity management ("Technical solution"). Finally the paper explains the merit of this solution in the business world and presents the alternatives for resolving the same problem ("Evaluation—stress tests").

Background: anti-money laundering

Since the attacks on the US (Sep'01), Madrid (Mar'04) and London (Jul'05), anti-terrorism has risen to the top of the security agenda in Europe. Much debate, various action plans, numerous communications and several concrete developments have taken place at EU level with their main focus being on tackling the international problem of money laundering. Among actions proposed lies the 3rd Anti-Money Laundering (AML) Directive (Official Journal of the European Union 2005) which implements the 49 Recommendations produced by the Financial Action Task Force (FATF) in 2003 (Financial Action Task Force (FATF). http://www.fatf-gafi.org), aiming to combat money laundering and terrorism financing, by providing information deriving from financial institutions concerning suspicious or unusual activities as indication of money laundering, and extending its scope to transactions with potential relation to financing terrorism. Directive 2005/60/EC—which constitutes the manifestation of Proposal COM(2004)448 (Proposal for a Directive on the prevention of the use of the financial system for the purpose of money laundering, COM(2004)448)—has, thus, re-formed the definition of money laundering as manipulation of money derived from crime (activities that try to either legalize money gained out of illegal activities or hide their legal origin) or collection of legitimate money or property for terrorist purposes. The 3rd Money Laundering Directive is the first concrete step that extends an obligation to monitor transactions beyond banks to third parties such as tax advisors, auditors, real estate agencies, notaries, insurance intermediaries etc. Member States are currently in the stage of implementing the directive. All European banks have to preserve AML systems and Know Your Customer (KYC) procedures in order to comply with European and national legislation. When other institutions start implementing AML solutions, the AML market is expected to broaden significantly.

The following figure depicts the positioning of applications and service for Financial Services Providers (Redshaw and Furlonger 2006) (Fig. 1):

Technologies installed in Financial Institutions fall into these main management categories:

- Client
- Information
- Transaction

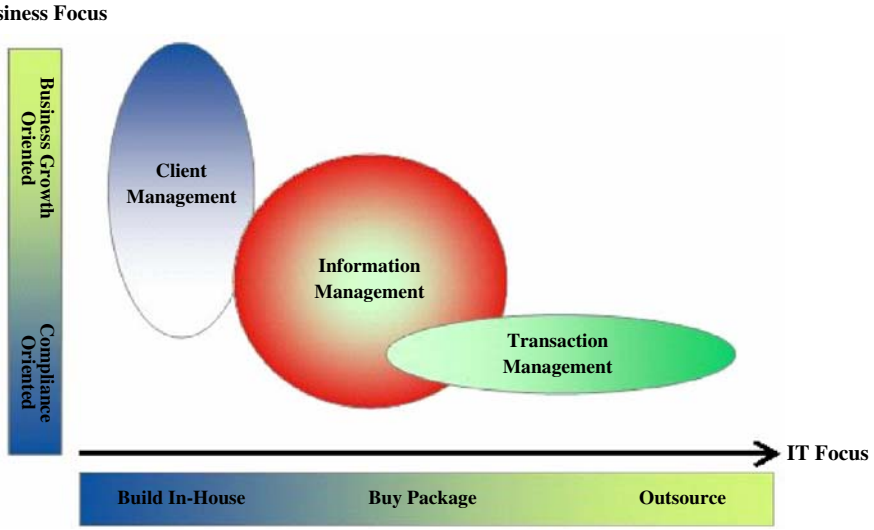

Fig. 1 Positioning of applications and service for financial service providers

The figure shows how these categories can be positioned for business and IT focus at Financial Institutions. Client management is the category that offers the greatest potential for growing the business—for most banks in the EU—and is the most likely to use applications that are built in-house, because there is a wide array of competitive differentiation. On the other hand, transaction management focuses on achieving compliance with the regulated aspects of contemporary legislation and has therefore little potential for growing the business. Finally, information management stands somewhere in-between, with some potential for business growth and a blend of in-house applications, third-party packages and outsourced services.

The starting point for current anti-money laundering and anti-terrorism measures is accurate and cost effective monitoring of transactions at a very large scale (in major financial institutions this could be in the region of 5–20 million transactions per day) using AML Systems administrated by Compliance Officers (CO) in each financial institution. The collected data must be reported to the appropriate intelligence agencies and the whole process must comply with international regulations such as the 3rd Directive, and national regulations such as the USA PATRIOT Act.

