We Connect the Systems that Power Education®

Security in SIF®

Safeguarding School Data

Steve Setzer, Senior Product Manager

May 2008

EDUSTRUCTURES

Edustructures LLC
891 W Baxter Drive
South Jordan, UT 84095
1.877.790.1261

www.edustructures.com

Contents

Executive Summary

> *Districts and states are responsible for protecting the confidentiality of personally reliable information about individuals whenever data are reported publicly.... This is not new; FERPA has been around since 1974.*
>
> --Glynn D. Ligon, Ph.D. and Barbara S. Clements, Ph.D., in Confidentiality and Reliability Rules for Reporting Education Data: A Best Practices Paper by ESP Solutions Group

As education agencies worldwide struggle to meet the rising demand for educational accountability, many are turning to the SIF®, (the Schools Interoperability Framework®) as a technical standard for data interoperability. The goal of SIF is to assure interoperability between disparate software applications for improved business processes, data accuracy and reliability, staff efficiency, and cost reduction. Ultimately, SIF offers information—not simply data—that allows teachers and administrators to better serve their students and report progress as legislatively mandated.

However, the enhanced accessibility to student and staff records leads to questions of data security—information protected by the Family Educational Rights and Privacy Act (FERPA) and other federal and state privacy laws. In answer, SIF's infrastructure offers secure data delivery built-in from the foundation, with a networked security model based on industry standards such as HTTPS and TLS to ensure only *legitimate* users have access to specific data.

This white paper outlines the SIF security model—including SIF 2 and all prior versions—and describes how a SIF implementation can be rendered more secure using the SIFWorks® integration platform, in particular the SIFWorks Enterprise Zone Integration Server (ZIS), which was the first ZIS to receive SIF certification against all four levels of security in the new 2.0r1 specification. Additionally, we'll offer best-practice recommendations for securing data in a SIF environment, including some comments on end point security.

Privacy, Security, and Data Accessibility

> *No Child Left Behind and FERPA are aligned.*
>
> --Ligon and Clements, op. cit.

As mentioned in the summary, FERPA (first enacted in 1974 and revised over the years) is the umbrella legislation designed to define access to and protect student education records and student and family privacy. The legislation pertains to any school, either pK-12 or higher education, public, or private, that receives funds under any program from the U.S. Department of Education. FERPA requires education agencies and institutions to have in place policies and procedures that ensure the confidentiality and security of student records.

Enter the No Child Left Behind act of 2002 "NCLB" (plus a growing list of local and other legislative accountability requirements). NCLB—enacted to ensure that each child in America is able to meet the high learning standards of the state where he or she lives—is one of the key drivers in the US behind educational accountability programs. The success of these programs, however, is dependant on vast amounts of timely and accessible data; states must provide aggregate and disaggregate analysis and reporting of students' standardized testing and achievement results (via longitudinal data systems). Capturing, transmitting and securing appropriate access for so much data can be challenging for even the most sphisticated enterprise.

Fortunately, education software vendors and educators envisioned and began to develop a technical standard for data interoperability in education prior to the passing of NCLB. As a result, the School Interoperability Framework (SIF) standard was born. Implemented as secure, service-oriented architecture (SOA), SIF can help ensure secure, reliable transmission of even the largest amounts of data. The basics and best-prqactice resommendations of SIF security in the follow paper are easy to understand and implement.

SIF Security

The SIF security model centers around SIF authentication and SIF transport encryption, based on the HTTPS, TLS and X.509 standards. Because SIF itself is concerned with the transport of data in a standardized format over an easily managed system, the SIF security model also focuses on securing the transport of data between applications (specifically, between the SIF Agent that represents each individual application and the SIF Zone Integration Server "ZIS" that brokers all SIF communications in a district or other entity).

HTTP / HTTPS as the Core Standard

The governing body for SIF, the SIF Association (SIFA), has adopted HTTP and HTTPS as the core transports for SIF. HTTP (Hypertext Transport Protocol) is the standardized set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) over the Internet. Because HTTP communications are conducted in "plaintext" (the normal representation of the data before any action has been taken to conceal it), it offers faster processing (CPU cycles are not used to encrypt and decrypt data) and it is easier to debug. However, because the data is not encrypted (any person with access to the path between browser and server can read the text), HTTP is best used in a secure environment, such as an isolated data center (see Secure SIF Communications). The use of HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) addresses the security issues by encrypting and decrypting HTTP traffic, providing adequate security for the transport of highly-confidential data.

