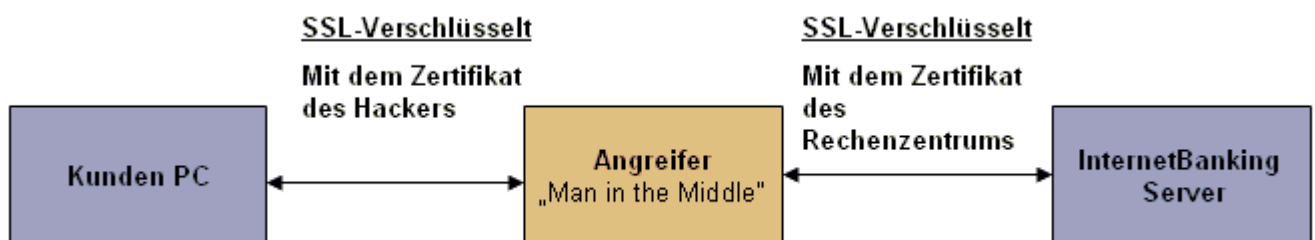


Information zu 'Man in the middle' und Überprüfung des Fingerprints

Worum geht es?

Immer wieder werden in Vorträgen oder auf Messen sogenannte "Live-Hacking"- Demonstrationen zu OnlineBanking gezeigt. Das eingesetzte Verfahren stellt in der Regel keine neue Enthüllung dar, sondern beruht oft auf einer sogenannten "Man-in-the-Middle"-Attacke.

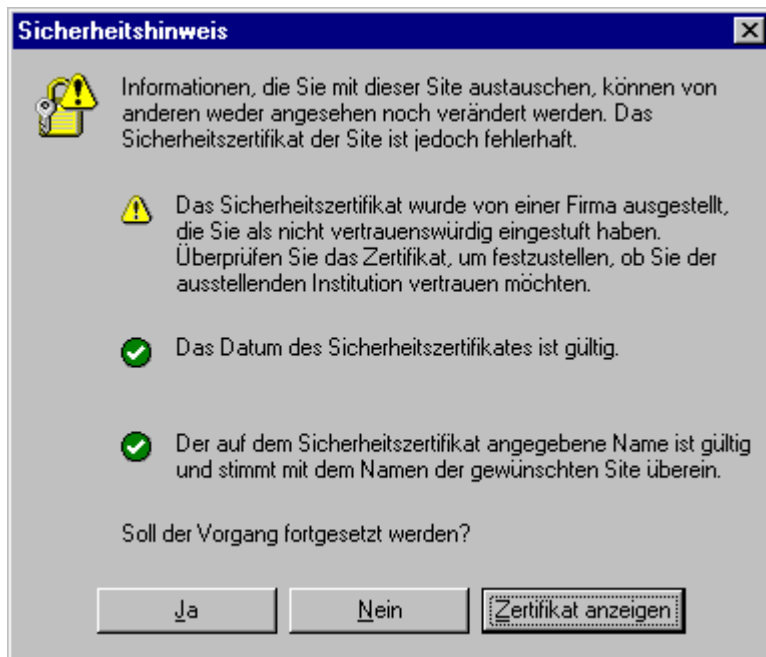
Wie der Name vermuten lässt, werden die Daten des Kunden z.B. durch eine Manipulation von IP- oder MAC-Adressen (Spoofing) nicht an die eigentliche Zieladresse weitergeleitet, sondern durch den Angreifer abgefangen. Durch diese Manipulation wird der Webbrowser des Kunden also nicht mit dem z.B. gewünschten InternetBanking-Server verbunden, sondern mit dem Server des Hackers. Auf eine Anfrage hin, kontaktiert der Server des Hackers zusätzlich den InternetBanking-Server und wartet auf Eingaben des Kunden.