The identification of the origin of transactions by financial institutions is a complex process that requires transformation of the data, which is impractical due to the large volumes of data involved. The ability of companies to collect transaction data has outstripped their ability to analyse it. Thus financial institutions depend on profiling to predict ‘normal’ behaviour, and look first for anomalies that may signify suspicious activity. Typical profiling methods include data mining, neural networks, statistical analyses, link-analysis, etc. The effectiveness of this approach depends on the context in which the technology is applied. The main limitation of current commercially available implementations is that they focus on analysing those financial transactions that reside within isolated financial institutions. The rules used to define anomalies are set locally, and when transactions trigger alarms, they are

investigated by the bank's own AML analysis team. Thus the detection of anomalies is not done in a consistent way across all financial institutions, and there is no automated correlation that could inform the construction of risk-based and trust-based models to fully implement the new EU directive.

So, existing systems offer only intra-bank automated AML analysis with inter-organisational communication being initiated only in case of anomaly detection restricting this way the monitoring process only to simple fraud detection, whereas the detection of complex illegal financial activities still remain an extremely time-consuming and costly process. This paper exploits Grid, in order to bring a new, widely adopted solution into the market, which will enable the exchange of essential information on suspicious customers. Through this process banks will be able to evaluate ML alarms more accurately, thus increasing ML detection percentages (industry standard is 5%–7%) and reducing the load of produced Suspicious Transactions Reports. The described process will take place in a secure and commonly trusted environment that will protect sensitive data of customers and will not expose data that could be exploited due to competition factors.

The process described in the aforementioned scenario will allow banks to engage in a rewarding procedure that will positively affect both institutions' compliance mechanisms. This effect is interpreted to:

- Increase the efficiency of AML procedures.
- Decrease the risk of reputation damage.

The final outcome constitutes a solution for more effective Money Laundering detection, based on existing AML software (e.g. MoneyWatch (Money Watch®, Anti-Money Laundering solution, http://www.exodussa.com/Default.aspx?id=1103&nt=19&lang=2) developed by EXODUS S.A.), currently installed in the banks' premises, and their collaborative operation through a Grid middleware service. In general this service enables banks (different or subsidiaries banks) to exchange information so as to improve the success rate of the AML application deployed to each bank. This information exchange is currently taking place in an informal way and it is based on trustful relations between people. The service that is offered, allows the banks to achieve information exchange in an automated, cost-efficient way and through secure and trustful communication channels. Each bank inside this collaboration environment is obligated through legal contracts to be trustworthy and reveal the real customer data requested, in order to achieve a beneficial result for all. At the same time, they all desire an inter-bank Anti-Money Laundering Framework working properly, in order to detect ML activity more efficiently and avoid huge fines by the regulators.

As mentioned, the solution uses existing commercialised products. The application of Grid, though, adds significant innovation, since it allows information exchange between financial institutions for the first time, thus making ML detection and prevention more effective and more efficient. The commercialised application triggers the dissemination of Grid potential in a market, where key players and end-users have not considered the respective advantages yet. Potential customers, namely financial institutions and, in due time, insurance companies, accountants and other end-users (as imposed by the 3rd ML Directive), will receive a faster and more efficient AML solution. The solution contributes significantly to both the avoidance

of compliance penalties, and the decrease of reputation risk. These benefits are provided to the customers at much lower prices, than the ones that characterize contemporary AML products.

Given that the information exchange between financial institutions concerns transactional data of high sensitivity, such as personal user data, client assets etc issues of security and trust between collaborating banks arise. Access to data belonging to third parties such as customers should be controlled by the system and security components must enforce data encryption and secure inter-banking communication, in order to ensure client data integrity and safety. Personal data exchange also has to do with ethical and legal issues and was a crucial factor of the presented solution. In Greece, the National Bank of Greece has recently issued Decision No. 281 ("ISOCRATIS", the Greek Bank of Legal Information in the Internet http://www.dsanet.gr/Epikairothta/Nomothesia/apof281_09.htm), which constitutes the transposition of the 3rd EU Directive into national law, stating that *t*he information exchange between Financial Institutions is allowed, as long as it refers to the same customer. The Directive is also expected to influence legislation in most European countries in the following period. Furthermore, another occurring problem is the risk of malicious use of collaboration privileges and access to corporate data for competition purposes. In this case, the Service Level Agreements between banks and the system monitoring components must prevent potential phishing attacks and corporate data access abuse.

