

# **ISL (Informer Systems Ltd.) SentryNET & e-SentryNET Technical Evaluation**

---

An NSS Group Report



First published August 2002 (V1.0)

Published by The NSS Group  
Oakwood House, Wennington, Cambridgeshire, PE28 2LX, England

Tel : +44 (0)1487 773307  
Fax : +44 (0)1487 773168  
E-mail : [info@nss.co.uk](mailto:info@nss.co.uk)  
Internet : <http://www.nss.co.uk>

©1991-2002 The NSS Group

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors. This report shall be treated at all times as a confidential and proprietary report for internal use only.

Please note that access to or use of this Report is conditioned on the following:

1. The information in this Report is subject to change by The NSS Group without notice.
2. The information in this Report is believed by The NSS Group to be accurate and reliable, but is not guaranteed. All use of and reliance on this Report are at your sole risk. The NSS Group is not liable or responsible for any damages, losses or expenses arising from any error or omission in this Report.
3. *NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY THE NSS GROUP. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT ARE DISCLAIMED AND EXCLUDED BY THE NSS GROUP. IN NO EVENT SHALL THE NSS GROUP BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.*
4. This Report does not constitute an endorsement, recommendation or guarantee of any of the products (hardware or software) tested or the hardware and software used in testing the products. The testing does not guarantee that there are no errors or defects in the products, or that the products will meet your expectations, requirements, needs or specifications, or that they will operate without interruption.
5. This Report does not imply any endorsement, sponsorship, affiliation or verification by or with any companies mentioned in this report.
6. All trademarks, service marks, and trade names used in this Report are the trademarks, service marks, and trade names of their respective owners, and no endorsement of, sponsorship of, affiliation with, or involvement in, any of the testing, this Report or The NSS Group is implied, nor should it be inferred.

# TABLE OF CONTENTS

---

<b>INTRODUCTION .....</b>	<b>1</b>
Hardware Tokens .....	1
Smart Cards.....	1
Biometrics.....	2
<b>ISL (INFORMER SYSTEMS LTD.) .....</b>	<b>4</b>
Cherry FingerTIP ID Board.....	4
SentryNET .....	5
PKI Support .....	9
e-SentryNET .....	10
Verdict.....	13
Contact Details .....	14

# TABLE OF FIGURES

---

Figure 1 - Installing the Cherry keyboard drivers .....	5
Figure 2 - the MMC snap-in for SentryNET user management .....	6
Figure 3 - Biometric enrolment .....	7
Figure 4 - PKI Components .....	9
Figure 5 - Using the SentryNET CSP integration.....	10
Figure 6 - e-SentryNET architecture.....	11
Figure 7 - Authenticating via e-SentryNET for Web page access .....	12

## The NSS Group

---

The NSS Group is Europe's foremost independent network and security testing facility.

Based in Cambridgeshire, England, and with additional labs and conference centre in the South of France, The NSS Group offers a range of specialist IT, networking and security-related services to vendors and end-user organisations throughout Europe and the United States.

The Group consists of two wholly-owned subsidiaries :

- *NSS Network Testing Laboratories*
- *Network Security Services*

**NSS Network Testing Laboratories** are available to vendors and end-users for fully independent testing of networking, communications and security hardware and software.

NSS Network Testing Laboratories also operates certification schemes for vendors and certification bodies, and currently provides certification of firewalls, VPN's, crypto products and PKI products.

Output from the labs, including detailed research reports, articles and white papers on the latest network and security technologies, are made available free of charge on the NSS web site at <http://www.nss.co.uk>

**Network Security Services** provides a range of security-related services to vendors and end-users including security policy definition, IDS, firewall and VPN implementation, network security auditing and analysis, and penetration testing.



## INTRODUCTION

---

The password problem is looming larger and larger for network administrators trying to get a grip on security. Why is that? Because, put quite simply, passwords alone are not secure. Users have a habit of choosing "easy to remember" passwords which revolve around names and birth dates, for example, and many even resort to writing passwords down and sticking them on the side of their monitor.

Even in places where security is not quite that lax, numerous success stories abound of successful *social engineering* attacks – where legitimate users are duped by hackers pretending to be from the IT department and asking for their password in order to perform some vital testing.

### Hardware Tokens

---

A more secure form of authentication is required, and one option is the hardware token system. One variation of this approach makes use of hand-held units which resemble calculators into which the user enters a numeric challenge raised by the authentication server. The token encrypts the challenge and the resulting reply is entered into the PC by the user. When the reply is checked by the authentication server, it knows beyond a shadow of a doubt that the user is who he says he is.