In implementing a production SIF environment, the typical practice is to initially set up all agent to ZIS connections using HTTP only, to make troubleshooting easier by avoiding certificate management and making the data stream human readable. Such an implementation only remains in HTTP during the initial setup and testing phases. Once all agent communications have been verified, the infrastructure is switched over to HTTPS and uses that tranport from then on for secure exchange of education data.

Components of the SIF Security Model

The SIF security model has three significant parts: authentication level, TLS/SSL version, and data encryption level (based on key length).

SIF Authentication

SIF authentication helps to ensure that only authorized SIF agents attach to a SIF zone and send or receive data. SIF authentication is based on X.509 certificates. Certificates may be self-generated or issued by a local or commercial certificate authority.

The SIF Specification defines four authentication levels as follows:

- 0 - No authentication required and the sender **does not** have to submit a certificate.
- 1 - A valid certificate **must** be presented.
- 2 - A valid certificate from a trusted certificate authority **must** be presented.
- 3 - A valid certificate from a trusted certificate authority **must** be presented and the CN field of the certificate's subject entry **must** match the host, which is originating the message.

An agent can be configured to return a certificate when one is requested, and to request authentication levels from other agents and the ZIS.

TLS/SSL Versions

Both SIF authentication and SIF data encryption are based on industry standards for secure communications over the Internet—the same standards that are used for commerce over Web browsers. Specifically, the SIF documentation recommends the use of TLS 1.0; connections based on SSL 3.0 and TLS connections using SSL 2.0 hellos are also permitted (SSL 2.0 and 3.0 are likely to be deprecated in future versions of the SIF specification).

The following behaviors are supported for Agents registered in both pull and push modes:

- TLS 1.0
- SSL 3.0
- TLS 1.0 - negotiated using an SSL 2.0 client hello
- SSL 3.0 - negotiated using an SSL 2.0 client hello

SIF Data Encryption Levels (Encryption Key Lengths)

The SIF Specification defines five encryption levels (representing symmetric key lengths):

- 0 - No encryption required
- 1 - Symmetric key length of at least 40 bits

- 2 - Symmetric key length of at least 56 bits
- 3 - Symmetric key length of at least 80 bits
- 4 - Symmetric key length of at least 128 bits

An agent can be configured to support encryption when requested, and to request specific encryption levels from other agents and the ZIS.

For more information, please refer to the current SIF Implementation Specification, available from the SIFA Web site (http://www.sifinfo.org/).

Best Practice Recommendations

Edustructures is a founding member and active participant in SIFA, the standards-setting organization behind the SIF specification. As a pioneer in developing and enhancing the SIF specification, and the leading provider of SIF solutions and services, Edustructures has unmatched expereince installing and supporting successful SIF implementations worldwide. Our implementation engineers have installed more SIF implementations than any other vendor, including hundreds of cases where data flows across district boundaries to a state office and hundreds more where agents are distributed to multiple locations in a district.

The recommendations offered in this section draw on the company's real-world experience, on the SIF specification itself, and standard best practices for IT security.

> *The Department [USED] remains strongly committed to enforcing the requirements of FERPA and ensuring that personally identifiable information is protected. Anonymous data procedures will ensure that the data are not traceable to individual students.*
>
> —LeRoy S. Rooker, Director, Family Policy Compliance Office, US Department of Education. November 18, 2004

Secure SIF Communications

As mentioner earlier, SIFA has adopted HTTP and HTTPS as the core transports for SIF. HTTP may provide adequate security if, for example, all applications and agents are in a single, highly secure data center. However, many configurations require the use of HTTPS. For example, if data is being transmitted from a district office to a state education office over the public Internet, HTTPS must be used to encrypt data from prying eyes and to assure FERPA guidelines are met.

In general, participating SIF Agents and the ZIS should be configured with X.509 certificates and the certificates exchanged to ensure SIF Authentication Level 2 or 3. While Level 1 provides encryption, Levels 2 and 3 provide additional assurance that the agent is in fact the correct agent to be sending or receiving data.

If at all possible, we recommend the use of TLS 1.0 for communications only. If you are using a SIF agent that does not support TLS, contact the agent developer and advocate to have the agent updated (only older SIF agents do not support TLS). This is a critical update as only TLS communications will be supported in future versions of the SIF specification (meaning your old agent will become obsolete).

