Results of the Swiss Priority Programme for Information and Communication Structures

MacPay: Macropayments for Uncorrelated Payments

Holger Petersen[1], Markus Michels[1], Daniel Som[1], Renato Cantini[2], Felix Baessler[2], Dimitri Konstantas[3], Jean-Henry Morin[3]
1 Entrust Technologies Europe, Glatt Tower, Zürich-Glattzentrum
2 Swisscom Corporate Technology, Berne
3 Centre Universitaire Informatique (CUI), University of Geneva

Aims of the project

Goods and services began being traded on the Internet without the use of any supporting technology. Consumers could select goods using WWW-based catalogues and when the payment phase of the transaction was reached, a variety of ad-hoc mechanism were used. These ranged from sending unencrypted credit card numbers across the network to the use of telephone or fax to transfer sensitive payment information. Unfortunately traditional payment systems, such as cash, credit cards and transfer of funds at point of sale are insufficient as payment mechanisms in this new environment without further adoptions. This is mainly due to security problems, the inefficiency of the systems and the related high costs of transactions.

To solve these problems, new payment systems are being tailored for the new requirements. The results are new forms of existing payment mechanisms, as well as completely innovative systems. At the same time while these payment systems for the future Internet commerce are being developed and tested, financial institutions, technology companies and telecommunication providers are developing and testing systems that are going to modify the cash market heavily.

Smart card based payment systems, currently being tested world-wide, provide transaction costs low enough to be used for any purchase that is currently done for cash. Moreover, the technology used for such smart card based systems is not fundamentally different from what is used in solutions for the global networks. That means that these cash replacement systems will merge with the new Internet payment mechanisms just as television will merge with other forms of information and communication transmissions. The aim of the project is to extend existing POS payment protocols for usage over open networks. This includes the loading of money into the card and the payment for goods over the Internet as well as the integration of the application HyperNews, that deals with the purchase of electronic documents in a pay-perview manner.

Key Results

The ECBS *Electronic Purse* TCD 101 working draft for POS payments was taken as technology basis. It is regarded as a new-generation payment scheme that is based on public key cryptography, while all other cash systems in use today are essentially based on symmetric cryptography. The scheme was adapted accordingly, such that it can be securely used over open networks.

Both guaranteed confidentiality of communication and robustness of protocol had to be reinforced by adding suitable error handling mechanisms.

In particular, the purchase transaction was secured by adding an asymmetric key exchange session before the actual protocol, while in the load transaction a derived secret key guarantees confidentiality. The protocol has been implemented on a JavaCard, which was one of the first commercially available JavaCards providing the required cryptographic functionality. The MacPay demonstrator consists of four separate workstations, that take the role of the issuing bank, the purse holder, the acceptor and the acquiring bank respectively. The smart card is connected to the purse holder's PC. The core functionalities of a payment scheme, i.e., load, purchase, balance inquiry, deposit and clearing were realized.

The HyperNews application requires that the payment is combined with the decryption of article key. During off-line payment, the money is transferred from the purse into internal card slots, that represent the credit of different information providers (IPs). The slots are cleared with the bank before the next loading of money to the card. The bank is responsible for distributing the money to the IPs accordingly. The HyperNews payment applet is loaded together with the purse applet into the JavaCard. This allows to demonstrate the full payment functionality together with off-line purchase of electronic articles. In particular, the user can download encrypted articles from an Information Provider, including the unencrypted title and an abstract, and can choose which article to purchase. The card controls the user's access to the full article after he has paid for it and also provides a receipt as proof of purchase. The receipt allows re-reading of already paid articles by the same user.

Technology and Know-How Transfer

The results could be used to realize value cards for supporting the HyperNews application.

The HyperNews application is under consideration for access control use in a large privately founded project by the "Association pour le Bien des Aveugles (ABA)".

The combined payment and access control mechanism used in the HyperNews application is a basic technology for the planned ElCom 2000 "StreamCom" project, which deals with encrypted data streams (like digital video).

Contact

For more information, please contact Dr. Holger Petersen, Entrust Technologies Europe'r[3] security engineering ag, Glatt Tower, 6.Floor, 8301 Glattzentrum.

MicPay: Micropayments for Correlated Payments

Holger Petersen[1], Markus Michels[1], Daniel Som[1], George Fankhauser[2], David Schweikert[2], Burkhard Stiller[2], Nathalie Weiler[2], Renato Cantini[3], Felix Baessler[3], Dimitri Konstantas[4], Jean-Henry Morin[4]

1 Entrust Technologies Europe, Glatt Tower, Zürich-Glattzentrum
2 Computer Engineering and Networks Laboratory TIK, Swiss Federal Institute of Technology ETH Zürich
3 Swisscom Corporate Technology, Berne
4 Centre Universitaire Informatique (CUI), University of Geneva

Aims of the project

Cash is the best suited conventional payment instrument for low-value transactions.