Although very secure, token-based systems have a couple of drawbacks. The first is that they need replacing every few years, and the second is that the authentication is one-way only – in other words, there is no way for the user to determine that he is communicating with a valid server.

### Smart Cards

---

Smart cards offer an alternative solution to the problem of access control and authentication. They also offer the additional advantage of being able to store digital certificates. With a smart card reader attached to the PC, the same card which perhaps provided access to the building can now provide the first line of authorisation for the network.

A smart card is similar in appearance to a standard credit card, both in size and choice of material. However, instead of the magnetic stripe on the reverse of a credit card, the smart card sports a small gold-coloured computer chip approximately one centimetre square. Such cards can also come in smaller sizes – basically just the computer chip on a plastic base – for use in cellular telephones. ISO standard 7816 defines the physical and logical features of smart cards, such as shape, position of contacts, their functions at the user interface, and their file structure.

Depending on the designated function of the smart card, the on-board chip can consist of anything from simple EPROM memory (i.e. in the case of a telephone card) to a full-blown tamper-proof "computer-on-a-chip", including an 8-bit microprocessor, RAM, ROM and EEPROM.

The on-board CPU can process, share and store information, allowing the card to be used in a variety of applications. As well as being able to store much more information than the standard magnetic strip card, the key advantage to smart card technology is the ability to process information in line with pre-programmed guidelines.

When the card is inserted into a smart card reader, it makes contact with electrical connectors that transfer data to and from the chip. Data written to the card can be stored either in the RAM or EEPROM, with the ROM used purely to store the microprocessor's operating system.

Whilst the RAM is used primarily as temporary work space for the on-board applications, the EEPROM is designed as a more permanent (though re-writeable) form of storage. Like the hard disk on a PC, the EEPROM provides a hierarchical file structure on which can be stored critical data (such as PIN numbers or cryptographic keys) and application programs (electronic cash, telebanking, symmetric encryption, and so on). Certain smart cards also contain a cryptographic coprocessor, that can handle asymmetric cryptographic algorithms, such as RSA.

Since most smart cards are used for security-related applications, it makes sense that the design is such that physical access to the chip contents is prevented except under certain rigorously controlled conditions. Typically, it is necessary to enter a four-digit PIN (Personal Identification Number) in order to provide access to the contents of a card, but this in itself is often considered insecure.

In other words, although we have replaced our simple password as the authentication mechanism for our network with something far more secure in the form of a smart card, the access to the authentication details on the smart card is still only protected by a "password" – and the four-digit PIN is probably even easier to crack than the password policy we have enforced on our network.

Of course, the advantage of the smart card is that – unlike the simple password – it requires that the attacker knows the PIN **and** has physical access to the card itself. It is this combination of authentication methods – *something you know* (the PIN) combined with *something you physically hold* (the card itself) that makes the smart card approach that much more secure. While your users have physical possession of their cards, a compromise is impossible.

Even so, there is a means to eliminate the need for a PIN altogether whilst increasing the level of security offered by the smart card – *biometrics*.

## **Biometrics**

---

Until now, maintaining security and controlling access to computer systems and applications through the use of passwords has been both a burden and inconvenience to users and a drain on administrative resources. Biometric solutions, which use a person's unique physical characteristics to ensure positive identification, offer an alternative to password protection, which is both more secure and reduces administrative costs.

The savings from converting password-based systems to those driven by biometric devices can be significant. This is especially true in circumstances where customer service and accessibility are essential, but security must be maintained. Businesses, schools, and government agencies have found that the return on their investment in biometric solutions is high when they are used to both deter identity theft, and preserve resources.

A biometric is a measurable, physical characteristic or personal behavioural trait used to recognise the identity or verify the claimed identity of an enrolled user. Typically physical features used for biometric identification are fingerprint, voice, retina or iris, and facial or hand geometry.

Retinal or iris scanning is extremely accurate but expensive to implement, and is warranted only in the most sensitive of security environments – military or financial, for example. For most ordinary users, the thought of a laser device scanning their eye is also a sensitive issue that some find less than appealing.

A typical voice recognition system is more affordable, and less intrusive, but is not always reliable. The human voice is subject to change during bouts of illness – a common cold could render access to the network impossible, for example – and in noisy environments it can be problematical even when voice patterns are constant.

Despite recent revelations in the security industry where it was demonstrated that some fingerprint recognition devices could be fooled using very simple tools, this technique is still considered the best choice for most applications because of its accuracy, speed, reliability, non-intrusive interfaces, and cost-effectiveness.

Fingerprints can be captured in different ways – current techniques include *optical*, *ultrasound*, or technologies based on *semiconductor chips*. Readers translate captured images of fingerprints into a digital code for further software processing.

