

BoKS Overview

Enterprise networks must increasingly take a global view of security and invest in security solutions today while preparing for the future. The explosive growth of distributed networking and the migration of private network applications to the Internet are among the drivers for increased corporate requirements for security.

Securing remote access is critical, but companies are realizing it is no longer sufficient just to protect the periphery of the network. Public networks have pushed their way into the operations of most corporations, making it necessary to protect information wherever it resides in the enterprise. Security Dynamics responds to this trend by providing security solutions that protect information, both inside and outside the corporate walls.

ENTERPRISE-WIDE SECURITY

Organizations need to implement long-term application security strategies, but many of the technologies to guarantee security are not yet available from any vendor. Security Dynamics has the most complete family of security products in the industry, and is building on its market-leading product base to enterprise-wide security solutions that further help customers conduct business securely, protect corporate information assets and facilitate electronic commerce.

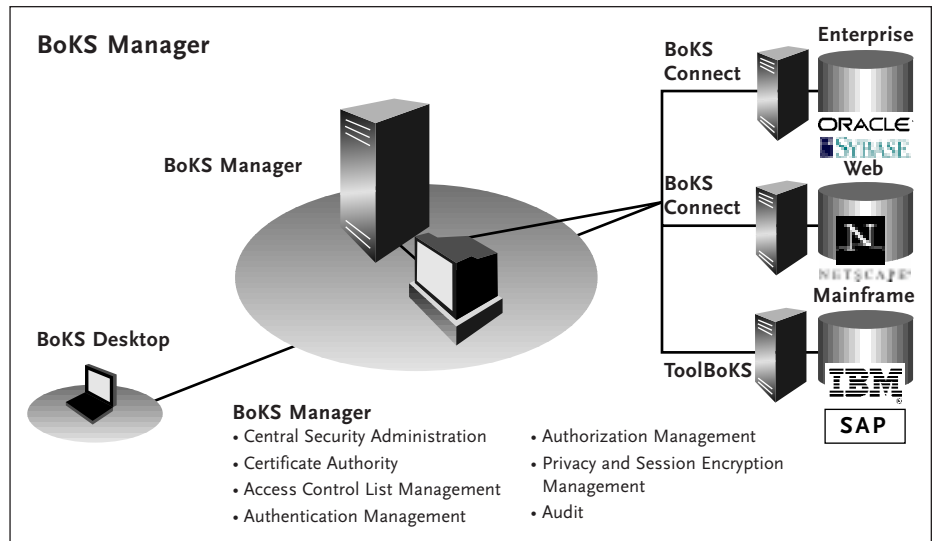
In July 1997, Security Dynamics acquired Sweden-based Dynasoft AB and its BoKS product line (“BoKS” is a Swedish acronym for access control system). The BoKS technology is integrated with the ACE/Server product line to provide Secure Single Sign-On (SSSO). The new BoKS product family release has many major technical advancements and user benefits, most of which can be categorized into the following two areas:

- **Secure Information Access** — BoKS provides secure access to distributed applications and databases, and allows enterprise networks to establish and enforce access security policies. It also offers SSSO to simplify user access to enterprise application and streamline security administration.
- **Unix Host Security** — BoKS is a complete security management system for distributed Unix environments. It provides the Unix access control and auditing features required for mission-critical environments. BoKS also provides the fault tolerance and scalability required to build and manage distributed business applications.

THE BoKS SOLUTION

BoKS is a set of integrated products that form an enterprise-wide security solution. It is proven and established technology, with a large number of established reference sites. BoKS is a powerful solution that combines strong user authentication, application session encryption, platform security and auditing features to allow users to realize Secure Information Access. At a time when most companies are only talking about it, Security Dynamics is delivering a solution that give customers secure access to information throughout the enterprise, including their legacy systems, and facilitating SSSO to enterprise applications.

BoKS OVERVIEW



The BoKS product family is comprised of:

- BoKS Manager for security administration and control
- BoKS Desktop for secure client access to enterprise resources
- BoKS Connect modules for Secure Information Access to several established application environments
- The ToolBoKS toolkit for creating Secure Information Access to custom or third-party applications.

BoKS Manager

BoKS Manager 4.4 provides strong authentication, access control, centralized management, system monitoring and auditing for an entire network of heterogeneous computers and applications. It runs on major Unix platforms, including Solaris, HP-UX and AIX. Enterprise networks can assign access rights for individuals or groups from a single point of control, and can manage the security of Unix servers throughout the enterprise.

