

# Using OpenCA in Business

Ulf Möller  
Robert Esterer

# Overview

- OpenCA at Secardeo GmbH
  - Internal use
  - Client projects
  - Seminars, workshops
- Comparing OpenCA and Windows CA
  - Advantages, disadvantages

# Who we are

Secardeo GmbH, Unterföhring

- PKI
- Digital signatures (esp. PDF)
- Security consulting

# OpenCA at Secardeo

- Certificates for
  - E-mail encryption
  - Signatures
  - Windows Smartcard Logon
- Software certificates and smart cards (mostly Gemplus)

# Our CA (1)

## Root and Issuing CA

Root exists only as encrypted PKCS#12

- OpenSSL
- Only signs root CRL once a year

Issuing CA managed with OpenCA

- All in one installation without data export/import

SuSE Linux, MySQL, Apache 2

# Our CA (2)

Up and running for 2 years

- First installation was 0.9.1-4 (December 2003)
- Switch to 0.9.2.4 last month

Signature keys for e-mail and Windows Logon

- Works with Mozilla and Outlook, key generation on the smart card using Windows + IE
- 0.9.1 profile used modified Perl scripts for Windows name

Encryption keys generated on the CA for backup

- Export to PKCS#12 and then import onto the smart card

Certificates for Windows DC and web servers (IIS + Apache)