Advanced software algorithms map the distinguishing characteristics of fingerprint ridge ends, splits, dots, arches, whorls, loops, ridge lines, valleys, bifurcations, upper and lower cores, and deltas. These characteristics are then converted to a unique “*digital fingerprint*” template that can be stored in a smart card or central database for subsequent matching and authentication operations.

## ISL (INFORMER SYSTEMS LTD.)

---

ISL designs, develops, manufactures and markets software products allowing the use of smart cards and/or the capture and comparison of biometrics, such as fingerprints, for security applications including network access, remote access, Web access and database access.

The company also offers a range of biometric hardware technology which includes Sony, Siemens, Cherry, Biolink, Precise Biometrics, BAC, Identix and Ethentica.

For the purposes of this test, we combined the Cherry FingerTIP ID Board (model G 83-14000) with SentiNET and e-SentiNET software.

### Cherry FingerTIP ID Board

---

The Cherry FingerTIP ID Board is a heavy duty USB keyboard with an integrated fingerprint sensor and smartcard reader (the latter is optional). The fingerprint sensor is a Siemens capacitive model, with a resolution of 513dpi, whilst the smartcard reader is the PC/SC 1.0-compliant Omnikey CardMan 2020.

Since additional parallel or serial cables are not required for the sensing devices (all the components operate via the single USB 1.1-compliant interface), connectivity is a cinch. In addition, the keyboard also ports two downstream USB ports for connecting additional USB devices. For those PCs without USB keyboard support, other models are available, with additional cables for the sensing devices.

We installed the keyboard on a Windows 2000 Server and it was recognised immediately. Drivers for the smartcard reader and fingerprint sensor were loaded from the SentiNET CD and the keyboard was ready for use within minutes.

In operation, the Cherry keyboards feel very solid and have a light, but positive, key action. The fingerprint scanner is located at the top right of the keyboard, which may initially feel strange to left-handed users, but is unlikely to cause significant problems in long-term use. Although some left-handers might claim that a centrally-situated scanner would eliminate any such potential problems altogether, the current position is probably the only viable one given that it is the only place on the keyboard where the use of the scanning device would not be fouled by the top row of function keys.

In the time available to us we were not able to perform extensive testing to determine accurately the FRR (False Reject Rate) and FAR (False Accept Rate) of the fingerprint sensor. However, throughout the test both the smart card reader and fingerprint scanner worked flawlessly under what we would consider to be normal operating conditions.

The inclusion of these sensors in the keyboard makes them very intuitive and straightforward to use – only by making security operations so seamless will they become a part of the average user's day-to-day working routine.

## SentiNET

SentiNET incorporates biometric authentication and verification techniques to secure network access by replacing the logon password with fingerprint authentication.

Fingerprint templates created during the enrolment process are stored as an attribute of a user account, either in the Security Account Manager (SAM) database in an NT4 environment, the Active Directory (AD) database in a Windows 2000 environment, the NDS database in a NetWare environment, or on a smart card or similar personal storage device. A live fingerprint capture is authenticated against a user's stored fingerprint templates during the logon process, and access to the network is either granted or denied depending on the result of this authentication attempt.

It is possible to install SentiNET on a standalone machine running Windows NT 4.0 Workstation/Server or Windows 2000 Professional/Server if required. In this configuration all user accounts are managed on a single computer, and the administrator adds a biometric capability to the accounts of users on that host. Verification of the users then takes place on the same computer.

A far more scalable and straightforward solution, however, is to eliminate the need for a dedicated host altogether and store the fingerprint templates directly in the Novell NDS, or Microsoft SAM/Active Directory database. Verification, too, is performed directly from the central security data stores, and this feature sets SentiNET apart from the majority of the biometric authentication systems currently available.

For the purposes of this test, we used Windows 2000 Advanced Server with Active Directory. The SentiNET service needs to be installed on every domain controller in the organisation in order to provide a centralised biometric authentication mechanism. This service handles the login requests from SentiNET clients on the network and interfaces to the Active Directory for network logins, and the biometric user can be enrolled to any server.



Figure 1 - Installing the Cherry keyboard drivers

Installation of all the SentiNET component is a cinch, the installation wizard handling everything in a single operation. This includes running the hardware installer to enable the use of the Cherry FingerTIP keyboard with integrated biometric devices, and installation of the management components in the form of extensions, or *snap-ins*, to the existing Microsoft user management utilities (such as *User Manager* or the *MMC*).

Strictly speaking, the service is all that is required on each of the domain controllers, though it would also make sense to install the biometric keyboard and client software too, given that the domain controller is one of the most critical components of the network in terms of security.

