

CIRCULAR



30 - 32 Grosvenor Street

Sydney NSW 2000

Australia

Telephone +61 (0)2
9256 0555

Facsimile +61 (0)2 9256
0426

**To: Clearing Members
NZ Agents**

No: 9/99

SFEIN Phase 2 Member Technology Questionnaire

The Clearing House is currently evaluating options that will enhance and extend the current SFEIN system.

In order that only a viable solution is pursued, we require Member feedback to establish what kind of technologies are acceptable to be delivered to Members' desktops.

Please review the following in consultation with the IT and audit departments of your organisation and indicate which of the following technologies are acceptable:

Member Name:

Technology

Acceptable (Y/N)?

1. Solution which requires a stand-alone Crystal Reports viewer application to view documents (supplied by Exchange)
2. Solution which requires a Crystal Reports browser plug-in to view documents
3. Solution which requires a stand-alone Adobe Acrobat viewer application to view documents (supplied by Adobe)
4. Solution which requires an Adobe Acrobat browser plug-in to view documents.

Security

The current SFEIN system is delivered over a public network (the Internet) using 40-bit browser encryption technology.

We understand that significantly increased security is required for the transmission of clearing data (one of the objectives of the next phase of SFEIN). We propose therefore using 128-bit encryption technology, which has been designed for the transmission of highly sensitive financial data over public networks, and is strictly licensed by the U.S. government only to institutions who require this high level of security.

128-bit technology may be utilised over the Internet, or, at additional cost and with an upper bandwidth limit (probably 64K), over a WAN connecting the Clearing House with members.

A press release from VeriSign, Inc., the U.S. company that has developed this technology, is attached for further information.

Should this security be unacceptable to members, then the Clearing House will need to explore and implement other measures, significantly delaying rollout and probably requiring Member use of alternative proprietary decryption technologies.

Could you please review the issues regarding 128-bit technology and your organisation, and complete the following:

Technology	Acceptable (Y/N)?
1. 128-bit technology over the Internet (proposed solution)	
2. 128-bit technology over a WAN	

Additional Member Comments:

.....
.....
.....
.....
.....
.....
.....
.....
.....

Please complete and return by: Tuesday, 16 February 1999 - FAX 9256 0426

Should you have any technical related queries, please do not hesitate to contact Andrew Turner on 9256 0673. General queries should be forwarded to the undersigned on 9256 0636.

SFE thanks you for the time taken to complete this questionnaire as the answers provided will assist us in developing appropriate technology relating to information delivery to and from Members.

VERISIGN GRANTED FIRST FEDERAL APPROVAL TO ISSUE CERTIFICATES ENABLING EXPORT OF STRONG ENCRYPTION FOR US-BASED COMPANIES AND INTERNATIONAL BANKS

VeriSign Global Server ID Enables 128-bit Communications and Commerce

MOUNTAIN VIEW, Calif. -- July 14, 1997 -- VeriSign (www.verisign.com), the leading provider of digital certification services for Internet access and electronic commerce, today announced that the United States Department of Commerce has approved VeriSign's plans to issue new VeriSign Global Server IDs, allowing approved organizations to use 128-bit encryption with Netscape Communicator and Microsoft Internet Explorer 3.0 or better clients located in the US or internationally. For the first time, US-based companies - with servers located in the US - and international banks -with servers located in the US and abroad - will be able to use strong encryption internationally for Internet communication and commerce.

VeriSign is the first and only certification authority (CA) to meet government requirements in order to issue the special certificates for 128-bit export. VeriSign's license was granted approval after review and consultation from the National Security Agency (NSA) and Federal Bureau of Investigation (FBI). Companies and banks that have been issued VeriSign Global Server IDs will be eligible to use 128-bit encryption internationally.

The first organizations and banks which have expressed interest in receiving these new certificates include Bank of America, Citibank, Federal Express, Long-Term Credit Bank of Japan Ltd., Sanwa Bank Ltd., Sakura Bank Ltd., Sumitomo Bank Ltd., Sumitomo Trust and Banking Company Ltd, and Wells Fargo Bank.

"As a current user of VeriSign Digital IDs to provide privacy for our customers, FedEx looks forward to using the new certificates to help us communicate more securely with our growing base of global customers," said Dennis H. Jones, Chief Information Officer for Federal Express Corp.

"Bank of America customers use the Internet today as a viable platform for conducting online banking and electronic commerce. Security is an important focus of our Internet services and as enhanced levels of security are developed, we make them available to our customers," said Libby Ghekiere, senior vice president at Bank of America's Interactive Banking Division. "We are working with VeriSign to provide our customers with the capability of using 128-bit encryption on an international basis for their online banking activities. It is an early and proactive step to support our international customers with a high level of security and confidentiality."

Mr. Yoshiaki Izumida, General Manager of the Electronic Commerce Banking Dept. of Sumitomo Bank Limited, one of the largest banks in the world, commented, "To provide electronic financial services successfully, one of our concerns is how to implement a strong encryption security system. With this first federal approval, Japanese banks are enabled to use VeriSign's Global Server IDs. We expect that this effort will help to expand real electronic commerce which will greatly benefit the Japanese market."

Going beyond recent government approval of strong encryption for financial institutions, this is the first solution that allows businesses and banks to establish strongly encrypted communications with clients located around the world, previously restricted under US cryptography export laws. Businesses with servers located in the US, for the first time, will be able to communicate internationally using 128-bit encryption with any customer who uses a Communicator 4.0 or Internet Explorer 3.0 client.

