Signieren von Dokumenten in OpenOffice.org

Marcus Mängel
INOPIAE GbR

Themenliste

1. Voraussetzung
2. Nutzen von digitalen Signaturen
3. Funktionsweise von Signaturen
4. Signieren von Dokumenten
5. Code Signing
6. Zertifikatsgenerierung bei CAcert

Voraussetzung

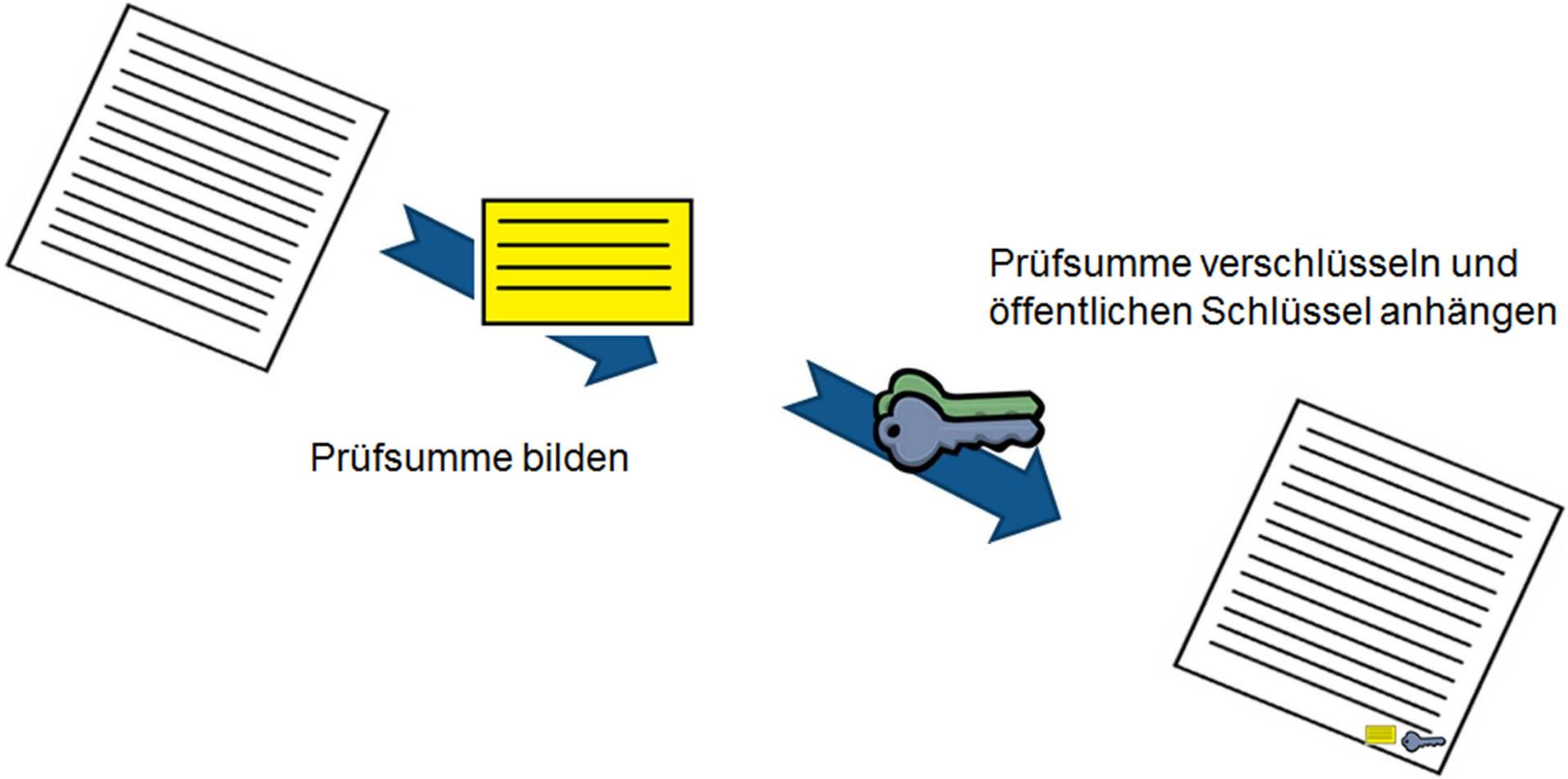
- OpenOffice.org
- Digitale Signatur (X.509 Standard)
  - CAcert
  - Verisign, Comondo
- Zertifikatsspeicher
  - Unix/Linux Zertifikatsspeicher der Browser
  - Windows Zertifikatsspeicher erreichbar über IE

Nutzen von digitalen Signaturen

- Digitale Unterschrift
- Ermöglicht es den Unterzeichner eines Dokumentes zu identifizieren.
- Zeigt den originalen Zustand eines Dokumentes an.
- Besonderes bei Makros und Programmen.
- Ermöglicht es dem Unterzeichner zu vertrauen.
- Zugriffskontrolle mit Zertifikaten, die den Signaturen zugrunde liegen.