The keyboard and client are required on every PC in the organisation that needs to make use of the SentiNET biometric/smart card function. If the organisation uses PKI (Public Key Infrastructure) it is also possible to install the CSP integration capability to enable certificates and private keys to be installed on the smart card.

Under NT 4.0 (Workstation and Server) and Windows 2000 (Professional and Server) the SentiNET logon component completely replaces the standard Microsoft GINA (G~~raphical~~ I~~dentification~~ a~~nd~~ A~~uthentication~~) module, whilst on Windows 9x clients a SentiNET Network Provider is added. These components allow the Windows logon process to be managed by SentiNET, taking the logon credentials from the smart card and prompting for a fingerprint scan in place of a PIN number or password. An API is also installed that provides access to the biometric and smart card capabilities from custom programs.

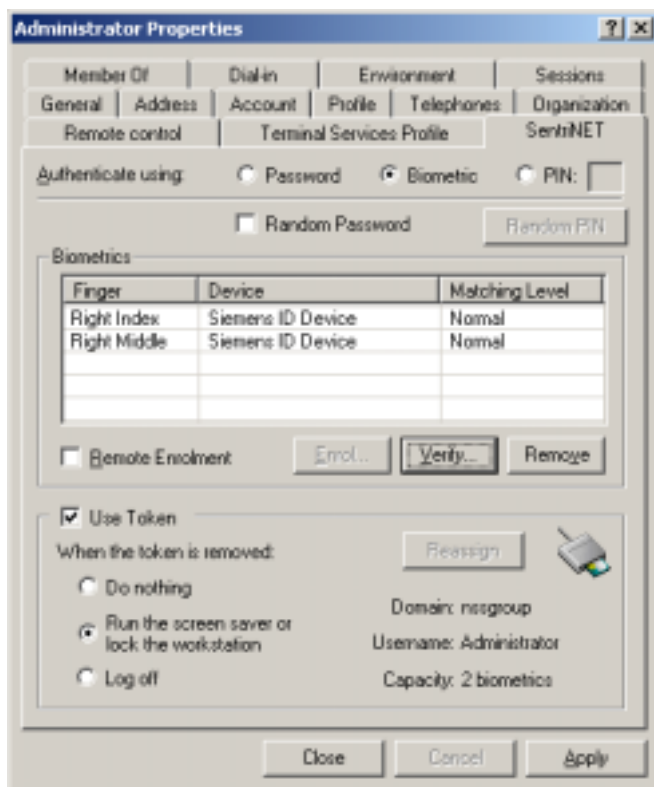


Figure 2 - the MMC snap-in for SentiNET user management

SentiNET administration is extremely easy, since it involves using extensions to the existing Microsoft management utilities such as the User Manager (under NT4) and the Microsoft Management Console (under Windows 2000). A snap-in is added to the MMC which simply insets an additional dialogue tab into the user properties screen.

When this page is displayed for the first time for a user, the authentication method is set to the default operation: *password*.

Checking the “Biometric” radio button allows the administrator to enrol users, allowing fingerprints to be used instead of passwords for network access.

A random password feature allows the replacement of normal user passwords with versions generated by the SentiNET software, making it impossible to log in to user accounts without using biometrics and making the stored passwords less susceptible to cracking using a dictionary-based attack. Note that once the *biometric* and *random password* combination is selected, it would be impossible for any user so enrolled to log on at any workstation that did not sport biometric devices. An option is available to allow users to log in either using biometric devices **or** using a known password on hosts which do not have biometric readers installed. This helps ease the pain of large-scale deployments.

Clicking the enrol button will cause the ‘*Biometric Enrolment*’ dialogue to be displayed. This allows the selection of a hardware device from the drop down list (if more than one device is installed) and the finger to be scanned by clicking the corresponding radio button on the picture. The software also allows the matching level to be changed from *Normal* to *Extra*.

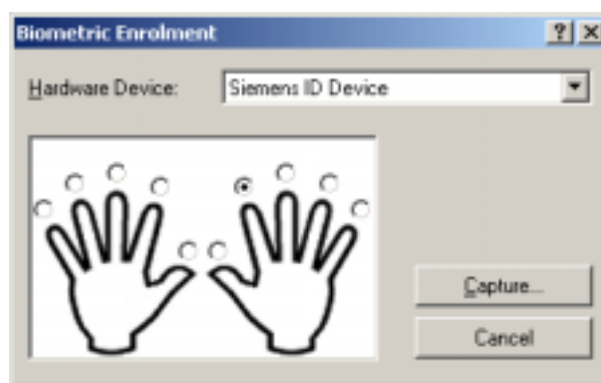


Figure 3 - Biometric enrolment

When considering biometric devices, there are two parameters that are important: *FRR* and *FAR*. *FRR* stands for *False Reject Rate*, and denotes the propensity for a device to reject valid users. Conversely, *FAR* stands for *False Accept Rate*, and refers to the tendency for a device to accept someone it should not. A high *FRR* – whilst increasing security – is frustrating for users and tends to lead to a rejection of the technology. On the other hand, a high *FAR* is inherently insecure, negating the benefits of the biometric approach.