Nevertheless, versatile as it is, it is limited in that no transaction can involve less than the value of the smallest coin (e.g. one cent). This poses a problem in a number of classes of goods and services where the value of the transaction is less than the smallest coin, like for example obtaining a single quotation for the current price of a share on the stock market or purchasing an isolated article from a newspaper. In conventional commerce, the solution to this is to use a subscription model for payment, where the buyer pays in advance a lump sum for accessing a large collection of low value items.

Although in the electronic commerce world the subscription model ensures that the content provider is paid for his services, this model does not address a large customer base of people who may only wish to use a service very occasionally. It also restricts the ability of people to try out a service. Thus it is clear that the subscription model does not adequately solve the problem of low value transactions in electronic commerce and that there is a need for a payment system that can efficiently transfer very small amounts, less than a cent, in a single transaction.

The first issue in the design of such a system is that communication, which itself costs money, must be kept to an absolute minimum. A system where the costs of conveying payment are greater than the payment itself is unlikely to succeed. A second issue stems from the fact that the low value per transaction means that the profit made on each transaction is small. Thus the server providing the required support must be able to process transactions at a high rate in order for the service to be viable. This gives rise to a further requirement, that micro-payment systems must be able to make the payment verification in an inexpensive way. Consequently a successful micro-payment system must not involve computationally expensive cryptographic techniques. In particular, emerging Internet based applications such as Internet telephony or distribution/purchase of electronic documents demand for a convenient, efficient payment method. The goal of the MicPay project is to design a smart card based solution for such small payments (in the order of magnitude of several cents) and to apply it to two application scenarios: continuous online charging for an Internet telephone call (IPPhone) and consecutive payment for a set of articles (HyperNews).

Key Results

The basic design of two micropayment schemes applicable to the two application scenarios has been performed. For the IPPhone application a hash-chain based micro-payment scheme has been developed where the identities of all service providers are included in the root of the chain. That makes the cashing of the hashchain easy and avoids fraud among the service providers. The protocol has been implemented on a JavaCard, which was one of the first commercially available JavaCards providing the necessary cryptographic functionality. For the IP Phone demonstrator, the Resource Reservation Protocol RSVP (RFC 2205) has been extended for carrying such hash chain payment information. The core extensions of RSVP for payments have been implemented in Java in order to integrate the needed micro-payment objects of the specified payment scheme. A first prototype illustrates the feasibility of the chosen approach: it allows for high audio quality IP telephony calls with a guaranteed bandwidth, if the user is willing to pay for his call, and in turn, the reserved network resources.

For the HyperNews application a balance based micro-payment scheme was developed, where the payment is combined with some operations inherent to that scenario, i.e., the decryption of encrypted article key. During off-line payment, the money is transferred from the purse into internal card slots, that represent the credits of different information providers (IPs). The slots are cleared with the bank before the next loading of money to the card. The bank is responsible for distributing the money to the IPs accordingly. The HyperNews demonstrator illustrates the off-line purchase of electronic articles using smart card based access control and payments. In particular, it is shown how the user can download encrypted articles from an Information Provider, including the unencrypted title and an abstract and can choose which article to purchase. The card controls the user's access to the full article after he has paid for it and also provides a receipt as proof of purchase. The receipt allows rereading of already paid articles by the same user.

Technology and Know-How Transfer

The close cooperation with the SPP project CATI (Charging and Accounting Technology for the Internet) offered the possibility to apply the designed and implemented micro-payment protocol in a real world Internet telephony demonstrator. The cooperation with the SPP project HyperNews offered the ability to apply the micro-payment scheme to an existing E-Business application.

The outcome of the project could be applied to design and implement value cards for supporting the HyperNews and IP Phone applications. In particular, the results achieved with the design of payment and charging extensions for protocols will be utilized in the M3I project that is part of the European Union's Fifth RTD Framework Program.

The HyperNews application is being considered for access control use in a large privately founded project by the "Association pour le Bien des Aveugles (ABA)".

The combined payment and access control mechanism used in the HyperNews application is a basic technology for the planned ElCom 2000 "StreamCom" project, which deals with encrypted data streams (like digital video).

