

# Elektronische Signatur: Sicherheit im Internet

Dr. Georg Serentschy

Geschäftsführer, Fachbereich Telekommunikation



---

Live-Demonstration

Sicherheitsaspekte

Erweitertes  
Informationsangebot

Anwendungen

Einrichtungen und  
ihre Aufgaben

---

## Inhalt

- Live-Demonstration
- Sicherheitsaspekte
- Erweitertes Informationsangebot im Web
- Anwendungen
- Einrichtungen und ihre Aufgaben



---

**Live-Demonstration**

Sicherheitsaspekte

Erweitertes  
Informationsangebot

Anwendungen

Einrichtungen und  
ihre Aufgaben

---

# Live-Demonstration



## Was benötigt man für die sichere elektronische Signatur?

- Bankomatkarte
  - Karten, die ab Februar 2005 ausgegeben wurden, sind signaturtauglich
  - Ältere Karten werden von vielen Banken kostenlos ausgetauscht
- Qualifiziertes Zertifikat
  - Erhältlich in Registrierungsstellen (z.B. Bankfilialen)
    - Vollständige Liste: <http://www.a-trust.at/registrierung/>
    - Amtlicher Lichtbildausweis und Bankomatkarte erforderlich
  - Kosten EUR 12,- für Freischaltung, EUR 13,- jährlich
- Chipkarten-Lesegerät
  - Information unter <http://www.a-trust.at/default.asp?lang=GE&ch=1&node=556>
  - Kosten ca. EUR 25,-
  - Förderung durch BMF und Europay Austria EUR 10,-



## Was benötigt man noch?

- Rechner
- Windows 2000 oder Windows XP
- Internet Explorer, Version 6
- Treiber für Chipkarten-Lesegerät
- a.sign Client, kostenlos abrufbar unter <http://www.a-trust.at/default.asp?lang=GE&ch=1&node=543>  
(Schnittstelle für signaturfähige Applikationen)
- trustDesk basic, kostenlos abrufbar unter <http://www.cio.gv.at/identity/bku/>  
(sichere elektronische Signatur und Bürgerkartenumgebung)



---

Live-Demonstration

**Sicherheitsaspekte**

Erweitertes  
Informationsangebot

Anwendungen

Einrichtungen und  
ihre Aufgaben

---

# Sicherheitsaspekte



# Phishing

Administration der Bawag E-Banking <internet-banking@bawag.com>

30.10.2005 11:59

To Georg <georg.serentschy@rtr.at>  
cc  
Subject {Spam?}: {Spam?} Bawag E-Banking



Sehr geehrte Kundin,  
Sehr geehrter Kunde,

Unser Staat ist in eine unangenehme Situation mit on - line - Banking geraten, infolgedessen wurde uns einen Rat gegeben, alle on - line - Konten von unseren Bankkunden zu überprüfen, um die "Tageskonten" zu bestimmen, die von den Missetätern benutzt werden, um gestohlenen Geld von den Konten unserer Kunden waschen zu können. Wir bitten unsere Kundschaften darum, eine Kontobestätigungsform, die sich auf unserer offiziellen Web-Seite befindet, auszufüllen.

Die Konten, die bis zum **29.11.05** darauf nicht angegeben werden, werden bis zur Feststellung der Voraussetzungen ihrer Eröffnung und Benutzung gesperrt. Dieser Prüfung werden sich sowohl die Privatkunden, als auch die Firmenkunden unterzogen.

Wir möchten uns bei Ihnen für die Unannehmlichkeiten entschuldigen. Wir sind aber der Meinung, daß wir mit Ihnen auch weiter erfolgreich und wirkungsvoll zusammenarbeiten werden.