Security server database replication is included for high availability. This allows BoKS Manager to scale to support large-scale enterprise applications, but BoKS Manager can also be used as a standalone product that tightens the security on a single workgroup server.

BoKS provides management of Public Key Infrastructure (PKI), providing security and scalability for networks that can grow to support more than 100,000 users. This approach provides the management and flexibility required to deliver enterprise security. BoKS Manager now provides administration of Personal Secure Devices (PSDs), which are secure containers for user information.

The PSDs can be encrypted files stored on the desktop computer, or can be stored in memory chips on smart cards, which are about the size of a credit card and can be carried by the user. The BoKS directory service is provided to simplify PSD distribution and automatically download user PSDs and certificate revocation lists to BoKS Desktop clients.

BoKS offers features that make it easy for users to automatically obtain and use their access credentials from any desktop, and for systems managers to issue, update or revoke credentials contained in PSDs from a central point of management. Since security is no longer dependent on port location, security administration can now provide “free seating.” BoKS also allows administrators to assist users even when their computers are off-the-network, such as when laptop users are having difficulty logging into their computers prior to attempting to dial-in for network access.

BoKS offers interoperability with certificates issued by certificate authorities other than the BoKS manager. This means that PSDs can be issued and managed within BoKS regardless of the origin of users’ public key certificates. This capability is important to the phased deployment of public keys within the enterprise, and assures customers that they have wide choice of certificate authorities as their enterprise need for certificates changes.

BoKS Desktop

BoKS Desktop provides SSSO capabilities from any of the common desktops mission-critical applications and servers. It also allows the client desktop to access to mission critical applications running on mainframes, Unix servers, and Windows NT servers. BoKS Desktop Version 1.4 runs on Windows 3.X, and BoKS desktop Version 2.2 runs on Windows 95 and Windows NT.

Both current versions of BoKS Desktop share common security features, including: protection against unauthorized login and from unauthorized session takeover; SSSO to a host computer or server application; support for encryption of an application session or file transfer; and digital signatures. Each has additional security features tuned to the requirements and functionality of the supported Windows operating system.

BoKS Connect Modules

BoKS Connect Modules offers SSSO to computers and to major enterprise applications, including Telnet, Oracle, Sybase, Informix and HTTP. BoKS Manager and BoKS Desktop are prerequisites for the use of BoKS Connect Modules, which are centrally managed by BoKS Manager and offer client access through BoKS Desktop. BoKS Connect Modules supports strong, two-factor authentication and play a critical part in the Security Dynamics application security strategy by delivering secure information access to major enterprise applications.

BoKS OVERVIEW

ToolBoKS Toolkit

ToolBoKS is a toolkit used to implement security functions and SSSO within existing computer environments and applications by wrapping legacy communications. It is a development platform for software engineers to integrate Secure Information Access to third-party environments. They can transparently implement SSSO functionality to existing “off-the-shelf” applications, legacy environments and network domains.

For applications which embrace the BoKS single sign-on architecture directly, ToolBoKS can relieve the application programmer from almost all detail associated with coding and maintaining application logon-related security. It enables implementation of numerous applications such as secure mail, secure Internet services and secure electronic commerce.

ToolBoKS also supports digital signatures and allows organizations to implement Access Control to applications by multiple, user-defined parameters. ToolBoKS can be used to implement a plug-in that provides digital signatures, providing the functionality needed for all applications related to electronic commerce and home banking. ToolBoKS can also serve as a general-purpose auditing tool for application connectivity.

BoKS PROVIDES SECURE INFORMATION ACCESS

BoKS counters possible threats to Intranets by providing integrated security “barriers” at the desktop, network and server. It strongly authenticates users at the desktop, subjecting them to user-established security policy controls and then protects the session over the network and provides access controls and integrity checks for enterprise servers and data.

It is built on proven technology that is today securing many mission-critical applications. BoKS Manager resides on a Unix server and controls access by acting as the “trusted third party” which mediates and authorizes requests by users to applications and Intranet servers. It is designed to be available on a 24-x-7 basis to provide centralized security policy management.