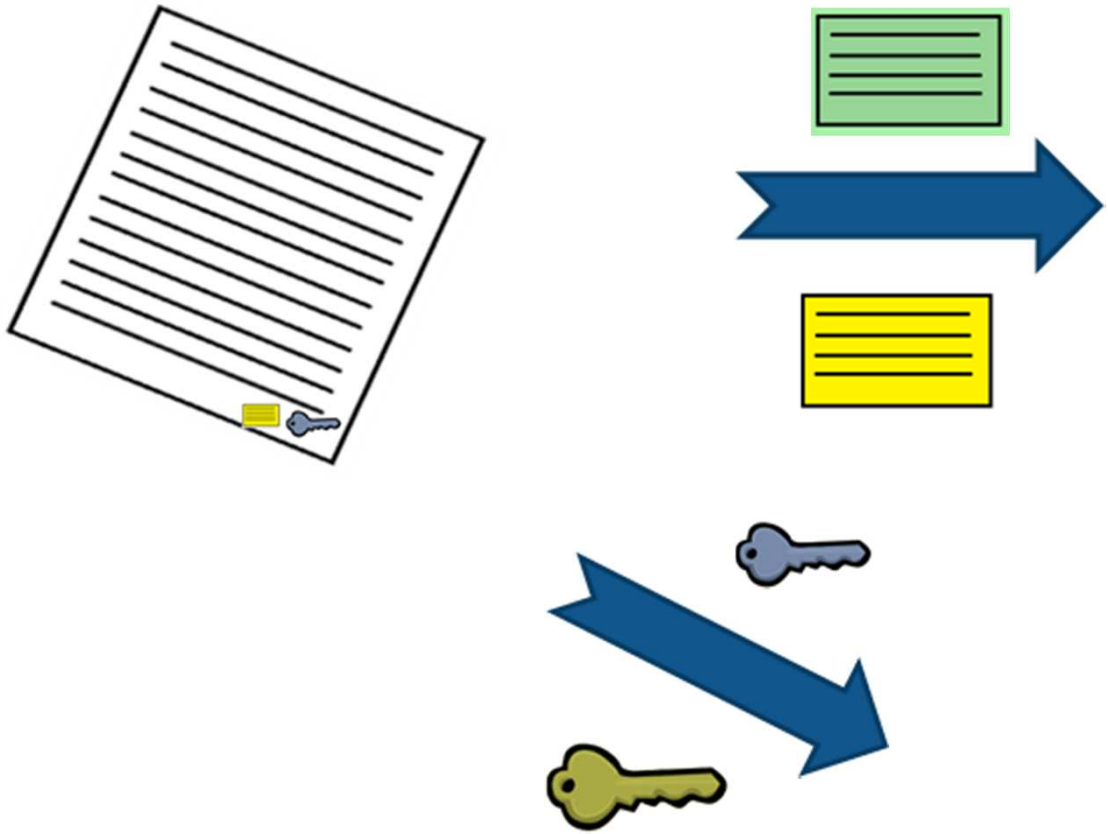
Funktionsweise von Signaturen

Signatur anfügen



Funktionsweise von Signaturen

Signatur überprüfen



Prüfsumme neu berechnen
Prüfsummen vergleichen

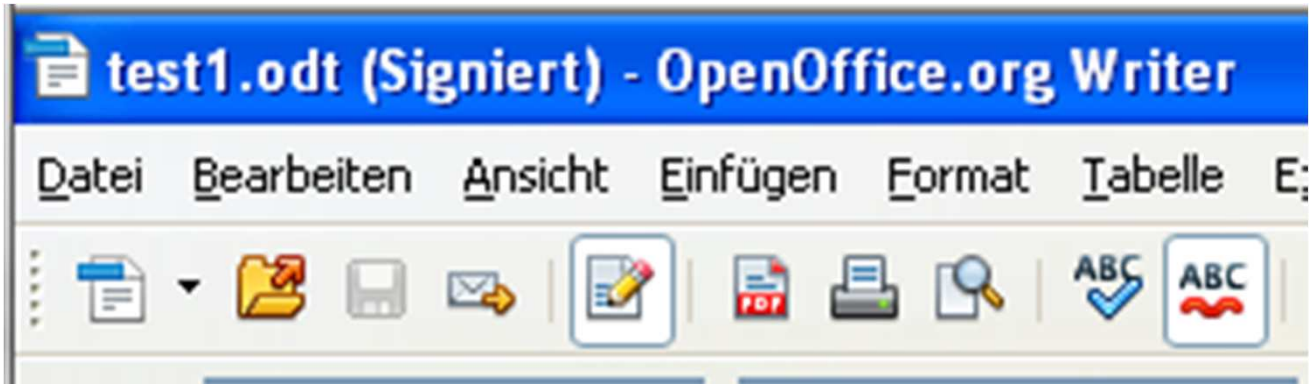
Gleichheit => unverändert