Using the ‘*Extra*’ matching level is likely to increase the *FRR*. Throughout the tests, however, we had only one instance of a false rejection, and not one false acceptance.

Clicking on the “*Capture*” button brings up the capture window, and the appropriate finger is placed on the sensor device. Only one reading of each fingerprint is required, and once the capture has been completed the template is stored (either in the SAM/Active Directory/NDS or on a token) and the user may repeat the capture using different fingers.

The number of biometrics that can be enrolled is dependent upon the storage medium. For network based storage (NDS, SAM or ADS) ten templates may be stored, whilst for smart cards the limit is generally two.

It is advisable after an enrolment has taken place that a verification is performed. This acts as a double check as it simulates a user's logon and requests a capture to compare against the stored template, confirming that it is usable. Where a biometric is found to be unusable, or where it is necessary to reduce the number of templates in order to store them on a smart card, the "*Remove*" button allows the deletion of biometrics that are no longer required.

Naturally, it is not always possible for users to be physically present at the administrator's workstation for enrolment. For this reason, SentiNET also provides a remote enrolment capability.

The "*Remote Enrolment*" check box allows the user to logon for the first time using a password, at which point they are prompted to scan their fingerprints at the client machine for use in subsequent logons. Unfortunately, because of the requirement for the user to know their password, the use of remote enrolment prohibits random passwords in the current release. ISL is working on fixing this problem in a future release.

Although it is possible to rely purely on fingerprint recognition as a means to authenticate network access, the use of smart cards provides enhanced levels of security. Smart cards allow for the storage of small amounts of data, which the user is able to remove from the system and carry with them. If a smart card is selected for use with SentiNET, the details as displayed in the property page (domain, user name and password) will be transferred to the token, including any biometrics, and are no longer stored in the central Windows/NetWare directory.

This is something of a mixed blessing. The removal of the user credentials from the central data store allows for increased privacy and ownership of those credentials for the user. The downside is that should a card be lost it is not possible to simply re-issue it, since the original enrolment details no longer exist. Instead, it would be necessary for the user to re-enrol from scratch with a new card.

When using tokens, two more options become available: *PINs* and *token removal actions*. PINs are basically four digit passwords and are not therefore particularly secure. This is why they are only allowed with a token that provides additional physical security (such as fingerprint recognition) and a lock out in the event of incorrect entries.

The token removal action controls what happens when a token that has been used to logon a user is removed. It is possible to specify that workstation should be locked or that the user should be logged off.

Once the enrolment has been completed, user authentication takes one of two forms. If fingerprint recognition is used alone, with no smart card, the user will call up the GINA interface with the usual CTRL+ALT+DEL key sequence, and enter the domain and user name. Instead of a password, the user is then prompted to place a finger on the sensing device, and the captured template is compared with that stored in the central NDS/SAM/AD database. If it matches, the user is logged on to the network – no password is required.

When tokens are used, life for the user is even easier – in this case, all that is required is to insert the smart card into the reader. The SentiNET GINA takes control at this point and the user is prompted to place a finger on the sensor.

If the live fingerprint scan matches the template stored on the card then the user credentials are retrieved from the card and the user is logged on to the network automatically.

## PKI Support

Where organisations have implemented a Public Key Infrastructure (PKI), the latest version of SentiNET provides a replacement for the Cryptographic Service Provider (CSP) to allow the normal PIN functionality of a PKCS#11-compliant smart card with the SentiNET biometric capability.