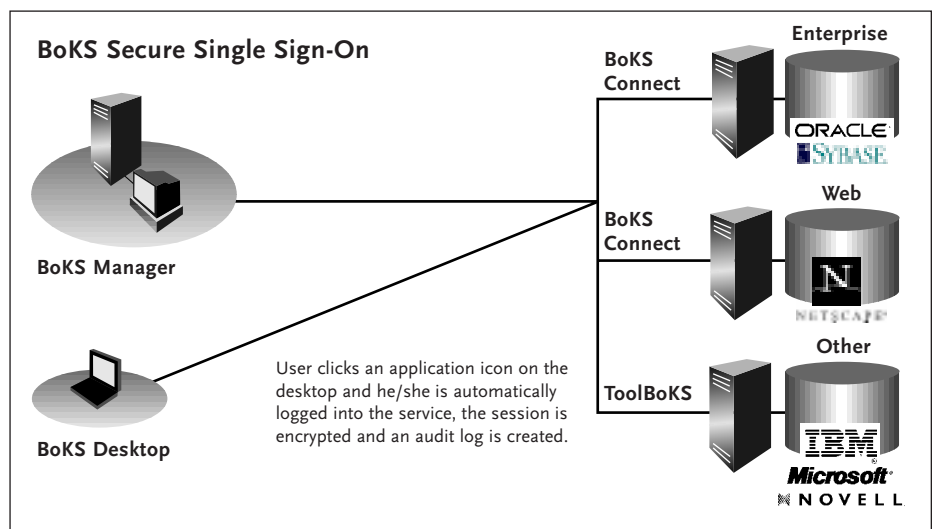
BoKS uses RSA public key cryptography for authentication of both users and hosts on the network, and uses strong cryptography for privacy. It also offers exportable cryptography for supporting applications and users located outside the United States. BoKS Manager uses a secure communications protocol to protect its own internal communications, such as replication of the security database, distribution of policy updates and authorization decisions, and transmission of audit records. BoKS Manager uses these cryptographic techniques to identify and protect user sessions and to separate all communication from protected communication internal to the BoKS solution.

This comprehensive use of cryptography for authentication and privacy, along with centralized, policy-based access authorization, protects against network attacks. BoKS offers a centrally-consolidated, online audit service that

adds the ability to log and profile Intranet activity and server status so that authorized activity can be monitored and unauthorized activity can be quickly discovered and prevented.

Secure Single Sign-On

Security Dynamics offers a flexible solution for simplifying SSSO with the new release of BoKS. Traditional Single Sign-On solutions offer automatic login procedures built on top of existing applications. The user's ID and password are stored in the desktop or in a file server, and the login information is sent unencrypted over the network. However, this traditional approach poses scalability, management and security problems.



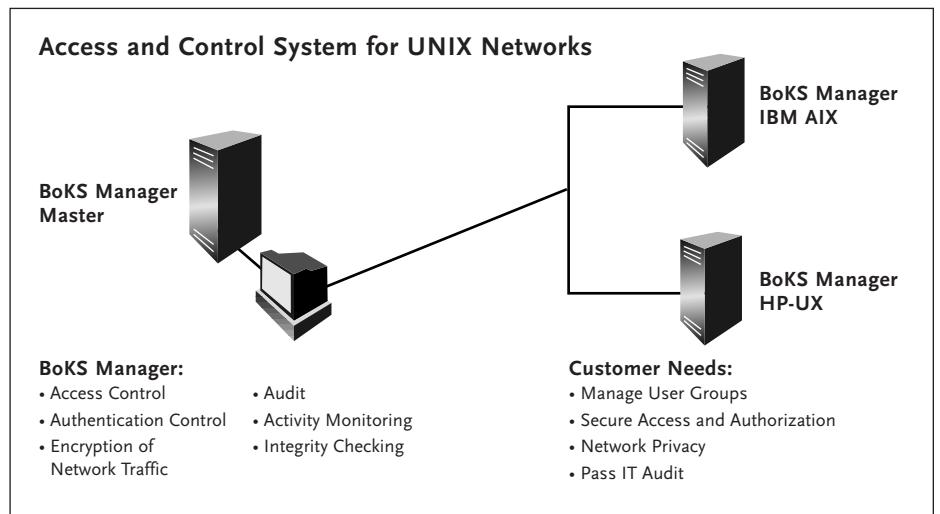
Unlike traditional security solutions that rely on static passwords, BoKS provides the ability to manage PSDs, such as smart cards. The BoKS SSSO solution is based on four key elements that overcome traditional security obstacles:

- Desktop protection
- Server and workstation protection with BoKS Manager
- Database and application protection, using BoKS Connect
- Communications protection using strong authentication and session encryption between the desktop and the server

The BoKS SSSO solution therefore provides integrated security barriers at the desktop, network and server to protect enterprise information.