Therefore, amongst the non-functional requirements of the software there are understandably many security requirements:

- All messages between financial institutions must be encrypted and signed to ensure data confidentiality and integrity.
- Access to each bank's data should be controlled by limiting inter-bank queries, to make sure that the data are used only for Money Laundering detection, rather than competition purposes.
- Each financial institution should only gain access to the Grid service under a specific account, as a result of a long-term service level agreement.
- The system should interact only with authenticated and authorized entities (users, external systems).
- The system should manage user authentication from heterogeneous authenticating systems.

Technical solution

Using grid in business collaboration

In the present section, a Grid-based Anti-Money Laundering system will be presented in an effort to take advantage of the Grid as an infrastructure supporting the analysis of transactions within a single bank but between organizations as well, bringing this way AML technologies closer to meeting new regulatory obligations. Issues of trust, security and operational management have been investigated both from the technical and business perspective.

By using Grid services, it is possible to overcome the fundamental limitation of the development of AML solutions that are meant to operate in a standalone basis. Such a Grid service allows financial institutions to extend and correlate their analysis methods using information from other institutions and also from their own business partners and customers. The following specific technical innovations are demonstrated in the AMONG solution:

- dynamic Grid ***security mechanisms*** provide a consistent framework for creating trusted networks that may span national boundaries, and allow a bank to provide secure access to AML information;
- dynamic Grid ***service level agreements*** allow the bank to define the level of access they can support, and implement service management methods to respond rapidly to requests without their resources becoming over-extended;
- interoperable Web Service specifications allow ***seamless data exchange***, facilitating the tracing of suspicious transactions and the correlation of data from different sources.

The resulting capabilities allow enhanced due diligence based on a secure exchange of information between the bank and other institutions. The middleware that is used is GRIA (Service Oriented Collaborations for Industry and Commerce, www.gria.org) which is the first Grid middleware designed from the start for commercial inter-enterprise service provision, and supports dynamic trust management and Service Level Agreement (SLA)-based management features. GRIA is a service-oriented infrastructure designed to support B2B collaborations through service provisioning across organisational boundaries in a secure, interoperable and flexible manner, using Web Service protocols based on key interoperability specifications and is available free and open source.

In our case, Grid technology and especially GRIA enables secure communication, using GRIA Security Components between financial organizations and provides SLA mechanisms for setting long term agreements between the two parts on authentication and acquiring limited access to each bank resources. The main implementation work that was required to create an experimental prototype consisted of deployment of the AML application within this infrastructure, and development of appropriate SLAs and corresponding monitoring, evaluation and accounting mechanisms. GRIA 5.3 provides many facilities of use in the current solution:

- a trade account service that supports setting up trade accounts (i.e. billing relationships) with a service provider, which can be used to keep track of consumers' credit limits and amounts owed, store policies for who can access services billed to each trade account, and validate service requests against these policies;
- an SLA management service that supports defining SLA offerings (known as SLA Templates in GRIA), and requests for SLA, based on these offerings, which can be used to keep track of and constrain service usage, store policies for who can access services under each SLA, and validate service requests against these policies;
- a service development kit that includes a Policy Decision Point (PDP) for storing dynamically updatable access policies local to each developed service, and a Policy Enforcement Point (PEP) that consults the local PDP and can also check whether a request is acceptable in the context of a billing relationship or SLA by validating security tokens using a trade account service or SLA management service;

- a client development kit that provides a graphical interface for managing GRIA resources (i.e. trade accounts and SLAs as well as application-specific resources) and accessing them through an invocation engine which can be configured to obtain the client's X.509 identity, Security Assertion Markup Language (SAML) assertions regarding group membership and tokens representing federations in a flexible manner.

