

**SecurSight™:
An Architecture
for Delivering
Secure Access
to Information**

INTRODUCTION

Security Dynamics Technologies Inc. (SDTI) – with its wholly owned subsidiary RSA Data Security – is the world leader in strong user authentication and encryption technologies. With more than 2.5 million SecurID tokens in use today and more than 300 million RSA encryption and authentication technologies installed worldwide, SDTI is the market leader in providing secure remote access to corporate networks. The introduction of SDTI's new SecurSight™ family of plug-in enterprise security solutions expands the Company's mission to provide customers with secure access to information wherever it resides in the enterprise. This paper provides an overview of the SecurSight products, and demonstrates how the SecurSight architecture uses industry-standard technologies to solve the problem of providing secure access to valuable business information, to enable new strategic applications, and to help companies implement business policy.

TABLE OF CONTENTS

INTRODUCTION	1
SECURITY OVERVIEW	3
DIGITAL CERTIFICATES: BUILDING BLOCKS OF ENTERPRISE SECURITY	4
SECURITY MANAGER: FLEXIBLE, SECURE MANAGEMENT	5
SECURITY DESKTOP: SECURE ENTERPRISE ACCESS	7
TWO-FACTOR USER AUTHENTICATION: SECURE ACCESS TO USER CREDENTIALS	8
SECURITY AGENTS: CONTROLLED ACCESS TO ENTERPRISE APPLICATIONS AND SYSTEMS	9
SECURITY AGENT TOOLKITS AND CDSA: BUILDING IN STANDARDS-BASED SECURITY	10
SECURE INFORMATION ACCESS: THE SALES PROFESSIONAL EXAMPLE REVISITED	10
SUMMARY: SECURITY ARCHITECTURE PRINCIPLES	12
ABOUT SECURITY DYNAMICS TECHNOLOGIES, INC.	13
GLOSSARY OF TERMS	13

SECURITYSIGHT OVERVIEW

SecurSight is a family of plug-in solutions that addresses a wide range of enterprise security needs, including: secure remote access via dial-up lines or virtual private networks; secure local network access; secure applications access for single sign-on, intranets and extranets; email security; and platform security for desktops and UNIX hosts. SecurSight is the integration of SDTI's traditional ACE/Server® product line and award-winning, patented SecurID® authentication with acquired technologies (the BoKS™ product line from DynaSoft AB, cryptography from RSA Data Security), and technologies gained through strategic relationships with partners that include Netscape, VeriSign and Worldtalk. SecurSight is the realization of SDTI's Enterprise Security Services strategy which was announced in 1997.

SecurSight is comprised of several principal components that are combined to create plug-in, interoperable enterprise security solutions: digital certificates, SecurSight Manager, SecurSight Desktop, SecurID strong user authentication, SecurSight Agents and SecurSight Agent Toolkits. While these products are based on sophisticated, state-of-the-art security technologies, the process of providing secure information access is virtually transparent to the end user. Further, these products can be added to an existing IT infrastructure in a modular, non-disruptive way, where and when they are needed.

Before examining each component in detail, it is useful to consider how they work together to solve a real-world information access security problem. Consider the example of a sales professional who needs secure access to pricing data stored in an Oracle database on the corporate network. To accomplish this task, the user simply needs to authenticate to the network and double-click on the application. In the SecurSight environment, the following transparent transaction occurs:

- 1) Using the strong, two-factor authentication of the SecurID token, the user authenticates to the SecurSight Manager.
- 2) The user's credentials – including certificates – are downloaded to the desktop.
- 3) The user launches the Oracle application.
- 4) The SecurSight Desktop automatically presents a certificate to the SecurSight Agent protecting the Oracle application.
- 5) An encrypted session between the user's SecurSight Desktop and the Oracle application server is automatically set up by the SecurSight Agent.
- 6) The SecurSight Agent automatically logs the user into the Oracle application.
- 7) The user gains secure access to the pricing data, and work ensues.

