Performance Report - November 1998

SEAL The United Nations Secure Infrastructure for Electronic Commerce and Trusted Transactions

By Carlos Moreira
Email: cmoreira@harmonic.gse.rmit.edu.au
Web Site: http://www.unicc.org/untpdc/welcome.html

Head UNTPDC, United Trade Point Development Centre, World Coordinator SEAL Insfrastructure

The Secure Electronic Authenticated Link Infrastructure (SEAL-I) is the basis for the deployment of a trusted geo-political secure infrastructure for the multi-purpose, global electronic exchange of information and value. The SEAL-I will provide a secure framework for cross-certification and interchange between national certification authorities. It will be based on a geo-political chain of trust, in which the United Nations, or a UN-endorsed body, will act as a Policy Approving Authority (PAA) which will coordinate policies and ensure the integrity of the Aroot@ certification process at a supranational level.

The SEAL-I will act as a global intranet/extranet connecting Certification Authorities via Secure Electronic Authenticated Links or SEALINKs. These SEAL Certification Authorities and SEALINKs are national or state-level nodes interconnected through an international hierarchy of trust that provides security for electronic transactions by administering digital signatures. The SEAL-I provides a secure link between traditional hierarchies of trust that enables electronic international trade and transactions while respecting existing geopolitical sovereignties. Furthermore, the SEAL-I can generate revenue streams through a variety of activities at several levels.

The SEAL-I will be regulated either by the UN or by an international body to be defined by governmental and private sector participants and endorsed by the UN. This body will grant and revoke the Secure Electronic Authenticated Link "SEALINK" status to national Certification Authorities on the basis of established and recognised legal criteria at SEAL Aroot@. The SEAL-I will be made available to all interested nations. It will comply with and will be certified to international standards for security, telecommunications and audit, as well as standard operating policies and procedures.

The SEAL Certification Authority (SEAL-CA) and the connections via the Secure Electronic Authenticated Link (SEALINK)

The SEAL-I or SEAL Public Key Infrastructure (PKI) will be represented at national level by the SEAL Certification Authority (SEAL-CA) which will be the higher certification level in each country. Each SEAL-CA will be connected to the UN Aroot@ via a Secure Electronic Authenticated Link (SEALINK) or Virtual Private Networks (VPN). SEALINKs therefore, will not be legal entities or organizations but just a secure link between the SEAL-CA and the SEAL Aroot@. The SEAL-CA should ideally be hosted by national research and development organizations or, alternatively, by non-profit SEAL-CA operating organizations.

The SEAL-I can also use a Virtual Private Network (VPN) to connect the SEAL-CA to the SEAL-RAs. This environment will be especially useful in developed countries where VPN are available. In developing countries dedicated links between the SEALINK and the SEAL-CA and UN Aroot@ will be required.

The SEAL-CA will be at the centre of the operation of the national network and will be country-specific. They will provide a number of services that enable electronic trading, including gateway and switching services into communities of interest. The SEAL-CA provides the certification to the Organizational Certification Authorities (OCAs), and encryption functions to the Registration Authorities (RAs). The Registration Authorities can be located at the "entry level" of the infrastructure where users will traditionally register. Examples of SEAL-RAs could be Trade Points, Chambers of Commerce, Banks, Post Offices, Tourism Boards etc.

The SEAL-CA is also a part of the country-specific PKI. By establishing a trusted hierarchy of government and regional business advisory bodies, the SEAL-CA helps eliminate concerns about security for online transactions and business. It assists the national PKI to validate its certification policy with other countries as they are considered policy certification authorities via its link to SEAL-I root and the UN.

The Global Aroot@ for all SEAL-I Certification authorities will be placed under the control of the UN or of a body endorsed by the UN with governmental and private-sector participation, which will provide the cross-certification environment for a secure and protected electronic SEAL-I between UN member countries. The coordination of electronic commerce policies and cross-certification efforts in countries interconnected by the SEAL-I will eventually lead to the international recognition of digital signatures for cross-border transactions.

The SEAL-CA relate to the UN as the Global Aroot@ and conform to the standards established by SEAL-I root. These standards define how to secure the SEAL-I, how to control access to critical applications, procedures to authenticate parties involved in network interactions, how to enable encryption for transmission of sensitive data, how to use digital certificates to control electronic access, etc.

The SEAL-CA of each country will be owned by a national association established under national regulations and with the endorsement of the competent ministry or national PKI. An official request to the United Nations or appointed body will be required if there is a need to use multiple certification or cross certification with other countries using the SEAL-I. The national request from the Ministry or official organization will appoint the location at which the SEAL-CA will reside in the country, the SEAL-CA will then be authorized to establish SEAL-RAs and if necessary, to establish a SEALINK environment in the country. In many countries, the SEAL-CA will occupy the same level as the PKI organization.

The SEAL-I incorporates links between Transaction Points/Trade Points, industry and government functions and the GTPNet. At a national level, the SEAL-I represents a sovereign nation's secure electronic gateway to the rest of the world. It is also the means by which that nation certifies entities within its jurisdiction as valid entities (including their constituents) to perform secure international transactions.