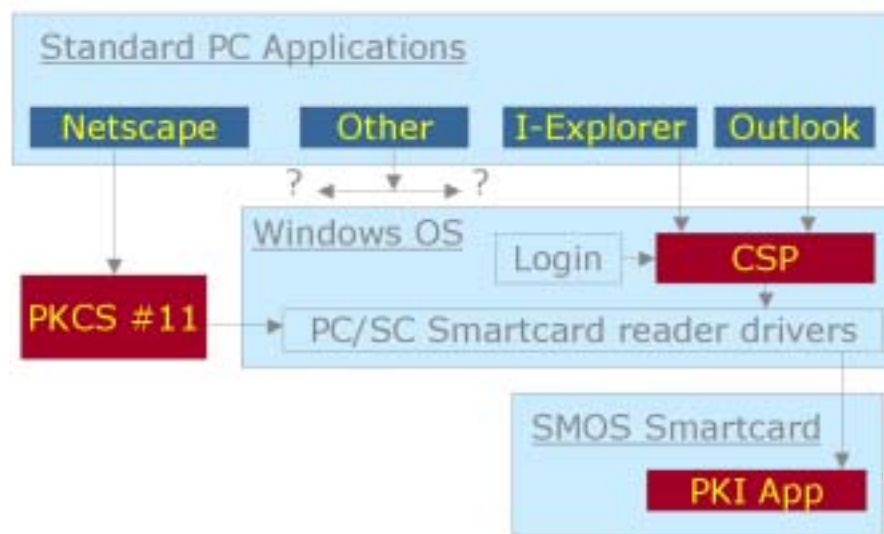


Figure 4 - PKI Components

In all respects, the user is enrolled and managed in the usual way, storing the SentiNET credentials on the smart card. In addition, the SentiNET CSP provides the means for storage of digital certificates and private keys directly on the card, with access controlled by fingerprint scans instead of the usual PIN number.

The application permits on-card key generation when the chosen card is capable of this operation. Where this capability is not available – or where central allocation of keys is preferred – off card key generation is supported. Multiple key support permits several keys to be associated to a card holder.

When the user requests a digital certificate from the Certification Authority (CA) the *SmartCard Solutions PKI Card Provider* (the SentiNET CSP) should be selected instead of the more usual *Microsoft Base Cryptographic Provider*. As the certificate is issued and private key pair generated, direct access to the smart card is required. At this point, the SentiNET CSP takes over and prompts for a fingerprint scan instead of a PIN number. If the scan matches the template stored on the card, then the certificate and keys are written.

Subsequent access to the certificate and private keys – either for Web access, digital signature operations (signing e-mails, for example) or data encryption – is also controlled by the same fingerprint operation, making the use of the smart card that much more secure.

Now the only person who can gain access to the private key is the real owner – verified by his or her fingerprint. It is no longer enough to have possession of someone else's card and guess (or otherwise acquire) the four-digit PIN number.

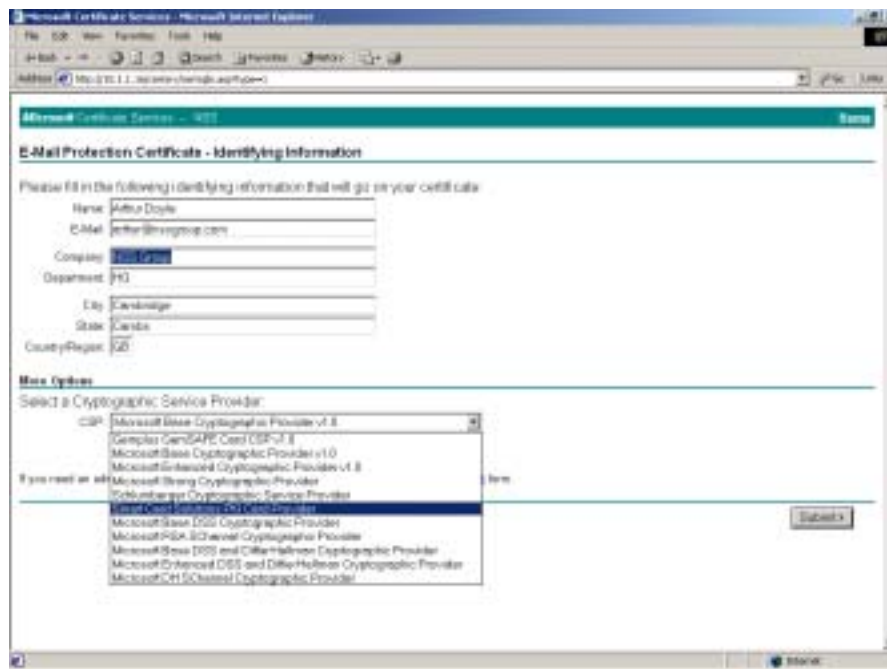


Figure 5 - Using the SentiNET CSP integration for PKI operations

## **e-SentiNET**

---

e-SentiNET is a suite of programs that allow a person's fingerprint to be used to authenticate their identity when accessing web pages.

e-SentiNET is simply an additional layer on top of the normal SentiNET components. As with normal SentiNET operation, therefore, the user's fingerprint templates created at enrolment are stored as an attribute of their user account, either in the Security Account Manager (SAM) database in an NT4 environment, in the Active Directory (AD) database in a Windows 2000 Server environment, in the NDS database in a NetWare environment, or on a smart card or similar personal storage device. Alternatively the fingerprint templates can be stored in an SQL database and accessed via an ODBC call. A live fingerprint capture is then compared against these stored templates during the authentication process, and access to the web page is either granted or denied depending on the result of this authentication attempt.

e-SentiNET needs to have files installed on both the client and server machines, but the fingerprint/smart card reader needs to be installed only on the client machine. e-SentiNET then uses an ActiveX control which is downloaded to the client Web browser and an ISAPI filter residing on the Web server.