This sequence of activities is the product of the SecurSight components, which are built on an architecture that provides a pragmatic, standards-based approach to enterprise security. SecurSight is "securityware" – a set of products and technologies that can be deployed throughout a customer's heterogeneous computing environment in a non-disruptive way. To understand how this process works, it is necessary to examine each component in detail. At the end of this paper, we will revisit the sales professional example, and provide more detail on how secure information access is actually achieved.

DIGITAL CERTIFICATES: BUILDING BLOCKS OF ENTERPRISE SECURITY

Digital certificates ("certs") are one of the building blocks of enterprise information security, and a foundational element of the SecurSight architecture. A digital certificate – a file that holds the public key and other user information – is used to vouch for a user's identity, and as such, serves as a user's electronic credentials.

In a public key infrastructure (PKI) environment like SecurSight, each user "owns" one or more public/private key pairs. As the names imply, a private key is kept secret and a public key is publicly known. The combination of public and private keys provide for stronger security than any other encryption scheme available today. For example, let's say a user wants to send information to another individual. If the user encrypts the information with the recipient's public key (e.g., prior to transferring the information), that information can only be decrypted with the recipient's private key, and therefore is only available to the intended recipient.

The private key is only known to the user, and is typically stored in an encrypted file on the user's desktop or on a smart card – and, obviously, must never be made generally available on the network. The public key, however, is made generally available as an integral part of a digital certificate. Digital certificates may be stored in a number of locations on the enterprise network – typically, they are made generally available through a user database such as a directory.

Through the combination of the public and private keys, users can perform a wide range of security functions, including gaining access to enterprise applications and systems, encrypting and sending files, and signing documents with digital signatures. A digital signature is data that accompanies an encrypted file, and that can be used to verify the identity of the sender and to attest that the file has not been modified since it left the sender.

Digital certificates are created and issued by a Certificate Authority (CA), a trusted third party that functions much like a notary public to vouch for the authenticity of the user's information. While CAs are typically third parties, some enterprises choose to operate their own CAs. The actual digital certificate is a data file that contains personal information about a user –

SECURSIGHT:

AN ARCHITECTURE FOR DELIVERING SECURE ACCESS TO INFORMATION

including name, physical location, email address, name of the CA, valid dates for the cert, and the user's public key. This information, with the digital signature of the certifying CA, electronically "binds" the owner of the cert to their public key. Since certs can act as a user's electronic identity, they can therefore establish a trusted relationship to facilitate secure access to enterprise resources and to enable new applications with a high degree of security, like electronic commerce.

While digital certificates can be used to provide digital authentication in a number of security-related solutions, they are not fully secure without strong user authentication. While a digital certificate can attest to the validity of a public key credential – that is, that the public key is associated with a particular named individual – the cert alone cannot confirm whether the individual presenting the public key certificate as proof-of-identity is in fact the rightful owner.

Consider the analogy of a passport. A private key without strong, two-factor user authentication is like a passport without a photo of its owner. The passport may be an official document with accurate information about an individual, issued by an official government agency (like a CA). But without a photo to allow a physical authentication (like a token or smart card), there is no way you can be assured that the person presenting the passport (or private key) is the intended and rightful owner of it.

In a PKI, knowledge of the private key is taken as the sole criteria for certificate ownership and authentication of the electronic identity. Since certs are generally available to all enterprise users, private keys must be strongly protected in order to protect the use of electronic identities. Thus, in a PKI, protection of a private key is paramount, and software-only protection of private keys (i.e., via a password) is too easily defeated by any number of highly recognized and widely available methods of attack. In other words, a private key cannot be protected without strong, two-factor user authentication – secure use of PKI can only be achieved by assuring that only the intended owner of a private key has access to it.

