The ScholarChip Platform
The Latest Web-Centric Technologies
Enterprise-Wide K-12 Smart Card Solutions

Platform Security

A ScholarChip White Paper
Platform Overview
ScholarChip™ Card LLC proposes its platform as an enterprise-wide solution for K-12 school districts. The ScholarChip™ Platform is built from the ground up to provide an integrated application for digital identity, attendance, hall/campus monitoring, truancy reduction, POS, security access and other mission critical functions. While the platform is frequently identified with the smart card identity token available to all students and staff, the application provides significantly more functionality. The implementation adheres to the latest web-centric technologies and provides a lightweight, easy to maintain suite of hardware and software tools to assist schools in securing their campuses and protecting the privacy of their students.

Important features of the platform are:

- Server-centric administrative security applications, identity management, as well as card issuance and control, thereby reducing both the hardware and network footprint.
- Three tiers of application and hardware, providing flexibility and reduced maintenance. Tier I consists of a cluster of servers and applications resident in the ScholarChip data center that orchestrate the entire process. Tier II consists of special purpose appliances or handheld devices resident at the school campus to provide a variety of applications. Tier III is the smart card hardware ID token issued to all members of the school community to provide the authentication necessary for accurate application access and distributed secure student records.
- A web-based application model requiring no installation of client software or special servers at the school campus or ongoing maintenance of such software or servers.
- A fully relational backend (Oracle®) for high performance and redundancy to ensure constant uptime and data security. The relational database allows for transparent redundancy using dual inserts and snapshot replication of all data tables.
- Remote and highly automated monitoring of the entire system at the ScholarChip data center to eliminate time consuming tasks normally assigned to the district’s IT staff.
- Open standards software to allow a district to leverage its investment well into the future.
- Support for Web standards such as XML over HTTP (SOAP) and SIF for easy integration with any future enhancements to the existing student management system.
- Extensive pre-built reporting tools (Crystal Enterprise) and custom reports, as well as exports for easy access to attendance data and OLAP integration into data warehouses.
- Easy import/export and integration with all Student Information Systems.
Platform Security
A. Student Data Security
ScholarChip considers student data security to be one of the highest objectives in designing and maintaining our application. We strive for “end-to-end” student data security to ensure the most secure environment, which translates into the following features:

- PGP encryption of all export and import files to guarantee protection of student data.
- Transmission via Secure FTP (SSL FTP) of all import and export files.
- The Management Site is a Secure Socket Layer (SSL) web site with certificates issued from GeoTrust.
- Attendance devices communicate with Tier I via HTTPS, with each Attendance Kiosk having a unique certificate.
- Secure site for classroom attendance application.
- Attendance Kiosks (and any equipment within reach of students or in public places) do not require keyboards, pointing devices, CD-ROM, Floppy drives and other similar devices thereby eliminating any security breaches through loading of files or applications.
- All Tier I acceptance of transaction requests and data is IP-contingent, thus reducing the possibility of corruption from outside sources.
- VPN access to the district and the ScholarChip data center is used to ensure user authentication.

B. Application and Network Level Security
The high degree of network security for the ScholarChip™ K-12 application is a result of a uniform corporate approach which is largely driven by our subsidiary, ScholarChip Payment Systems, used by college and university clients. Some of the relevant highlights are:

- **Intrusion Detection.** We have both intrusion detection devices (IDS) and intrusion protection devices safeguarding the network from a variety of attacks. Attack signatures are updated regularly (the system is Snort based). Regular scans are carried out to monitor system vulnerabilities.
- **Host-Based Security.** We also provide host-based security analysis based on event logs and full bandwidth usage on all NICs. Our network infrastructure provides *layer three* management to reduce the possibility of out-of-limits behavior by any host.
- **Physical Security.** Our data centers have strict physical security with biometric access and 24 hour guards. All server cabinets are locked and access is monitored via remote controlled cameras.
• **Administrator Access.** We utilize NIST standards of password hardening and administrator account naming to prevent direct attacks against any host. Certain hosts also require token access (three factor security).

• **Virus Protection.** All Tier I and Tier II devices run Symantec Anti-virus for Enterprise. Virus updates are scheduled every night.

C. **Backend Security**

Tier I (backend) security is part of our data center overall security plan. Highlights of the plan are:

• **Firewalls.** We utilize inward and outward facing firewalls for maximum security. The firewall provides three zones: External, DMZ and Private. Application servers are normally placed in the DMZ zone and access any database or file servers through an inward facing firewall. Database and file servers are placed in a private zone with access to the application servers allowed through firewall protocol rules. We also use network segmentation for added security. All our servers have at least two NIC interfaces. We do not use wireless networking in our backend (security and speed dictate that as all servers have Gigabit NICs). All ports are closed by default and are only opened through firewall protocol rules.

• **IP Rules.** We make extensive use of IP rules to limit access to servers.

• **Change Management.** We employ an enterprise-wide change management system (CVS-CMS) to store different versions of source code and application parameters. We use development and production servers that are highly isolated from each other.

• **Hardware Security.** Our locked cabinet approach to the backend provides a second level of hardware security. The first level being the data center biometric entry and 24 hour guards.

• **Use of Secure Socket Layer (SSL).** We use Secure Socket Layers for all web-based applications.

• **DoS and DDoS Attack Prevention.** Standard Denial of Service attacks (ping of death, buffer overflow, smurf and teardrop) are handled by our firewall and IPS services. Distributed DoS attacks are handled by a combination of services among them IPS, use of hot spaces in a different IP space (a procedure possible due to having two data centers, New York City and Long Island, NY) and by disabling most unused network services.

• **User Authentication.** We require two-factor user authentication for access to backend servers.
• **Out-of-Band Access.** We do not allow out-of-band access to the backend servers. IPMI, IP KVM and other devices must be accessed from within the data center.

• **Direct Login Policies.** User login passwords are changed frequently and are strictly role-based.

• **Web-based Login.** Login to web sites (such as the Management Site) is handled by an application layer separate from the server login. We do not use Active Directory or similar technologies to manage user login. This is impractical because of the large number of users (in one of our Payment Systems applications we have 400 colleges with 5,000 users). It is also undesirable to allow users access to the internal directory, even if role-based security is carefully followed. Instead, the login security layer is database driven and uses internal encryption methods (typically, one-way hashes) for password security.

• **Certificates on Tier II Hardware.** Tier II hardware accessing services on Tier I have installed certificates for encryption both at the client and the server. The Web Services server allows only communication with valid client certificates. The exception to this rule is the classroom attendance application where user certificates are not required.