Der Kunde glaubt also mit der Bank zu kommunizieren und der InternetBanking-Server geht davon aus, einen Kunden zu bedienen. In Wirklichkeit kommunizieren beide legitimen Kommunikationspartner (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 "Verschlüsselungs-Symbol" im Webbrowser. Da die verwendeten Schlüssel (Zertifikat) jedoch die des Angreifers sind, kann dieser die Daten wiederum entschlüsseln. Somit hat ein Angreifer die Möglichkeit z.B. Überweisungsdaten zu verändern und diese unbemerkt an das Banksystem weiterzuleiten.

Was ist zu beachten?

Der Bankkunde hat verschiedene Möglichkeiten, einen solchen Angriff zu erkennen und sich zu schützen: Wir setzen für unsere InternetBanking-Anwendung ein SSL Zertifikat mit hoher Verschlüsselungsstärke (128Bit) ein. Dadurch ist 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 eBanking-Login Seite. Sobald Unstimmigkeiten im Zusammenhang mit den Zertifikatsdaten auftreten, erhält der Nutzer einen entsprechenden Warnhinweis, hier ein Beispiel (exemplarisch eine Meldung des Internet Explorers).



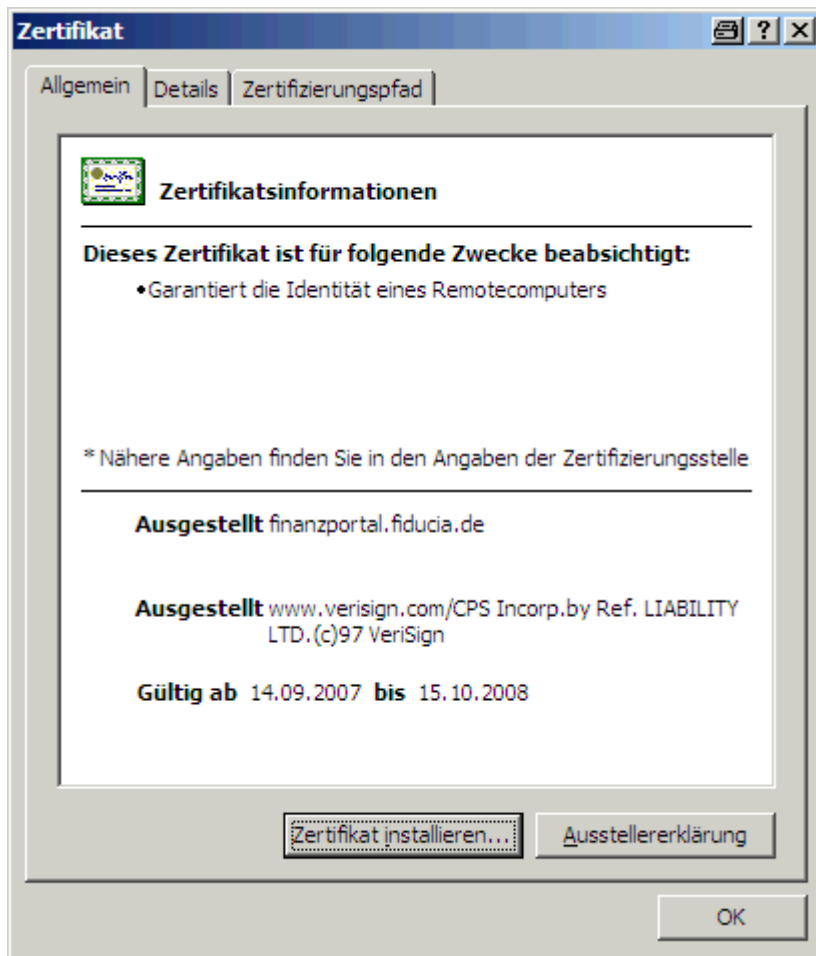
Mögliche Hinweise könnten sein:

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

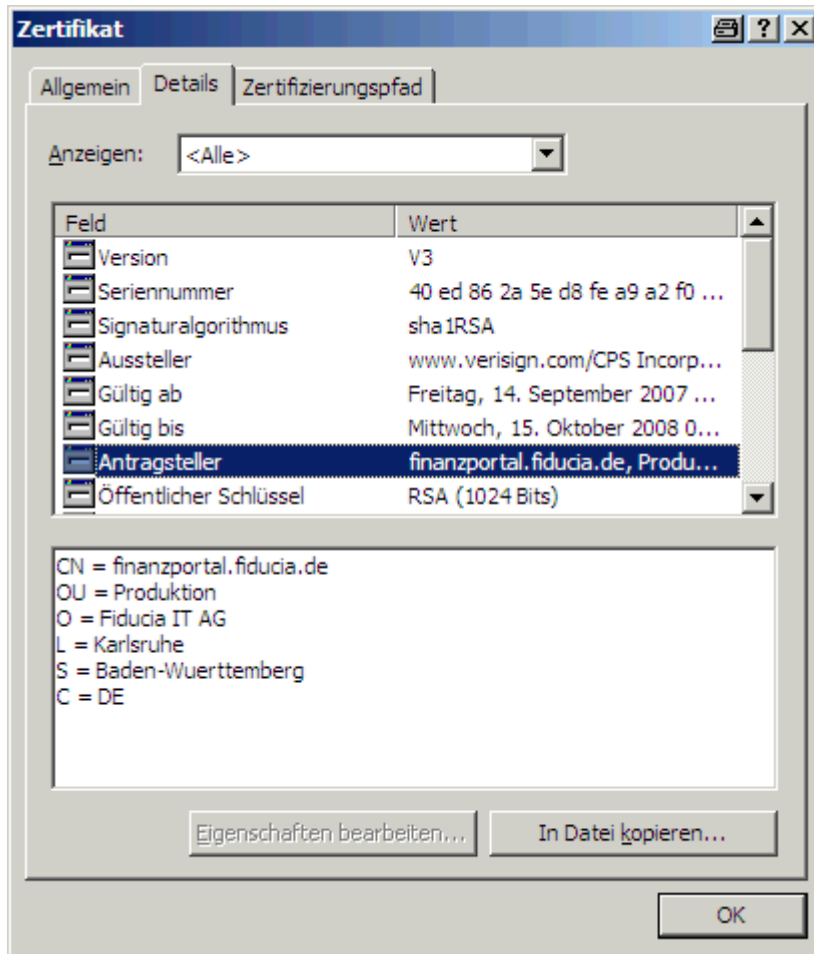
Falls hier Fehler- bzw. Warnmeldungen angezeigt werden, sind diese Meldungen niemals ohne Überprüfung des Zertifikats mit "JA" zu bestätigen!

Wichtig!