Main AMONG scenario

To present the architecture we first provide the main scenario of AMONG, so that the reader can get a better understanding of the modules used in the architecture. A simple scenario is consisted of two banks: the first bank needs to query the second bank about a customer suspected of performing Money Laundering activities and get his personal details to ensure it is the same person, as well as his risk score (a number indicative of the possibility of him being a Money-Launderer), with the system performing some sort of mapping, so that it corresponds to a common climax for all collaborators. In real life more than two collaborators will be involved, as the first bank will be able to query multiple Financial Institutions at a time, having a different Service Level Agreement with each one of them. The AML information received by each bank will be subject to further analysis by the AML System of the first bank, taking into account the trustworthiness and reliability of each other bank, to conclude to a concrete profile and risk assessment of the customer in question. However, only two banks are shown here just for simplification purposes.

Firstly, we will describe the functionality of the AMONG solution, in order to present the service workflow. Then we will provide the main components used in the architecture, including GRIA and AML product components. We consider two Banks, namely Bank X and Bank Y. The following design uses X as the service provider bank and Bank Y as the client. In a real deployment, Bank Y would use the AML Services of many banks and would also provide an AML Service to other banks. The multiplicity and symmetry of the relationships is not shown in the figures or generally mentioned in the text to avoid complicating the explanations. The Compliance Officer (CO) of Bank Y, using the Bank's internal AML system, has identified a suspicious customer (or potential customer). He wants to see whether the particular customer has also been identified as suspicious by Bank X—a fact that would solidify Bank Y's information on the customer's risk score. The overview of the scenario is depicted in Fig. 2. The CO initiates a request to Bank X using the Internal Revenue Service (IRS) number of the investigated person to ask for the customer's details for verification purposes. Bank X checks whether Bank Y has access to its database, based on a X.509 keystore and Account Management mechanisms, ensures the queries performed have not reached the limit and can reply in the two following ways:

- No information: The statement can either imply that the particular person cannot be found in the bank's records or that the particular customer has a risk score below a commonly agreed threshold (e.g. "high"). This way the bank can protect other institutions from querying all of its customer records.
- Customer details: The system returns the customer's full name, date of birth and country of residence to Bank Y.

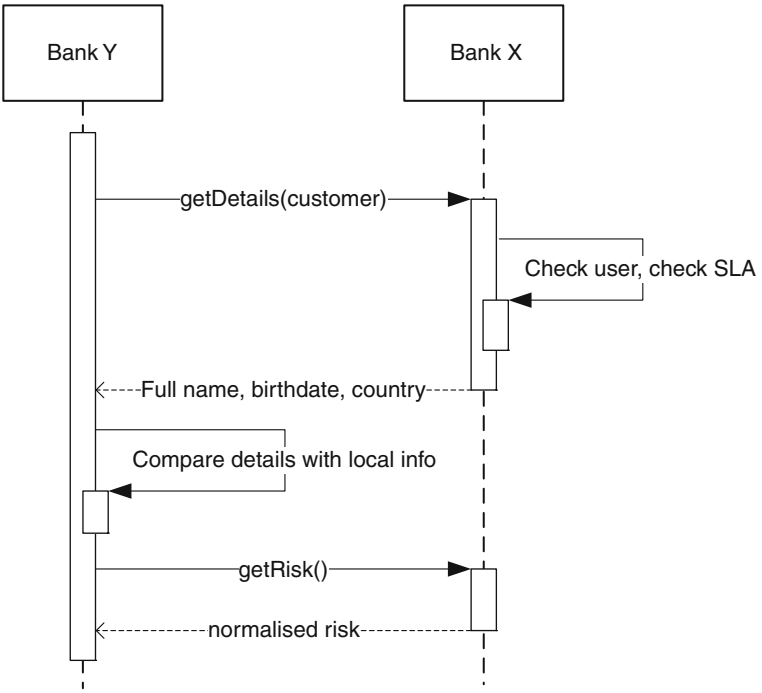

Fig. 2 Overview of the main interaction between the client and service banks

The system at Bank Y performs an automatic check on the personal details to confirm that they match the locally-held records. This is to ensure that Bank X and Bank Y are communicating about the same person. If the Bank Y AML system detects an inconsistency in the received data, the CO of Bank Y will move on with a manual analysis and check whether this differentiation constitutes fraudulent behaviour or the IRS number is false. This process could be time consuming (due to the involvement of manual analysis), and is out of the scope of this paper.

If the matching of the data is successful, then the AML system of Bank Y will ask for the risk score of the customer. Bank X will return the risk score in a normalised form that allows the mapping of the score to that used by Bank Y's AML system. This way the service guarantees interoperability among different AML solutions. Once the risk score is received, the CO at Bank Y will use it to inform the decision about what risk score will the bank give the customer itself. This is not an automatic process.

