Overview

TokenControl 2.0

Overview

TokenControl, the ideal consistent solution for PKI.

SyTrust TokenControl is a sophisticated and professional solution in addition to or instead of Smart Cards. It is a secure and cost effective alternative to a company spread roll-out of very expensive Smart Cards.
SyTrust TokenControl also solves the Key History Problem, even in a PKI based Smart Card environment.

TokenControl integrates itself seamless into the SyTrust Suite and offers you the possibility, to secure your company's surroundings both, commercially and professionally.

☑ BENEFITS

Key-Administration
with:
- Key archiving
- Key recovery
- Key management

Smart Card Substitute
TokenControl may be used irrespective of SmardCards.
You decide when, where and how you roll-out SmardCards.

Smart Card backup
TokenControl is the ideal fallback solution for lost or damaged smartcards.

Key History/Data access
Because TokenControl saves all keys for each user, you are always able to access coded data. Even old keys can be reinstated which enables you to open and read old files.

Document encryption
Due to the implementation of key archives and key history it is now possible to encrypt documents conformable with company policies.

! HIGHLIGHTS

Clear migration path
Mixed installations and simultaneous use with hardware Smart Cards by utilizing the clients, normal Smart Card support

Inexpensive roll-out
Easy installation procedures for the client software permit an inexpensive and quick roll out into comprehensive IT-structures.

High security levels
Up to date methods of authentication and a modern central management provide a high security standard for soft token usage.

Performance / Scalability
Linear sacability of up to 254 devices with performance of up to 100.000 requests per hour accommodate even peak demands of large companies.

TokenControl

Technical Reference

Use-Cases	migration path towards SmartCard support for slow SmartCard RollOut management-only (partial) SmartCard RollOut old encryption-key storage manager access to employees encryption keys lost card bridgeover inexpensive SmartCard replacement
Software-Basis	Apache 1.3.19 Apache SSL (mod_ssl) OpenSSL 0.9.6a
Storage	Oracle DBMS (encryption configurable) LDAP (optional) mySQL file-system additional encryption layer configurable (AES) proprietary, secure hardware box
Operating Systems	Solaris 2.7 Solaris 8 intel Linux Windows 2000 (optional) HPUX (optional) AIX (optional) S/390-Linux (optional)
Management	SNMP Traps E-Mail alarming (optional) SNMP v3 (optional) Tivoli (traps only, optional)
Client Support	Celocom Middleware ActivCard Gold (optional) PKCS#11 (optional) Microsoft CSP (optional) proprietary API PKCS#12 based Middleware
Access Control	certificate based (SSL client authentication) HTTP-basic authentication (username, password) IP-Address based NTLM authentication Netware, Kerberos, Radius (planned) custom modules
Features	storage using PKCS#12 key format flexible password locking after failed logins multiple keys per user handling of old keys password synchronisation
Administration	policy based flexible handling of user-groups workflow-based access to keyarchive (optional) workflow-based password recovery
Configuration GUI	Web-GUI (webmin-based) Windows-GUI (optional)
Crypto Accelerator (HSMs)	PKCS#11 (generic) Baltimore Keyper nCipher nFast nCipher nShield
Scalability	Apache multitasking/multithreading child control in terms of CPU and memory usage automatic, optimal child forking