

Secure Systems – The Company

Secure Systems specializes in a development of computer security and integration solutions. The company was established in 2003 and since that time we have developed a number of know-how technologies and products, working on both enterprise and individual user security solutions. All technologies used in the products of Secure Systems are exclusively created by the company.

Secure Systems has offices in Europe: Switzerland and Latvia. Our most significant direct and indirect customers are Citigroup, Eurofighter GmbH, SCM Microsystems, Eutronsec, BIOMETRY.com and others.

Secure Systems often acts as a sub-contractor, helping our partners in system integration and IT development tasks. We are helping to design, implement and deploy final solutions to our partners. We offer OEM branding and software extensions to partner's software, helping those gaining immediate benefits in front of their competitors.

Secure Systems is committed to provide high-class innovative security solutions at a very competitive cost, providing necessary technical support and consulting. Besides that we offer significant discounts for distributors and resellers of our off-the-shelf products.

The Technologies

Secure Systems develops a number of proprietary products and technologies. We offer:

- Two-factor **authentication** and **security** solutions (ControlSphere): - 2 -
 - Secure authentication and access control to Windows - 2 -
 - Disk and data Encryption solutions - 3 -
 - Most convenient and complete Single-Sign-On technologies - 4 -
 - Enterprise solutions and extensions for data security and control - 4 -
- **Digital Right Management** (DRM) solution is capable of managing typical risks with proprietary company data and intellectual assets. The solution restricts company employees from unintentional or malicious distribution of a sensitive data to 3rd parties. - 5 -
- **Biometrical** and three-factor authentication solutions which we develop together with our partners. We offer **face**, **voice**, and **fingerprint** (optionally combined) authentication solutions. - 6 -
 - **BIOMETRY.sso** is a ready to use biometric single sign on solution which replaces the need of manual password typing by biometric authentication. - 6 -
 - **BIOMETRY Physical Access** is a physical access solution which relies on two-factor authentication by combining the use of RFID or contact cards with biometric verification at the physical access terminal. - 6 -

ControlSphere - convenience and security

ControlSphere is a computer security and automation solution designed to protect user data and automate most of authentication tasks for the user at work and home environments.

ControlSphere secures user data, protects privacy and eliminates the need of remembering and typing any passwords. The solution integrates common authentication and data storage procedures on a PC and substitutes them with strong two-factor authentication (with smartcards or USB tokens) making itself a central security and SSO point.

ControlSphere is a modular solution consisting of four general services which can be used separately or in combination. These are:

- **Windows and Network Logon service** allows quick and easy access to multiple computers with multiple Windows accounts by using a single smartcard/token device.
- **Hard disk and file encryption service** allows transparent hard disk and file/folder encryption with variety of options.
- **Password Management service (SSO)** allows password and other secure data storage on a portable secure device. This data will be automatically delivered to requesting Windows programs and WEB forms.
- **Enterprise Token Management System Server** is an enterprise control and configuration module of ControlSphere. It automatically synchronizes and controls secure data on user's smartcard devices.

ControlSphere – Secure Windows and Network Logon

Logon service of ControlSphere is a powerful and customizable solution for Windows authentication. Its main functional highlights are listed below:

- ☑ ControlSphere allows quick and easy access to multiple computers with multiple Windows accounts by using a single smartcard/token device.
- ☑ No need to acquire security certificates or install Certificate server as well as other 3rd party software required for traditional Windows smartcard logon.
- ☑ User can logon to Windows and Active Directory by just typing device PIN.
- ☑ User does not need to know or remember actual Windows account password(s).
- ☑ ControlSphere provides Windows session and user desktop protection. User is allowed to access his data as long as the device stays connected.
- ☑ Extensive customization options guarantee full compliance with different enterprise security and data access policies.
- ☑ Tight integration with other services of ControlSphere is provided. No need in secondary authentication for hard disk encryption or password management (SSO) functionality.

ControlSphere - Hard disk and File/Folder Encryption

Encryption service enables “transparent” hard disk and file/folder encryption. It combines encryption technology based on AES256 algorithm, storing encryption keys on secure smartcard/USB token devices. The main technological highlights are:

- ☑ ControlSphere protects sensitive information from unauthorized access, copying, modifying, and theft on personal computers, removable media devices and network locations.
- ☑ Encrypted data is transparently decrypted when it is read from the disk and encrypted before it is written. The data becomes accessible to a user as a part of the file system upon successful authorization to a smartcard/token device.
- ☑ Encrypted data storages are automatically or manually merged with Windows file system, becoming accessible to all programs. Access to encrypted information can be blocked on the authorized smartcard/token removal event.
- ☑ Standard user profile (My Documents, Desktop, My Favorites, temporary folders, etc.) can be substituted with an encrypted environment, securing user documents and leaving no traces of user activity on a computer.
- ☑ Encrypted containers can be of a static or dynamic size. Statically-sized containers are ideal for data exchange performance and are mostly used as secure virtual hard drives.
- ☑ Dynamically-sized containers are ideal for secure data exchange between users over unprotected networks, email or by other means. They are well suitable for manual or automatic backup processes too.
- ☑ ControlSphere provides boot-time disk encryption feature for Windows Workstations and Servers, protecting database services and mail servers.