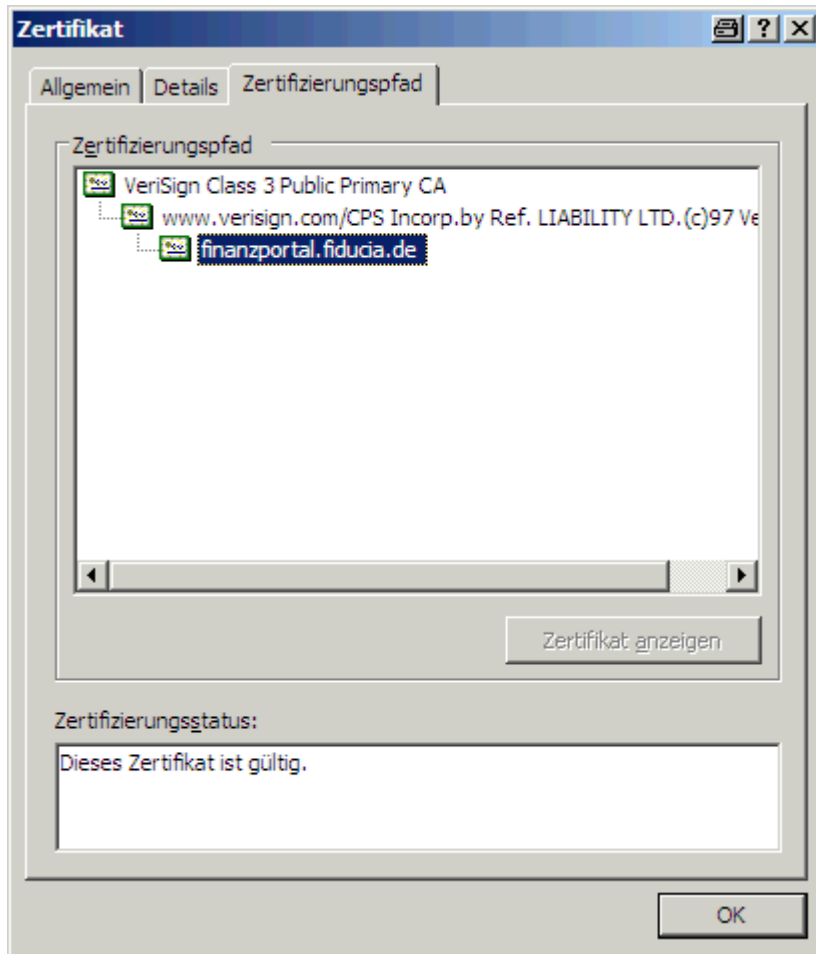
Ist das Zertifikat noch gültig? Wenn ja und es erscheint trotzdem ein Fehler:
Ist Ihr Systemdatum noch aktuell? Unsere Zertifikate sind immer auf die Internetadresse **finanzportal.fiducia.de** ausgestellt.



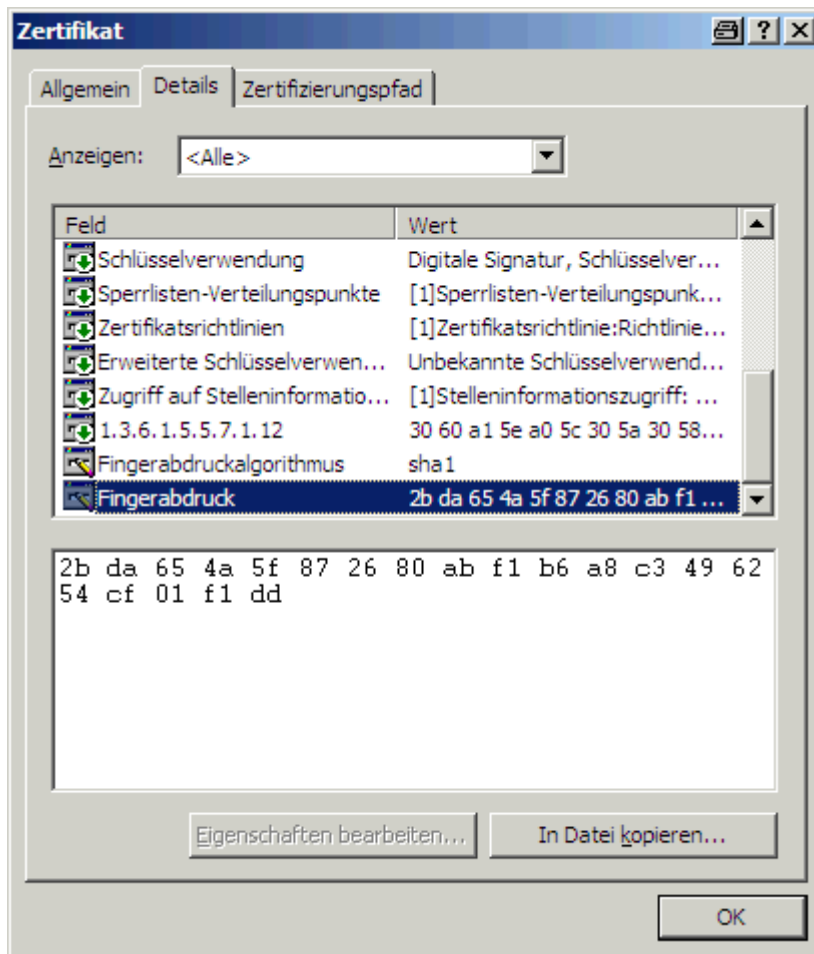
Das Zertifikat ist auf die **FIDUCIA IT AG** ausgestellt (Antragsteller).