SECURSIGHT MANAGER: FLEXIBLE, SECURE MANAGEMENT

SecurSight Manager provides the core security and administration services on top of which secure access solutions are built. As such, it provides a central point for implementing and managing the business policy specifying which users get access to what information resources. SecurSight Manager combines the time-synchronous authentication of ACE/Server with public key management, privilege management, audit and Certificate Authority services – all managed through a browser interface.

SecurSight Manager provides a range of security services. *Authentication* manages the process of authenticating users to network resources – to guarantee that users are who they claim to be – and therefore protecting user credentials. SecurSight supports a number of associated authentication

services, including Security Dynamics' traditional ACE/Server/SecurID, SDTI's new SSL v3-based client server security protocol (CSSP), and defacto industry standards such as RADIUS and TACACS+.

Privilege Management services track and control users' access rights to specific enterprise resources. In the same way that identity certificates are generated to vouch for a user's identity, privilege attribute certificates (PACs) are generated to vouch for which resources a user is authorized to access. PACs aid the performance and scalability of SecurSight by simplifying trust relations around privilege. Because their valid lifetime is short, "revocation lists" normally associated with identity certificates are not necessary. Since PACs are downloadable to any SecurSight Desktop, they provide users – wherever they are in the extended enterprise – with secure access to information, wherever it resides in the enterprise.

SecurSight Manager's *Audit* service provides audit logs that track all events, including user authentication, access to applications and systems, time of day, and location of access. The *Certificate Authority* is responsible for issuing and managing X.509 v3 digital certificates and integrates with SecurSight Manager. SecurSight Manager will also interoperate with other standards-based certificate authorities, including those from Netscape, Microsoft and VeriSign.

Key Management, which is closely related to the CA service, provides the range of services necessary to manage the generation, transport, revocation and renewal of public and private keys associated with certificate use. In addition, Key Management addresses key escrow and recovery services. Using the industry standard LDAP, the *Directory Server* services provide a mechanism for storing certificates and other user information in a standard directory.

The *Personal Security Device Manager* service supports the issuing and management of the personal security device (PSD), a secure container that holds a user's credentials and that can be downloaded to any SecurSight Desktop. The PSD is critical to the SecurSight functions involving portable enterprise credentials, and facilitates the realization of SecurSight security solutions, like secure single sign-on. Security Dynamics' branded PSD is called the SecurSight "Passport." The PSD will be discussed in greater detail in the SecurSight Desktop section of this paper.

SecurSight Manager features a *Browser-based Console*, ensuring that administrators can perform secure administration functions from any desktop anywhere. The Manager supports *Role-based Administration*, to let organizations define and distribute administrative roles throughout the enterprise.

Management in SecurSight is achieved via a hierarchical system of Managers, with multiple domains each managed by their respective Manager. This system allows SecurSight to scale to support large numbers of users across the extended enterprise. Supporting this hierarchy are the Replication and Cross-realm services.

**SECURSIGHT:
AN ARCHITECTURE FOR DELIVERING SECURE ACCESS TO INFORMATION**

Replication ensures that if one master Manager fails – due to network failure, hardware failure, etc. – there are multiple back-ups to service user access requests. *Cross-realm* services provide a method for a local Manager to query other Managers in the enterprise to locate user security information, if that information does not already reside on that local Manager. These services ensure that SecurSight Manager can scale to the global enterprise, and is "24x7," non-stop available. SecurSight solutions built over these services will also scale and be non-stop available accordingly.

The Manager takes advantage of many industry standards to ensure interoperability with leading enterprise management, Certificate Authority and directory service products. The Manager uses Java and C application programming interfaces (APIs) to interface with leading enterprise management products; PKCS #12 now (and PKIX in the future) to interoperate with standard CA products; and LDAP to facilitate the use of standard directory service products. In addition, the SecurSight components are designed meet the multiple language requirements of worldwide use. SecurSight Manager runs on Windows NT, Sun Solaris, HP-UX and IBM AIX.