The SEAL-I acting as a national PKI performs the following functions: Delegates trust, and administers and audits certification within its domain; conforms to international standards, and ensures the compliance of subsidiary entities with regulatory and statutory requirements; issues smart cards and provides key management services; incubates SEAL-CAs, SEAL-RAs, Transaction Points/Trade Points; and generates revenue for itself by a toll on all value transactions passing through it.

Technical dimensions

The SEAL-I is a series of networked file servers that perform a variety of specified bridging functions, both vertically and horizontally. The SEAL-I interconnects Transaction Points/Trade Points with industry and government functionality in and between countries or regions (depending on the defined catchment area). The SEAL-I constitutes a Virtual Private Network (VPN) or secure international extranet of entities working in areas such as international trade, telehealth and distance education.

Physically, the SEAL-I hub resides in a secure site in each nation or duly designated geopolitical entity. The Global Aroot@ must be protected by an accredited bunker that is independently rated to ITSEC E3 to meet Certification Practice Statement requirements, including protection of the cryptographic material it accommodates. In this way the

bunker will provide the high assurance required for long-lasting, secure global trading infrastructure. The Global Bunker will need to meet the E3 high-security assurance level according to the IT Security Evaluation and Certification (ITSEC) scheme. More information on the ITSEC scheme is available at http://www.itsec.gov.uk/docs/formal.htm#UKSP01

A physical bunker is required because it is impossible to determine electronically if the root key has been compromised. A physical means is necessary to ascertain if a break-in has occurred, and a facility must be able to provide an hour=s resistance to be safe. Perimeter alarms will detect the first attempts to force entry, alerting nearby security guards; other >rings= of security will be provided by high-security locks, walls and a safe. Besides the bunker, high assurance is provided by strong cryptography and rigorous policies and procedures. All three elements must be maintained at a high security standard, since the weakest link can bring the SEAL-I down.

Functional dimensions

Administratively, the SEAL-I acts as the interface between the UN Global root, SEAL-I root, and the SEAL-CA and SEAL-RA, or equivalent Transaction Points/Trade Points and other communities of interest that link to the global SEAL-I. Empowered by SEAL-I root and the international acceptance of the SEAL-I root Certification Policy, the SEAL-I in turn, confers authentication and power of certification on the entities at the next level below it in the hierarchy of trust. Transaction Points/Trade Points and other recognised entities can thus communicate directly with one another at any level of the global infrastructure. The SEAL-I prevents unwanted intrusions by enterprises that have not been accredited by a certifying organisation such as a Transaction Point/Trade Point. When fully operational, the SEAL-I will allow enterprises throughout the world to obtain information about one another, secure in the knowledge that their counterparts have been certified by a Transaction Point/Trade Point or other authenticating organisation. The SEAL-I will also facilitate links to trade-related services allowing secure electronic access to banking, insurance and transport companies.

Virtual Dimensions

As a secure international extranet the SEAL-I performs the following functions: Integrates diverse communities of interest; transparently interconnects the WWW (TCP/IP), X25, X28 and other existing international networks; hosts or incubates SEAL-CA, SEAL-RA and Transaction Points/Trade Points using the SEAL Centres Incubators and SETO Incubators; provides a secure conduit for all value transactions flowing through the SEAL-I and related communities of interest such as the GTPNet and G77 Network, and therefore a means for national governments to monitor electronic trading within their jurisdictions for purposes of taxation, foreign exchange control and so forth; and ensures that standards are maintained and procedures followed in transacting electronic trading.

National SEAL-I and their correspondent SEAL Certification Authorities and SEAL Centres will manage the following functions regarding the infrastructure within their jurisdictions:

- Policy: create and maintain guidelines; audit policy compliance.
- IT operations: transmit/receive transactions; audit transactions.
- Risk: manage fraud; underwrite risk.
- Stakeholder certification: create and maintain certificates; create and maintain smart cards.
- Government interfaces: legal; tax; treasury; foreign affairs and trade; securities.
- Finances: accounting, billing; and provision of commercial consulting services relating to Transaction Point/Trade Point development.

The following assumptions about the SEAL-I functionality regarding value transactions have been made in developing this operating model:

- The national SEAL-I and correspondent SEAL Certification Authority must audit every value transaction conducted by a Transaction Point/Trade Point in its geopolitical jurisdiction (usually national) with regard to (1) generation of revenue by a per-transaction charge and (2) collection of information about transactions to satisfy government requirements of the country or geopolitical entity in which the Transaction Points/Trade Points operate (for example, tax, legal).

- Given that the SEAL-I provides transaction integrity, authentication and non-repudiation, encryption is mandatory for all value transactions and at the user=s discretion for non-value transactions.

- The national SEAL-I will provide a delivery guarantee service by use of transaction tracking, recovery and roll-back facilities for all value transactions as a matter of course; and as an optional charged service at the user's discretion for non-value transactions.

- The national SEAL-I will support existing transaction processes, but will not be restricted to current payment models as these may constrain innovation.