[Home] [Current Edition] [Compendium] [Forum] [Web Archive]
[Email Archive] Guestbook] [Subscribe] [Advertising Rates]

The United Nations Secure Infrastructure for Electronic Commerce

By Carlos Moreira
Head
United Nations Trade Point Development Center UNTPDC
United Nations Conference for Trade and Development UNCTAD
http://www.unicc.org/untpdc/welcome.html
http://www.untpdc.org/untpdc/welcome.html Email: cmoreira@urgento.gse.rmit.edu.au

SEAL aims at providing an open and comprehensive approach to global secure electronic commerce over the GTPNet, Internet, public information networks and private IntraNets.

Moving from closed environments to interoperability through the SEAL Global Secure Chain concept.

The Secure Electronic Authentication Lab VRML Access

Why do Trade Points need a Secure Electronic Authenticated Link SEAL to perform Secure Electronic Trading operations. As we know, the world of Electronic Trading and Information Technology is constantly under development. We are constantly seeing new computerization processes, and new concepts of communication are continually emerging. Placing all this in a business environment, such tools are being seen as inevitable in today's world of Electronic Trading. However, it must be noted that Electronic Trading can only seriously help one's business and provide a proper competitive edge if it is looked into as part of a proper business re-engineering process. There is a global believe that network security is simply a technological issue related to software and servers, but in reality, it involves people and processes as well.

Businesses need to move securely now so as to ensure that the potential provided by Electronic Trading is maintained with regard to productivity, customer satisfaction and globalisation, and all with a sense towards international trade. A way to solve one business problem in todays fast running electronic world is by allowing companies around the world in setting their network security policy in order to assure that a security solution will meet their company's objectives effectively. The security policy must correlate and integrate with their current or planned information systems architectures. This process will, in turn, drive enterprise-wide policies, procedures, standards, and guidelines for security in the IT environment, both developmentally and operationally.

In a global scale the GTPNet is consider the best and only global architecture which could secure electronic commerce under the certification process of the United Nations umbrella. Trade Points are already certify centers on which UNCTAD provides the first level certification before they are considered operational. This certification is provided following pre-established and mutula agreed trade efficiency guideliness. The next step is to inteconnect this environment via a Secure Electronic Authenticated Link which provides the authorization and authentication of each individual node. The SEAL network security solution focus on five main areas and form a solid framework to implement a Secure Electronic Commerce network security policy.

- **Access Verification and Control.** Information is verified, controlled and access is granted by a predetermined security policy.
- **Privacy by Secure Links.** Secure communication means that other people on the network cannot see the contents of the message being sent.
- **Authorization/Authentication.** Granting rights for users to perform actions that would otherwise be disallowed and making sure that communication is conducted with the intended user.
- **Integrity.** The property of data or information resources have not been improperly altered or destroyed.
- **Management.** Consistent framework for managing the security products and procedures.

How to Secure the GTPNet

Most Trade Points and related Trade Facilitation bodies (Customs, Transport, Banks, Insurance, etc) together with Trade Promotion Organizations local and and state governments have complicated data communications networks that have evolved over several generations of computing systems. The networks routinely run many different protocols through Wide Area Networks (WANs) and Local Area Networks (LANs). The WANs are usually based on a variety of different services over costly leased lines to maintain a high degree of availability, security and data integrity. In addition, most companies have Internet connectivity and routinely run World Wide Web (WWW) sites that are loosely coupled, if at all, to their corporate networks. The reasons for the latter are many and frequently include security and data integrity issues. This adds to the complexity of managing the Web site and complicates remote site management for most companies.

The first objective of the SEAL architecture is to provide solutions for creating secure, virtual private networks over public lines such as the Internet and via Secure Intranet Links and to evaluate the problems Trade Points face when trying to build Virtual Private Networks (VPNs) over public media and assist them on how these can be overcome.

Research and Development project *- Participating agencies*

1. United Nations Trade Point Development Centre UNTPDC
2. Silicom Graphics
3. Cray Research
4. Telstra
5. MCI
6. Informix
7. Logica
8. Netscape
9. Cisco
10. SUN Microsystems
11. Oracle
12. Gateway 2000

Participating Universities

1. Royal Melbourne Institue of Technology, Melbourne, Australia
2. Computer & Network Services, University of the Witwatersrand, Johannesburg, South Africa
3. Centre of Computing Services and Telecommunications (CCST) of the Hong Kong University of Science and Technology, Hong Kong
4. Sternberg Astronomical Institute Moscow University, Moscow, Russia
5. Macquarie University , Sydney, Australia
6. Faculty of Math and Physics Charles University, Prague, Czech Republic
7. SunSITE Poland by ICM , in Warsaw, Poland.
8. Interuniversity Consortium of the Northeastern Italy for Automatic Computing CINECA, Italy
9. University of Minnesota, Office of Information Technologies, Minnesota, USA
10. Science University of Tokyo, Japan

The above universities are hosting the UNTPDC and SEAL Sites, you can access the Mirror Sites by adding /UNTPDC/ at the end of their URL.