Architecture

To implement the above scenario a loosely coupled service oriented architecture has been designed. The following figure (Fig. 3) shows a typical deployment of an AML product, along with the additional components required. For simplification purposes the client has only been shown at Bank Y and the service at Bank X. It is expected that both banks would install both the client and the service to provide service to each other in a symmetrical manner. Also, only a few of the AML components have been shown at Bank Y.

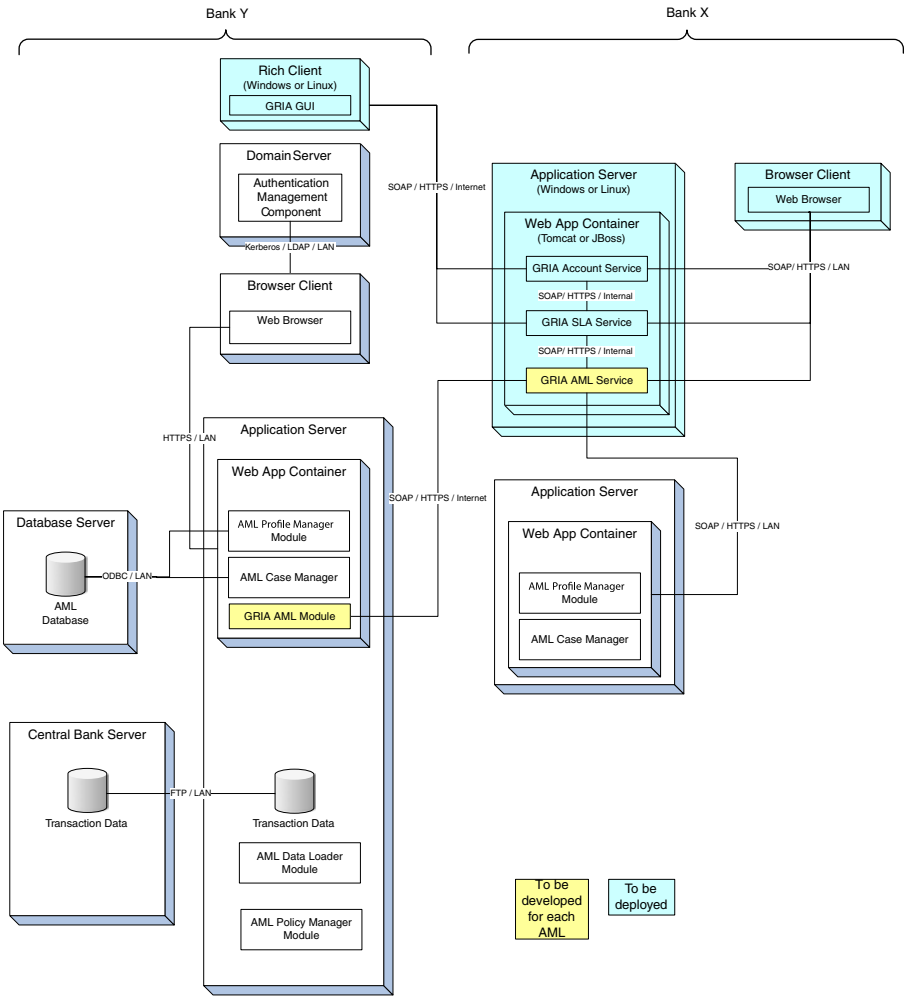

Fig. 3 A typical deployment diagram of the basic components

In brief, the components are:
Service provider (Bank X)

- A generic AML product providing some internal web services.
- The additional components required to provide an external AML service, hosted on a Windows or Linux Application Server:
  - The GRIA Trade Account Service: the account service defines the root of trust between two banks and keeps track of any charges made by the service bank to the client bank for using the AML Service. It provides the ability for a client to request an account, for the service provider to approve/deny requests and for both sides to manage accounts.
  - The GRIA SLA Service: the SLA service defines the service level agreement between the service and client bank and manages the AML Service, ensuring that the usage of the AML Service does not exceed the

agreement defined in the SLA. It provides the ability for a client (with an existing account) to view the available SLA templates, propose an SLA and for the client and service provider to monitor and manage SLAs.
- The GRIA AML Service: the AML Service provides a secure and managed front-end to the service Bank's existing AML system. It allows a client (with a valid SLA) to query the service bank for certain pieces of information regarding their customers for the purposes of AML.
- A web browser client for monitoring and managing the GRIA services through their web interfaces.