Öffentlichen Schlüssel gegen
Root-Zertifikat prüfen

Zertifikatskette vorhanden =>
Identität bestätigt

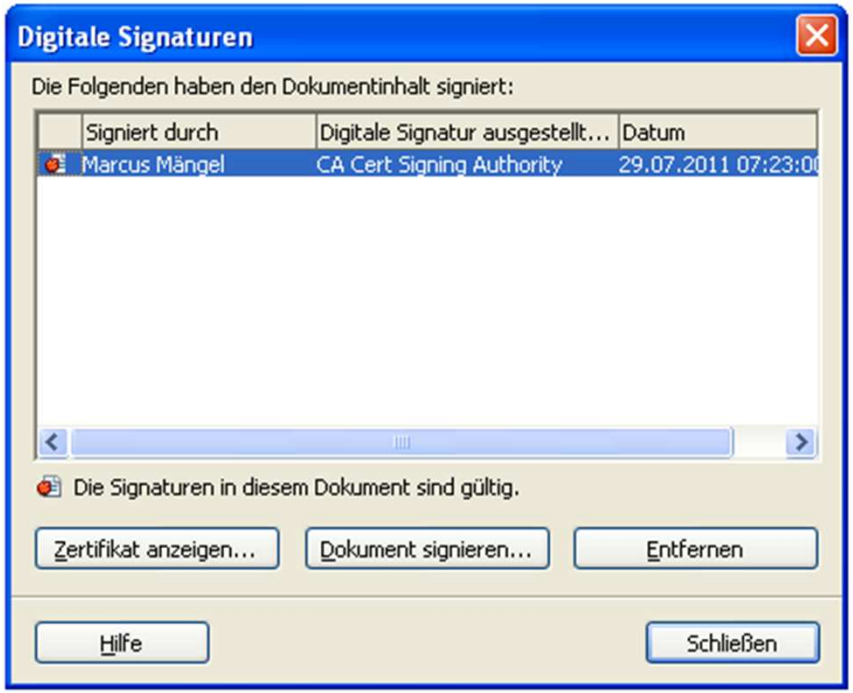
Signieren von Dokumenten

Beim Öffnen eines Dokumentes wird im Titel angezeigt, dass das Dokument signiert ist.