SecurSight Manager services provide a complete framework for managing the life-cycle of digital certificates and the use of certificates to gain secure enterprise access. Just as a private key without strong user authentication is not fully secure, digital certificates without a management framework are effectively useless in the enterprise. SecurSight Manager, in concert with the other SecurSight components, has been engineered to provide a smooth migration path for current customers making the transition to PKI-based and other standards-based security.

SECURSIGHT DESKTOP: SECURE ENTERPRISE ACCESS

SecurSight Desktop provides users with secure access to resources from anywhere in the extended enterprise. SecurSight Desktop includes native support for both PKCS #11 and CSP. Through these interfaces, customers can access Web-based applications and S/MIME mail through either a *Netscape or Microsoft Browser*, while using SecurSight certificates.

The Desktop provides an *Applications and Domain Access* service, the core service associated with secure single sign-on and secure access to networked computers and applications. Once an application has been "registered" to utilize secure single sign-on, authorized users gain transparent access to it. With reduced or single sign-on, once a user has authenticated to the Desktop, they are transparently authenticated to applications and servers that otherwise would have required the user to enter additional passwords and/or other sign-on information.

As part of its local security services, the SecurSight Desktop includes SDTI's award-winning *File Encryption* technology to encrypt and protect locally stored individual files or folders, and a *Digital Signature* service for digitally signing and protecting the integrity of files. In addition, the Desktop provides

strong *Login* services, integrated with SDTI's strong authentication token technology and the Windows 95 and NT operating systems.

Critical to enterprise access, SecurSight Desktop includes the Personal Security Device (PSD), a secure container that holds a user's access credentials. The PSD, or "Passport," is a strongly encrypted file that holds a user's credentials: digital certificates; private keys; file encryption keys for encrypting and decrypting files locally; the SoftID seed value for using time-synchronous authentication and accessing ACE/Agents with a smart card; and legacy credentials (like passwords or tickets) for accessing proprietary or non-PKI applications.

The PSD is portable and can be downloaded at login to any SecurSight Desktop or, alternatively, can be stored on a smart card and carried by the user. As such, it provides a user with a means to securely access information from any SecurSight Desktop in the extended enterprise. Since the PSD contains the user's critical private key, it must be protected with strong, two-factor user authentication via a SecurID token or smart card. Two-factor user authentication is required before a PSD may be "unlocked" – that is, its contents made available to the user.

TWO-FACTOR USER AUTHENTICATION: SECURE ACCESS TO USER CREDENTIALS

As mentioned earlier, allowing for secure access through all entry points of the enterprise to applications and resources, and protecting the private key, are the critical elements of any PKI environment, including SecurSight. Security Dynamics has built its core business by providing strong, two-factor user authentication to enable secure remote access to corporate networks. The same strong, two-factor user authentication must be applied to protecting the private key, and thereby access to enterprise IT resources.

Two-factor user authentication is defined as something the user knows (a PIN) and something the user has (a token or smart card). SDTI authentication solutions have traditionally been implemented via SecurID hardware tokens, SoftID authentication software or SecurID smart cards, working in concert with the ACE/Server authentication server. This two-factor method provides significantly stronger security than traditional, static passwords, which are easy to guess or capture via "cracking" or "sniffing" programs, and which therefore put enterprise security in jeopardy.

Similarly, since programs are widely publicized and available to either divert desktop files or directly attack desktop password mechanisms, PKI or other products using passwords to protect digital credentials (i.e., the private key) force customers to employ weak user authentication in conjunction with strong digital authentication. The net result is weak security.

Using two-factor user authentication to protect a private key ensures that credentials are used only by their rightful, intended owner. While tokens are

SECURsIGHT:

AN ARCHITECTURE FOR DELIVERING SECURE ACCESS TO INFORMATION

often the user authentication method of choice today, over time smart cards will be used to protect digital credentials and to facilitate access to PKI-enabled applications. The SecurSight solutions have been built to support both the traditional, time-synchronous authentication methods, and the PKI authentication methods simultaneously. This means that users can leverage their existing investments in SDTI token technology while deploying PKI.