Client (Bank Y)

- Standard AML software components.
- The Domain Server is shown in Bank Y along with the module used for authentication purposes. The client software must integrate with this existing authentication mechanism.

The additional components required by the current solution are:

- The GRIA GUI Client: may be used to manage GRIA Trade Accounts and SLAs. Ultimately it may be that these use cases are dealt with by further integration with the client AML software, but as they are very infrequent it is not required.
- A GRIA AML Module integrated in the AML product portal (or to the AML GUI Client) to interface to the AML Service.

An important part of this solution is to design a system that allows different AML systems to interoperate and so generic AML products are shown at both the client and the service provider bank . The design makes this easy by limiting the integration between the basic components and the AML system to two well-defined points:

1. The GRIA AML Service: for a different AML system at the service bank a different back-end to the AML Service would be written to obtain the necessary information from the AML system. The web service interface would remain the same to ensure compatibility.
2. Client side: on the client, the integration point is between the AML portal and the GRIA client libraries. As will be seen, the number of different interactions the client AML software will make with the system is quite small so this does not represent a significant problem.

What needs to be deployed and what needs to be developed for every different AML system can be seen in the following Component diagram (Fig. 3), having marked with special colours the components needed for AMONG:

Although the overview of the scenario presented in Fig. 2 seems quite simple, all the additional components shown in Fig. 3 are required to provide the security and management aspects of the system.

GRIA trust and security

The system requirements are fully covered by GRIA. GRIA components were designed specifically for business to business relationship management using

bipartite agreements, localised security and management control. GRIA components may also be used to implement more traditional centralised VOs though they are lacking some management tools that can make this easy.

As mentioned, Identity Management and authentication are very important in AMONG. GRIA services and the GRIA client share the same trust and security system. All these services and their resources are protected in the same way, and require authentication for each client program. In a managed GRIA deployment, the client cannot do anything until they have a valid trade account. The client must apply for an account and (commonly) the service provider approves the account manually. The service provider might for also perform a credit check on the client or confirm his identity in some way, because although he will be identified by his X.509 credentials (Internet X.509 Public Key Infrastructure Certificate and CRL Profile, www.ietf.org/rfc/rfc2459.txt), GRIA does not have a list of trusted certificate authorities (CAs), instead anyone can be approved with his credentials being trusted thereafter. This process is very important because once the service provider approves a trade account he is permitting the client to obtain SLAs and use the services without any further manual intervention. It is this manual approval step that is the most important function of the service, in order to secure the whole process, without actually harming the flexibility. The accounting for usage is optional and depends upon whether the SLAs provided by the SLA service actually include any charges. Furthermore, the currency used by the Account Service and SLA Service does not have to be a real currency; it can be some sort of token and used as a high level count of usage rather than cost.

All messages sent through GRIA between the client and the service are digitally signed following the WS-Security standard (Web Service Security specification, WS-Security, Soap Message Security, Available from: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf) to ensure the message integrity. In addition, the messages are usually transmitted over an HTTPS transport to encrypt the contents and prevent eavesdropping.

The GRIA service infrastructure includes an implementation of the standard Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Information Point (PIP) and Policy Administration Point (PAP) design pattern (Secure Service PDP. http://grid.ece.ntua.gr/NextGRIDWiki/index.php/Secure_Service_PDP) using GRIA-specific interfaces, along with a service and resource security state model defined in XML. This provides a dynamic security system for resources where access control rules can be added and removed by authorized persons and a static policy for the service and resources defining which operations are available to clients of which role when the service or resource is in each state. For instance, the policy for the query resource would state that the *getRisk* operation could only be used by a client with the *owner* role when the resource was in the *IRSMatch* state. The client would obtain the *owner* role through matching an access control rule that specified that he could be an *owner*.