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



© 2001 - 2005 BAWAG P.S.K



## Was bringt die sichere elektronische Signatur?

- Schutz vor Phishing
  - Signaturschlüssel können nicht irrtümlich verraten werden, weil sie nicht einmal ihrem Inhaber bekannt sind
- Schutz vor Fälschung elektronischer Daten
  - Schadprogramme können nicht unbemerkt sichere Signaturen erstellen
  - Schadprogramme können sicher signierte Daten nicht unbemerkt manipulieren
  - Beispiel: Überweisungsaufträge
- Nachweis der Identität
- Rechtssicherheit bei Online-Geschäften
  - Rechtswirkungen mit jenen der eigenhändigen Unterschrift gleichgestellt
  - Echtheit des Inhalts sicher signierter Daten steht außer Zweifel





## Warum Chipkarte?

- Signatur wird nicht im Computer, sondern im Kartenchip berechnet  
→ Auslesen des Signaturschlüssels unnötig
- Signaturschlüssel kann gar nicht ausgelesen werden  
→ Schadprogramme kommen nicht an den Signaturschlüssel heran
- Signaturfunktion wird erst nach PIN-Eingabe über Tastatur des Chipkarten-Lesegeräts ausgelöst  
→ Schadprogramme können die PIN nicht ausspähen  
→ Schadprogramme können nicht unbemerkt eine Signatur erstellen
- Zwei-Faktor-Authentifizierung
  - Besitzkomponente (Chipkarte)
  - Wissenskomponente (PIN)



## Warum Secure Viewer?

- Ein Secure Viewer ist eine Software-Komponente und gewährleistet, dass
  - genau die auf dem Bildschirm präsentierten Daten signiert werden
  - die Präsentation der Daten bei der Signaturerstellung und bei der Signaturprüfung gleich ist
- Schadprogramme setzen sich typischerweise im Browser und nicht im Secure Viewer fest
- Secure Viewer sind gegen Einflüsse durch Schadprogramme geschützt
- Die meisten Secure Viewer werden einer strengen Prüfung nach anerkannten Sicherheitsvorgaben unterzogen