Signieren von Dokumenten

Über Datei – Digitale Signaturen wird die hinterlegte Signatur angezeigt



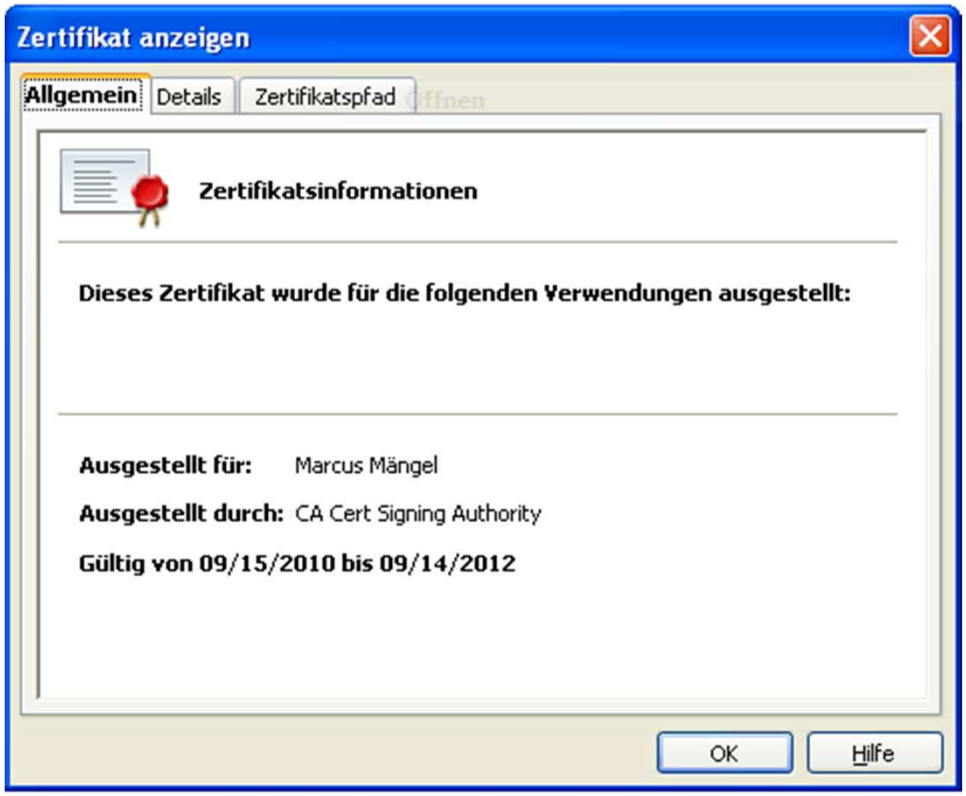
Signieren von Dokumenten

Symbole für den Status einer Signatur

Symbol in der Statusleiste	Signaturstatus
	Die Signatur ist gültig.
	Die Dokumentsignatur ist OK, aber die Zertifikate konnten nicht verifiziert werden. Die Dokumentsignatur und das Zertifikat sind korrekt, aber nicht alle Bestandteile des Dokuments sind signiert. (Siehe unten stehenden Hinweis für Dokumente, die mit alten Versionen der Software signiert wurden.)
	Die Signatur ist ungültig.

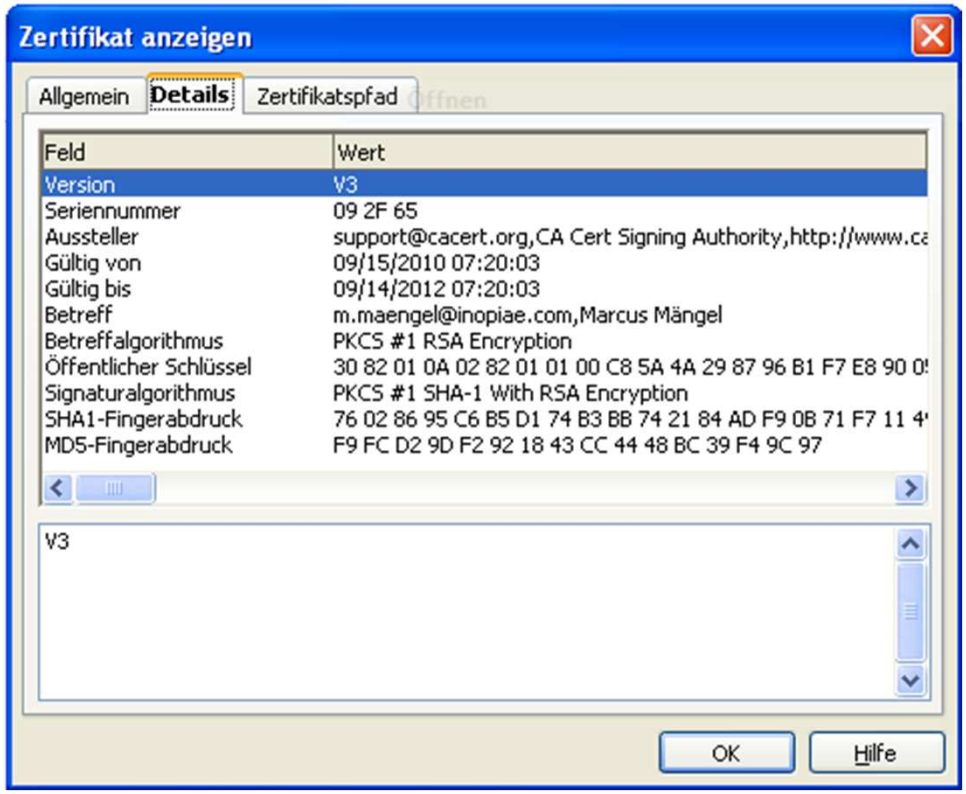
Signieren von Dokumenten

Anzeigen der Signatur (1)