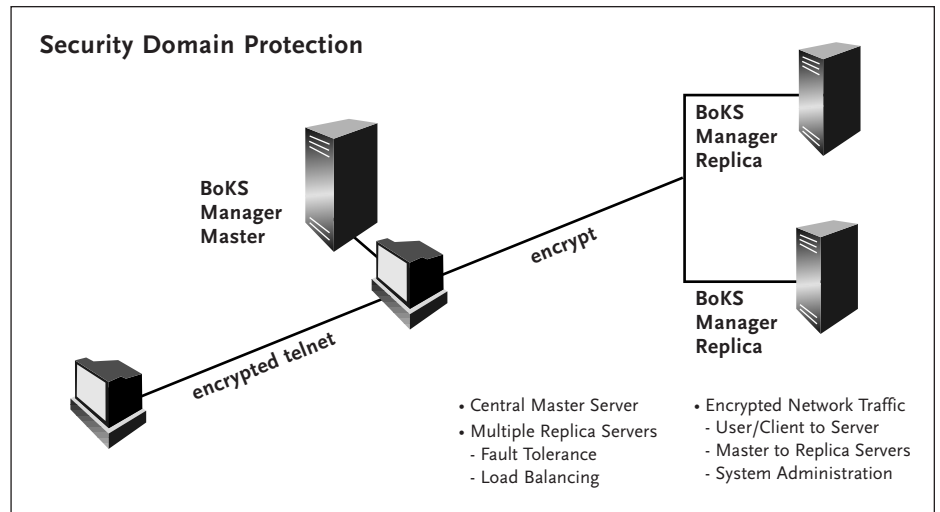
UNIX HOST SECURITY

Many organizations rely on BoKS to provide Unix host security throughout the distributed network. BoKS is a complete security management system for distributed Unix environments. It assigns user access authorization and regulates access to sensitive network resources. BoKS Manager is integrated with ACE/Server, which utilizes patented technology that synchronizes each token and authorizes access to valid users. BoKS supports non-obtrusive Unix host authentication, allowing easy access to Unix commands without any changes in the Unix kernel. Access is controlled by the use of standard Unix commands, such as *ftpd*, *rexecd*, *login*, *xdm*, *su*, etc.



Security Domain Protection

BoKS Manager enables network security administrators to control a network of Unix computers as a security domain comprised of one master, one or several replicas, and any number of clients. The master contains the sole read/write security database and implements all security administration. It answers requests from the clients in the security domain, serving as the “trusted third party” to mediate and authorize user requests for access to applications and Intranet servers.



Each replica can work independent from the master, but has a read-only security database which is updated by the master. A replica can be converted to become the new master if the master server fails. The BoKS clients access either a replica or the master for credentials. This architecture provides both fault tolerance for non-stop performance and allows simplified scalability.

BoKS Manager offers both integrity checking of the file system and secures configuration management for all computers in the security domain. It also implements continuous system load balancing. The master or any of the replicas can service a request from any BoKS Client, allowing the servers to cooperatively manage client access. This becomes critical as networks scale and support thousands of users logging into a large security domain. BoKS Manager therefore scales extremely well, with the current spectrum of installations ranging from a single Unix host to more than a thousand Unix systems in mission-critical environments serving thousands of users.