Finally, as mentioned, a long-term Service Level Agreement between the two banks limits the number of queries performed per day, in order to avoid “phishing attacks” from the querying bank. For the purposes of monitoring the SLAs’ usage, an SLA Violation Notifier tool, developed in the context of BEinGRID project as well, dispatches notifications regarding SLA query limit breaches to all interested

parties. To receive notifications, an interested party must subscribe to a notification system, implemented in the SLA Service of GRIA. Each subscription consists of a specific SLA the subscriber is interested in and a web service URL to which the notification will be sent. Only authorised users can subscribe to these notifications. Each time a new query by Bank Y overcomes a specific limit, the constraint manager of GRIA will create a *NotifyAction* instance and execute it, resulting in a *notify* operation being invoked in the AML services subscribed to this SLA (Bank Y AML Service and/or Bank X AML Service). This way Chief Compliance Officers (CCOs) of the two banks can get feedback on the SLA resource usage and maybe renegotiate the SLA terms with other banks if the number of queries frequently reaches the agreed limit (Fig. 4).

Evaluation—stress tests

The basic objectives of AMONG were achieved, building a trustful and efficient platform, enabling different AML Systems to collaborate securely. The expected evaluation on the AML efficiency and the increased AML success rates will be done in the long term by Financial Institutions adopting the solution. Since a pilot program is already built, the System is expected to go commercial at the beginning of 2010, when a Beta version will be ready. However, before the platform is adopted by banking groups, the system must be put into some kind of "stress tests", in order to validate that the system can cope with extreme operational circumstances:

Interoperability: Interoperability is a major requirement of AMONG, as the System must interoperate with different AML software installed on different platforms (Windows or Linux). The MoneyWatch AML software, which was initially used, operates only on Windows Server. Using the VMWare application,

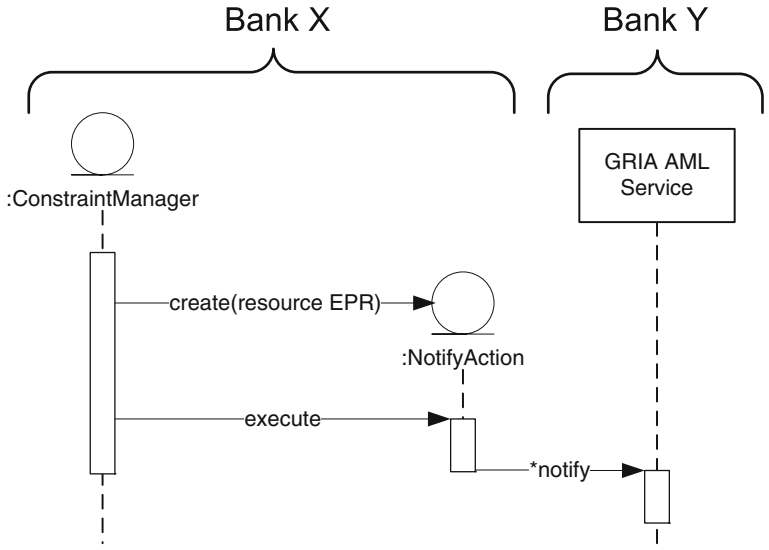

Fig. 4 When an SLA limit is reached, the ConstraintManager creates a NotifyAction

however, it was successfully deployed on Linux via a Windows Virtual Machine, a case that can be realized for AML applications working on any operating system.
Security and Authentication: As mentioned, the Identity Management and authentication are really crucial, especially when exchanging customer personal information. However, even if there was undesirable access to the data transported from end to end, by providing Transport Layer Security through https connection the decryption of the data was made practically impossible in real time, using any kind of brute force. GRIA services issue X.509 certificates based on users' local Kerberos or Active Directory credentials and nobody else can be identified as a user, without having a specific keystore stored in his client folders.
Dynamicity: Checking the dynamicity of managing the SLA lifecycle, we tested the GRIA SLA Service having different usage constraints in the SLA (e.g. running activities) and changed the billing tariff many times, adding more bands and requiring more notifications (different each time) to be sent by the Monitoring and Evaluation component.
Scalability: As a scalability test, the system operated normally having many collaborating banks and performing parallel queries to all of them for an investigated client.