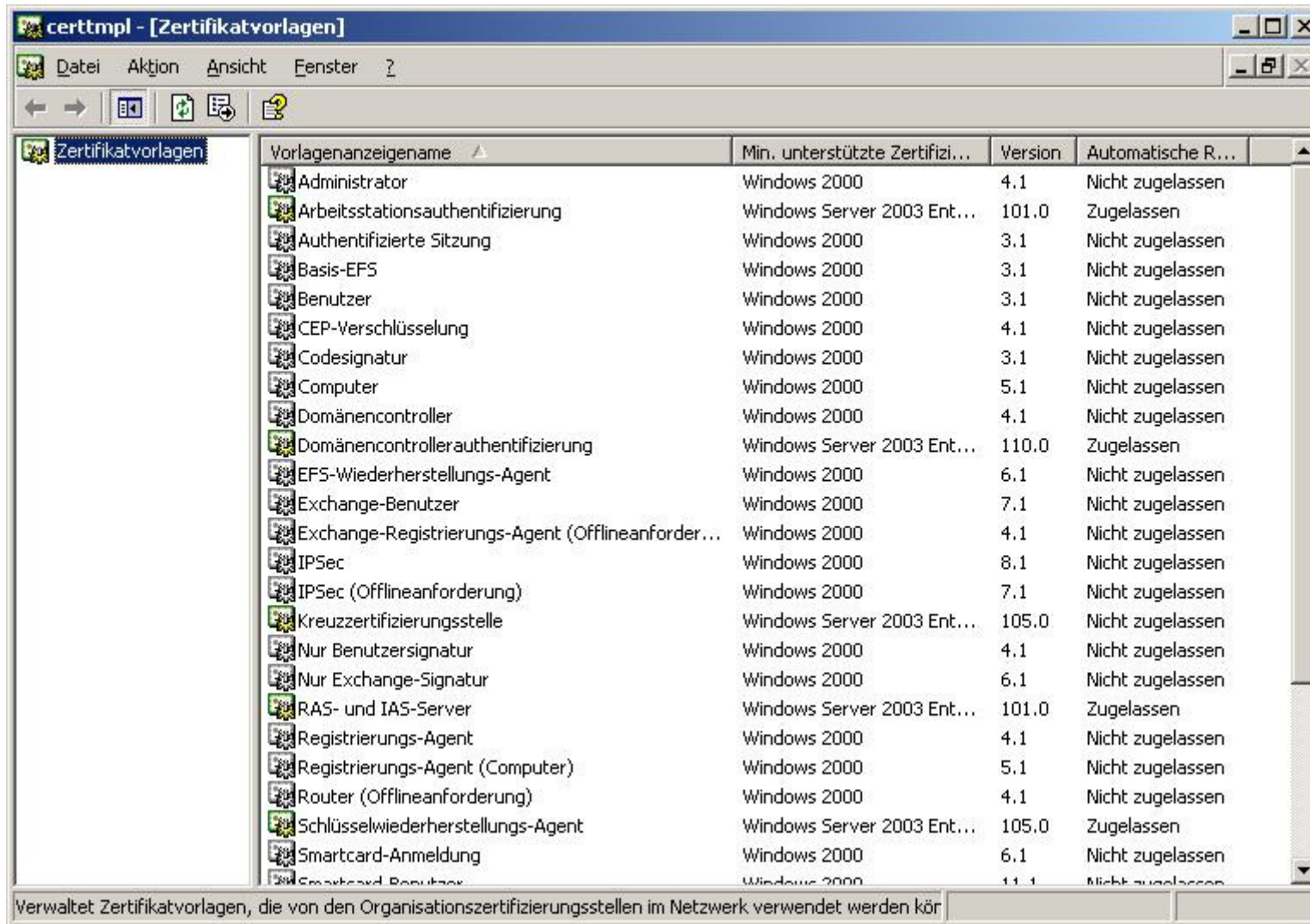
# OpenCA vs Windows CA

	OpenCA	Windows CA
<b>+</b>	Security Modularity Stand-alone Easy to extend Many add-ons	GUI – simple user interface Automation (CRLs, certs) Easy backups AD integration
<b>-</b>	Hard to configure No automation No key backup	Unprotected CA key Tied into the OS You need to trust Microsoft Creating new modules is very difficult

# Customer feedback

- Main issue is the configuration:
    - Base config in XML
    - ACLs in XML
    - \*.conf files for interface config as text
    - Cert templates as text
- > You have to edit 3 files in 3 different directories and 2 different formats to access a modified public interface through http and request a certificate with a newly created profile.
- Import/export only looks at hierarchy levels, multiple RA/Public interfaces under the same CA end up sharing their data.
- > An option “Export to [RA Name/Number]” would be nice

# Certificate templates

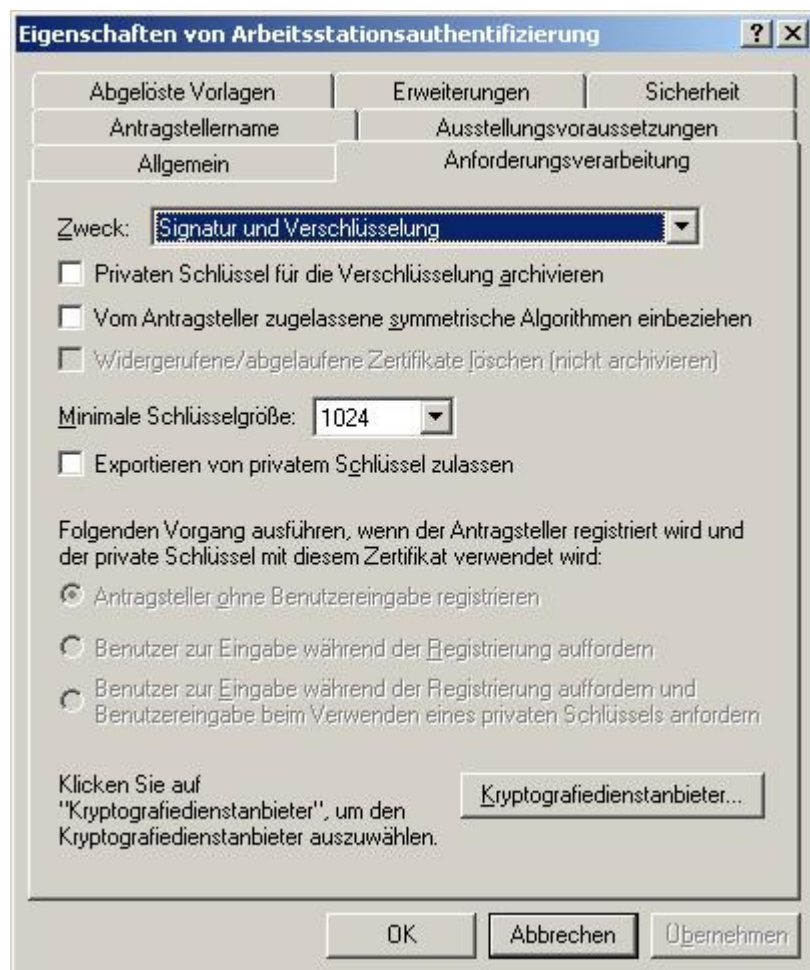


The screenshot shows the Windows Certificate Templates console (certtmpl) window. The window title is "certtmpl - [Zertifikatvorlagen]". The menu bar includes "Datei", "Aktion", "Ansicht", and "Fenster". The toolbar contains navigation and management icons. The main area displays a list of certificate templates with the following columns: "Vorlagenanzeigename", "Min. unterstützte Zertifizi...", "Version", and "Automatische R...".