SECURsIGHT AGENTS: CONTROLLED ACCESS TO ENTERPRISE APPLICATIONS AND SYSTEMS

SecurSight Agents are deployed to protect specific applications and systems. SecurSight Agents work in concert with the SecurSight Manager and Desktop, to permit only those users who are authorized by policy to access applications, networked computers, and remote access devices including firewalls, virtual private networks, communications servers and others.

There are two types of Agents: 1) "Wrapper" Agents for legacy applications and systems, and 2) ACE/Agents for secure remote access via dial-up lines, the Internet (firewalls) or virtual private networks, as well as for local file and print servers. Agents are either available directly from SDTI or are available from our business partners, embedded into their products.

Wrapper Agents are software programs that "front end" existing non-PKI-aware applications, acting as a proxy server to the application and operating at the network layer (i.e., at the port level). Wrapper Agents provide security services transparently – without the need to re-write applications to gain access to certificate-based security services. Applications that have been "wrapped" are unaware of the presence of the Agent – the application performs as if SecurSight were not installed, but "listens" to the network and can accept connect requests only through the Agent's services.

Wrapper Agents build certificate-based services into applications running on UNIX and NT servers. The Wrapper Agents provide non-PKI applications with certificate-based authentication, privilege, session encryption, credential mapping, automatic sign-on and audit, all within the context of the SecurSight PKI environment. Wrapper Agents are available today for: applications, including Oracle, Informix and Sybase; networked computers, supporting Telnet and NT domain login; and Web applications via http. Additional Wrapper Agents for other application environments and systems will be available over time.

The second type of Agent is the ACE/Agent, which is part of the traditional SDTI solution for securing remote access and corporate networks. Through SDTI's partnerships with more than 70 leading security technology vendors, ACE/Agents are currently embedded in remote access devices, communications servers, firewalls, operating systems, virtual private networks and virtually any other product used today to protect the perimeter of the network and important network resources.

SECURITYSIGHT AGENT TOOLKITS AND CDSA: BUILDING IN STANDARDS-BASED SECURITY

SecurSight Agent Toolkits are sets of security tools and technologies that let independent software developers, consultants and customers develop and deploy SecurSight Agents for other third-party or internally developed applications. By creating and deploying Agents through a SecurSight Toolkit, the detail associated with coding and maintaining application-level security is virtually eliminated for the applications programmer.

The Wrapper Agent Toolkit lets application developers build Wrapper Agents for infusing standards-based PKI security into existing non-PKI-aware applications. Agents built via the Wrapper Toolkit plug-in seamlessly into the SecurSight PKI environment. The Wrapper Toolkit today leverages a number of security standards, including X.509 v3, RSA BSAFE™, PKCS and SSL v3.

Security Dynamics' vision of industry-standard security for the next generation of applications will be achieved by supporting CDSA in SecurSight. CDSA – the Common Data Security Architecture – is the emerging industry standard for IT security, endorsed by The Open Group and by leading IT vendors, including IBM, Intel, Netscape, GemPlus, Schlumberger, RSA, Security Dynamics and others.

By using RSA's Certificate Security Suite™ (CSS) – a set of APIs and components that let product developers embed standard, CDSA-based security in their applications – SDTI will ensure that SecurSight services are CDSA-compliant. Application developers will likewise use CSS (or other CDSA-compliant tools) to build CDSA awareness into their applications and systems, by coding security calls to the CDSA service APIs. These CDSA-compliant applications and systems can then plug-in seamlessly into the SecurSight environment, and leverage CDSA security natively (without the need to use Agents).