Basic Principles

- The secure level of the transaction chain depends on the weakest component

Total security is only possible via dedicated secure links

- To provide domestic and international data communication, processing services and interface software to Trade Points and related organizations around the world.
- The security chain must gurantee global transaction security, from the smart card insertion in the SEAL terminal to its processing at the SEAL server level.
- The system adaptability must preserve the integrity of the security chain.
- The security chain gurantees security and interoperability

Main Principles

1. To guarantee each transaction authenticity
2. To guarantee each transaction recovery
3. The security level of a system is that of its weakest link

The links of the SEAL Global Secure Chain

- Confidentiality
- Aunthentication
- Signature
- Integrity
- Registering
- Validation
- Transfer

Research and Development Projects

1. Global Trade Point Network: United Nations
2. Electronic Trading Opportunity ETO System
3. Secure ETO Smart Card - Secure ETO R&D: digital signatures and a tentative proposal for a public key authentication framework - Innovatron
4. Validation & Authentification R&D (Electronic Notary DOCLOC)
5. IT Warehouse - Mirror Sites
6. Chinese Government: The Secure China Link : China Trade Point Development Centre, Ministry of Technical and Economic Cooperation MOFTEC
7. United Nations Economic Commission for Asia and the Pacific ESCAP. International Trade Centre, ITC - UNCTAD/WTO.
8. Universities,
9. SUNSItes.
10. Internet Site Incubator : Trade Points, ETO Associates
11. Internet Servers benchmarking: SUN, IBM, SGI, Digital
12. Secure Intelligent SITE R&D: ANZ Bank, Schoellers Bank.
13. Secure Electronic Transaction (SET): Innovatron, VISA, Mastercard
14. Digital Content Generation (DCG) - Silicom Graphics - Sun - Illustra -DISC
15. Internet Infrastructuring & Interconnectivity: Telstra, GEIS, IBM, BT, SITA,MCI
16. Software Development: Sun, IBM, GEIS, Oracle, Informix, SGI
17. Intelligent Terminals & Kiosk - Kompass International
18. Early Warning Interactive System (GIFT)

System Description

SEAL aims at providing an open and comprehensive approach to secure electronic commerce over the Internet, public information networks and private IntraNets.

It combines development of software applications for secure electronic commerce, integration into smart card and kiosk technology and development of global infrastructures for secure links using private Intranets.

The current phase of SEAL addresses a coherent security model and a generic, open security architecture for the electronic marketplace.

This architecture is independent of specific hardware, software, or network architectures. The most fundamental electronic commerce services, such as secure offering, order, payment and information delivery, are also integrated in this first phase.

Background

Networked information systems are experiencing a tremendous growth in terms of users and traffic as well as publicity. The dominating application, the Internet-based World Wide Web (WWW), is still dominated by free-of-charge information systems, but this is expected to change dramatically in the near future.

WWW will be used for all sorts of electronic commerce and trade. The same development can be expected for the IBC networks and "Information Highways." This is particularly visible with the introduction of the Electronic Trading Opportunity ETO system developed by the UNTPDC and opeartional on the Internet since 1993. ETO is the first full EDIFACT trading mechanism operating on Internet and IntraNet environments.

There are numerous projects and services that aim at electronic commerce via Internet. Many are US-based. Most of them aim at closed solutions and concentrate on electronic payments only.

None of them aims at the complete electronic marketplace. None of them provides a coherent model or architecture. Moreover, not even the non-technical and security requirements on such an electronic marketplace are understood completely.

Main Objectives

- a detailed description of commercial, legal, social, and technical requirements and options for an electronic marketplace;
- a coherent model and a generic, open architecture of an electronic marketplace, independent of specific hardware, software, and network architectures;
- specifications, designs, prototype implementations and evaluations for services enabling electronic commerce;
- information to the technical, scientific and general public, standardisation, and other ACTS projects.

Technical Approach

SEAL is developed by an interdisciplinary consortium, combining experts from hardware and software companies, telecommunications groups, financeial institutions, IT providers, universities and EDI.

The non-technical requirements part of SEAL is based on the existing expertise within the consortium, as well as on expert surveys performed in different countries with Trade Points.

The development and trial part is organised in three phases, each phase corresponding to an enhanced set of services and trials.

The current phase concentrates on two topics:

1. The development of a framework and architecture for secure electronic commerce.
2. Within this framework and architecture, the provision of the most fundamental electronic commerce services, namely, offering, ordering, payment, and delivery for information services.

The following phases will concentrate on extending the architecture and developing more advanced services, e.g.:

1. Notary Services. For instance, "fair exchanges" will facilitate digital analog of registered mail, contract signing, purchases, etc., where no party can be dishonest with the others by not fulfilling their part of the commitment.
2. Attribute certificates or credentials with specific privacy properties.
3. Multi-media specific security services like protection of intellectual property rights.

SEAL uses and integrates existing architectures, tools, and services where appropriate. Initially, security toolkits developed by Cryptomathic and GMD will support the necessary authentication and certification

functions. Payment toolkits will support cash-like (ecash) and credit-card (iKP/SET) payments.

Development is driven by market requirements and the state of the art in security and on-line information services. Requirements for multi-party security and the protection of the users' privacy receive prime attention.

Key Issues, Expected Results

SEAL develops and will publish a generic architecture for secure electronic commerce over the Internet.

This will include a design and a Java-based prototype implementation of a security toolkit for electronic commerce.

The toolkit offers all necessary security services, based on the concept of "service managers" that provide a generic service interface to "service modules" that actually provide the required service. New "modules",

corresponding to specific service implementations and products, can easily be integrated.

Although the initial version of the toolkit will be based on existing modules only (like the payment modules "ecash" and "iKP/SET"), new protocols and modules will be developed and integrated where necessary for the subsequent phases.

This concept allows for specific configurations (e.g., some modules might not be required by some users, or might not be allowed to be used in some countries) and ensures interoperability of different modules to the extend possible.