Es ist darauf zu achten, dass der Zertifizierungspfad nicht unterbrochen ist




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



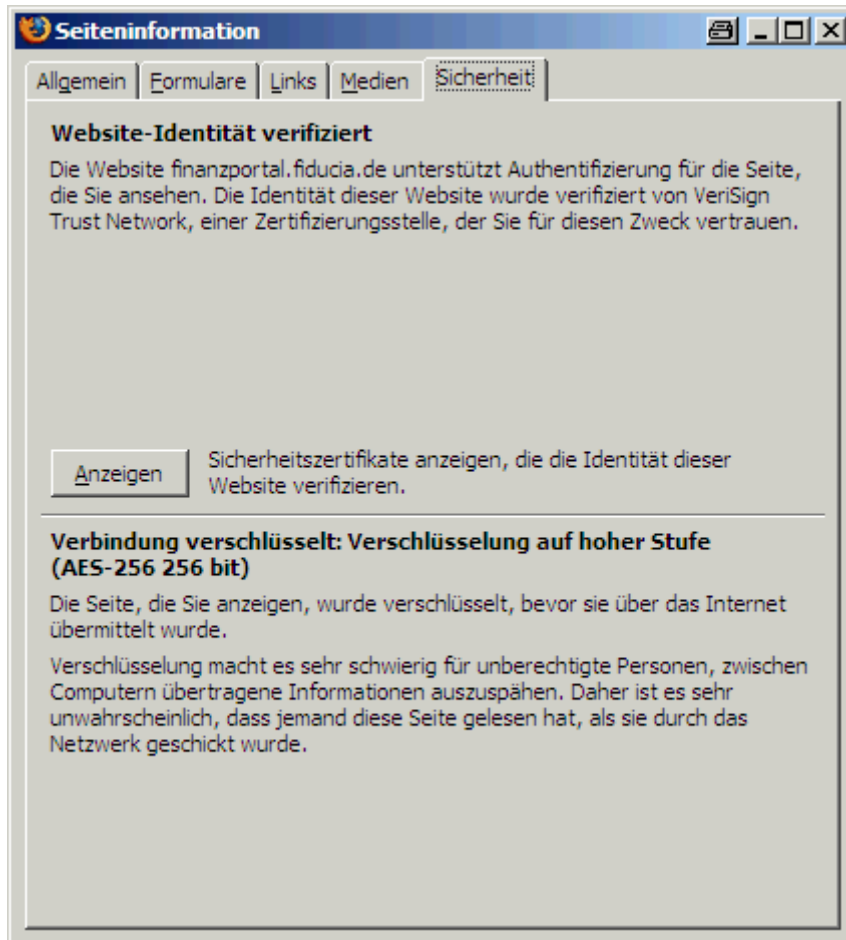
Sollte Ihnen im Zusammenhang mit diesen Prüfungen "Ungereimtheiten" auffallen, empfehlen wir Ihnen:

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

Einstellungen im Firefox

Doppelklick auf finanzportal.fiducia.de 

Im Reiter 'Sicherheit' den Button 'Anzeigen' anklicken



Die 'Fingerabdrücke' im Reiter 'Allgemein' überprüfen.