Contact

For more information, please contact Dr. Holger Petersen, Entrust Technologies Europe/ r^3 security engineering ag, Glatt Tower, 6.Floor, 8301 Glattzentrum.

Charging and Accounting Technology for the Internet

Burkhard Stiller[6], Torsten Braun[2], Bernhard Plattner[6], Roland Balmer[2], Florian Baumgartner[2],David Billard[1], Gabriel Dermler[3], George Fankhauser[6], Noria Foukia[1], Manuel Günter[2], Ibrahim Khalil[2], Helmut Kneer[4], Simon Leinen[5], Christian Matt[4], Peter Reichl[6], David Schweikert[6], Nathalie Weiler[6], Urs Zurfluh[6]

1 Centre Universitaire d'Informatique CUI, University of Geneva; 2 Computer Networks and Distributed Systems, Institute of Computer Science and Applied Mathematics IAM, University of Berne; 3 IBM Research Laboratory, Zürich; 4 Institut für Informatik, University of Zürich; 5 SWITCH, Zürich; 6 Computer Engineering and Networks Laboratory TIK, ETH Zürich

SPP ICS Electronic Commerce Projects, "CAPIV – Charging and Accounting Protocols in the Internet and in Virtual Private Networks" No. 5003-54559/1 and "MEDeB – Management, Evaluation, Demonstrators, and Business Models" No. 5003-54560/1

1. Project Objectives

The objectives of the CATI project (Charging and Accounting Technology for the Internet), consisting of CAPIV (Charging and Accounting Protocols in the Internet and in Virtual Private Networks) and MEDeB (Management, Evaluation, Demonstrators, and Business Models), include the design, implementation, and evaluation of charging and accounting mechanisms for Internet services and Virtual Private Networks (VPN). They develop the enabling technology support for open, Internet-based Electronic Commerce platforms. Their main components encompass usage-based transport service charging methods of high-quality Internet transport services as well as methods for advanced and flexible configurations of VPNs. To complete a real-world applicable solution, security-relevant and trust-related issues in charging, accounting, and billing processes are integrated. Furthermore, the investigation and development of pricing and cost models for Internet services is performed to obtain practical experiences in incentive-compatible dynamic pricing models. This work is complemented by important application scenarios, such as an Internet telephony application as well as an Electronic Commerce scenario, in order to demonstrate the applicability and efficiency of the developed approaches.

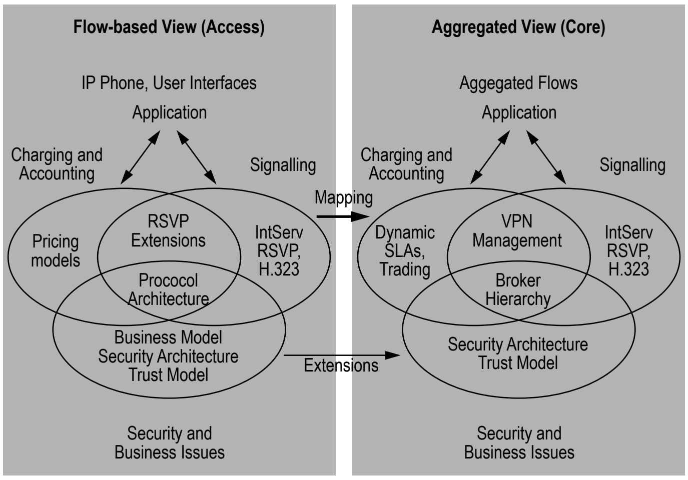

Fig. 1: Technical Structure of CATI

2. Problem Overview

For enabling high-quality Internet transport by economic incentives for E-Commerce scenarios, a set of charging, accounting, and management mechanisms for value-added Internet services are required. While starting with an approach based on the Integrated Services Architecture (IntServ), the project has laid recently a stronger focus on the Differentiated Services Architecture (DiffServ) as well. The IntServ approach utilizes known signalling protocols, such as the Resource Reservation Protocol RSVP, whose extension to carry charging relevant data within the networks on a per-flow basis is adequate. For the DiffServ approach an appropriate signalling approach is under development, which considers the DiffServ Bandwidth Brokers as well as Service Level Agreements (SLA) as important components for a charging solution. In addition the DiffServ/IntServ interoperability is envisioned to be able to support multi-provider scenarios in a much stronger focus. The development of a common technical concept has been performed, in which all project tasks are integrated, where the design and implementation of VPN management functions consider many DiffServ-related issues as prerequisites for future systems.