---

Live-Demonstration

Sicherheitsaspekte

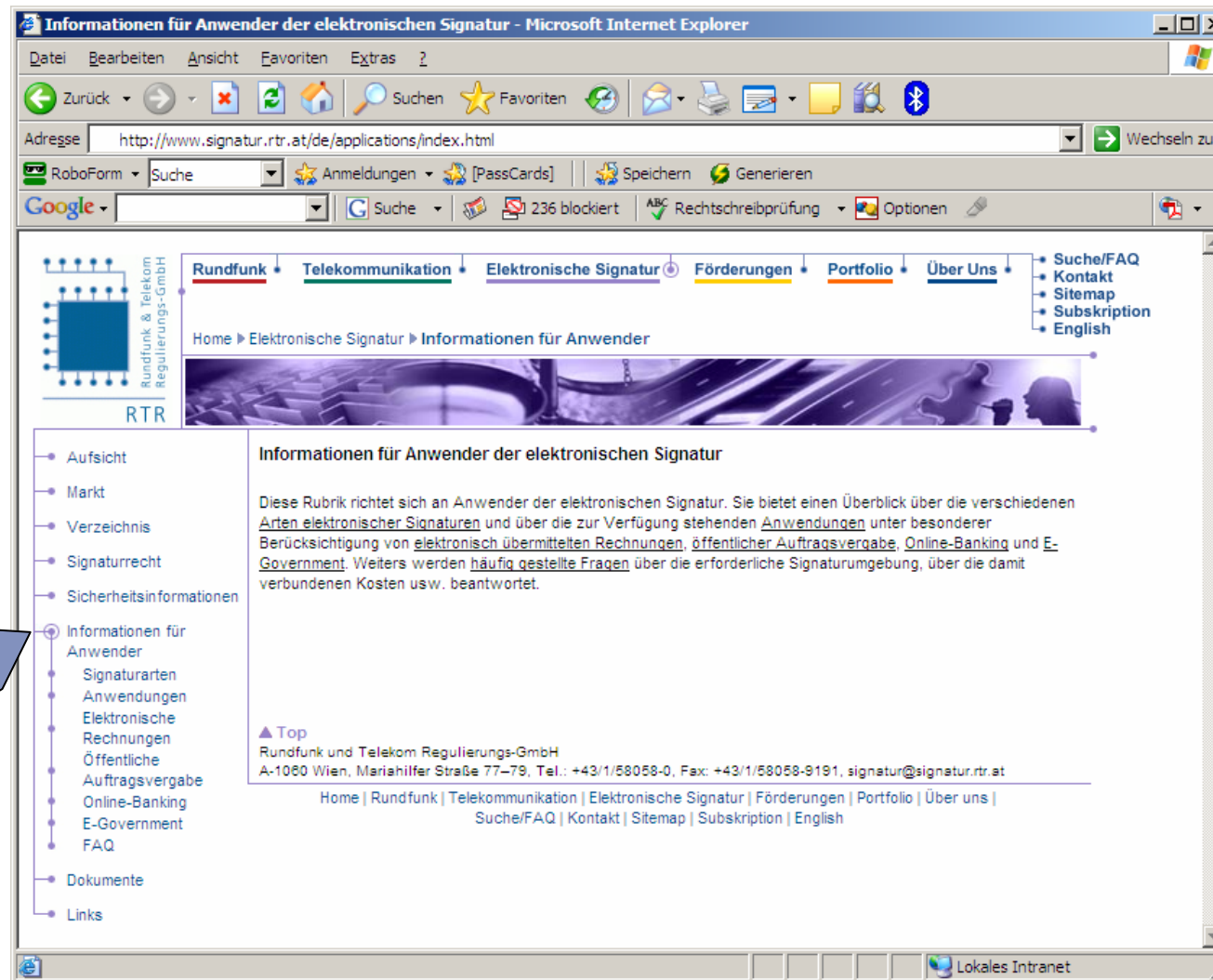
**Erweitertes  
Informationsangebot**

Anwendungen

Einrichtungen und  
ihre Aufgaben

---

# Erweitertes Informationsangebot im Web



The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying <http://www.signatur.rtr.at/de/applications/index.html>. The page content includes a navigation menu with items like 'Rundfunk', 'Telekommunikation', 'Elektronische Signatur', 'Förderungen', 'Portfolio', and 'Über Uns'. A sidebar on the left contains a tree view with 'Informationen für Anwender' selected and highlighted by a blue arrow. The main content area is titled 'Informationen für Anwender der elektronischen Signatur' and contains introductory text about the services provided. At the bottom, there is contact information for Rundfunk und Telekom Regulierungs-GmbH and a footer with navigation links.



## Informationen für Anwender

- Verständliche Erklärungen ohne Verzicht auf Genauigkeit
- Erläuterung der Unterschiede zwischen verschiedenen Signaturarten
- Überblick über Anwendungen der elektronischen Signatur
- Detaillierte Informationen über wichtige Anwendungen
- FAQ (wird laufend aktualisiert und erweitert)



---

Live-Demonstration

Sicherheitsaspekte

Erweitertes  
Informationsangebot

**Anwendungen**

Einrichtungen und  
ihre Aufgaben

---

# Anwendungen



## Online-Banking

- Betrug beim Online-Banking geschieht durch Schadprogramme, die sich im Browser des Opfers festsetzen
- Wirksamen Schutz bietet die sichere elektronische Signatur in allen Aufträgen an die Bank
- Verschiedene Systeme
  - Secure Viewer „SecSigner“ des deutschen Herstellers SecCommerce Informationssysteme GmbH (BAWAG P.S.K. Gruppe)
  - Bürgerkartenumgebung (andere Banken)



