

## Sicherheit im Onlinebanking

Informationen zu 'Man in the Middle'- Attacken und zur Überprüfung des sog. Fingerprints

Bei der sogenannten "Man in the Middle"-Attacke werden – wie der Name vermuten lässt – die Daten des Kunden z.B. durch eine Manipulation von Adressen von Datenpaketen (IP- oder MAC-Adressen, Spoofing) nicht an die eigentliche Zieladresse weitergeleitet, sondern vom Angreifer abgefangen. Der Webbrowser des Kunden wird in diesem Fall nicht mit dem gewünschten InternetBanking-Server verbunden, sondern mit dem Server des Hackers. Der Server des Hackers kontaktiert dann den InternetBanking-Server und wartet auf Eingaben des Kunden.



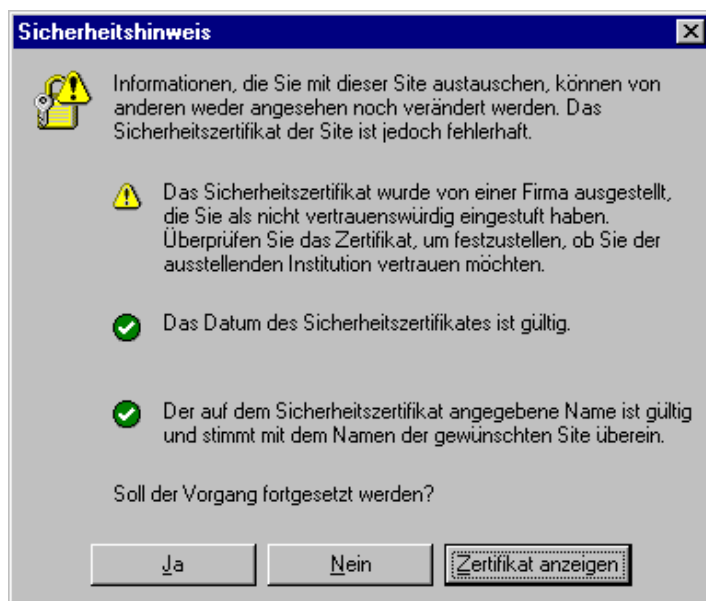
Der Kunde wiederum glaubt, mit der Bank zu kommunizieren. Der InternetBanking-Server geht davon aus, einen Kunden zu bedienen. In Wirklichkeit kommunizieren beide – InternetBanking-Server und Kunden-PC – mit dem Server des Hackers. Gelingt dieses Szenario, so kann eine verschlüsselte Verbindung zum "Opfer" aufgebaut werden. Es erscheint auch das "Verschlüsselungssymbol" im Webbrowser. Da die verwendeten Schlüssel (Zertifikate) jedoch die des Angreifers sind, kann dieser die Daten auch entschlüsseln.

Somit hat ein Angreifer die Möglichkeit z.B. Überweisungsdaten zu verändern und diese unbemerkt an das Banksystem weiterzuleiten.

**Sie haben verschiedene Möglichkeiten, einen solchen Angriff zu erkennen und sich davor zu schützen!**

Wir setzen für unsere InternetBanking-Anwendung ein SSL Zertifikat mit hoher Verschlüsselungsstärke (128Bit) ein. Dies gewährleistet, dass ein Dritter auf dem Übertragungsweg nicht unbemerkt Ihre persönlichen Daten entschlüsseln und somit ausspähen kann. Nähere Informationen finden Sie auch im Menüpunkt "Sicherheitshinweise" auf der Seite eBanking-Login.