In due course, besides these important technological developments, business cases are considered jointly. They include the basics of packet-based networks, where the Internet determines the most prominent example, and are currently focussed on a flow-based approach of selling communication services. One of the major factors allowing the selling of these services is a set of appropriate pricing models. Finally, business views are backed by a security and trust model, which currently allows for the description of basic roles and relationships between participants in an e-commerce scenario and relate it to the technical networking environment.

3. Technical Areas

Within the CATI project, a number of intermediate results have been achieved. The basic CATI scenario and architecture have been described, delimiting an overall framework for detailed design and implementation issues. They cover the role of Quality-of-Service (QoS) provisioning and that of VPN usage by introducing the roles of customers, Internet Service Providers (ISP), and financial institutions. Signaling issues for IntServ, DiffServ, and their combination are integrated, which is demonstrated by an IP - telephony application as well as in an e-commerce scenario. The aspects of multiprovider models have been taken care of explicitly by the description of SLAs, their negotiation, their trading, and their scopes. A general graphical user interface for Internet applications utilizing the charging extensions has been implemented. It covers to a great extent services and QoS requirement specifications as well as payment system-related informations. An overview of the combined technical areas of CATI is depicted in Figure 1.

3.1 Internet Access Domain

The IntServ model of the Internet Engineering Task Force (IETF) based on RFC 1633 has been extended with charging and accounting mechanisms by defining new RSVP (RFCs 2205/2206) objects and performing first implementation steps. At this point the close cooperation with the SNF MicPay project needs to be stated, where an electronic micro-payment scheme has been developed and its requirements have been designed and partly implemented by new RSVP objects within the same CATI implementation.

3.2 Internet Core Domain

For the VPN management tasks, the QoS-enabled, secure, and Internet-based VPN management system's design has been implemented. It encompasses for QoS mechanisms the DiffServ model (RFCs 2474/5 and 2597/8) and maps fine-grained IntServ mechanisms onto Differentiated Services. These areas determine success issues for VPN provisioning in todays Internet services market, since VPNs determine a cost-sensitive alternative for leased lines or frame relay networks. While supporting a multi-provider scenario, the following tasks are provided: charging and accounting between customers and peer providers as well as automatic service negotiation, establishment, and maintenance based on a service configuration interface for customers, a RSVP/DiffServ-Gateway. This goal is achieved by a generalization of the Bandwidth Broker concept of DiffServ, introducing a broker hierarchy of services. The services implemented for CATI encompass QoS and VPN support.

3.3 Pricing Internet Services

The design of Internet services pricing models and its evaluation are in progress. The design is based on the classification of related work and an identified set of dimensions, such as service categories, pricing components, and charging parameters. A newly developed approach CHiPS (Connection-Holder-is-Preferred Scheme) proposes an auction model for dynamic price determinations in an incentive-compatible fashion. CHiPS solves the problem of synchronization issues of auctions between multiple ISPs, which originally is due to characteristics of the Delta Auction for continuously performing auctions. Therefore, the smart market approach is applicable to Internet packet flows, e.g., determined by explicitly reserved flows via RSVP. Furthermore, investigations on the optimality problem of prices for dynamic volume-based multi-class traffic prices are in progress. The ISP's point of view on pricing models in practice has been documented as well as a discussion on cost recovery schemes in a business environment.

3.4 Trust and Security Model

Since the transfer of charging information in an open Internet requires securing actions, a security model as well as a trust model have been developed. The trust model is applicable in a generalized e-Commerce scenario, where end-users, ISPs, payment providers, and a Public Key Infrastructure (PKI) determine the roles. Appropriate trust relationships between these roles are defined, taking into account common business practices and available protocols. Afterwards, this general model is directly applied to the IP telephony application scenario, which in turn cooperates with the MicPay project for the development of a micro-payment scheme. Work in the security domain considers, amongst others, the IP Security approach (RFC 2401-12) as well. The developed security architecture distinguishes between data flows and control flows and formulates three views. The reservation view involves the end-user (customer) and the closest ISP (access ISP). The service view determines an end-to-end relation between two customers and the intermediate ISPs. Finally, the clearing view encompasses the information exchange between the payee and the payer (either of the above defined roles), which depends on the payment scheme utilized. All of these views are based on the designed phases in the business model.