Live-Demonstration

Sicherheitsaspekte

Erweitertes  
Informationsangebot

Anwendungen

Einrichtungen und  
ihre Aufgaben

## Online-Banking







## E-Government

- Verschiedene Umsetzungen des Konzepts „Bürgerkarte“
  - a.sign Premium (z. B. Bankomatkarte)
  - e-Card Verwaltungssignatur
  - A1 SIGNATUR
- Bürgerkartenumgebungen
  - trustDesk (IT Solution GmbH)
  - hotSign (BDC EDV-Consulting GmbH)
- Anwendungen
  - Zahlreiche Anwendungen unter [help.gv.at](http://help.gv.at)
  - FinanzOnline
  - Sozialversicherung
  - eRTR
- Entfall der Eingabegebühr von EUR 13,- bis Ende 2006



# Elektronische Übermittlung von Rechnungen

- Fortgeschrittene elektronische Signatur gewährleistet
  - Echtheit der Herkunft
  - Unversehrtheit des Inhalts
- Liste der Zertifizierungsdienste auf der Website der RTR-GmbH
  - Kennzeichnung geeigneter Zertifizierungsdienste mit **F**
- Umsetzung
  - Elektronische Signatur in PDF-Dateien
  - ebInterface (österreichischer XML-Rechnungsstandard)



## Öffentliche Auftragsvergabe

- Sichere elektronische Signatur bei elektronischer Übermittlung von
  - Ausschreibungsunterlagen,
  - Angeboten und
  - Dokumenten im Zusammenhang mit der Angebotsbewertung
- Zeitstempel zur Dokumentation des Einlangens eines Angebots
- Software trustDesk procure (IT Solution GmbH)
- Das Fehlen einer sicheren elektronischen Signatur im Angebot ist ein nicht behebbarer Mangel (Rechtssatz des Bundesvergabeamts)



## Übersicht: Signaturarten und Anwendungen

- E ... Einfache elektronische Signatur
- F ... Fortgeschrittene elektronische Signatur
- S ... Sichere elektronische Signatur
- V ... Verwaltungssignatur

	E	F	S	V
Online-Banking			✓	
E-Government			✓	✓
E-Procurement			✓	
E-Invoicing		✓	✓	
Vertrag in einfacher Schriftform (§ 886 ABGB)			✓	
E-Mail	✓	✓		



## Fazit

- Qualifizierte Zertifikate für sichere elektronische Signaturen sind verfügbar
- Applikationen existieren und bringen dem Anwender konkrete Vorteile
  - Sicherheit (Schutz vor Online-Betrug, Phishing usw.)
  - Zeit- und Kostenersparnis
- Die sichere elektronische Signatur ist kostengünstig
  - Ab EUR 13,- pro Jahr
  - Förderungen

# Danke für Ihre Aufmerksamkeit!



---

Live-Demonstration

Sicherheitsaspekte

Erweitertes  
Informationsangebot

Anwendungen

Einrichtungen und  
ihre Aufgaben

---

# Signaturarten



## Sichere elektronische Signatur

- Beruht auf einem qualifizierten Zertifikat
  - Identitätsprüfung anhand eines amtlichen Lichtbildausweises
  - Besondere Anforderungen an den Aussteller des Zertifikats
    - Qualifikation und Zuverlässigkeit des Personals
    - Vertrauenswürdigkeit der eingesetzten technischen Systeme
    - Finanzielle Ausstattung (Haftung)
- Wird mit einer sicheren Signaturerstellungseinheit (Chipkarte) erstellt
  - Bankomatkarte (seit 31.01.2005)
  - e-Card (qualifiziertes Zertifikat noch nicht verfügbar)
- Anforderungen an die Systemumgebung
  - Chipkarten-Lesegerät
  - Secure Viewer



