

Security BOX ENTERPRISE



Security BOX Enterprise is a security solution meeting the data confidentiality, integrity, and authenticity information requirements of businesses.

Security BOX Enterprise has application components guaranteeing the confidentiality of data shared, stored or exchanged via e-mail clients. Security BOX Enterprise also offers safe deletion and the digital signing of files, a unified connection with the Windows system, as well as security token or smart-card support. Security BOX Enterprise can protect information on all types of terminals: desktop computers, file servers, USB keys, PDAs, and smart phones.

Thanks to its administration tools, Security BOX Enterprise lends itself to easy, large-scale rollouts, in keeping with the enterprise's security policy.

A comprehensive modular suite



Security BOX Team

The Security BOX Team is used to define security rules both on desktop computers and on file servers used as a shared area.

Any files contained, copied or created in these secured folders are encrypted "on-the-fly", in an entirely transparent manner, without any user intervention.

Security BOX Team is designed for deployment where multiple users need simultaneous, ongoing access to confidential information stored in shared files – for example, key R&D projects, private asset management in the financial industry, or supply-chain strategies in manufacturing.

The security rules are defined by the security administrators, project managers or users themselves.



Security BOX Mobile

Security BOX Mobile is the security solution for PDAs and smartphones. It includes user authentication, confidentiality of locally-stored files and personal information, and the

confidentiality of email – including attachments – downloaded and stored on mobile devices. Supported on Microsoft Windows Mobile*, Security BOX Mobile integrates seamlessly into existing security infrastructures protecting sensitive information against the loss or theft of mobile devices.

Security BOX Mobile can be used to implement secure push mail functionalities.

* list of peripheral devices available at <http://www.arkoon.com/mobile>



Security BOX Disk

Security BOX Disk implements a digital data vault for individual use. Encrypted data is stored in a virtual volume, decrypted only when access is required, on the fly. Only the authenticated, authorized user has access to the information.

Security BOX Disk ensures absolute confidentiality of sensitive data on lost or stolen PCs or a removable device (USB key).



Security BOX Mail

Security BOX Mail is the email client security component of Security BOX Enterprise. It provides for digital signature and information confidentiality for incoming and outgoing

email, internal to the enterprise or in external (third party) exchanges. Security BOX Mail is compatible with S/MIME and X.509 to deliver the highest levels of security while remaining fully compatible with other standards-compliant solutions.



Security BOX File

Security BOX File delivers "on demand" encryption and decryption of individual files when saved to non-secure media or for transfer by non-secure channels data

encryption (and decryption) so that the Security BOX encryption can be integrated into application scripts.

Security BOX File can also be used to communicate with people who do not have the Security BOX solution, doing so by generating self-extracting encrypted files.



Security BOX Shredder

Security BOX Shredder is a secure, irreversible way to delete the content of files.

Security BOX Shredder can also be used to efficiently and safely delete files in the Windows recycle bin.



Security BOX Sign

Security BOX Sign is the digital signature component of Security BOX Enterprise, certifying any type of document to facilitate electronic transactions for business and

administrative procedures. Drag-and-drop functionality makes it extremely simple to use, generating a signed, encapsulated file in CMS format.



Security BOX MANAGER

Security BOX Manager allows the creation and management of user accounts, private keys and certificates, and the deployment of a simplified certificate policy.

Security BOX AUTHORITY MANAGER

Security BOX Authority Manager is the full featured management tool for Security BOX Enterprise. Adapting to the most demanding enterprise policy management requirements, Security BOX Authority Manager implements multi-level certificate authority functionality. It supports simultaneous local and remote access for multiple administrators with differentiated rights and roles. Hardware Security Modules are supported for secure generation and storage of CA keys. Security BOX Authority Manager can be used in client/server mode via Internet Explorer.

Specifications



Strong Authentication

Security BOX uses connected (logon) mode for access to the user's security account. User secrets are implemented through management of password complexity, smartcards, and security tokens.

Certification

The Security BOX cryptographic library is Common Criteria certified at level EAL4+.

Key-management

In order to guarantee safe data exchanges, Security BOX comes with a key-management infrastructure (PKI) to generate, certify, publish, and revoke keys and certificates. The Security BOX's solution can interface with enterprise PKIs already installed.

The Security BOX produces and uses digital certificates respecting the X509 V3 standard. It manages the extensions and attributes required for e-commerce, the dematerialization of information.

Security BOX Enterprise can be used to renew user keys centrally and transparently for users.

Installation

The appropriate Security BOX modules are easily installed on user PCs, either by individual users or using automated, centrally-managed large-scale and deployment tools.

Unified connection

Security BOX supports the unique connection mechanism for the sharing of user authentication with the Windows system: the Security BOX's solution securizes the users Windows password. In this way, access to all applications and data protected by Security BOX Enterprise can be done using just one single authentication, for each user.