3.5 Business Model

Based on the technical necessity of roles and relationships, similar to the trust model assumptions, business roles have been defined. They encompass the end-customer and a customer premises network as well as two types of ISPs, access ISPs and core ISPs. Depending on these roles, the semantics of an SLA is interpreted and its content may vary. The business model itself introduces additionally the role of an e-commerce provider, offering services or goods in general. The business process as described in the model consists of four phases, each of which involving the determined roles and the utilized communication protocols. (1) The contracting phase sets up business conditions between business partners. (2) The reservation phase is applied to IntServ and establishes the service conditions and follows the reservation view as stated in Section 3.4. (3) The service phase corresponds to the service view and includes the actual performing of the negotiated service. Finally, (4) the clearing phase contains, dependent on the payment scheme negotiated, the payment and the billing process.

3.6 Demonstrators

For enabling high-quality Internet transport by economic incentives for e-commerce scenarios, a set of charging, accounting, and management mechanisms for value-added Internet services are required. They are in the progress of being implemented within CATI or have been finished prototypically already. These demonstrators are based on basic architectural work and concept definitions such as the definition of an integrated CATI scenario and architecture for Integrated Services/Differentiated Services (IntServ/DiffServ) models in support of charging, accounting, and Virtual Private Network (VPN) management mechanisms which is complemented by a security, a trust, and a business model.

- Design and implementation of charging and accounting extensions in reservations which are demonstrated by a sample IP telephony application and an adequate graphical user interface. The IP telephony application currently utilizes Microsoft's Netmeeting product and the ITU-T H.323 signalling protocol in addition. The prototypical demonstrator consists of at least three PCs running NetBSD (Linux in the future for routers) and the Crossbow IntServ architecture implementation, where in the case of the demonstrator two end-systems are interconnected by a router. Microsoft's Netmeeting – an IP telephony application – is running on both end-systems and utilizes an H.323 proxy for signalling purposes between them in addition to the extended interface of RSVP (Resource Reservation Protocol). During the IP telephony usage charging informations are calculated within the router depending on its pricing model applied. These informations are exchanged and distributed to connected end-systems and presented through their graphical user interfaces to the IP phone user. Therefore, the user is always aware of the current costs of the communication he has to pay for.
- Design and implementation of VPN service management based on a hierarchy of brokers which is demonstrated by a Web-based VPN configuration user interface. For all VPN management tasks, the QoS-enabled, secure, and Internet-based VPN management system's design has been implemented currently for a single-provider case, even though designed for the multi-provider case. The current implementation provides charging and accounting between customers and peer providers as well as automatic service negotiation, establishment, and maintenance based on a service configuration interface for customers. A Web-based configuration interface allows for the seamless integration of underlying technology such as the generalized Bandwidth Broker hierarchy of the DiffServ architecture. The demonstrator utilizes end-systems interconnected by IOS-driven Cisco routers as well as Linux-based router extensions for experimentation purposes. In addition, the transport of video or audio flows between subnetworks, utilizing the RSVP/DiffServ-Gateway implementation, has been demonstrated.
- Design and simulation of pricing model behaviors for dynamic market prices by a dedicated and specialized implementation of a simulation program for the newly developed approach called CHiPS. CHiPS applies the smart market paradigm on flow charging and

solves the problem of synchronization issues of auctions between multiple ISPs in multi-provider scenarios.

- Design and simulation of (i) bandwidth broker signalling in DiffServ networks and of (ii) Service Level Agreement (SLA) trading. First, a set of detailed signalling simulations investigate control scenarios for various inter-broker communication schemes, e.g., adaptive or fine-grained notifications. These simulations determine the trade-off between establishing end-to-end QoS guarantees and the control's scalability.

Secondly, a specialized simulation has been implemented to study statistical resource guarantees in a DiffServ environment. Since SLAs include essential information on inter-provider service provisioning, they may be used to describe individual flows or aggregates. The simulation includes SLA traders which operate on flow aggregates, performing on a slower time-scale signalling than per-flow signalling. Initial simulation results show that profit-driven routing decisions for traffic described by SLAs can be suitable for DiffServ core networks.

- Application and development of an accounting and flow detection tool. Communication service user affiliations have often expressed their intention to charge individual users or organizational units such as departments or institutes for the volume of network traffic generated. So far, the technical and administrative complexity involved with this has prevented them from doing so. Therefore, tools through which individual users can inform themselves about their amount of network usage have been utilized. Heuristics have been developed to aggregate flow accounting data generated by routers into categories suitable for charging.