On the Web server the ISAPI filter uses the user credentials posted by the client to authenticate users against the server/domain resources.

When running as a stand alone member server, the Microsoft Internet Information Server (IIS) needs to have the SentiNET Service installed and running. This service handles requests from e-SentiNET and interfaces to the local SAM database to extract the stored templates associated with a user for use in the comparison against a live fingerprint capture.

If the Web server is part of a domain or ADS tree the service needs to be installed on all the domain controllers. New biometric users can be enrolled at the server using the usual SentiNET extensions to the normal Windows management utilities, or by connecting to the remote enrolment page on the Web server. Users will need to input their ID and password in order to proceed to the fingerprint enrolment stage.

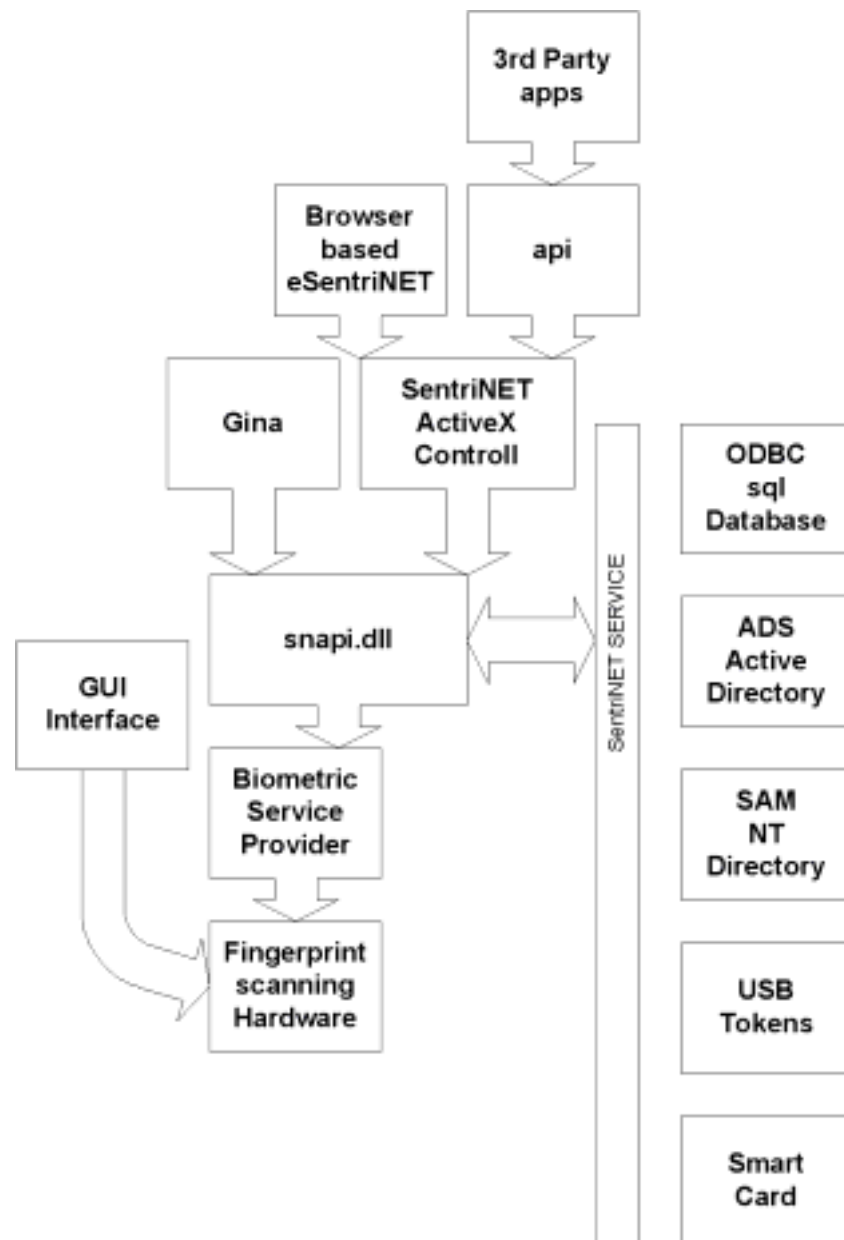


Figure 6 - e-SentiNET architecture

The ActiveX control gives a flexible approach which allows developers to interface with e-SentiNET directly and modify their own Active Server Pages for a fully integrated total solution.