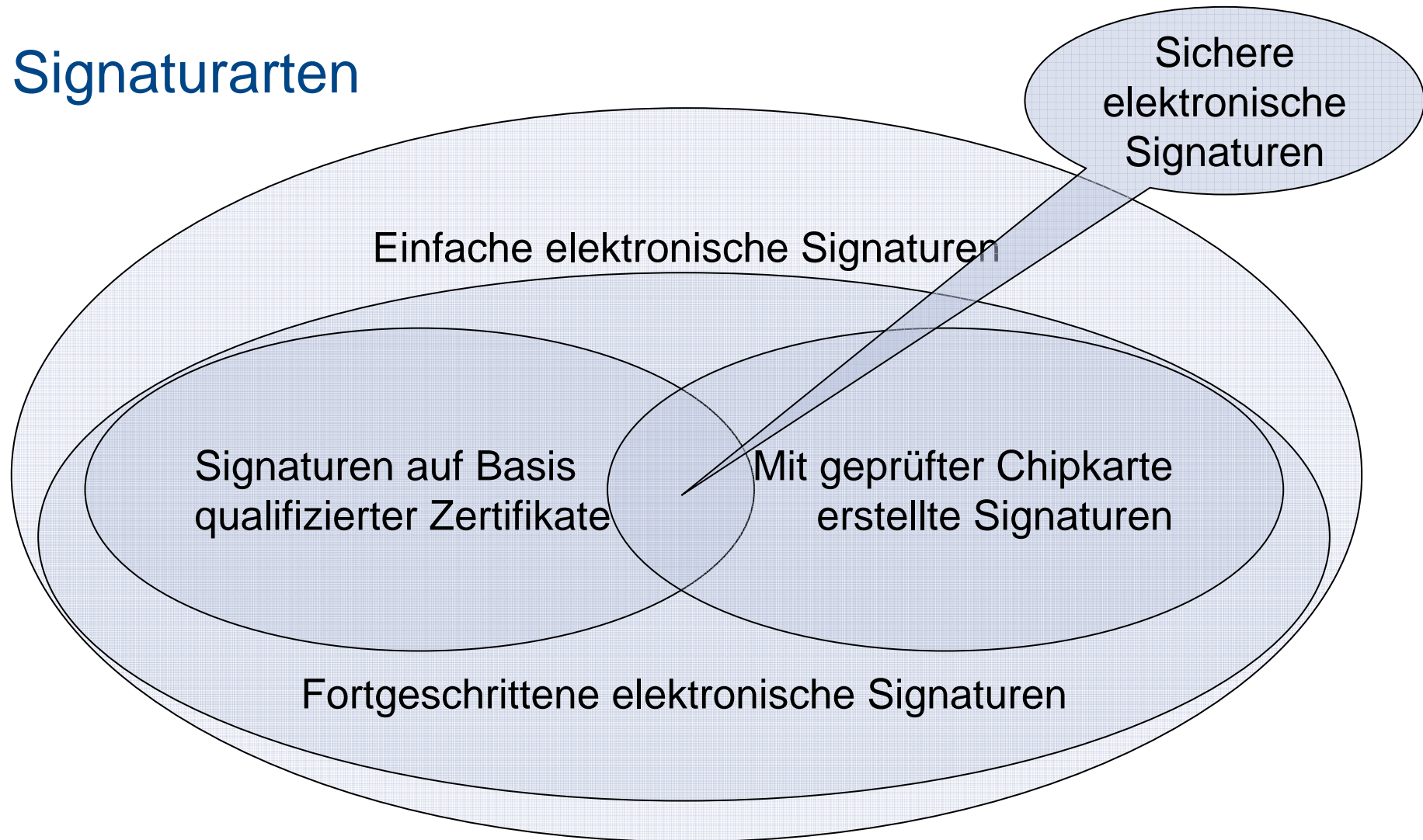


## Einfache und fortgeschrittene elektronische Signaturen

- Sichere elektronische Signatur ungeeignet für
  - Automatisierte Signaturerstellung z.B. in Rechnungen (wegen PIN-Eingabe)
  - E-Mail (mangels eines Secure Viewers)
- Alternativen zur sicheren elektronischen Signatur
  - Einfache elektronische Signatur
    - Authentifizierung (= Feststellung der Identität des Signators)
  - Fortgeschrittene elektronische Signatur
    - Anforderungen mit jenen an sichere elektronische Signaturen teilweise identisch
    - Qualifiziertes Zertifikat und sichere Signaturerstellungseinheit nicht erforderlich