3.7 Key Achievements

The work in CATI and its proposed solutions is compliant as far as possible with a number of standards and quasi standard products as mentioned above. The proof-of-concept for a valid usage-sensitive pricing scheme as well as a suitable and efficient charging and accounting implementation has been performed by means of an IP telephony as a sample application. In particular, CATI has achieved up to now the following four key issues, ranging from important conceptual work and evaluations, including its documentation, to prototypical implementations:

- Definition of an integrated CATI scenario and architecture for IntServ/DiffServ models in support of charging, accounting, and VPN management mechanisms which is complemented by a security, a trust, and a business model.
- Development and evaluation of pricing and cost models for the Internet.
- Design and implementation of charging and accounting extensions in reservations which are demonstrated by a sample IP telephony application and a graphical user interface.
- Design and implementation of VPN service management based on a hierarchy of brokers which is demonstrated by a Web-based VPN configuration user interface.

4. Know-how and Technology Transfer

The IntServ model for the future Internet has been extended with charging and accounting mechanisms by defining new RSVP objects and performing first implementation steps. The close cooperation with the SNF MicPay project resulted in a demonstrator for the MicPay project which includes the trust model developed for CATI and MicPay jointly.

Besides these important technological developments, business cases are considered as well. They are concerned with the basics of packet-based networks, the Internet in particular, and are currently focussed on a flow-based approach of selling communication services. One of the major factors allowing the selling of these services is a set of pricing models, whose applicability and changes as well as extensions, in turn, are part of the CATI project.

These investigations are closely performed with the CATI project partner SWITCH, determining an Internet Service Provider in a university-driven market situation.

The architectural discussions of moving towards a DiffServ-based Internet environment are of importance to our industrial partner IBM. Therefore, the integration work of IntServ and DiffServ, its signaling tasks and mapping problems, SLA topics and handling mechanisms, and the integration of charging and accounting tasks is transferred.

Some upcoming SNF projects, such as ANAISOFT, INVENT, and StreamCom, will utilize some of the solutions developed within CATI and will combine mobile agent technology, workflow applications, and charged VPN services. Furthermore, a future European research project in the 5th framework program called M3I exploits the charging-relevant topics of CATI to allow for the investigation of market-managed multi-service Internet mechanisms and scenarios.

Project Manager and Contact:
Prof. Dr. Burkhard Stiller,
Computer Engineering and
Networks Laboratory TIK, ETH
Gloriastrasse 35, 8092 Zürich,
Tel: 01 632 7016, Fax: 01 632
1035, stiller@tik.ee.ethz.ch,
http://www.tik.ee.ethz.ch/~cati

An Electronic Market of Workflows

Claude Stricke
Logistics, Economy and Management (LEM), Lausanne

Objective

Managing processes is crucial for efficient organizations. Groupware tools like Workflow Management Systems (WFMS) can provide a support by enabling explicit design of processes and automated tracking during execution. But more and more, processes span organizations boundaries, for instance when services are outsourced (e.g. development of a web site or shipping of products). How to coordinate internal and external resources in such cases? How to ensure that the selected service's provider will execute his part of the process in the expected cost and time and will match the needed quality?

The goal of ACE-flow prototype is to demonstrate that an electronic market of workflows can enable such support. Any companies, industry associations, trade associations, etc. that would see their cases demonstrated in ACE-flow project, can contact the authors of the project.

Outsourcing of services and inter-organizational process management

The outsourced service can be considered as a sub-part of a process initiated in the customer's organization. This process is composed of a set of tasks, one of them being the outsourced service. The outsourced task will produce a result that will be used by the customer's organization in order to complete its process. Thus, the whole process could be considered as an inter-organizational workflow that should be defined and managed in order to ensure that it produces the desired level of quality in time and budget.

Market-based management of workflows

In order to ensure that the outsourced task will meet customer's demand, services can be accessed through an electronic market managed by a third party. The customer's organization can look up for types of services that correspond to its need and place orders by specifying detailed requirements. The third party is in charge of selecting the provider(s) that best match the customer's requirements, by requesting offers, collecting and comparing replies. When a provider has been selected, it will start the service at the planned date. During execution, the customer will receive progress status and eventually the final results.

