

Sicherheitszertifikate der DKB AG und ihrer Partner

Prüfen Sie die Zertifikate zu Ihrer eigenen Sicherheit mit Hilfe der unten aufgeführten Fingerabdrücke!

Ihre Daten werden durch das Verschlüsselungsverfahren SSL (Secure Socket Layer) geschützt, das vor dem unbefugten Zugriff durch Dritte schützt. Wenn die 256 Bit-Verschlüsselung aktiviert ist, können die Daten von Dritten weder gelesen noch verwendet werden.

Das geschlossene Sicherheitsschloss rechts neben der Domainanzeige Ihres Browserfensters zeigt Ihnen, dass Ihre Daten verschlüsselt übertragen werden. Mit einem Klick auf das Schloss-Symbol ist überprüfbar, ob ein auf die Bank oder ihre Partner ausgestelltes Zertifikat die Echtheit des Kommunikationspartners bestätigt. Ist das Schloss einmal geöffnet oder das Zertifikat hier nicht aufgelistet, sollten Sie keine sicherheitsrelevanten Daten eingeben.

So überprüfen Sie die Sicherheitszertifikate der Deutschen Kreditbank AG und ihrer Partner:

Internet Explorer:

Das Schloss-Symbol erscheint bei einer sicheren Verbindung in der Statusleiste oben rechts. Durch Doppelklick auf dieses Symbol öffnet sich das Dialogfenster mit Eigenschaften und Inhalten des Zertifikates.

Firefox:

Das Schloss-Symbol in der Statusleiste unten rechts erscheint bei einer sicheren Verbindung geschlossen. Mit Klick auf das Schloss-Symbol in der Statusleiste öffnet sich das Dialogfenster mit den Sicherheitsinformationen. Über die Schaltflächen „Anzeigen“ können Sie sich das Verfallsdatum („Validität“ - „Läuft ab am ...“) anzeigen lassen und sehen, ob das Zertifikat für die Deutsche Kreditbank AG oder für ihre Partner („Herausgegeben für ...“) ausgestellt ist (das aktuelle Zertifikat der DKB AG ist gültig bis 31.08.2013).

Dies sind die aktuellen Zertifikatsdetails für das Zertifikat für banking.dkb.de:

Ausgestellt von: Allgemeiner Name (CN): VeriSign Class 3 Extended Validation SSL SGC CA

Organisation (O): VeriSign, Inc.

Organisationseinheit (OU): VeriSign Trust Network

Ausgestellt für: Allgemeiner Name (CN): banking.dkb.de

Organisation (O): Deutsche Kreditbank Aktiengesellschaft

Organisationseinheit (OU): Terms of use at www.verisign.com/rpa (c)05

Seriennummer: 5B:D8:D5:1B:49:40:1B:1D:C6:CA:E4:C7:6E:A5:20:54

Der Fingerabdruck und das Ablaufdatum muss mit den unten benannten Angaben übereinstimmen.

Beim Gebrauch des Firefox sollten Sie darauf achten, dass bei den Kontaktformularen der Homepage dkb.de sowie nach dem Einloggen in das Internet Banking in Ihrer Browserleiste ein grüner Balken angezeigt wird, die sogenannte „Green Bar“. Diese Erweiterung zeigt als zusätzliche Sicherheits-Information die Zertifikats-Eigentümer und CA Aussteller-Information an, wenn der Browser ein VeriSign, thawte und/oder GeoTrust EV Zertifikat enthält. Diese Zusatzinformation ist verfügbar, wenn auf das Schloss-Symbol in der Adressleiste oder unten rechts geklickt wird.

Wie überprüfe ich den elektronischen Fingerabdruck im Internet-Banking?

Der elektronische Fingerabdruck ist ein Code, der aus mehreren Ziffern und Buchstaben besteht. Zur Überprüfung gehen Sie bitte wie folgt vor:

Internet Explorer:

Nachdem Sie das Zertifikat aufgerufen haben, finden Sie als letzten Eintrag unter „Details“ den Fingerabdruck. Dieser muss identisch sein mit dem nachfolgenden Code:

ce 23 f0 90 b7 b4 6c 4b 03 bf ac e6 df 05 f9 86 a4 fc 7d

Firefox:

Nach Klick auf das Schloss-Symbol finden Sie in den Sicherheitsinformationen über die Schaltfläche „Zertifikat anzeigen“ den Eintrag „Fingerabdrücke“. Der „MD5 Fingerprint“ (Fingerabdruck) muss identisch sein mit dem nachfolgenden Code:

9A:F6:1F:31:2A:43:31:EE:71:F0:20:92:15:2B:79:1C

Bei Firefox finden Sie zusätzlich den o.g. Fingerabdruck des Internet Explorers („SHA1 Fingerprint“):

CE:23:3F:F0:90:B7:B4:6C:4B:03:BF:AC:E6:DF:05:F9:86:A4:FC:7D

Dieses Zertifikat ist gültig bis zum 31.08.2013.