Conclusions

The AMONG platform delivers mainly business benefits and is indented to be exploited as a market product by the end-user of the developing consortium, which is a bank. Therefore, an evaluation of the system by means of benchmarking the performance of AMONG is of very small value. The use in real-time conditions is going to produce clear indications as to whether the system will deliver what is promised. This, involves a business risk that the bank partner (end-user in the phase of development) is willing to take by using it for intra-banking purposes, that is, by testing AMONG's performance within the group of banks that operate under the same brand name. The testing will take place in a comparative manner by using AMONG in parallel with the existing standalone AMLs systems. However, in the phase of development the AMONG system was tested so as to mainly guarantee that the requirements (both functional and non-functional) have been met. For this reason, the money laundering systems and the databases of two banks were simulated using existing AML market products and actual bank databases that were anonymized and the data scrambled. At the end, the aggregation of heterogeneous information systems (different AML products) is feasible in the frame of AMONG as the layer of their interfaces is abstracted by the Grid service layer

- High-end Grid security components are providing increased security throughout the whole flow of information that is exchanged between heterogeneous systems and data
- The SLA enforcement, along with security provides a trust enforcement framework for effective business collaboration
- Identity of customer is not compromised at any stage of the business process
- Identity management is done through sophisticated Grid security components delivered by GRIA

Moreover, the undeniable business benefits AMONG are:

- **Holistic viewpoint of the AML environment**: COs understand that a holistic viewpoint can provide a clearer picture of a Money Launderer's activities. Moreover, the risk of identifying a client as a potential Money Launderer is —if not reduced— distributed among the trusted network of banks.
- **The broadening of the market**: Insurance companies, casinos and other businesses have to apply procedures that encompass enhanced due diligence and KYC processes. An extensible solution can be widely accepted by the target market, as long as pricing modification accompany the technical ones.

On a different notion, another approach for all bank to bank communications would be to go through a central trusted third party with no direct bank to bank communication at all. This hub and spoke model has the advantage of simple configuration and management at each bank (only a single relationship to manage) and also provides the ability to anonymise any requests so that a bank providing an AML service does not know which other bank is running a particular query.

However, there are two disadvantages of this model:

1. Banks may want to control their relationships with other banks, permitting or blocking access on a case per case basis. This is possible in this model but not as direct as when each bank controls its relationships through bipartite SLAs.
2. Currently, there is no suitable trusted third party. It may be that in the future, the central bank or financial services authority could play this role.

A halfway house between the simplicity of having a single agreement with a central third party and the relative complexity of each bank managing agreements with another bank is to keep the bipartite agreements between banks, but standardise the arrangements through a third party so that the management is simpler. That is, each bank wishing to cooperate over AML could join a consortium and sign up to legal agreements standardising their relationships with the other consortium members. The third party could then provide the services necessary to help manage a bank's relationships with the other banks, such as a central identity authority and registry of SLA templates. The main disadvantages of this method are that:

1. Banks may want to evaluate their AML systems and credibility differently depending on who is the other collaborating bank. This might result in different pricing policies in each collaboration, taking into consideration the risk of collaborating with a certain partner.
2. Banks entering in a collaboration through a trusted third party make themselves liable to the credibility of a great number of other banks the participation of which may not be able to control. Given that money laundering is not illegal for the banks themselves but it is for the society (the money launderer who uses bank products is basically making money for the bank) it might be the case that some banks are allured by the probability of making money and are willing to take the risk. Therefore, a bank needs to be very sure about which bank do they choose as their collaborator, something not very easy through trusted third party solutions.

Acknowledgement This work has been supported by the BEinGRID project and has been partly funded by the European Commission's IST activity of the 6th Framework Programme under contract number 034702.

References

Cachón G, Fisher M. Supply chain inventory management and the value of shared information. Manage Sci. 2000;46(8):1032–48.

lacovou C, Benbasat I, Dexter A. Electronic data interchange and small organizations: adoption and impact of technology. MIS Quarterly. 1995;19(4):465–85.

Moody J. The truth about the trusts. 1904.

Mukhopadhyay T, Kekre S, Kalathur S. Business value of information technology: a study of electronic data interchange. MIS Quarterly. 1995;19(2):137–56.

Official Journal of the European Union, "Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing", 26 October 2005, http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_309/l_30920051125en00150036.pdf.

Porterfield T. Diversity in business-to-business information exchange: an empirical analysis of manufacturers and their trading partners. Transp J. 2008;47(3):36.

Redshaw P, Furlonger D. Markets in financial instruments directive: the triple hit for technology vendors. Gartner—Industry Research, December 2006.