VeriSign Global Server IDs will provide privacy and security for business-to-business, intranet, and business-to-consumer applications. Stronger encryption for data transmitted overseas will benefit not only companies with international offices, but those that have customers, suppliers and other key business partners outside the US. Consumers, merchants with Web storefronts and corporations can do business globally, confident that their electronic information or transactions are protected by the strongest encryption technology possible. Global Server IDs will be issued to approved organizations by VeriSign or its international affiliates, including VeriSign Japan KK and Persetel, which issues VeriSign certificates in South Africa.

Prior to VeriSign's new 128-bit export approval, U.S. export regulations restricted the export of strong (128-bit) encryption to establish a secure communications channel when either the server or the browser

were located outside US borders. Companies will not need to escrow their keys in order to take advantage of this program. Secure communication can now be established between:

- servers located in the US and browsers located globally, when the servers have a VeriSign Global Server ID
- browsers located in the US and servers located overseas, when the servers have a VeriSign Global Server ID
- browsers and servers located overseas, when the servers have a VeriSign Global Server ID

VeriSign, with its well-established technology, infrastructure and practices can ensure that:

- Global Server IDs are created with today's strongest cryptographic technology and utilize 1024-bit digital signatures to validate themselves
- Global Server IDs will only be granted to legitimate businesses that meet the necessary U.S. government qualifications
- Global Server IDs can not be obtained under false pretenses
- The full lifecycle services offered by VeriSign, including 24 hour, 7 day a week revocation, will ensure the integrity of the program

Companies that meet federal eligibility criteria will be issued a VeriSign Global Server ID and will be able to use the encryption-fortified version of Netscape Enterprise Server or Microsoft Internet Information Servers outside the US. Companies holding Global Server IDs can deploy 128-bit capable servers without submitting to US Government key recovery requirements.

"Close to one third of VeriSign's business comes from international and multinational companies," said Stratton Sclavos, VeriSign president and CEO. "These customers have long expressed a desire to be able to communicate more securely overseas. Thanks to the cooperation of the US Government, we are now able to offer law-abiding companies a legal alternative for secure communication and commerce."

The mechanism for enabling this interaction is available today with Netscape Communicator client software and will be available for Internet Explorer 3.0 and 4.0 browsers. Upon encountering a server, the browser will check to see if the server has been issued a Global Server ID. If the browser sees such an ID, then it will initiate a session at stronger levels of encryption.

128-bit encryption provides a significantly greater amount of cryptographic protection than 40-bit encryption, the maximum-strength protection the U.S. government has allowed U.S. software companies to export. It is increasingly necessary to employ larger keys to counter the increasing computing power of potential criminals. In a recent experiment sponsored by

RSA Data Security, a 40-bit encoded message was cracked in approximately eight hours. A 128-bit message is 309,485,009,821,345,068,724,781,056 times harder to unscramble than a 40-bit message. If the technology applied to crack the 40-bit message in eight hours were applied to break a 128-bit message, it would take more than two trillion years.

Previously, if either the server or client in a communication session were exported outside of the US, the session key used securing the session could be no stronger than 40-bits without violating US export law. This made it difficult, for example, for a company with plants in the US and plants, suppliers and partners in Europe to use strong encryption for their communications globally.

VeriSign Japan, KK, a subsidiary of VeriSign, Inc., mirrors VeriSign's certificate offerings by localizing its services for consumers and corporations for applications such as secure Web commerce, electronic credit payments and home banking.

Export versions of Netscape Communicator are available today at www.netscape.com.

Existing versions of Microsoft browsers and servers will be updated with a single file (SCHANNEL.DLL) available from www.microsoft.com at the end of July.

###

Other Industry Support:

CITIBANK

"Citibank is pleased to be part of this step forward in providing heightened online security to our customers around the world. We expect VeriSign's digital certification of 128-bit browser security to be an important part of our efforts which will give our customers the confidence that, regardless of where they are, their online transactions are secure," commented Michael Grandcolas, senior technology architect for Citicorp Development Center.

MICROSOFT

"Strong encryption for our corporate and individual customers is essential to make the Internet a critical component for communications and commerce. This approval from the Commerce Department is significant progress in establishing a global digital marketplace," said Mike Dusche, Microsoft's worldwide financial services industry manager. "The US Government is sending a strong message to the world by approving these applications from Microsoft and VeriSign and we're happy to be working with them to provide VeriSign Global Server IDs to our customers."

NETSCAPE

Taher Elgamal, Chief Scientist for Netscape commented, "Offering our customers outside the United States the same level of encryption as we offer here is extremely important to Netscape. This approval and our work in the privacy and security arenas helps bring international customers stronger level of encryption."

VISA

Todd Chaffee, senior vice president from Visa commented, "We are pleased to see that VeriSign is working with the government and other technology companies to further electronic commerce on a global scale. The banks have been waiting for this added level of security for some time now. Finally, both US-based and international banks can communicate and perform commerce more efficiently with a much stronger security solution than was previously available."

WELLS FARGO

"Using VeriSign's Global Server IDs, customers can feel confident that they are using the highest level of security available from the browser market today and the ability to deliver this level of access internationally as another dimension to the quality of service that Wells Fargo is able to offer." said Louis Gasparini, vice president of internet distribution systems for Wells Fargo Bank.

Copyright 1997 VeriSign Inc. 1390 Shorebird Way, Mountain View, CA 94043. All rights reserved. VeriSign is a servicemark and trademark of VeriSign Inc. Digital ID and Digital ID Center are service marks of VeriSign Inc. All other trademarks are properties of their respective owners.

Katrina Maunder
Manager; Clearing Services

08/02/99

SYDNEY FUTURES EXCHANGE CLEARING HOUSE PTY LIMITED
ACN 050 615 864

A wholly owned subsidiary of Sydney Futures Exchange Limited
Address all correspondence to PO Box N680 Grosvenor Place Sydney NSW 2000 Australia