SECURE INFORMATION ACCESS: THE SALES PROFESSIONAL EXAMPLE REVISITED

Now, having reviewed each SecurSight component in detail, it is useful to revisit the example of the sales professional trying to access the Oracle database, to understand how this secure access to information was actually achieved:

- 1) Using the strong, two-factor user authentication of the SecurID token, the user authenticates to the SecurSight Manager.
- 2) If the personal security device (PSD) is not already present on the SecurSight Desktop, the SecurSight Manager transparently downloads the PSD with the user's credentials – including digital certificates – to the SecurSight Desktop and unlocks the PSD.
- 3) The user double-clicks on the icon to launch the Oracle application.

**SECURsIGHT:
AN ARCHITECTURE FOR DELIVERING SECURE ACCESS TO INFORMATION**

- 4) An identity certificate is automatically presented to the SecurSight Manager. The Manager uses that certificate to authenticate the user, and then checks its own privilege management service to determine whether this user is authorized by policy to access the Oracle application at this time.
- 5) If the user is authorized, the SecurSight Manager generates a privilege attribute certificate (PAC) – in X.509 v3 format – by using certain X.509 v3 extensions to add the user's local Oracle name and other privilege information to the general data already found the user's identity certificate. The PAC is then signed by the SecurSight Manager, which also acts as a "Privilege Authority."
- 6) The signed PAC is sent to the SecurSight Desktop.
- 7) The SecurSight Desktop presents the PAC to the SecurSight Wrapper Agent for Oracle. The Oracle Agent checks the certificate to verify that it is valid. If the certificate is valid, the Agent extracts the local Oracle user name.
- 8) Since the Oracle Agent is acting as a proxy for the Oracle application on the network, the Agent already has as part of its function a server identity certificate for the Oracle application. The Oracle Agent uses the PAC and server identity certificates in conjunction with SSL v3 to set up an authenticated, encrypted session between the SecurSight Desktop and the Oracle server.
- 9) Once the encrypted session is set up, then Oracle Agent uses the local Oracle user name (or other information) that it extracted from the PAC to assemble a standard Oracle login connection request for this application, and then passes that request to the Oracle server.
- 10) The Oracle server logs the user in, and the Agent generates and sends to the SecurSight Manager an audit record indicating that a sign-in has occurred.
- 11) The user securely accesses the pricing data from the Oracle database, and work ensues.

As mentioned earlier, through this entire transaction all the user "sees" is their login with the SecurID token, which is performed only once per session, and the Oracle application launch.

This is the realization of the SecurSight architecture, where state-of-the-art security technology has been applied to implement business policy. All of the SecurSight enterprise security solutions are similarly constructed, to help customers take a pragmatic approach in using certificates and security to solve business problems.

SUMMARY: SECURSIGHT ARCHITECTURE PRINCIPLES

Throughout this paper, and through the discussion of the SecurSight components, a core set of technology concepts and architectural principles were revisited time and again. These are the critical requirements which Security Dynamics holds as essential to delivering enterprise security solutions to customers:

- Use strong, two-factor user authentication to guarantee protected access to all entry points of the corporate network (local and remote), and to ensure that private keys associated with using certificates are strongly protected.
- Use public key certificate-based services for subsequent protected access from the desktop to applications and systems anywhere in the enterprise.
- Seamlessly support PKI-aware desktop applications from both Microsoft and Netscape.
- Deploy agents to ensure secure access to applications and systems, and therefore to information.
- Deliver wrapper agents for existing non-PKI-aware applications.
- Deliver native security support for applications via CDSA services and APIs, and other key industry standards.
- Deliver reduced sign-on today, with a commitment to single sign-on in the future.
- Deliver flexible, comprehensive management and audit security services, with mission-critical, 24x7 availability.
- Don't just deliver technology – deliver business solutions to customers.

The SecurSight family of plug-in enterprise security solutions builds on Security Dynamic's leadership role in securing remote access to corporate networks to provide customers with secure access to information wherever it resides in the enterprise. SecurSight solutions are industry standards-based, and can be deployed throughout the global enterprise in a modular, non-disruptive way, where and when they are needed. SecurSight is designed to help customers fully leverage existing investments in SDTI products and technologies, while they deploy PKI.