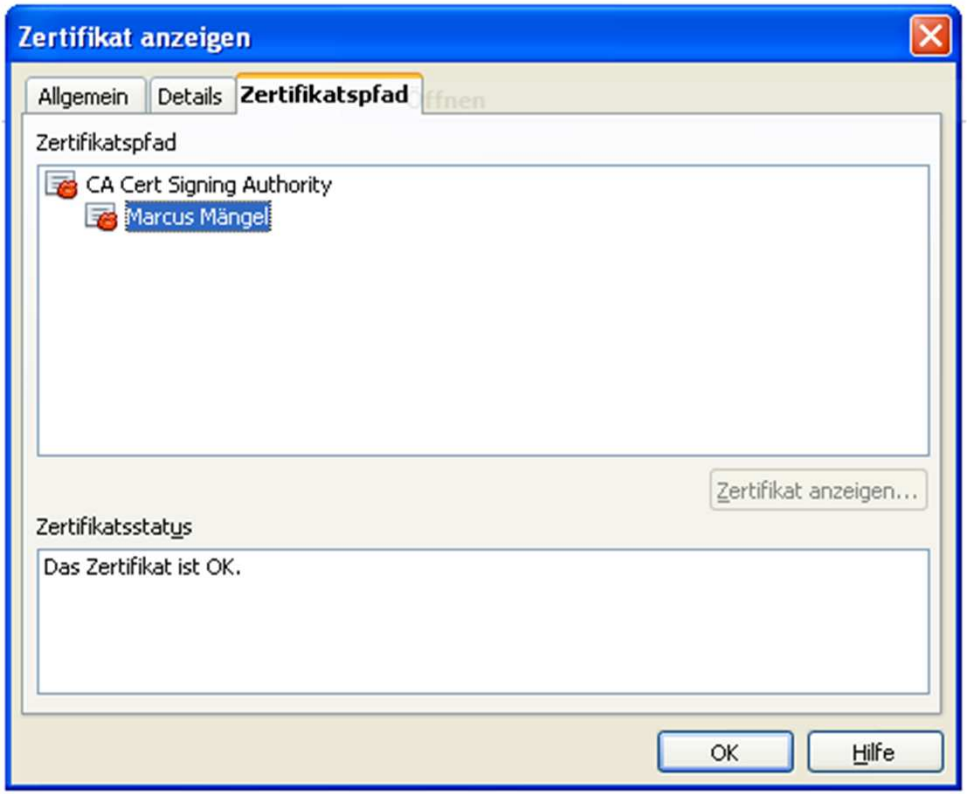
Signieren von Dokumenten

Anzeigen der Signatur (2)



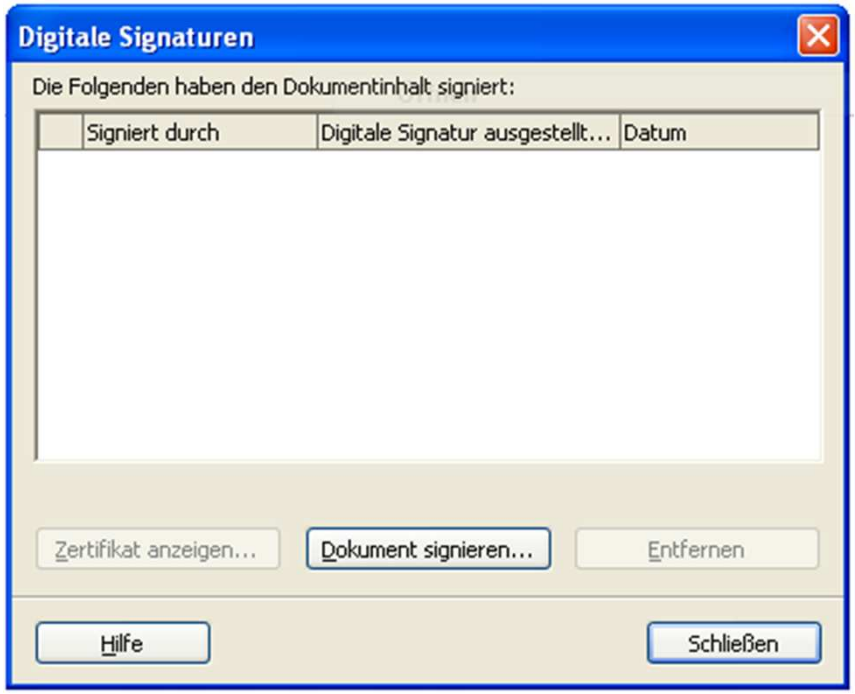
Signieren von Dokumenten

Anzeigen der Signatur (3)