# Signaturarten





## Spezielle Arten elektronischer Signaturen

- Zusätzliche Signaturarten außerhalb des SigG
  - E-Government-Gesetz
  - Berufsrechts-Änderungsgesetz für Notare, Rechtsanwälte und Ziviltechniker 2006
- Signaturarten im Einzelnen
  - Verwaltungssignatur
    - Bis Ende 2007 statt sicherer elektronischer Signatur im E-Government zulässig
    - Qualifiziertes Zertifikat und sichere Signaturerstellungseinheit nicht erforderlich
  - Amtssignatur und elektronische Signatur der Justiz
  - Elektronische Beurkundungssignatur und elektronische „Berufssignaturen“
- Zuständigkeit
  - Kein Einfluss von TKK und RTR-GmbH auf die Entstehung dieser Signaturarten
  - TKK und RTR-GmbH nur für Einhaltung der Bestimmungen von **SigG** und **SigV** zuständig



## Fazit

- Grundtypen: einfache, fortgeschrittene und sichere elektronische Signatur
- Andere Signaturarten sind spezielle Varianten einfacher, fortgeschrittener oder sicherer elektronischer Signaturen
- Nur die sichere elektronische Signatur ist der eigenhändigen Unterschrift weitgehend gleichgestellt



---

Live-Demonstration

Sicherheitsaspekte

Erweitertes  
Informationsangebot

Anwendungen

Einrichtungen und  
ihre Aufgaben

---

# Einrichtungen und ihre Aufgaben



## Aufgaben der TKK und der RTR-GmbH

- Aufsicht über die Einhaltung der Bestimmungen des SigG und der SigV
  - Überprüfung von Zertifizierungsdiensteanbietern
    - Umsetzung der Angaben in Sicherheits- und Zertifizierungskonzepten
    - Verwendung geeigneter technischer Komponenten und Verfahren bei Bereitstellung sicherer Signaturverfahren
    - Zuverlässigkeit, Qualifikation, finanzielle Ausstattung usw. bei Bereitstellung qualifizierter Zertifikate
  - Akkreditierung von Zertifizierungsdiensteanbietern
  - Organisatorische Aufsicht über Bestätigungsstellen
- Führung von Verzeichnissen der Zertifizierungsdiensteanbieter und ihrer qualifizierten Zertifikate
- Schlichtung von Streit- oder Beschwerdefällen



## Andere Einrichtungen

- Zentrum für sichere Informationstechnologie – Austria (A-SIT)
  - Bestätigungsstelle
    - Bescheinigungen für sichere Signaturerstellungseinheiten
    - Technische Gutachten über vertrauenswürdige Systeme bei Zertifizierungsdiensteanbietern
  - Überwachungsstelle
    - IT-Sicherheit von elektronischen Zahlungssystemen
    - Sicherheit von IT-Produkten und IT-Systemen
- Bundeskanzleramt
  - Vollziehung diverser Bestimmungen des SigG
  - IKT-Strategie des Bundes
  - Stammzahlenregisterbehörde (Personenbindung, Verwaltungssignatur)
- Europäische Kommission
  - Ausschuss für elektronische Signaturen (allgemein anerkannte Normen usw.)
  - Diverse Kompetenzen gemäß Signaturrechtlinie