ControlSphere - Password Management (Single Sign On)

Users can store all their password records and other sensitive data (e.g. credit card numbers) on secure devices and maintain this information with ControlSphere. In addition to that ControlSphere can automatically distribute this data to all Windows and WEB programs when it is requested.

- ☑ ControlSphere detects and automates nearly all password requests across the system for native Windows authentication processes, all programs and WEB forms.
- ☑ Password automation **eliminates** the need of **remembering** and **typing** user names, **passwords** and other authentication data. This information is automatically (or manually) distributed to password-requesting programs in a secure manner.
- ☑ This sensitive information is filled in directly into the authenticating application and neither mouse nor keyboard is used. Thus there is no chance for malicious "sniffer" programs (if there any are infecting the system) to capture the data.
- ☑ Users can perfectly tune the password automation rules for their programs and WEB forms to eliminate all manual operations completely.

ControlSphere - Enterprise Token Management System (TMS)

The Token Management System is a comprehensive set of tools and functions designed to help companies control the lifecycle of their smartcard/USB token fleet.

TMS functions are integrated in ControlSphere client itself and communications with the server are mostly implicit to users. The main TMS highlights are listed below:

- ☑ Token Management System (TMS) provides full control over secure data on the ControlSphere-enabled smartcards/USB tokens.
- ☑ TMS database holds centralized company-wide token, user and security group registry.
- ☑ Device contents are automatically synchronized with the TMS database, including device PIN changes. The replication is done implicitly and securely.
- ☑ TMS server provides easy individual and mass data/configuration deployment function across company devices. Updates are pushed to user devices implicitly to users.
- ☑ TMS database maintains device update history automatically. Devices can be restored to their backed-up state remotely using the push technology of TMS.
- ☑ TMS supports remote device blacklisting should a device be lost or stolen. Contents of such a device will be remotely wiped should someone try to use it.
- ☑ TMS supports remotely PIN/password reset function for locked devices.

Digital Right Management – protection for confidential data

The Problem:

Data and information protection has never been that important as today. Companies spend millions of dollars safeguarding their intellectual property and sensitive documents, but losing this battle.

ControlSphere DRM offers a transparent data protection suite which is capable of addressing typical today's risks:

- Employees can unintentionally or maliciously send inner data out.
- By leaving the company, employees can take sensitive data with them.
- Employees can lose their portable computers or storage devices.
- Competitors can spy or bribe company staff to steal sensitive data.
- Computer viruses or malicious software can delete or export the data.
- A hacker can steal company data over the Internet using exploits or security holes.

The Solution:

ControlSphere DRM is a centrally managed client-server solution for confidential data protection. It secures sensitive company data by not only encrypting user workspace, but as well protecting files and company data from unauthorized copying and distribution by employees.

ControlSphere DRM allows employees to work with company data using their standard programs and tools. At the same time they cannot export, print, send out or even exchange the sensitive data through clipboard to unauthorized locations or programs.

In addition to the protection function, ControlSphere DRM provides convenient permission-based data exchange functionality between company employees and administration.

Usage of ControlSphere DRM can be easily combined with a standard ControlSphere security solution for ultimate employee authentication and complete Single-Sign-On without the need of remembering any typing any passwords.

Biometric Authentication – you just need to be

Secure Systems has developed a biometric data acquisition and processing framework which is integrated with other security technologies of the company. It can acquire visual (face), audio (voice) and fingerprint data of a person for identification and authentication purposes.

Thanks to the flexibility of the framework, it can be easily integrated into partner solutions, giving them extra benefits in front of their competitors.

Besides the default biometric processing algorithms, the framework allows a quick integration of custom biometric algorithms and models.

BIOMETRY.sso – biometric single sign on solution

BIOMETRY.sso is based on the biometric framework and replaces the need of remembering and typing any passwords. It uses face and optionally voice channels combined with random challenge-response mechanism for ultimate security and reliability.

The product uses Password Management service of ControlSphere in combination with biometric features, allowing seamless integration with Windows authentication, 3rd party programs and WEB forms.

BIOMETRY.sso performs background user monitoring in front of the PC and blocks access to SSO-activated programs once the user steps away from his desktop.

BIOMETRY Physical Access

This physical access solution relies on two-factor authentication by combining the use of RFID or contact cards with biometric verification at the physical access terminal.

The cards used for physical access can be used in combination with our logical access solution (ControlSphere) for an ultimate enterprise-wide security on both physical and logical (computer access) levels.

Custom Development projects – everything is possible

Besides the ready to use solutions Secure Systems offers further customization options with our products should this be necessary. We can design and implement custom security solutions according to individual enterprise or partner needs.

- ✓ Our solutions can cover additional logical and SSO requirements (including automatic password changing) for existing enterprise environment and servers.
- ✓ Our solutions can restrict or enforce usage of specific services or programs in customer infrastructure and bind their usage with a smartcard/token authorization only.
- ✓ We offer an **authentication replacement technology** within existing enterprise software. Our solution will self-integrate into installed software and dynamically replace their standard authentication prompts with a desired authentication method: smartcard/token devices, biometrics or other.
- ✓ Everything is possible... this is our motto.