Effectively there are 3 different ways to use e-SentiNET:

- **Plug and Go** – Here the e-SentiNET installation installs an ISAPI filter and redirects user connections from a predetermined folder for authentication with their fingerprint before giving access to the directory and any files contained therein.
- **Using the ActiveX control directly** – The ActiveX control supplied can be plugged directly into the IIS web server pages to create a fully integrated solution.
- **Using the API** – The ActiveX control interface can be used to integrate the SentiNET authentication directly into 3<sup>rd</sup> party applications.

During installation, the administrator selects the target server environment (IIS, Netscape or Apache) and the target URL which will be protected by e-SentiNET. Entering a blank URL will protect the entire site, whilst entering a directory/folder name will protect that directory and all sub-directories below it. If a mistake is made here, or should the requirements change, the only way to alter the protected directory is to make changes in the Windows Registry. We would hope that in a future release ISL will consider providing a more user-friendly means to amend the protected resource following installation.

Once e-SentiNET is activated the Web site can be accessed as normal until the user directs the browser to a URL within the protected area. At this point, the ISAPI filter looks for an e-SentiNET identifier (session cookie), and if this is missing the browser is redirected to the User Authentication page.



Figure 7 - Authenticating via e-SentiNET for Web page access

The authentication page loads and runs the e-SentiNET ActiveX Control, and the user is either prompted for their user ID (if no smart card is present) or the user credentials are lifted from the smart card. Clicking on the *Scan* link then causes the ActiveX control to initiate a fingerprint scan which is sent to the server for verification, or compared with the template stored on the smart card.

If the fingerprint does not match, access is denied. If successful, however, the e-SentiNET identifier (session cookie) is returned to the client browser which runs it through a hashing algorithm and reconnects with the user name and session cookie.

The ISAPI filter verifies this new connection passes it through to the protected page. The session cookie is stored locally for further validation until the web browser is closed down.

## Verdict

---

No one can pretend that the deployment of a biometric authentication system is easy. It is necessary to physically access every client machine, for example, in order to install the keyboard/sensor devices and the appropriate software. In large networks, that can be quite a daunting task.

Once that painful process has been completed, however, password management becomes much easier for both the user and the administrator. Traditional passwords can be eliminated altogether via the use of SentiNET's random password feature, ensuring that the smart card and fingerprint are the only methods allowed to access network resources (and also allowing the actual user passwords to be of a length and configuration that would be unfeasible for the average user to remember).

Apart from the few inevitable forgetful users who manage to lose their smart cards, requiring a re-enrolment process, the problems caused by forgotten passwords – and the costs associated with the resulting support calls – are all but eliminated. Even the lost smart cards are a non-issue, since they cannot be used without the corresponding finger of the original owner!

Security policy is also easier to define and manage, since it is no longer necessary to change passwords on a regular basis – the bane of most users' lives, and the prime cause of the Post-It note password crib sheet which is found hanging from many a screen or keyboard.

Although there are numerous biometric authentication systems available, one of the key advantages offered by the SentiNET solution is that no separate template database (often requiring a dedicated host) is required. Where tokens are not in use, then existing secure storage areas are used for the templates – in the form of the SAM or Active Directory – and existing management tools are used by the administrator throughout the system. The management burden is therefore reduced considerably.

In those environments making use of PKI, the new CSP integration capabilities also mean that users' digital certificates and private keys can be stored on the smart card during the certificate request process. Subsequent access to the certificate and keys is then controlled by the same fingerprint scanning operation that is used for network access.

Finally e-SentiNET takes biometric authentication onto the Web, controlling access to protected areas of the corporate Web site via that same smart card and fingerprint combination. One smart card – and one enrolment process – can thus provide numerous opportunities for securing corporate systems if all the SentiNET options are installed.

The net result of a move to biometric authentication should be a significant increase in security. The great thing about this system, however, is that the users will actually find the whole authentication procedure that much more straightforward.

Security really shouldn't be this easy!

## **Contact Details**

---

**Company name:** ISL (Informer Systems Ltd.)

**E-mail:** sales@isl-secure.com

**Internet:** <http://www.isl-secure.com>

**Address:**

Grosvenor House  
Market Street  
Bromsgrove  
Worcestershire  
B61 8DA  
United Kingdom

**Tel:** +44 (0)1527 571700

**Fax:** +44 (0)1527 571701