msctrustgate.com
TRUSTED INTERNET SPECIALISTS

White Paper

IT Security for Digital Signatures

msc trustgate.com (478231-X)
(*CA License No.: LK0022000*)

G / F, Belatuk Block, Cyberview Garden,
63000 Cyberjaya, Selangor Darul Ehsan,
Malaysia.

Tel: + 603 8318 1800
Fax: + 603 8319 1800
http:// www.msctrustgate.com

VeriSign Trust Network℠

Introduction

The purpose of this document is to outline the security strategy for the Smart Schools project. IT security will be crucial to its ability to provide secure and well-managed services, and to ensure that students are provided with the appropriate content.

The Smart Schools network is a national network, operating across private and public communications channel. When fully operational, it will support hundreds of thousands of students, teachers, administrators and parents. The sheer size of the user population will mean that the users will unfortunately include curious, careless, or malicious users who may not share the security goals and values of the network operators.

The network contains a mix of information assets, some of which are highly sensitive, and others that will be critical to the day-to-day activities of the education system. Each element of the network must be protected from attack or inappropriate access from outside the network, and from within its boundaries. Further, the network is connected to the Internet with its rich variety of content, both appropriate and inappropriate for students.

The security requirements of Smart Schools network can be categorized into three groups;

- Requirements to protect the network from **outside attack**, including attacks from the Internet, and attacks from other users of the national network.
- Requirements to apply appropriate access **control within the network**, and to ensure the network continues to operate free from the effects of malicious code.
- Requirements to **control** the **content** that is made available to students and staff.

These are further described as follows:

Outside Attack

Outside attacks include unauthorized attempts to enter the network, to deny service to the network's authorized users or to inflict damage on the network's users and systems with malicious code. The network must support remote access to its resources to both its own users, and to contractors or support personnel who will manage and maintain the network. The network must therefore be able to distinguish and provide secure access to legitimate external users.

Internal Security

Insider threats include unauthorized attempts to view, modify, or deny rightful users access to resources. Students viewing tests, modifying electronic versions of report cards, or accessing confidential human resource information concerning teachers are examples of potential problems here. As well, the administrative systems in the network may be used fro e-commerce or procurement purposes and these could be misused in a variety of ways.

Control of Content

This includes controlling of content that is retrieved from outside the network, ensuring content that is developed within the network is appropriate and well-protected.

A matter of trust

Security's old paradigm of control and prevention where access was the exception, not the rule, does not suit the open, connected environment. In an open environment the new security model emphasizes trust – enabling parents, educators and students to communicate and participate more openly and efficiently, supporting learning without fear of vandalism, loss of private or confidential information, spoofing and other forms of online security risks.

Students and parents need to be able to trust those who dispense information and advice online. The field is open for unqualified, non-trusted parties to dispense information, advice or counseling to students seeking them. There will be those who claim to be qualified and those who would claim to be somebody whom they are not. If trust is to be built into smart schools processes, privacy confidentiality and integrity of its content must be at its core.

PKI (Public Key Infrastructure) with its digital certificates is been regarded as today's de facto on-line security standard and provides the highest level of trust solution through its basic functionality for:

- Ensuring that parties, like students, teachers, administrators and parents, can be certain of each other's identity online.
- Privacy and confidentiality of information and messages.
- Integrity and non-repudiation of messages and transactions.
- Overcoming the inherent weaknesses of id/password access control.

Security Culture

Secure systems are the result of a security culture. This means that security must be a consideration in all major design decisions during the development of the network and the applications, and that security activities continue through out the life of the network. Just as design engineers cannot build a successful system without a target in mind, the security of the network cannot be designed without a high level Security Policy, which defines the will of the organization to protect its assets. This policy is the basis of all security activities through out the life of the network and systems. It identifies who is responsible for security and the processes that the organization follows to manage its risks.

In every large project, responsibility for security must be ultimate assigned to a single person. This person must have the support of the organization's senior managers to oversee the security design, approve it, and accept any remaining

risk on behalf of the organization. This security watchdog role is crucial during the system's development, and through out its operational life.

Security Technology: A Multi-layered Approach

Secure networks include layers of technology, which collectively reduce the risk to acceptable levels. The technology approach would be as follows:

- Dividing the network into security domains that have similar security postures (i.e. public areas, administrative segments, and dedicated segments (or virtual segments) for communities of interests).
- Separating the domains with perimeter security as appropriate. Perimeter security would be applied using a combination of firewalls, routers and witches.
- Connecting users across “non-trusted” networks using VPN technology
- Monitoring key interfaces using intrusion detection technology.
- Screening content at perimeters using content-aware filtering devices (blacklists and white lists).
- Automatically examining Web, email, FTP, and other content from viruses and inappropriate material.
- Integration of a Public Key Infrastructure (PKI) is crucial
- Installing access control and logging mechanisms on high risks systems
- Security-hardening critical servers
- Penetration testing security-critical systems.

Security operations

Technology alone will not ensure the security of this network. Security is a process. Just as network management is crucial to the ongoing success of the network, security management will also play a crucial role.

A senior security architect will oversee the security development of the network, and a security officer will be responsible for the security of the network during operation.

Security management activities will include:

- The management of users and accounts.
- The management of privileges and access, including firewalls.
- Content management.
- Review of security audit trails and logs.
- Response to security alarms and events (incident response).

Other factors that will be important to the ongoing security of the network include:

- Training and security screening of staff.
- Configuration management of security critical devices.
- Business resumption planning in the event of natural or security related outages.
- Ongoing operational security audits
- Ongoing technical audits.

Summary of processes

To ensure that all of the above occurs, a methodical approach is required. The steps in this approach are as follows:

- Develop a Security Policy for Smart Schools.
- Develop “Statement of Sensitivity” to determine the sensitivity of the network’s information and tangible assets to loss of confidentiality, integrity, and availability.

- Conduct a Threat and Risk Assessment to determine where the most likely attacks are, and the relative risks for these attacks.

Based on this, develop a prioritized set of risks.

- Develop security requirements.
- Implement the requirements in the design.
- Conduct a pre-implementation review to determine if the security requirements were achieved, and the security policy has been respected.
- Develop security operating procedures for the network.
- Hire and train security staff to operate the network.
- Engage third-party auditors to review the security practices and technology of the network on a regular basis.
- Engage a third-party trust solution to authenticate thus authorize access to the network and allow the user to digitally sign for the transaction to ensure integrity and non-repudiation offering the smart school network the highest form of trust.

Conclusion

The preceding discussion shows that a combined technical and procedural effort is required to secure and maintain the security of Smart Schools network. The design and operations of the network should follow industry-wide best practices to provide the highest level of security at a reasonable cost. This will guarantee the network functions as it was intended and provides maximum benefit to its user community.