SecurSight addresses a wide range of enterprise security needs through a comprehensive set of security components, built on a standards-based architectural framework for supporting the implementation of business policy. As such, SecurSight can meet organizations' needs to conduct business securely, while protecting their corporate information assets.

ABOUT SECURITY DYNAMICS TECHNOLOGIES INC.

Security Dynamics is the leading provider of enterprise network and information security solutions that help companies conduct business securely, protect corporate information assets and facilitate business-to-business electronic commerce. With more than 2.5 million users of its SecurID® authentication technology, Security Dynamics is the world leader in strong user identification and authentication. Its wholly owned subsidiary RSA Data Security, Inc. is a leading supplier of software components that secure electronic data, with more than 300 million copies of RSA encryption and authentication technologies installed worldwide. RSA technologies are part of existing and proposed standards for the Internet and World Wide Web, ISO, ITU-T, ANSI, IEEE, and business, financial and electronic commerce networks around the globe.

GLOSSARY OF TERMS

Asymmetric Encryption	See Public Key Encryption.
Authentication	The process of identifying an individual to determine if he or she has the right to access a computer network, workstation or Web site. Authentication methods include passwords, SecurID tokens, smart cards and biometric devices.
Certificate Authority (CA)	A trusted third-party organization or company that issues digital certificates used to create digital signatures and public/private key pairs.
Certificate Security Suite (CSS)	A set of APIs and components from RSA that let product developers embed standard, CDSA-based security in their applications.
Common Data Security Architecture (CDSA)	An emerging industry standard for IT security endorsed by The Open Group and leading IT vendors, including IBM, Netscape, GemPlus, Schlumberger, RSA, Security Dynamics and others.
Digital Certificate	A file that serves as a user's electronic credentials. The certificate holds the public key and other user information that is used to authenticate a user's identity.
Digital Signatures	Data that accompanies an encrypted file, and that can be used to verify the identity of the sender and attest that the file has not been modified since it left the sender.
Encryption	The process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key.
File Encryption	This technology is used to encrypt and protect locally stored individual files or folders.

Firewall	A device (or software in a router) that links an organization's internal network to the Internet and restricts the types of traffic that can pass, to provide security.
Key Management	Closely related to a certificate authority (CA) service, it provides the range of services necessary to manage the generation, transport, revocation and renewal of public and private keys associated with certificate use.
LDAP	See Lightweight Directory Access Protocol.
Lightweight Directory Access Protocol (LDAP)	A simple protocol that allows users to access and search disparate directories over the Internet.
Local Authentication	The authentication that takes place when the user logs into a personal computer.
Personal Security Device (PSD)	The PSD or "Passport" is a strongly encrypted file that holds a user's credentials, including digital certificates; private keys; file encryption keys for encrypting and decrypting files locally; the SoftID seed value for using time-synchronous authentication and accessing ACE/Agents with a smart card; and legacy credentials (like password or tickets) for accessing proprietary or non-PKI applications.
PKCS	See Public Key Cryptography Standards.
PKI	See Public Key Infrastructure.
Private Key	Part of the public/private key pair, the private key is the only means to vouch for the identity of the owner of a digital certificate, which includes the public key.
Privilege Attribute Certificate (PAC)	A file generated to vouch for which resources a user is authorized to access, simplifying trust relations around privilege.
Proxy Server	A system that caches items from other servers to increase access speed. A proxy first attempts to find data locally, and if it's not there, retrieves it from the remote server where the data resides permanently.
PSD	See Personal Security Device.
Public Key Cryptography Standards (PKCS)	A set of standards for the implementation of public key encryption. Includes both algorithm-specific and algorithm-independent implementation standards.
Public Key Encryption	This encryption scheme use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it.
Public Key Infrastructure (PKI)	A distributed system of users and computers that verify the identity of a person seeking authorization to use a computer system or the network, and then associate a public key with that user in a highly secure manner.

