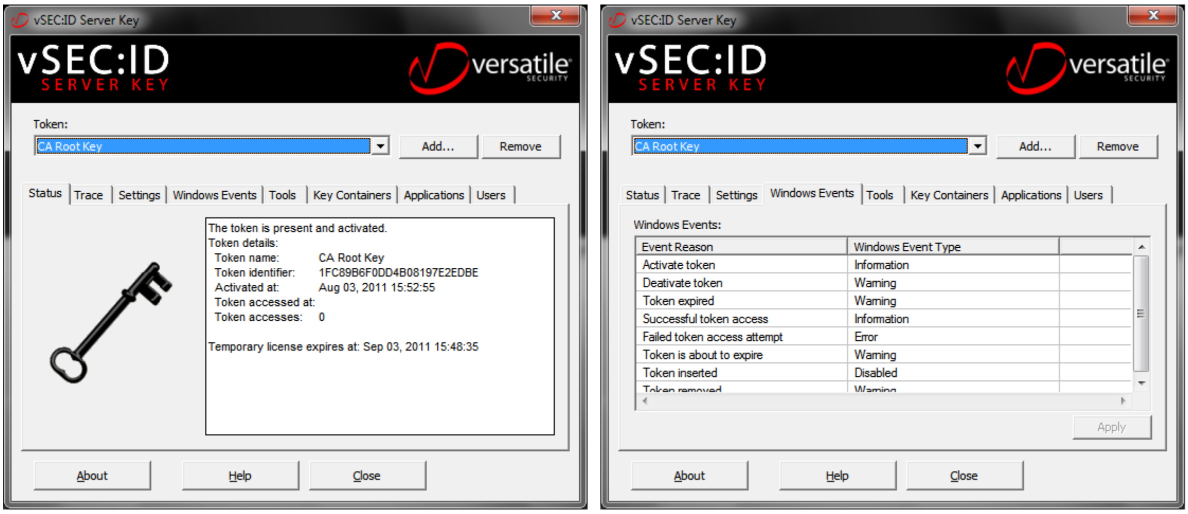
vSEC:ID® Server Key

Using vSEC:ID Server Key, servers can quickly and cost effectively be upgraded to use hardware protected keys instead of file based keys.

Smart Cards for Server Side Cryptographic Key Operations

Often organizations are making large investments to use hardware tokens such as smart cards for their users' authentication, digital signatures, encryption and other security sensitive operations. But the same organizations are not investing in protecting the keys or credentials of the servers. The servers' keys are used for handling the access control systems and even issue new user credentials. These very sensitive servers are often using security measures that are comparable with a simple password –this is an IT security weakness.

One of many use cases that vSEC:ID Server Key is perfectly suited for, is to use the solution to secure your corporate certificate authority, this is described further below. Other possible use cases include server side transaction signing/encryption, server key storage for SSL/TLS or VPN and as logon certificates for system/services accounts.



The token is present and activated.
Token details:
Token name: CA Root Key
Token identifier: 1FC89B6F0DD4B08197E2EDBE
Activated at: Aug 03, 2011 15:52:55
Token accessed at:
Token accesses: 0

Temporary license expires at: Sep 03, 2011 15:48:35

Windows Events:

Event Reason	Windows Event Type
Activate token	Information
Deativate token	Warning
Token expired	Warning
Successful token access	Information
Failed token access attempt	Error
Token is about to expire	Warning
Token inserted	Disabled
Token removed	Warning

Figure 1: Administration application example

Certificate Authority using vSEC:ID Server Key

In a Public Key Infrastructure (PKI) a Certificate Authority (CA) is used to issue certificates. The root CA, or to be more precise, the root CA's private key, is the most trusted key and therefore the most sensitive key in the whole PKI. This key needs to be secured and it must not be possible to steal or make an illegal copy of. The solution used by all security aware Certificate Authorities is to use hardware tokens for storing and using the private keys. Such hardware tokens are for example HSMs (Hardware Security Modules). HSMs can be described as powerful smart cards, developed to be used by servers and enable the servers to do many thousands of cryptographic operations per minute, but unfortunately they are very expensive.

As an alternative, the vSEC:ID Server Key enables the CA to use normal smart cards to secure its keys. The smart card, from a security perspective, is similar to the HSM. A normal smart card can do hundreds of cryptographic operations per minute – this is more than enough for most corporate CAs. The price of one smart card is a fraction of the cost of an HSM.

The system

The vSEC:ID Server Key system has three main components:

1. A Windows service that handles the security relevant functions;
2. A minidriver that slots into the Microsoft system minidriver architecture. This minidriver is communicating with the Windows service (1.);
3. An administration application, that communicates with the Windows service and provides a user interface that displays the status and makes it possible to change the settings.

Every time a smart card passphrase (PIN) is requested by MS CAPI to perform crypto operations on the smart card, the minidriver (2.) talks to the service (1.) to check if the requested operation is granted according to the specified rules. If so, it securely provides the smart card passphrase and the crypto operation can be performed. The rules can be set in the administration application (3.) on a per token basis. Because the rules are set per token, it means that vSEC:ID Server Key does not interfere with other use of smart cards on the host machine.

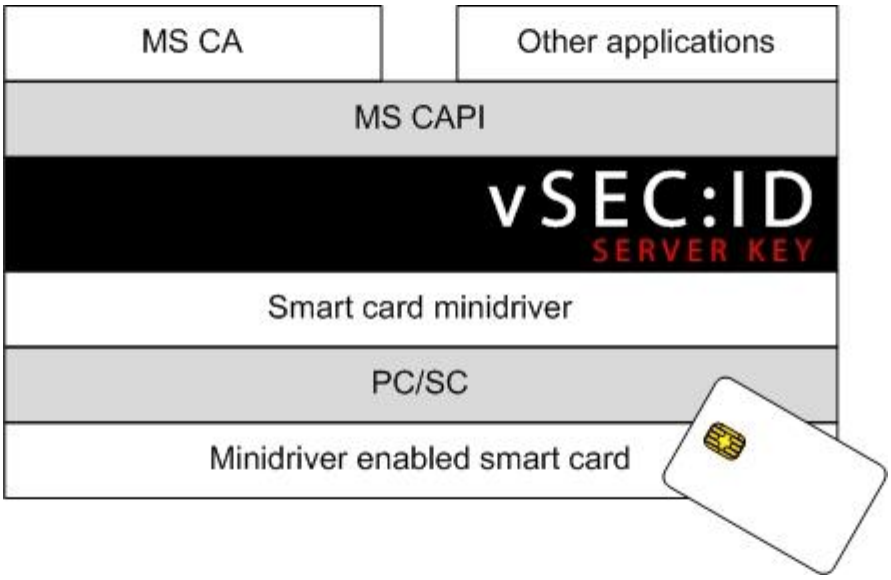


Figure 2: Architectural overview

Technical Specifications

Operating Systems

- MS Windows 7
- MS Windows 2008 Server (R1 and R2)

Smart cards

- All smart cards that are accessible through mini drivers, i.e. works with the MS Base Smart Card CSP, are supported

Limitations

- The smart cards need to be attached physically to the server where vSEC:ID Server Key is used

Security features

- Smart card use from server application
- Microsoft Crypto API interface
- Policy configuration
- Whitelist for applications and accounts
- PIN handling (change, unblock)
- Trace and audit logging
- Support for Windows event system
- Key management (backup, generation…)
- Multiple simultaneous tokens / cards

versatile
SECURITY