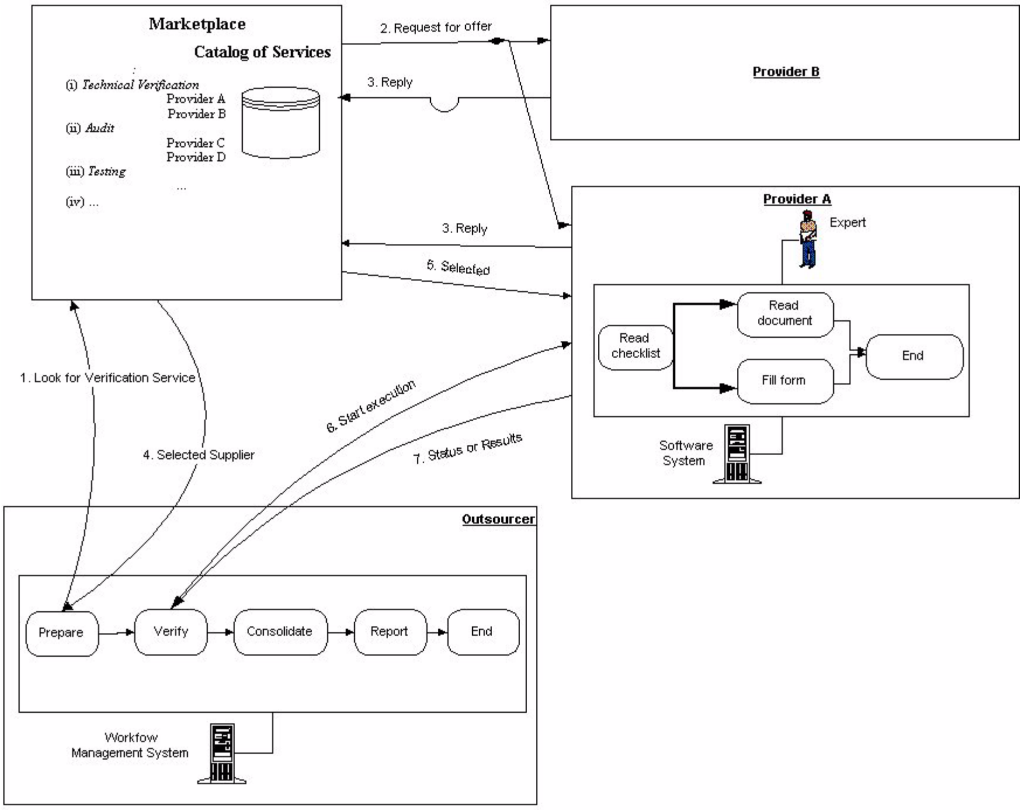

Fig.1: Cases

Cases

Figure 1 illustrates a simplified case where the outsourcer searches for a service related to "technical verification". A catalog managed by the electronic marketplace is browsed and when a suitable type of corresponding service is found, the outsourcer can place an order. Services can be of any kind: transport of materials, production of components, market survey, printing of a brochure, scaffolding in construction project, testing in software development, etc. They might be described in different catalogs that would be specialized by domain (e.g. construction, software, marketing, logistics), because each of the domains has its own semantics to describe their services.

Realization

A software system is being prototyped to demonstrate the concepts. It consists of a set of workflow systems and an automated trader system. The workflow systems reside in different organizations and the trader system acts as an intermediary among the customers and suppliers of services, maintaining information about their offers and requests. The traded services are treated as workflows. Figure 2 features the different components.

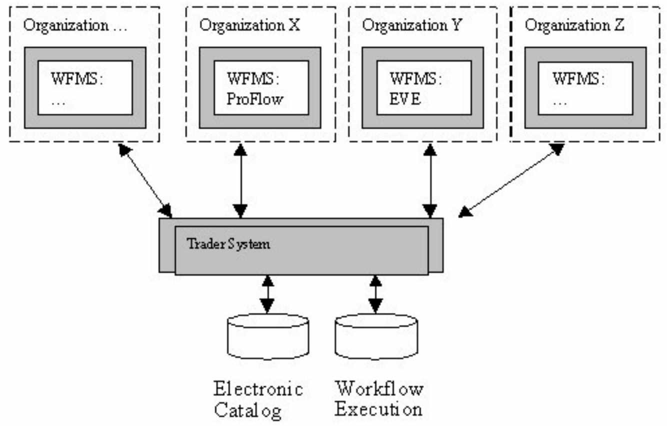

Fig. 2: Workflow system

ACE-flow is realized jointly by the group of Logistic, Economy and Management (LEM) at EPFL, by Database Technology Research Group at IFI, University of Zürich. Two software companies build the prototype by extending their own products and developing the required interfaces: R&ED for the electronic catalog and SER Systeme for the Workflow Management Systems.

