Appendix I Security Framework of ETS

1 Security Framework

Security is the key to ETS. The ETS makes use of a combination of security technologies and concepts to construct the framework of the ETS security architecture.

Security can be categorized into 5 layers:

Layer	Description
Operation	Security measures can be deployed successfully only with proper operational policy and procedures.
Application	It is the layer for the ETS business process, in which a balanced solution between usability and security control should be made.
System	It is the most frequent access layer from operators and administrators.
Network	It is the first layer of defense against security threats of hackers originated from the Internet.
Physical	It is the first layer of defense against security threats from internal access.

As Operation and Physical security are related to the operation procedure of HK Electric's system operation, this proposal will focus on the Application, System and Network security aspects of the system.

1.1 Application Security

The following diagram depicts the application security framework of ETS.

The system makes use of the following technologies in constructing the application security framework:

	Suppliers	ETS
Privacy	**Strong File Encryption** ← **SSL** →	**Strong File Encryption**
Authentication	**User Account** **Digital Certificate (iCert)** **Digital Signature**	**User Account** **Optional: Fingerprint Identification**
Integrity	**Checksum** **(Hash Value)**	**Checksum** **(Hash Value)**
Submission Record	**Encrypted File** **Acknowledge Receipt with Time Stamping and Hash Value**	**Electronic Tender Box** **(Encrypted until closing time and decrypted by Procurer private key)**

Application Security Framework

- SSL

Secure Socket Layer (SSL) technology is used in ensuring the confidentiality of the data transmitted over the HTTP protocol.

- Login ID/Password

Login/Password is used in controlling the access to the system and to help ensure the identity of the logged in user. While this is not sufficient for authentication, it is the basic requirement.

- Digital Signature (PKI)

To authenticate the suppliers who submit tender offers, the system makes use of the industry standard Public Key Infrastructure (PKI). Each supplier is to apply for an iCert (issued by sub-CA in HK Post) during initial registration. During tender offer submission, the system will make use of this iCert to generate a digital signature which will be attached to the submitted tender offer. This digital signature is analogous to the supplier's signature on paper.

- Hashing (MD5)

Hashing is used in ensuring the integrity of the submitted tender offers. Like the digital signature, a Hash value of the submitted tender offer will be generated during tender offer submission. This hash total can then serve as a kind of checksum at the ETS Web/Application server.

- Asymmetric Encryption (RSA)

Asymmetric encryption based on RSA algorithm is used for the encryption of the tender offer documents. The encryption key used is the public key of the procurer. In this way, only the procurer having its private key can decrypt the content of the tender offer. By controlling the access of this private key, it is used as the tender box opening key. In fact, the Tender Box Opening Program makes use of this key to conduct the tender box opening procedure. To ensure the security of the system, it is advisable that the public key for asymmetric encryption be changed annually to avoid being tempered.

- Fingerprint Identification

This is an optional feature for authenticating the identity of the tender box opening personnel of the procurer. This can be implemented in the PC dedicated to tender box opening. Whoever attempting to login the PC will have his/her fingerprint verified first.

1.2 System Security

System security consists of a) Server access and b) Database access security.

Server Security

Server access security is controlled by the Windows NT server access control which is user ID/password based. Optionally, fingerprint identification machines can be added to provide extra level of security.

STS does not require the creation of a specific user account in the NT server where STS is installed. Therefore, the NT server containing STS can have only one account "Administrator". This simplifies the

administration and avoid security exposure due to the presence of application specific NT accounts in the server.

To further enhance the server access security, it is advisable that a fingerprint identification device be installed in the server. This device requires the user to have his/her fingerprint verified before he/she is granted access to the system. Even if the system passwords are leaked out, the device will not allow unauthorized persons to log in. Moreover, it is also advisable that the system passwords be changed periodically. The recommended frequency of change is once every three months.

Database Security

Database security is controlled by the built-in security mechanism of SQL Server, which is also user ID/password based. In the database, access authority is segregated into different accounts based on their roles.

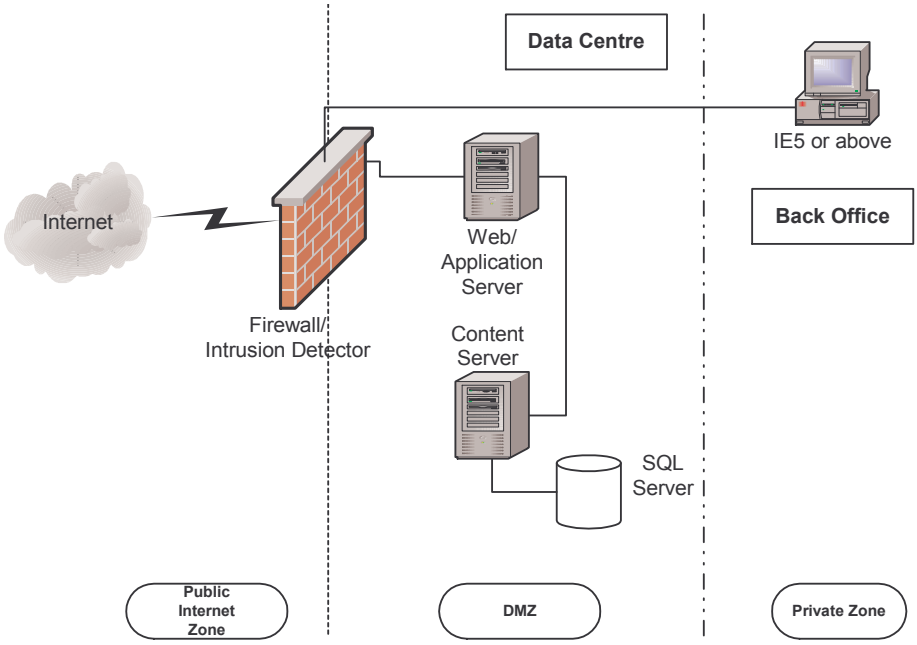
STS does not make use the SA (System Administrator) account of the SQL Server. Instead, it makes use of a less powerful "Data Owner" account to access the data in the SQL Server. The advantage of this approach is that the SA password will not be required for the day-to-day system operation. The SA password can be kept by an independent party to ensure security to the database. For example, the SA password can be split into two halves, each kept by a Senior Procurement Officer who does not have physical access to the system console.