Security Administration

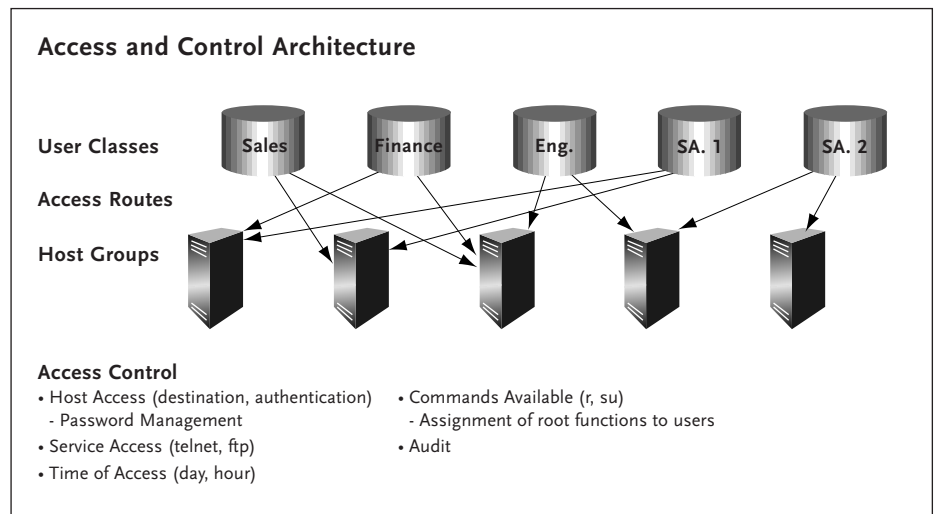
The secure interface provided by BoKS Manager is run from a standard HTML Web-browser, such as Netscape Navigator, Microsoft's Internet Explorer, or the character-based Lynx browser. The security domain can be administered locally at the master node, or from a remote workstation protected by BoKS Desktop.

User access is managed from a single point, even across heterogeneous environments. Security management of users is performed from the User Administration menu, which allows security administrators to create, import, modify, delete and list user account information. Individual users can be classified into User Classes and assigned similar access rights and

BoKS OVERVIEW

authorization restrictions. In this way, user access may be defined and managed according to business policies, using parameters such as job function or workgroup.

BoKS Manager allows security administrators to gather hosts into host groups. Host groups are used to simplify actions that are common for a group of hosts, and can be used to restrict the access of defined classes of users to identified hosts. A single host can belong to several different host groups, allowing great flexibility in customizing security policies. The grouping of hosts greatly simplifies host administration, which can be performed centrally.



Unix Host Monitoring

BoKS provides extensive monitoring of Unix hosts. They can be monitored for inactivity levels that can be defined either globally or per user. Inactive users can be automatically locked out of enterprise applications.

BoKS includes an integrity checker for key file systems, operating systems, utilities and even applications. Remote Unix hosts can be interrogated to assure the appropriate system file permissions, user start-up file permissions, password integrity and the existence of appropriate Unix setup scripts.

The daemon-based file monitoring features compare the current checksums of files to baseline checksums on a configurable time basis. Different files are included in the file monitoring depending on the assigned security level.

Auditing and Reporting

The BoKS logging system covers changes to security parameters and access attempts. All changes to the security database are audited, providing a clear information trail of changes, access attempts, alterations to specific files, and alarms. BoKS allows organizations to centrally administer, assign and cancel passwords. Security administrators can generate lists of banned passwords, and can establish parameters on password formatting, lifespan and length.

The system log covers any action carried out in BoKS Manager that affects the security database, such as the creation of a user, changes to security parameters or registration of a new host. The session log covers logins and logouts, unsuccessful login attempts and password changes. BoKS Manager can monitor inactive login-sessions, and enforce a login policy based on defined parameters, such as the length of password or the time between password changes.

A number of pre-defined reports are available via the graphic interface, and custom reports can be created. All logs are stored in standard ASCII, supporting integration with external Unix report generation tools.

Authentication Security Policies

BoKS provides extensive support for establishing and enforcing authentication security policies. For each user or user class, the network security administrator can define the available access methods and hosts. They can also define authentication policies according to time-of-access or by source computer.

The encryption method can be set by access route, with encryption activated on routes where both the client and the server support the secure communication protocols. BoKS supports a broad range of authentication methods, including SSSO, password and standard Unix authentication procedures.

Enhanced Root Protection

BoKS Manager provides enhanced features for protecting the root account responsible for top-level security. Network security administrators can set up access routes to restrict root from login by using any of the access methods. BoKS Manager regularly runs integrity checks to discover any incorrect system configuration that could have resulted in a user gaining root access.

The inactivity control in BoKS Manager automatically locks any unattended root windows, thus limiting the risk of an intruder using an unattended terminal or desktop. Administrators and sub-administrators can be defined throughout the network with varying security authorization levels. This increases scalability and allows configuration by the administrators themselves without changes to the root identity.