Finally, for each agent-to-ZIS connection, use the highest SIF Data Encryption level supported by the agent. As noted earlier under products, not all agents support all encryption levels, but if an agent supports multiple levels, the highest level supported by both that agent and the ZIS will provide the greatest security.

Securing Data Outside the SIF Channel

Software applications, their SIF agents, and the SIF Zone Integration Servers connecting them also need to be configured securely outside of SIF. SIF does not obviate the need for other standard information technology security practices; it operates in concert with them. SIF secures the transportation of data, while other measures secure the data at the endpoints of SIF transport.

For example, many software products have log files or logging databases which store SIF data for easy resolution of problems. Unfortunately, these logs are themselves in clear text; they have to be, because the SIF data encryption has to be decrypted as part of the agent or ZIS operations. Most products also have message queues and other locations where part of the SIF message traffic is stored temporarily or permanently.

To ensure proper data security external to the SIF infrastructure, we recommend the following practices:

1. Follow generally good security practices related to passwords, user accounts, and so on;

2. Review and apply any security related information provided by each product's vendor or developer;

3. If a product (ZIS, agent, or application) has configurable logging, turn the logging down to a minimal level, or turn it off completely. This will minimize the amount of data duplicated in the logs; for many products it will also improve performance. Turn logging up only when you need to diagnose a problem; turn it back down as soon as the problem's resolution has been verified;

4. Ensure that only authorized personnel have access to the computers running software products and to the disk storage for those products;

5. If a product has multiple user access (such as the SIFWorks Enterprise ZIS with its Web-based console), provide user accounts only to authorized personnel.

Robust SIF Solutions

The Edustructures SIFWorks® integration platform represents state-of-the-art application integration technology for education. With SIFWorks, SIF-compliant applications can communicate to share information securely, reliably, and in real-time. Edustructures' comprehensive suite of SIF-based solutions addresses all forms of horizontal SIF integration (district-based SIF interoperability), SIF-based unique student ID management for states, vertical reporting and longitudinal data collection, and SIF agent development.

Edustructures recommends the use of the following solutions to assure the most robust, secure SIF implementation:

SIFWorks® Enterprise Zone Integration Server (ZIS): At the heart of any SIF implementation you'll find a ZIS. The ZIS is the central messaging system responsible for moving data in a SIF enabled enterprise. The SIFWorks Enterprise ZIS is the market's most widely deployed ZIS and supports all SIF Authentication Levels, all SIF-supported TLS and SSL methods, and all SIF Data Encryption levels. The SIFWorks Enterprise ZIS is installed on a central (district) or on-site (school) server, that automates the secure exchange of data between disparate applications within schools, districts, and states, eliminating data isolation and streamlining cross-application reporting. The cross-platform nature of the SIFWorks ZIS enables greater choice; Edustructures has successfully deployed the ZIS on operating systems as disparate as Windows, NetWare, Mac OSX, Solaris, and Linux.

Edustructures SIF Agents and the SIFWorks ADK® (Agent Development Kit): It is important to note that not all SIF agents are configured to support all SIF data encryption levels. However, Edustructures-developed SIF agents (available for many of the market's leading software applications), and the SIFWorks ADK, (which is used by Edustructures and many other companies to build SIF agents), supports all security aspects of the SIF specification.

For details on specific SIF-Certified application agents, review the Certification Statement at the http://certification.sifinfo.org Web site.

Conclusion

The Schools Interoperability Framework is a unique solution for education, addressing the challenges presented by the demands of NCLB reporting and FERPA privacy issues. Use of SIF's own security capabilities, together with proper security measures at the end points of the SIF infrastructure, can help keep personal data secure while districts and state agencies reap the benefits of standards-based data integration.

About Edustructures

Edustructures is the recognized leader in SIF integration solutions for education, making it possible for market-leading solutions to reliably and securely share data in real-time. Edustructures delivers:

- Premier SIF technology—the SIFWorks® integration platform is the foundation of more SIF implementations, in the U.S. and internationally, than any other SIF solutions provider
- Comprehensive Professional Services—best practiced-based implementations and ongoing customer support assure SIF success
- Strategic industry relationships—ensuring that *we connect the systems that power education*™

For more information about Edustructures, please visit www.edustructures.com, or call toll-free at 877.790.1261.