

# SafeGuard® Cerbalon Certificate-based Operating System Logon

## Logon to the operating system with smartcards

Cerbalon = Certificate-based logon.

### Overview

- SafeGuard Cerbalon enables users to perform certificate-based log on to the Windows operating system with any smartcard.
- Allows the use of chip cards that have been issued in national eID projects or rolled out across a company.

#### The problem with certificates

Many customers believe that Windows 2000 and XP already support certificate-based logon to the operating system with smartcards, using Kerberos technology. So why should they also buy Cerbalon, when Kerberos is already provided as a standard tool?

The fact is that there is a problem with Kerberos: Kerberos requires its own very specific extensions in the certificates, otherwise users will not be authenticated. However, only a few certificates contain these extensions. Otherwise they require the company to operate its own PKI.

Microsoft has also recognized this problem, and plans to make improvements, but not before Longhorn. In the meantime Microsoft is supporting the Utimaco Cerbalon solution, for example in the Belgian eID-card project.

## Key Features

Cerbalon enables certificate-based logon to the operating system in non-certificate-based IT infrastructures, and so meets an enormous need.

- Neither a special certificate extension nor a server component are required as the destination for the logon to the operating system.
- Existing X.509 authentication certificates can be used for the operating system logon.
- Cerbalon replaces the original Windows password with a value that is calculated by the smartcard. The user does not know the new value and no longer requires it not for the operating system logon: Cerbalon perform Single Sign On to the operating system.
- The new "Windows password" is 63 characters long and is calculated with asymmetrical encryption. This Windows password is resistant against all known attacks (dictionary attacks, L0phtcrack, etc.) Users do not see it, and so cannot write it down or pass it on to others.
- Mobility: users can use Cerbalon logon both to domains and local. There is no need for an online connection to the server. Roaming users also supported.
- Standard smartcards are supported. Cerbalon stores no data on the card. (Incidentally, the generated Windows password is not saved anywhere.)

## Benefits

### Benefits for users

- Users do not need to remember the Windows password since Cerbalon uses Single Sign On to log them on to Windows. And since eID cards replace personal identity papers (which are a requirement in Germany and some other European states), users always have eID cards with them, so they can always benefit from using them.
  - ▶ No more complex password rules for Windows.
  - ▶ No problems after a forced password change.
  - ▶ One password less to remember.
- Smartcard PINs are easier to remember:
  - ▶ short (usually 4 to 6 digits).
  - ▶ No on-going password change.
- Routine prevents the user from forgetting the smartcard PIN (which can easily happen if it is otherwise only used rarely, for digital signatures).

### Benefits for security officers

- Since eID cards replace personal identity papers, the users look after them.
- Logon to operating system according to the principle of "possession and knowledge" via an additional hardware security component.
- Windows passwords are resistant against attacks.
- A company with Cerbalon does not need to invest in its own , but can instead use the offerings of any Trust Center– including cards from state

# SafeGuard® Cerbalon Certificate-based Operating System Logon

projects (citizens card, electronic personal identity papers, eID).

- A simple method for protecting confidential data within the framework of a company-wide security policy.

## Benefits for administrators

- Since eID cards replace personal identity papers, the users keep them with them at all times, which cuts the number of forgotten tokens.
- The number of forgotten passwords falls, as does the associated effort (and cost) for the helpdesk.
- Requires no server components or changes to the infrastructure.

## Benefits for decision-makers

- Low initial costs and so low TCO, because no additional components (PKI, server etc.) are required.
- High ROSI (Return Of Security Investment) as the users can no longer forget their Windows passwords and Cerbalon is resistant against attacks on Windows passwords.

## Forgotten passwords

Of course, Cerbalon does not completely protect against forgotten passwords – a user can still forget their smartcard PIN. However, the risk of this is low as PINs are usually simple and are not constantly being changed.

But if a user does forget their smartcard PIN, the card must be unblocked or the user is given a new card (a normal procedure).

If this has happened, or if the user has forgotten their card, they can no longer logon to the operating system, as no-one knows their Windows password. They can be helped easily in this case by the Administrator, who gives them a new Windows password.

## Target markets

- Countries with eID projects:
  - ▶ Officials: often the government introduces eID cards and gives them to administration staff first, as eID cards for e-government applications.
  - ▶ Large companies that operate on a purely national basis (for example, rail, post, health organizations such as health insurance companies and hospitals, savings banks).
- Small to medium-sized enterprises and organizations for which investment in a PKI is not cost-effective. They can buy certificates and smartcards cheaply from Trust Centers or eID projects.

## The competition

- Microsoft – Kerberos/PKINIT
  - ▶ Free standard tool but requires specific certificate extensions in the entire certificates chain (usually requires Windows CA).
  - ▶ Microsoft is working together with Utimaco and is itself promoting Cerbalon.
- Control Break International (SafeBoot) has announced a similar solution to Cerbalon.

## Technical specifications

- Operating systems: Windows NT2000, 2000, XP Professional; all with Intel Pentium or compatible processors.
- X.509 certificates for user authentication.
  - ▶ Certificates from any PKI.
  - ▶ Smartcards from any manufacturer.
  - ▶ Smartcard middleware (PKCS#11, CSP) is not part of the product, needs to be ordered from card provider separately.
- Central software installation by Windows Installer.