Sobald Unstimmigkeiten im Zusammenhang mit den Zertifikatsdaten auftreten, erhalten Sie als Nutzer einen entsprechenden Warnhinweis. Hier exemplarisch eine Meldung des Internet Explorers:



Mögliche Hinweise können sein:

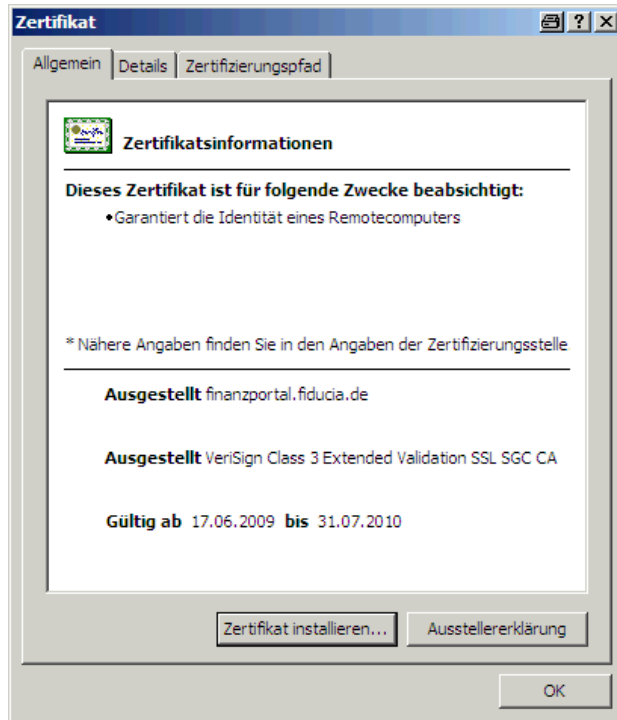
- Der Zertifikataussteller ist nicht vertrauenswürdig.
- Das Zertifikat ist noch nicht oder nicht mehr gültig.
- Der Name der Internetseite, auf die das Zertifikat ausgestellt ist, weicht von den Zertifikatsdaten ab.

**Werden hier Fehler- bzw. Warnmeldungen angezeigt, bestätigen Sie diese niemals ohne Überprüfung des Zertifikats mit "JA"!**

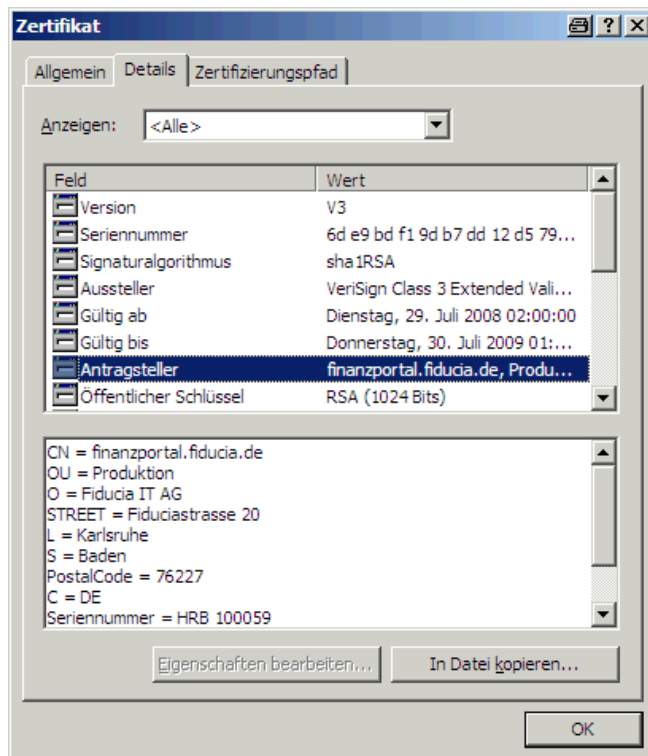
**Die wichtigsten Punkte sind:**

Ist das Zertifikat noch gültig? Wenn ja und es erscheint trotzdem ein Fehler: Ist Ihr Systemdatum noch aktuell?