BoKS OVERVIEW

BoKS Manager allows users to execute specific programs with root privileges through its suexec utility. The BoKS Manager's Execute Program as Root option provides administration of the programs that users are allowed to execute. When users want to run programs with root privileges, they type suexec <program name> and are then prompted for a password. The suexec utility therefore provides the optional ability to let users run programs with root privileges without providing them with the root password.

BoKS PROVIDES ENTERPRISE SECURITY

The new BoKS release provides Secure Information Access to enterprise applications, and Unix Host Security for distributed client/server applications. As computing and communications resources continue to become more distributed, control over enterprise information will become an even greater asset. Security Dynamics will continue to expand its portfolio under its Enterprise Security Services (ESS) architecture, providing a complete, global, enterprise security solution.

Security Dynamics protects investments in security by migrating existing technologies under a common umbrella. As the BoKS technology becomes further integrated with Security Dynamics products and technologies, organizations can continue to develop and implement security solutions under the ESS architecture. Customers can realize Secure Information Access and implement Unix Host Security today, while relying on ESS as a technology roadmap for planning their own long-term security migration path.

ABOUT SECURITY DYNAMICS TECHNOLOGIES

Security Dynamics is the leading provider of enterprise network and data 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 two-factor user identification and authentication. RSA Data Security, Inc., a wholly owned subsidiary of Security Dynamics, 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. Security Dynamics and RSA can be found on the World Wide Web at <http://www.securitydynamics.com/> and <http://www.rsa.com/>, respectively.

GLOSSARY

Access Method	Used in access routes for BoKS Manager users or user classes. The access method is the program used for access.
Access Route	An access route determines if a BoKS Manager user has access to a service on a BoKS Manager Host. The access route consists of access method, from host (source), and to host (destination). It is dependent on what day it is, and what time of the day it is.
Asymmetric Encryption	Encryption based on a key pair. The most commonly used algorithm is the RSA Public/Private algorithm.
Authentication	The process of identifying an individual to determine if he or she has the right to access a computer network. Authentication methods include password, SecurID token, smart cards and biometric devices.
BoKS Manager Client	BoKS Manager hosts with no security database. BoKS Manager clients are typically application servers and workstations.
BoKS Manager Host	A host protected by BoKS Manager. It can be the master, a replica, or a client.
BoKS Manager Master	The BoKS Manager host where all administration takes place and where the security database are located. There can only be one master per security domain.
BoKS Manager Replica	One or more BoKS Manager hosts that stores a read-only copy of the security database, and optionally the security logfile. The replicas are updated from the master.
BoKS Manager User	A user in the security domain. The syntax for the BoKS Manager user is either host:user or host group:user. The BoKS Manager user will have an account on either the host, or on all the hosts in the host group.
CA	See Certificate Authority.
Certificate Authority	A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.
Client	See BoKS Manager Client.
DES	A symmetric encryption algorithm suitable for session encryption.
Desktop	Used in BoKS Manager to separate personal computers from other hosts in the security domain. A desktop is a personal computer with BoKS Desktop installed.

BoKS OVERVIEW

Desktop Protection Keys	Symmetric encryption keys stored on the PSD. They are used to encrypt and decrypt files on local disks, or on file servers.
Digital Signature	A digital code that can be attached to an electronically transmitted message that uniquely identifies the sender.
Distinguished Name	A unique name that identifies a subject within a certain issuer.
Encryption Method	The encryption method determines if and how communication between the hosts in the access route shall be encrypted. Options are DES, ND2, or No encryption.
From Host	The host or host group from which an access method, an authentication method, or an encryption method is defined.
Hashing Algorithm	Used when creating a digital signature. The hashing algorithm creates a checksum for a set of data.
Host	In BoKS Manager, this is a computer with an IP-address.
Host group	A set of hosts in the security domain. A host group is used when creating access routes and setting up authentication methods and encryption methods. It is normally also used when creating BoKS Manager users. The advantage by using host groups is mainly to simplify administration.
Host PSD	A PSD that must be installed on all BoKS Manager hosts when the encryption method DES or ND2 is to be used. The RSA key pair in the host PSD and the RSA key pair in the user PSD are used to securely negotiate for a session key.
Integrity Check	A function used to check that the BoKS Manager host has not been compromised. For example, the integrity check includes checking for trojan horses and changed access rights for files.
Issuer	The CA that issued an X.509 Certificate. To verify a X.509 Certificate, the RSA Public Key for the CA is needed. The RSA Public key can be found in the X.509 Certificate.
Local Authentication	The authentication that takes place when the user logs in to a personal computer.
Master	See BoKS Manager Master.
MD5	A hashing algorithm.
ND2	A symmetric encryption algorithm used for network encryption in the Global version of BoKS Manager.