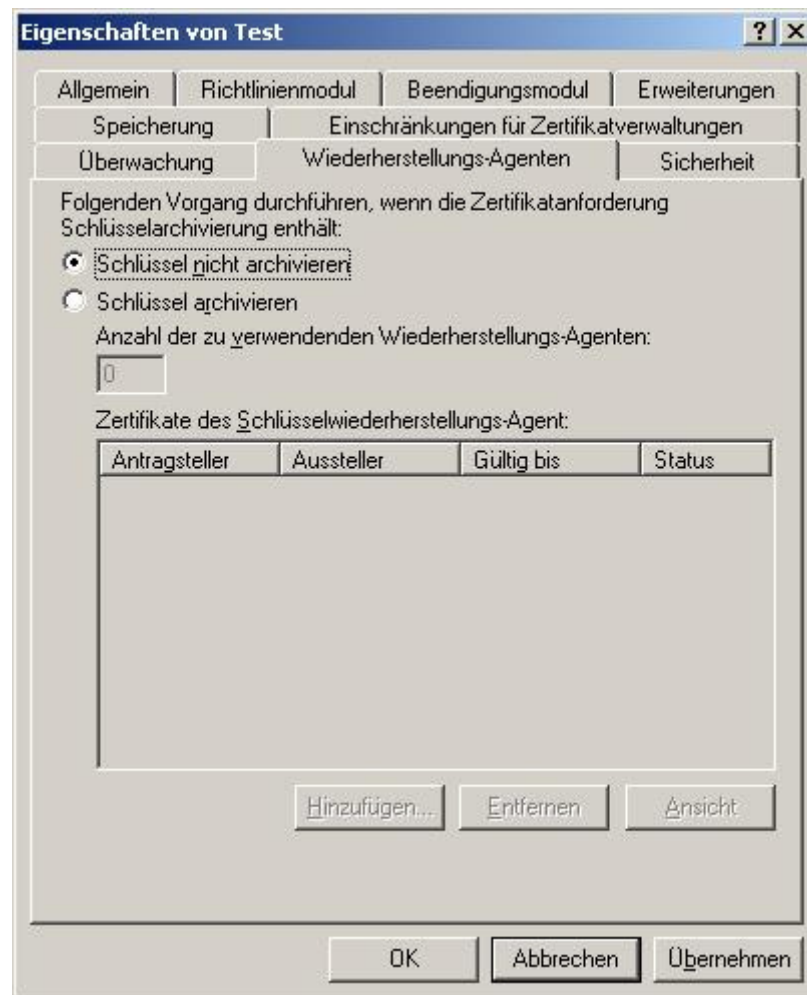
Vorlagenanzeigename	Min. unterstützte Zertifizi...	Version	Automatische R...
Administrator	Windows 2000	4.1	Nicht zugelassen
Arbeitsstationsauthentifizierung	Windows Server 2003 Ent...	101.0	Zugelassen
Authentifizierte Sitzung	Windows 2000	3.1	Nicht zugelassen
Basis-EFS	Windows 2000	3.1	Nicht zugelassen
Benutzer	Windows 2000	3.1	Nicht zugelassen
CEP-Verschlüsselung	Windows 2000	4.1	Nicht zugelassen
Codesignatur	Windows 2000	3.1	Nicht zugelassen
Computer	Windows 2000	5.1	Nicht zugelassen
Domänencontroller	Windows 2000	4.1	Nicht zugelassen
Domänencontrollerauthentifizierung	Windows Server 2003 Ent...	110.0	Zugelassen
EFS-Wiederherstellungs-Agent	Windows 2000	6.1	Nicht zugelassen
Exchange-Benutzer	Windows 2000	7.1	Nicht zugelassen
Exchange-Registrierungs-Agent (Offlineanforder...	Windows 2000	4.1	Nicht zugelassen
IPSec	Windows 2000	8.1	Nicht zugelassen
IPSec (Offlineanforderung)	Windows 2000	7.1	Nicht zugelassen
Kreuzzertifizierungsstelle	Windows Server 2003 Ent...	105.0	Nicht zugelassen
Nur Benutzersignatur	Windows 2000	4.1	Nicht zugelassen
Nur Exchange-Signatur	Windows 2000	6.1	Nicht zugelassen
RAS- und IAS-Server	Windows Server 2003 Ent...	101.0	Zugelassen
Registrierungs-Agent	Windows 2000	4.1	Nicht zugelassen
Registrierungs-Agent (Computer)	Windows 2000	5.1	Nicht zugelassen
Router (Offlineanforderung)	Windows 2000	4.1	Nicht zugelassen
Schlüsselwiederherstellungs-Agent	Windows Server 2003 Ent...	105.0	Zugelassen
Smartcard-Anmeldung	Windows 2000	6.1	Nicht zugelassen
Smartcard-Benutzer	Windows 2000	11.1	Nicht zugelassen

Verwaltet Zertifikatvorlagen, die von den Organisationszertifizierungsstellen im Netzwerk verwendet werden kör...

# Templates



# CA itself



# Conclusion

OpenCA offers great features and emphasizes security

Designed from a technical point of view, not for a streamlined user experience

Microsoft CA is easier to use for standard tasks

# Thank you for your attention!

[ulf.moeller@secardeo.com](mailto:ulf.moeller@secardeo.com) / [robert.esterer@secardeo.com](mailto:robert.esterer@secardeo.com)

[www.secardeo.com](http://www.secardeo.com)

089 / 18935890