Das Wildcard-Zertifikat schützt beliebig viele Subdomains der DKB-Domain. Es lautet:

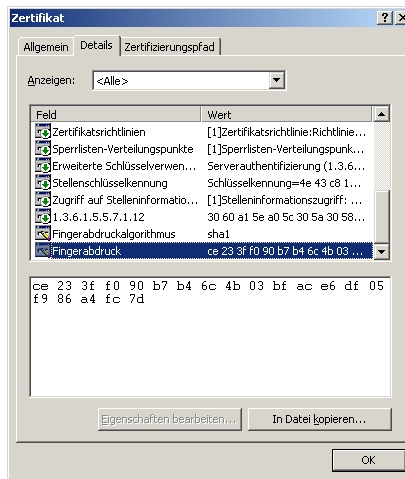
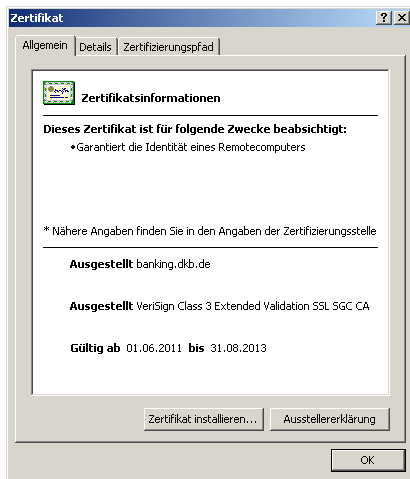
81 ce 6a 06 92 68 dd eb 4e de 42 bf db 87 35 4e 27 18 a5 e4

Stimmen die Fingerabdrücke nicht mit den o.g. überein, sollten Sie keine sensiblen Daten in die aufgerufene Seite oder das Online Banking eingeben.

Falls Sie eine Banking-Software wie z. B. StarMoney benutzen, ist ein Abgleich des elektronischen Fingerabdrucks nicht erforderlich. In diesem Fall wird die Zertifikatsprüfung automatisch durch die Software vorgenommen.

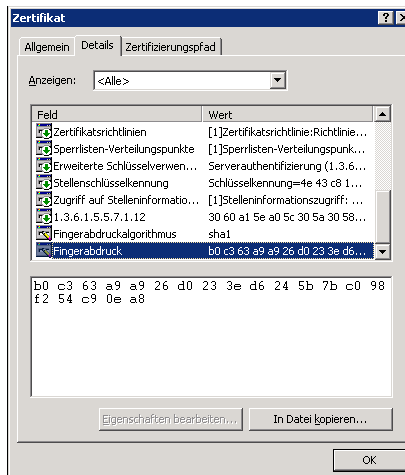
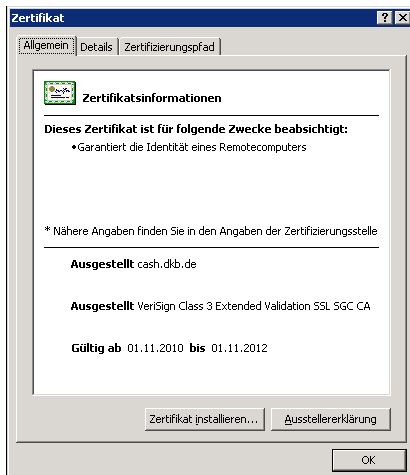
Internet-Banking

<https://banking.dkb.de> (EV-Zertifikat)



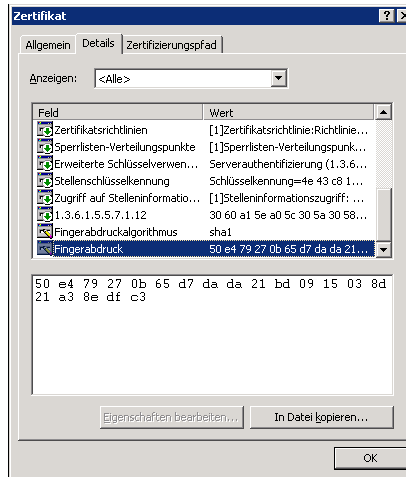
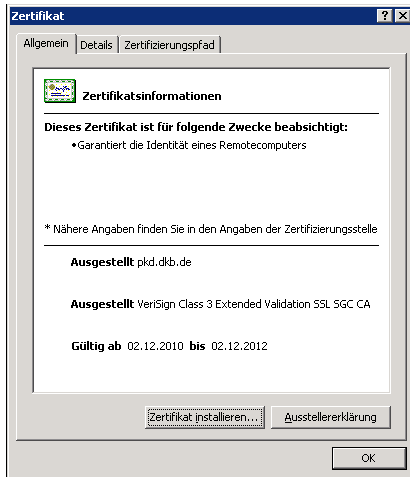
DKB-Cash