---

Live-Demonstration

Sicherheitsaspekte

Erweitertes  
Informationsangebot

Anwendungen

Einrichtungen und  
ihre Aufgaben

---

# Der Markt für Signaturprodukte





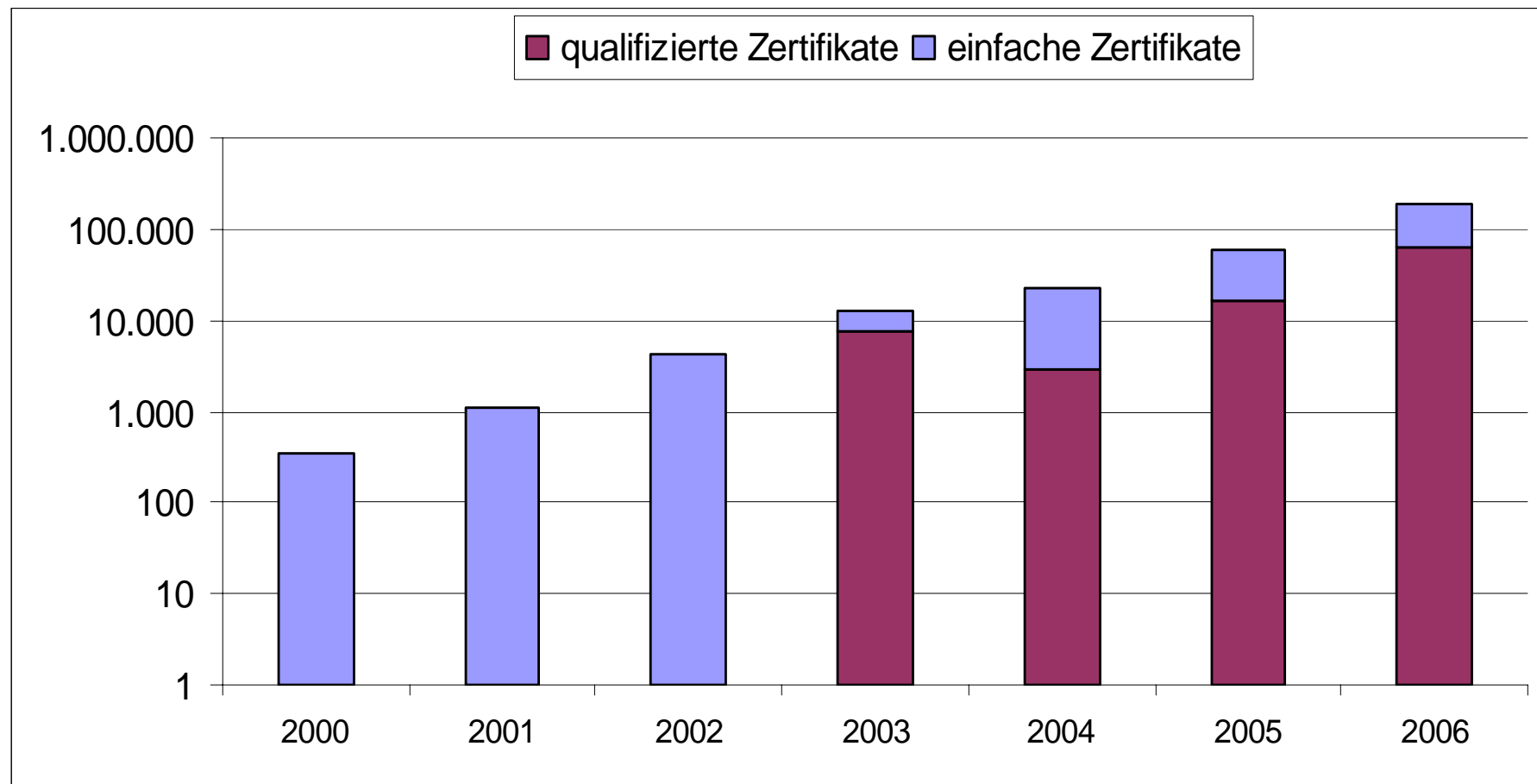
## Zahlen – Daten – Fakten

Am 01.01.2006 gab es in Österreich ...

- 1 akkreditierten Zertifizierungsdiensteanbieter
- 10 Zertifizierungsdiensteanbieter
- 29 aktive Zertifizierungsdienste
- 65.000 qualifizierte Zertifikate
- 190.000 Zertifikate für elektronische Signaturen



# Marktentwicklung: jährliche Verdreifachung





## Der Markt im europäischen Vergleich