**SECURsIGHT:
AN ARCHITECTURE FOR DELIVERING SECURE ACCESS TO INFORMATION**

Role-Based Administration	Allows organizations to define and distribute administrative roles throughout the enterprise.
RSA Public/Private Key	This is the most popular asymmetric encryption algorithm implemented for the authentication of users.
Secure Single Sign-on (SSSO)	The process by which a user authenticates once to gain access to multiple applications and resources without having to authenticate for each resource and manage multiple passwords.
Secure Sockets Layer (SSL)	An open standard proposed by Netscape Communications for providing secure (encrypted and authenticated) WWW (and other applications, such as mail, FTP and Telnet) service over the Internet. Uses RSA public-key encryption.
Securityware	A set of products and technologies that can be deployed throughout a heterogeneous computing environment in a modular, non-disruptive way.
SecurSight	The Security Dynamics family of standards-based, plug-in enterprise security solutions that address a wide range of security needs, including secure remote access via dial-up lines or VPNs; secure network access; secure application access for single sign-on, intranet, extranet, and email security; and platform security for desktops and Unix hosts.
SecurSight Agent	Software programs that "front-end" an application server and transparently provides security services without the need to modify applications.
SecurSight Agent Toolkits	Enable developers to create and deploy SecurSight Agents for other third-party or internally developed applications and other security domains.
SecurSight Authentication	Stands for strong, two-factor SecurID authentication in multiple form factors, including tokens, soft tokens, software smart cards and smart cards.
SecurSight Desktop	Provides users with a launching pad to securely access resources from anywhere in the extended enterprise. It includes strong encryption functionality to protect locally stored files, as well as secure single sign-on (SSSO) capabilities from the desktop to mission-critical applications and servers. It stores authentication credentials, including digital certificates, in a PSD residing on the desktop.
SecurSight Manager	Provides the core security and administration services on top of which secure access solutions are built. As such, it provides a central point for implementing and managing the business policy specifying which users get access to what information resources. SecurSight Manager combines the time-synchronous authentication of ACE/Server with public key management, privilege management, audit and Certificate Authority services - all managed through a browser interface.
Secure/Multipurpose Internet Mail Extensions (S/MIME)	A protocol that adds digital signatures and encryption to extended Internet electronic mail.
Session Encryption	When the information transferred between two hosts is encrypted to ensure the privacy and integrity of the data.

Smart Card	A plastic card, similar to the size and shape of a credit card, that contains a microprocessor chip with both secure storage of public/private key data and cryptographic processing capabilities.
S/MIME	See Secure/Multipurpose Internet Mail Extensions.
SSSO	See Secure Single Sign-on.
SSL	See Secure Sockets Layer.
Symmetric Encryption	See Private Key Encryption.
Two-Factor Authentication	A form of authentication that requires two distinct items to ensure user authenticity. Factors could include a token, personal identification number (PIN), biometric or smart card. A bank-issued ATM is the most common example of two-factor authentication.
Virtual Private Networks (VPNs)	Provide the medium for using the public Internet backbone as a channel for private data communication to connect multiple remote users or remote offices to an enterprise network.
Wrapper Agents	Software programs that "front-end" legacy, non-PKI-aware applications and systems to transparently provide security services such as certificate-based authentication, privilege and session encryption.
x.509 Certificate	A container for subject related information. The x.509 certificate contains, for example, the Distinguished Name, the RSA Public key, the issuer and digital signature.

SecurID and ACE/Server are registered trademarks, and BoKS and SecurSight are trademarks of Security Dynamics Technologies, Inc. BSAFE and RSA Certificate Security Suite are trademarks of RSA Data Security, Inc. All other products and service names mentioned herein are trademarks of their respective owners.

©1998 Security Dynamics Technologies, Inc. All rights reserved.

Printed on recycled paper.

SS AWP 0398

SecurityDynamics