<https://cash.dkb.de> (EV-Zertifikat)



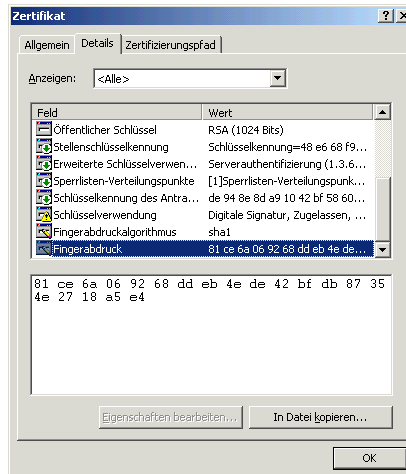
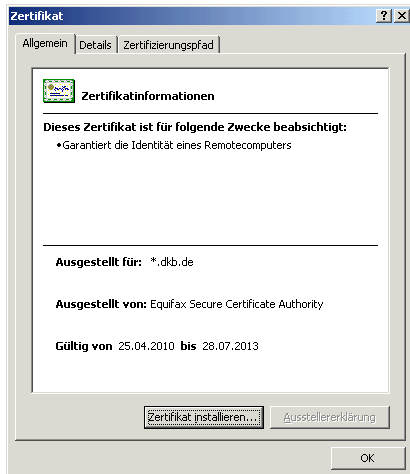
DKB-Privatdarlehen

<https://pkd.dkb.de> (EV-Zertifikat)

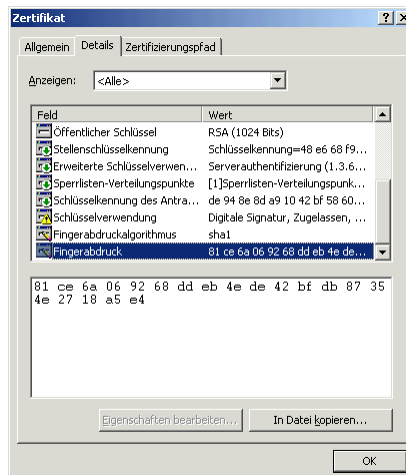
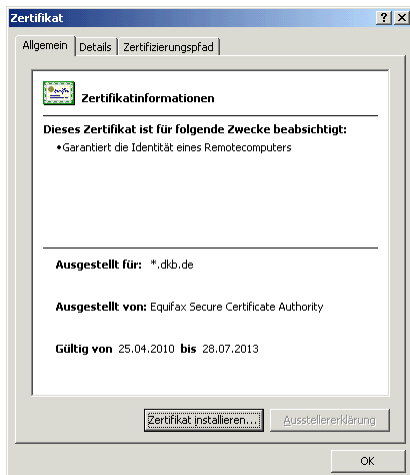


DKB-Energie

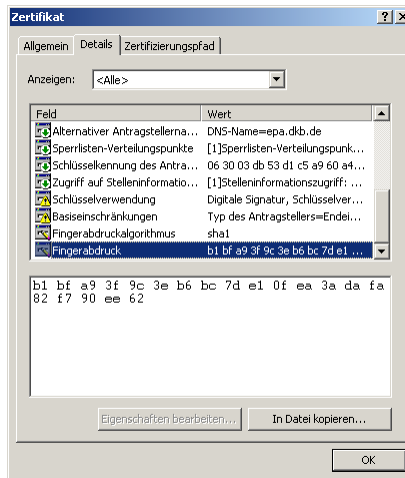
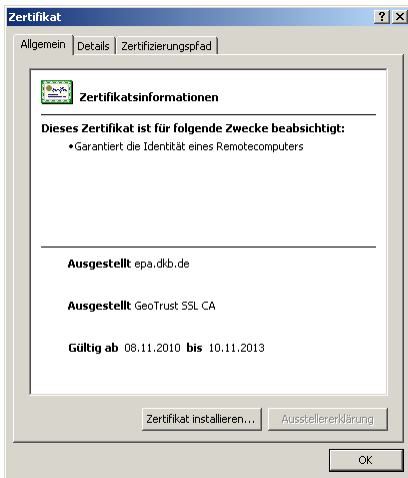
<https://pde.dkb.de> (Wildcardzertifikat)