Security policy

Security BOX can be configured to allow an individual user or an enterprise administrator to apply a general enterprise security policy, or to adapt their installation to individual requirements. The security policy automatically updates itself on the user computers.

Key recovery

Security BOX supports key recovery mechanisms in conformity with legislative requirements concerning data encryption.

Secure information exchange

The Security BOX handles the authentication of senders and the confidentiality of information exchanged via e-mail clients. The Security BOX delivers strong authentication of Web accesses (SSL V3).

Mobile device security

Security BOX protects sensitive information on vulnerable mobile platforms: laptop PCs, USB keys, PDAs / smartphones.



Digital signature

Security BOX implements digital signature processes as defined in

EU directive 1999/93/EC, and conforms to French government requirements for paperless transactions. User signature keys can be certified by authorized certification service providers.

Features and benefits



Protect your most sensitive corporate information

Security BOX Enterprise is a complete and integrated software suite featuring an extensive range of encryption products to meet your security requirements.

BENEFITS //////////////////////////////////////

- Protection of data archived, exchanged or used.
- Protection of data on all media (local hard disk, shared server, smart phone or PDA, removable device...).

User involvement

Security BOX Enterprise integrates with the users computer and complete transparency. Users need no knowledge of security.

BENEFITS //////////////////////////////////////

- Information is made secure on the fly without any user intervention.
- The information can be accessed by authorized users, both from inside and outside the enterprise.

Reduce deployment and operating costs

Security BOX Enterprise centralizes management of your trust infrastructure and PKI, easily integrating with pre-existing enterprise PKI deployments.

BENEFITS //////////////////////////////////////

- Management of users and keys from the same administration tool.
- Invisible installation on computers.
- Automatic updating of the solution configuration.



Specifications



Security BOX Software Suite	
Supported standards	CMS; S/MIME 2,3; LDAP; X.509 (1, 2, 3); CRLs; PKCS (1, 5, 7, 10, 12); Smartcards and USB tokens (PKCS 11); IPsec; IKE; NAT traversal
Encryption Algorithms	RSA up to 2048 bits (4096 bits for imported keys); DES/3DES up to 192 bits; AES up to 256 bits; RC2 up to 256 bits; RC4 up to 256 bits; RC5 up to 256 bits; MD5; SHA-1; RIPE-MD160; HMAC; Diffie-Hellman groups 1 (728 bits) and 2 (1024 bits)
Plateformes supportées (utilisateurs et serveurs)	Microsoft Windows (Vista et XP)
Supported Platforms (users and servers)	Microsoft Windows 2000 and Windows XP operating systems Email Clients (Security BOX Mail) Microsoft Outlook (2000, XP, 2003); Microsoft Outlook Express; Lotus Notes (5.x, 6.x); Netscape Messenger; Eudora light
Supported smartcards and tokens	PKCS#11-compatible smartcards and security tokens. Security BOX Enterprise implements Common Criteria EAL4+ certified digital signature technologies, class 3+ certificates for authenticated acts.
Public Key Directories	Security BOX Enterprise supports LDAP connectivity to control the production and revocation of users' public keys and the use of these keys for encrypted data exchanges. For each user account Security BOX maintains a local directory with the public keys of known trusted contacts. Security BOX can also access public key directories via an enterprise LDAP server.

Authority Manager	
Administrator management	- Identify and configure different classes of Security BOX administrators: Principal administrator, auditor, certificate admin, account admin Adapts to your enterprise organizational model
User management	- Manages users individually or by functional group. - Decrypts data encrypted by the user with the recovery account (legal constraints). - Distributes user accounts to computers. Handles all operations related to user management
Security policy management	- Distribute security policy updates to relevant users Automates security policy updates
Application configuration	- Supply each user with the required configuration for each application in the Security BOX suite Facilitates end-user take-up of encryption tools
Enterprise directory	- Synchronizes with an LDAP directory. - Shares encryption certificates between users. Makes it easier to use the Security BOX solution
Smartcard/ USB token customization	- Used to store keys and secrets in the card. Strengthen security using physical, removable authentication devices
Logging and audit	- Logging of all administrator operations Allows tracing and auditing of modifications applied to individual accounts
Hardware Security Module	- HSM support for secure generation and storage of CA keys Strengthen Security BOX Authority Manager security
Internal certification authority	- Manages the lifecycles of keys and certificates in a centralized manner. - Manages certificate requests issued by users on public pages of the solution. - Manages and publishes revoked certificate lists (CRL). Utilization of complete and integrated key-management infrastructure.
Certificate Authority interconnection	- Ensures interoperability with existing PKI or external CA - Integrate received certificates with user accounts Facilitate the integration of Security BOX Enterprise in existing security infrastructures

Visit our web site for a complete list of product features and specifications: www.arkoon.com



1, Place Verrazzano - CS 30603
69258 Lyon Cedex 09 - France
Tél : +33 (0)4 72 53 01 01
Fax : +33 (0)4 72 53 12 60
www.arkoon.com



Security BOX