To ensure the database security, it is advisable that the SA password and the Data Owner password be regularly changed to avoid exposure. The recommended frequency of change is once every three months.

1.3 Network Security

The design for the network secure infrastructure of the system composes of 3 major zones, they are:

- Public Internet Zone
- Demilitarized Zone – For controlled access
- Private Zone – For Internal access only



(1) Public Internet Zone

The Public Internet Zone refers to the Internet area, where the Public Internet Users access to the ETS.

(2) Demilitarized Zone

This is an area that contains servers where users from the Internet can directly access. It contains the web/application server for serving the HTTP requests from users. Security control is particularly important in this zone as it is directly interfaced to the Public Internet Zone.

(3) Private Zone

This area contains servers where no direct access is allowed from the public Internet. Most of the services provided here are accessible by the web servers only. This area also provides services for internal users to access the ETS in a controlled and secured way.

Demilitarized Zone's (High Risk Zone) Infrastructure

This section describes how the proposed secure infrastructure addresses the network security requirement.

(1) First Tier Security with Intrusion Detection Solution

In order for the whole firewall solution to be completed, we will deploy the intrusion detection system placed at the public Internet zone. Since firewall is not natively designed for intrusion detection, it cans only handles four types of intrusion, which are far from enough.

An Intrusion Detection System (IDS) captures network traffic and interprets attacking patterns based on the database. If IDS find any abnormal network activity on the network, it does not only block the connection to prevent further attack but also informs system administrator in form of alerts.

With ISS RealSecure Network Sensor deployed before DMZ, you can monitor network packets and look for signatures that could indicate an attack against your network. On the other hand, the RealSecure Workgroup Manager, a monitor console, can be used as the central management point for the network sensor.

Another consideration is the upgrade path. With ISS RealSecure version, it continues to enhance its family of products, with independently licensed modules that can be purchased and deployed as needed. The components of the RealSecure family are:

RealSecure Network Sensor

This is the RealSecure Sensor that looks at all the traffic on a single segment. RealSecure Sensor runs on dedicated workstations to provide network intrusion detection and response. Each RealSecure Sensor watches the packet traffic traveling over a specific network segment for attack signatures – telltale evidence that an attempted intrusion is taking place. When RealSecure Sensor detects unauthorized activity, it responds immediately by terminating the connection, sending email or pager alerts, recording the session, reconfiguring select firewalls or taking other, user-definable, actions. In addition, RealSecure Sensor passes an alarm to the RealSecure Manager or a third-party management console for administrative follow-up and review

RealSecure Workgroup Manager

The console provides the capability to manage network engines and system agents from the same user interface. Both types of detector use the same alarm formats, report to the same database, and use many of the same reports. This module is bundled at no charge with the network engine and the system agent.

(2) Second Tier Security Solution with Firewall

A firewall is placed between the un-trusted network, (i.e. the Public Internet Zone and the Demilitarized Zone) and the trusted network (i.e. the Private Zone). The firewall is hosted on a single computer that controls all traffic traveling between two networks and examines content as it passes through the firewall. This examination is on inbound, outbound, and/or bi-directional traffic. Examination of the traffic content is based on a set of rules. Firewalls allow an administrator to create rules that specify the actions to be taken by the firewall on every packet it receives. These actions can include:

User Authentication

Access Control - Accepting the packet and forwarding it to the appropriate destination
Network Address Translation.

Content Security

In this area, CheckPoint Firewall-1 is proposed for its recognized technologies on the IT market. Checkpoint Firewall-1 enables enterprises to define and enforce a single, comprehensive Security Policy that protects all network resources. Its patented Stateful Inspection Technology and the Open Platform for Security (OPSEC™) deliver a highly scalable solution that is able to integrate and centrally manage all aspects of network security, including third-party security applications, services and platforms. A family of add-on modules extends FireWall-1's capabilities to all levels of security and management.

Besides, CheckPoint Firewall-1 is much more than just a firewall. It interoperates with multiple applications and supports a variety of functional modules to provide the industry's only solution for Secure Virtual Networking, including:

CheckPoint Firewall-1

The CheckPoint Firewall-1 provides carrier-class performance by offering the utmost in serviceability and performance. Besides, an optional StoneBeat solution can allow extra firewall node to be added to the cluster unit online and it can scale up to maximum 16 nodes, to provide load-balancing function, which delivered a fault tolerant security solution by having a recovery clustering node. Each of the firewall nodes should have the Ethernet interfaces as follows:

Interface 1	Gateway to the Internet for browsing and transaction
Interface 2	Connected to the DMZ Web servers farm
Interface 3	Connected to the Private Zone

Anti-virus and Anti-vandal

To protect the system from virus problems, an anti-virus & anti-vandal gateway software, NAI VirusScan Security Suite is proposed in this proposal. NAIVirusScan Security Suite is a powerful content inspection and security policy enforcement product housed at the Web/Application Server. It is designed to provide protection against malicious content such as viruses, vandals (malicious Java and ActiveX), data exposure, and other inappropriate content.