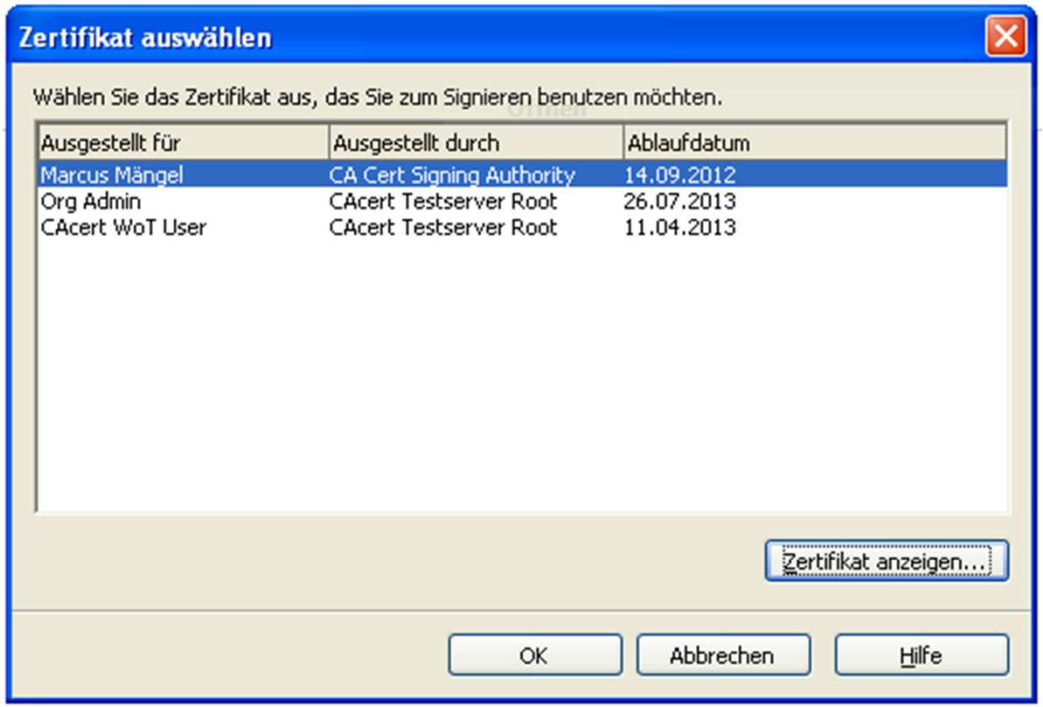
Signieren von Dokumenten

Neu signieren über Datei – Digitale Signatur



Signieren von Dokumenten

- Auswählen eines Zertifikats aus dem Zeritifikatsspeichers

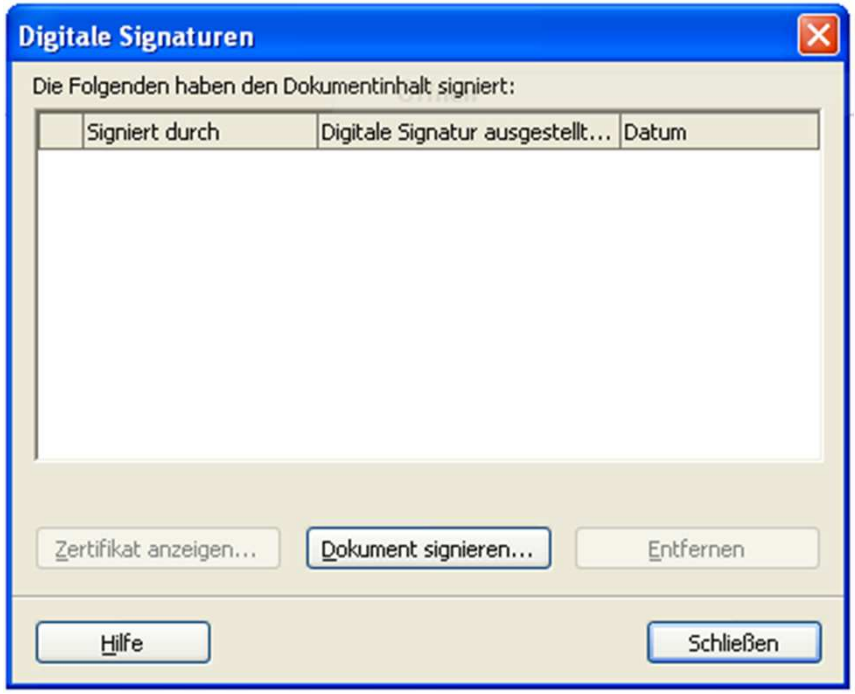


Code-Signieren in Dokumenten

Beim Öffnen eines Dokumentes mit Makros

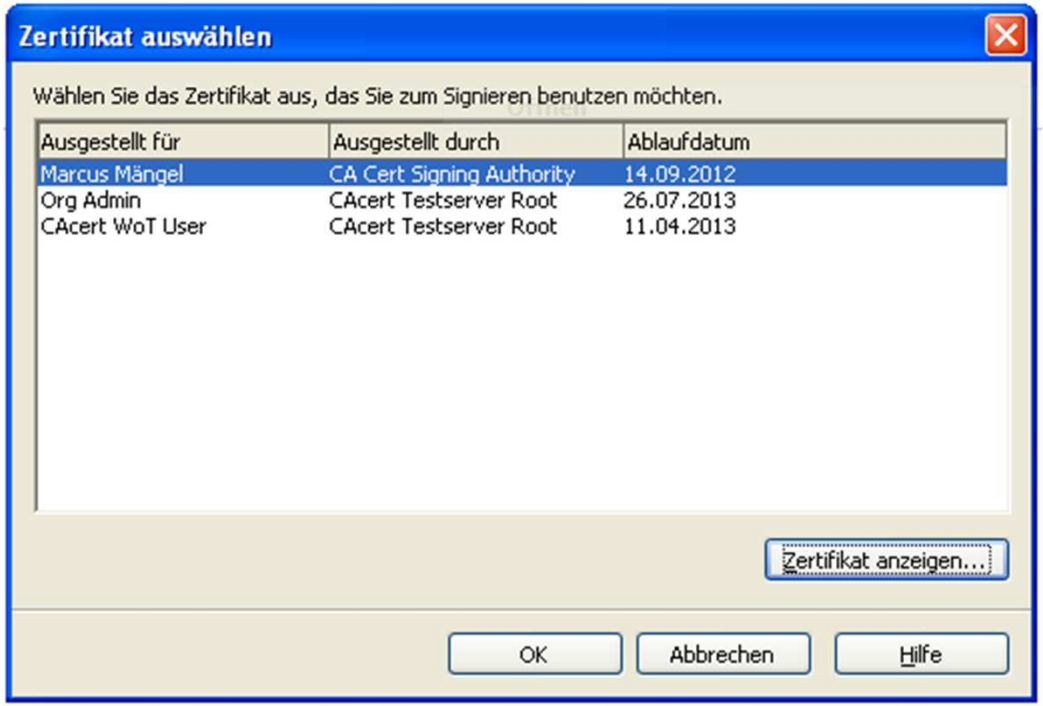
Code-Signieren in Dokumenten

Einfügen einer Signatur über Extras – Makros – Digitale Signaturen



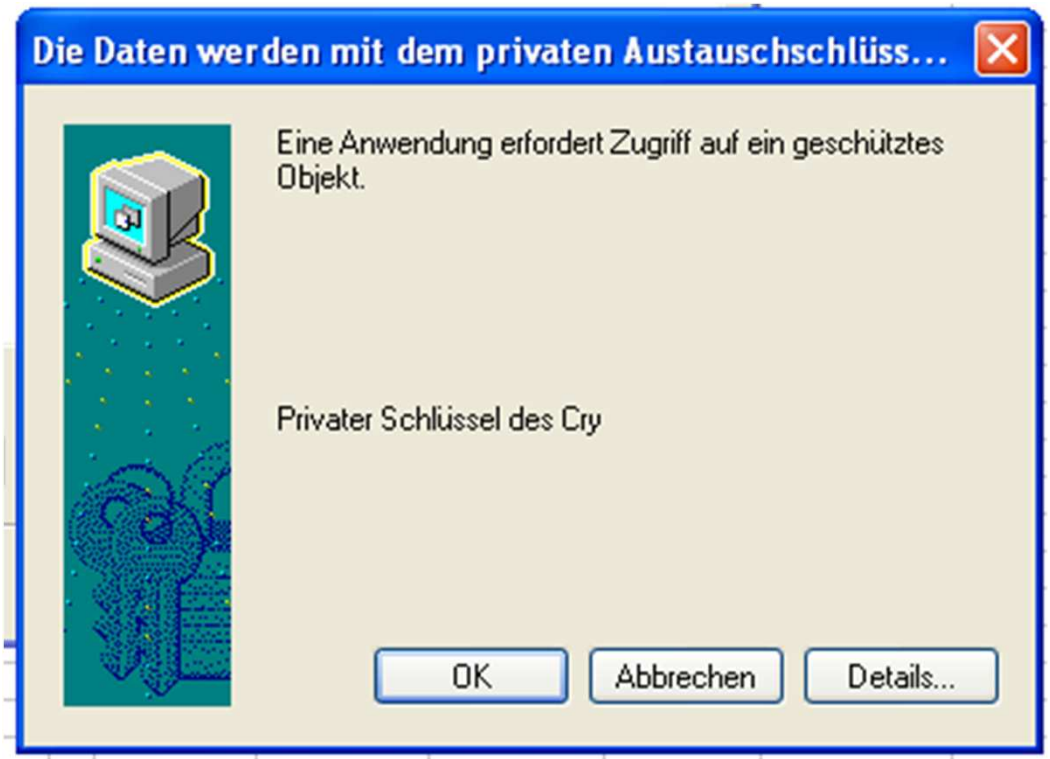
Code-Signieren in Dokumenten

Auswählen der Signatur aus dem Signaturspeicher



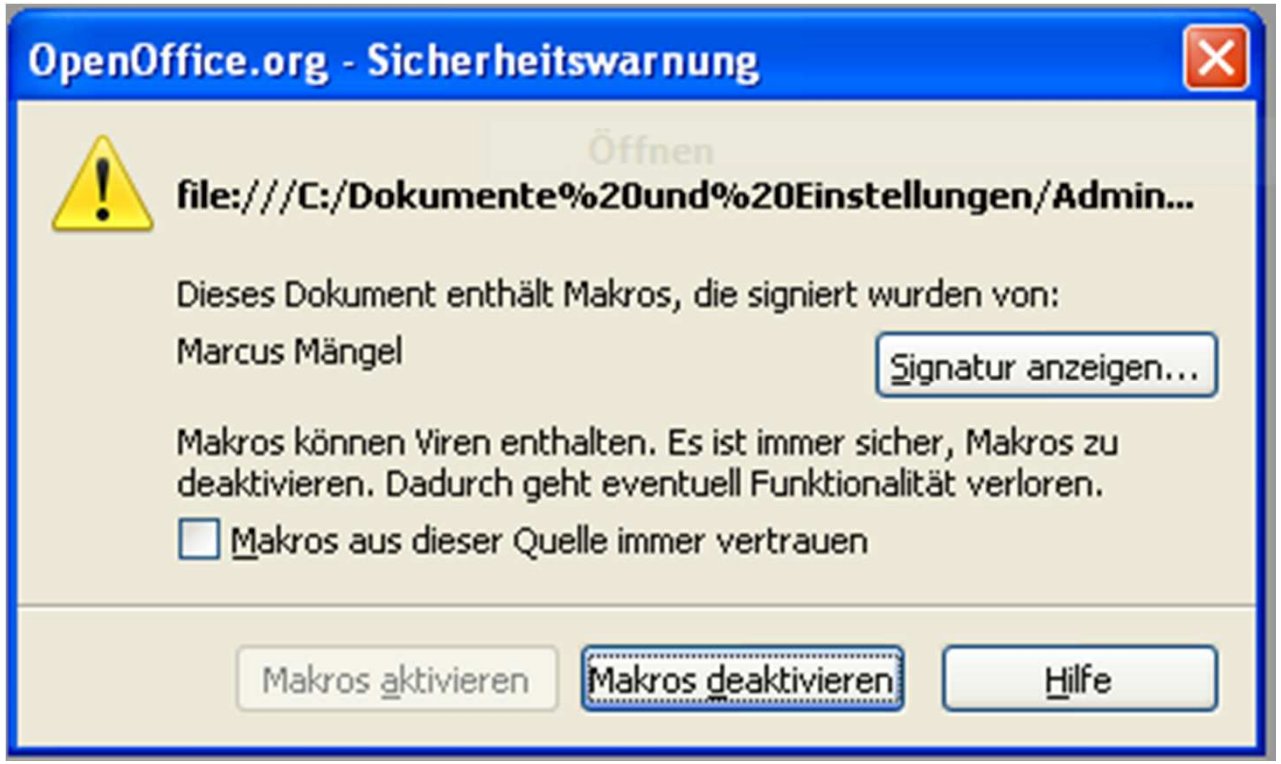