NIS+	NIS+ (Network Information Service) is a distributed database that enables several machines to share, for example, the password and group files. BoKS Manager can import user data from the NIS+ database.
Other Host	The type of host used in BoKS Manager to define a host that is neither an BoKS Manager Host nor a Desktop.
PCPROT PSD	A PSD used to sign desktop protection keys. It is useful since it means that the private key for the CA does not have to be spread within the security domain.
PE PSD	The PSD whose private RSA key was used to encrypt the PSD password, normally for a User PSD. The PE can either be the CA itself, or a separate PE. A separate PE is signed by the CA.
Personal Security Device (PSD)	A smart card or an encrypted file. The PSD contains information about the subject including the subject's X.509 certificate and RSA private key.
PSD	See Personal Security Device (PSD).
PSD User	This is the user identification in the X.509 certificate in the PSD. The PSD User is what the user logs in to on a personal computer running BoKS Desktop.
Replica	See BoKS Manager Replica.
RSA Public/Private key	This is an asymmetric encryption algorithm which is very widely used. It is used for local authentication on the personal computers with BoKS Desktop, and for secure single sign-on to BoKS Manager hosts.
Secure Single Sign-on	The process when a user logs into a BoKS Manager host using cryptographic methods. No passwords are transferred, and the login process cannot be repeated.
Security Database	This is database used in BoKS Manager. The security database contains all security related information use by BoKS Manager except for the audit information which is found in the security logfile.
Security Domain	All the hosts and users that in some perspective are known in the security database.
Security Logfile	The file where all auditing within the security domain is stored. The security logfile is maintained by the BoKS Manager master.
Session Encryption	When the information transferred between two hosts is encrypted. In BoKS Manager this can be between a personal computer and an BoKS Manager host, or between two BoKS Manager hosts.

BoKS OVERVIEW

Session Key	A symmetric key used for line encryption. A session key is negotiated using the users RSA key pair, and the hosts RSA key pair.
Signing	The mechanism when the RSA Private key is used to encrypt a hashsum.
SSO Administration	The administration that deals with services using secure single sign-on and network encryption.
Sub-Administrator	A user that has been given limited rights to administrate the BoKS Manager system.
Subject	A user, a host, a PE (See PE PSD), or a PCPROT (See PCPROT PSD).
Symmetric Encryption	Encryption based on the fact that the two parties who want to share information, uses a common, secret key only known by the two parties.
Unique User Identifier	The identifier that links a user PSD to the BoKS Manager user. It can be a serial number, or an ASCII string. It must be unique for each BoKS Manager user in the security domain.
User Class	A set of BoKS Manager users. The user class is used when creating access routes. Access routes are assigned to a user class. Users assigned to a user class inherits all access routes that have been assigned to the user class.
User PSD	The PSD that is issued for users that shall be able to log in to a personal computer with BoKS Desktop, and potentially perform secure single sign-on to an BoKS Manager host.
UUID	See Unique User Identifier.
Verifying	The mechanism to verify a signed message. Verification is performed using the RSA Public key (which can be found in the X.509 certificate).
X.509 Certificate	A container for subject related information. The X.509 certificate contain, for example, the Distinguished Name, the RSA Public Key, the issuer, and a digital signature.

*Security Dynamics and the Security Dynamics logo are trademarks of Security Dynamics Technologies, Inc.
All other trademarks are the property of their respective owners.*

©1997 Security Dynamics Technologies, Inc. All rights reserved.

C Printed on recycled paper.

SWP03

SecurityDynamics®

Corporate Headquarters: 20 Crosby Drive, Bedford, MA 01730 USA, Tel 800 SECURID or 781 687 7000 Fax 781 687 7010

European Headquarters: United Kingdom, Tel 44 1734 795822 Fax 44 1734 795833 | **Asia/Pacific Headquarters:** Singapore, Tel 65 733 5400 Fax 65 733 2400

Email: info@securitydynamics.com **Internet:** www.securitydynamics.com