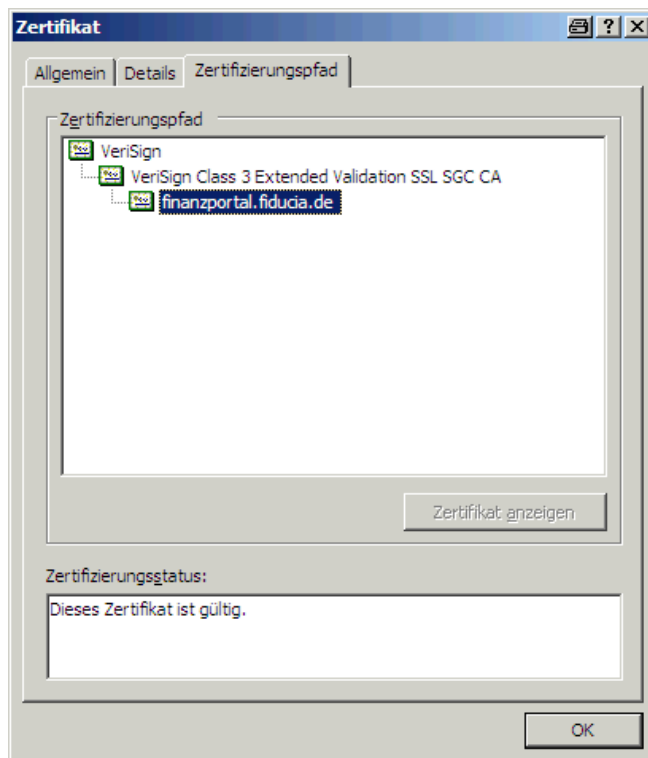
Unsere Zertifikate sind immer auf die Internetadresse **finanzportal.fiducia.de** ausgestellt.



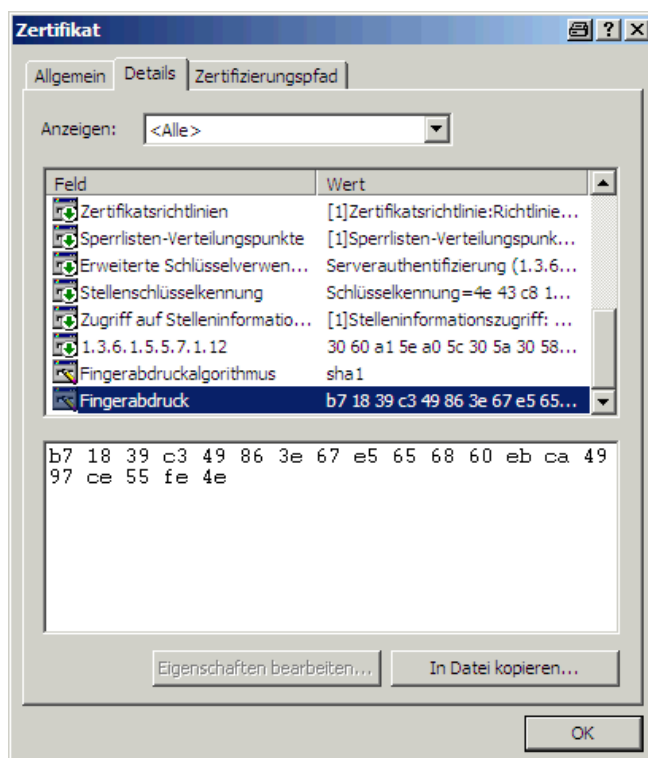
Das Zertifikat ist auf die **FIDUCIA IT AG** ausgestellt (Antragsteller):



Achten Sie darauf, dass der Zertifizierungspfad nicht unterbrochen ist.



Der "Fingerabdruck" ist das entscheidende Merkmal zur Überprüfung des Zertifikats:



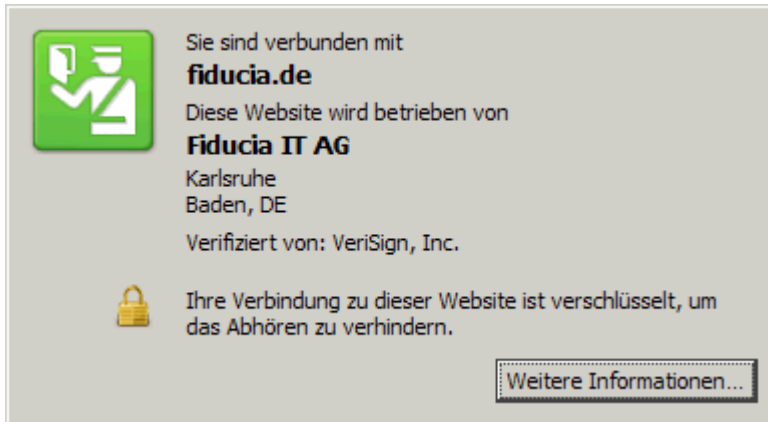
Fallen Ihnen in Zusammenhang mit diesen Prüfungen "Ungereimtheiten" auf, empfehlen wir:

- Bestätigen Sie den Hinweis niemals mit "JA".
- Trennen Sie ggf. Ihre Internetverbindung.
- Wenden Sie sich an Ihre Kundenbetreuung.


## Einstellungen im Firefox

Klick auf  in der Adresszeile

Es wird Folgendes angezeigt:



Sie sind verbunden mit  
**fiducia.de**  
Diese Website wird betrieben von  
**Fiducia IT AG**  
Karlsruhe  
Baden, DE  
Verifiziert von: VeriSign, Inc.

 Ihre Verbindung zu dieser Website ist verschlüsselt, um das Abhören zu verhindern.

[Weitere Informationen...](#)

Klicken Sie bitte den Button „Weitere Informationen“ an

... und im folgenden Fenster im Abschnitt „Sicherheit“ den Button „Zertifikat anzeigen“



Seiteninformation - <https://finanzportal.fiducia.de/ebpg01/entry?rzid=XC&rzbk=0102>

Allgemein Medien Berechtigungen **Sicherheit**

Website-Identität

Website: **finanzportal.fiducia.de**  
Besitzer: **Fiducia IT AG**  
Validiert von: **VeriSign, Inc.**

[Zertifikat anzeigen](#)

Datenschutz & Chronik

Habe ich diese Website früher schon einmal besucht? **Nein**

Speichert diese Website Daten (Cookies) auf meinem Computer? **Ja** [Cookies anzeigen](#)

Habe ich Passwörter für diese Website gespeichert? **Nein** [Gespeicherte Passwörter anzeigen](#)

Technische Details

**Verbindung verschlüsselt: Hochgradige Verschlüsselung (AES-256 256 bit)**  
Die Seite, die Sie ansehen, wurde verschlüsselt, bevor sie über das Internet übermittelt wurde.  
Verschlüsselung macht es für unberechtigte Personen sehr schwierig, zwischen Computern übertragene Informationen anzusehen. Daher ist es sehr unwahrscheinlich, dass jemand diese Seite gelesen hat, als sie über das Netzwerk gesendet wurde.

Es wird danach folgender Fingerabdruck angezeigt:

Zertifikat-Ansicht: "finanzportal.fiducia.de"

Allgemein Details

**Dieses Zertifikat wurde für die folgenden Verwendungen verifiziert:**

- SSL-Server-Zertifikat
- SSL-Server mit Step-up

**Ausgestellt für**

Allgemeiner Name (CN)	finanzportal.fiducia.de
Organisation (O)	Fiducia IT AG
Organisationseinheit (OU)	Produktion
Seriennummer	24:05:B5:1E:D2:17:95:0A:46:CA:EF:00:1F:8A:FB:AA

**Ausgestellt von**

Allgemeiner Name (CN)	VeriSign Class 3 Extended Validation SSL SGC CA
Organisation (O)	VeriSign, Inc.
Organisationseinheit (OU)	VeriSign Trust Network

**Validität**

Ausgestellt am	17.06.2009
Läuft ab am	31.07.2010

**Fingerabdrücke**

SHA1-Fingerabdruck	B7:18:39:C3:49:86:3E:67:E5:65:68:60:EB:CA:49:97:CE:55:FE:4E
MD5-Fingerabdruck	16:D6:F1:4C:B5:6E:0D:3B:69:B0:A3:2F:44:50:13:FF

Schließen