Code-Signieren in Dokumenten

Bestätigen der Signatur



Code-Signieren in Dokumenten

Öffnen eines Dokumentes mit Code-Signing Zertifikats



Zertifikatsgenerierung bei CAcert

- Anmelden bei Cacert www.cacert.org
- Root-Zertifikate in Browser importieren
- Einloggen und Zertifikat nur mit Email-Adresse
- Name im Zertifikat
  - 50 Überprüfungspunkte, mindestens
    2 Überprüfungen der Identität

Zertifikatsgenerierung bei CAcert

- Zertifikat für Codesigning
  - 100 Überprüfungspunkte, mindestens 3 Überprüfungen der Identität
  - Erfolgreiches Bestehen der CAcert Assurer Challenge (CATS)
  - Freischaltung der Codesigning-Funktionalität über Support

Zertifikatsgenerierung bei CAcert

- Zertifikate für Firmen und Organisationen
  - Feststellung der Identität der Organisation
  - Benennung eines CAcert-Assurer als Administrator
  - Feststellung der Identität des Antragstellers
  - Administrator kann Zertifikate für die Organisation erstellen
  - Administratoren können wechseln

Unterstütze CAcert

- Werde Assurer
- Helfe mit beim Testen der Neuerungen
- Helfe mit beim Entwickeln der neuen Roots
- Helfe mit die Software weiter zu entwickeln
- Helfe mit um CAcert Audit-ready zu bekommen.