Contact:
Claude.Stricker@epfl.ch,
Tel.: 021 693.5351

A Secure and Reliable Platform for Electronic Commerce

Allan Coignet
Operating Systems Lab. (LSE)

Introduction

Mercurio aims at the provision of a service creation environment for e-commerce services. This is motivated by the observation that pure WWW technology (as we see it at the moment) is not sufficient to realize a variety of services provided over the Internet. The main goal is to enable operators of e-commerce service centers (sometimes called electronic malls) to develop, deploy, operate, and manage (potentially complex) e-commerce services that are tailored to the business provided as an e-commerce service and the single vendor in a fast and cost-efficient way. The focus of the project is on the aspects of service security and reliability as well as on the provision of functionality to achieve liability, provability, and fair exchange for e-commerce interactions.

Technology

Service security, liability, provability, and fair exchange are mainly achieved through the use of cryptographic mechanisms and protocols. In order to support the fast acceptance of e-commerce, it is an explicit goal that the platform must not require any additional hardware at the buyer's side. All technical solutions shall work as much as possible with the current de-facto standard products, standards, and technologies. In order to support immediate acceptance, the new solutions shall evolve from accepted technologies rather than the development of insular new technologies. The scenario for which Mercurio is developed is characterized by WWW browsers as the access technology, CORBA as the core of the middleware, Java-applets as the download technology, and SSL as the cryptographic framework.

Key Results

Mercurio provides a development platform for the fast and cheap development of secure and reliable e-commerce services for the Internet as it is. It enforces provability using fair-exchange protocols relying on the SSL (Secure Socket Layer) protocol. This make possible to prove later on that a transaction has been executed between the two parties. The proofs are automatically generated by the protocol and enforce the fairness during the transaction.

The topology of the developed platform shows that the vendor's e-commerce services are hosted by its provider (for SME, because they don't want to care about the maintenance of their site), so the vendor interacts with the buyer through this intermediate host. This means that the vendor/buyer interaction can be through a simple internet connection, from home or work (Figure1).

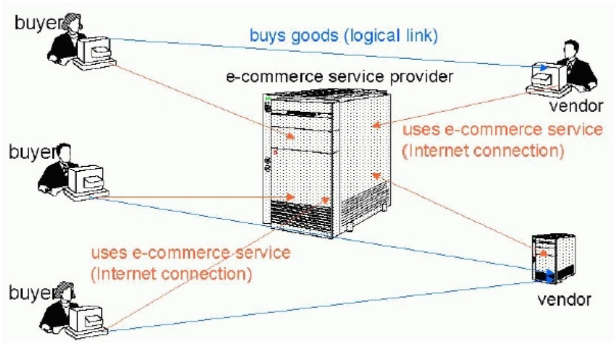

Fig. 1: Interaction

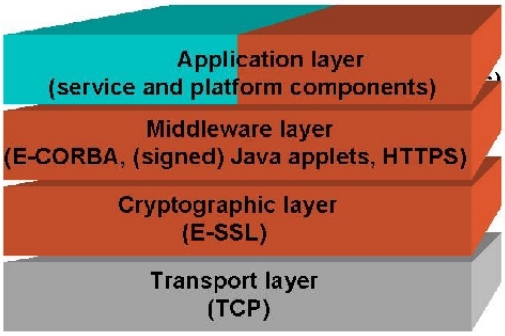

Fig. 2: Architecture

The environment for which we develop the platform is characterized by the assumption that the creation and operation of e-commerce services is a business in itself. An e-commerce service provider offers two interfaces for each service, one to buyer, and one to the vendor. The e-commerce service provider guarantees security as well as availability and acts as on-line TTP or retailer.

We have developed a suitable layered architecture for the platform, which takes into account the real-world constraints mentioned above (Figure 2).

The architecture provides new functionality at several layers. Control and management of the security functionality as well as the replication of services and objects is realized at the application layer. The middleware layer, the Distributed Processing Environment (DPE) below, which provides non-repudiation and (secure) multicast, consists mainly of an enhanced CORBA implementation (E-CORBA). As the secure transport layer, E-CORBA uses an enhanced SSL implementation (E-SSL). This E-SSL is the enhancement of SSL from an implemented protocol to an infrastructure supporting non-repudiation and cryptographic multicast.

Dissemination of the results

The Mercurio platform has been used to develop a translation business over the Internet in collaboration with an SME (CB-Service) and CSCS (Manno). The aim is to allow internet users to ask for the translation of a text. There are different phases during this process. An information phase where the buyer asks for pricing regarding the specificity of his text. Then the signature of the document that binds the buyer with the seller for the work that will be provided, for this non-repudiation is needed. Finally the delivery phase where the seller gives back the translated text to the buyer, this phase also requires non-repudiation. We might enter into the after sales phase if the buyer is not happy with the quality of the translated text.

Contact

Allan Coignet
(Allan.Coignet@epfl.ch)