<https://aktionen.dkb.de> (Wildcardzertifikat)



<https://epa.dkb.de> (Wildcardzertifikat)



Unter einigen URLs bekommen Sie eine leere Seite angezeigt. Hier können Sie die Zertifikate mit den entsprechenden Fingerprints folgendermaßen überprüfen:

Auf der rechten Seite der Browserleiste wählen Sie unter dem Menüpunkt ‚Sicherheit‘ den ‚Sicherheitsbericht‘ aus. Dort können Sie sich in der Website-Identifizierung das Zertifikat anzeigen lassen und den Fingerprint mit dem hier Hinterlegten abgleichen.

Hinweis für die Prüfung von DKB-Partner-Seiten

Zu Ihrer Sicherheit sollten Sie die Fingerabdrücke unserer Partner auch immer prüfen. Die Partner-Domains sind teilweise per iFrame, mit externen Grafiken oder durch Trigger-URLs eingebunden. Beim Internet Explorer nehmen Sie die Prüfung wie oben erklärt vor; bei Firefox funktioniert die Prüfung der Fingerabdrücke von Partnerseiten so:

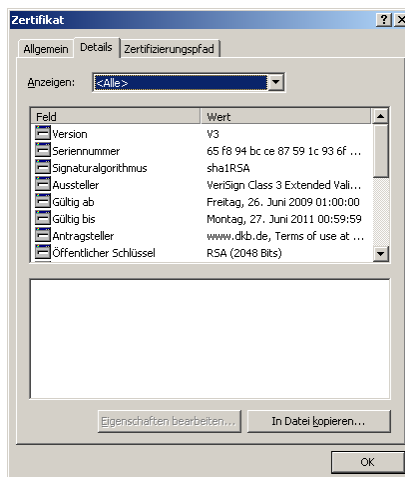
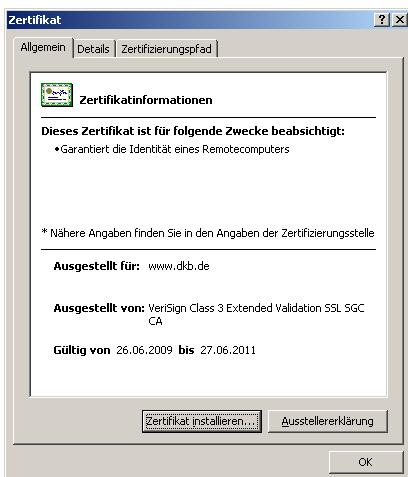
Beispielseite:

https://www.dkb.de/kundenservice/sicherheit/sicherheit_beim_bezahlen_im_internet/registrierung/index.html

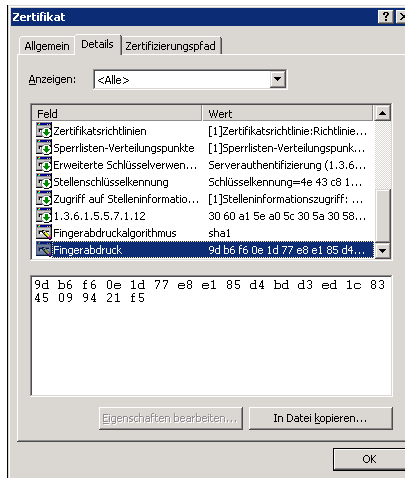
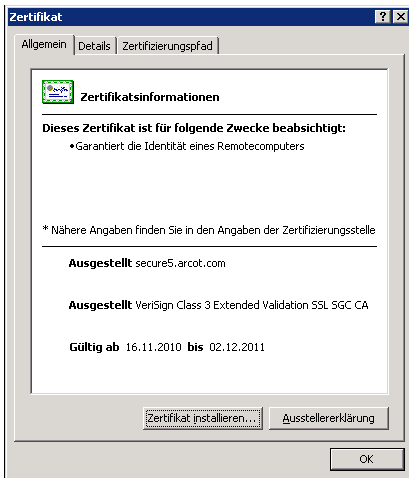
- den Bereich des iFrames per Rechtsklick auswählen
 - » „Nur diesen Frame anzeigen
- Dann landen Sie auf der eingebunden Webseite
 - » https://secure5.arcof.com/vpas/dkb_visa/enroll/enroll.jsp?locale=de_DE&bankid=5400
 - » erst hier können Sie das Zertifikat/ den Fingerabdruck des Partners prüfen

KFZ Versicherungsrechner

<https://www.insurancestation.de/>



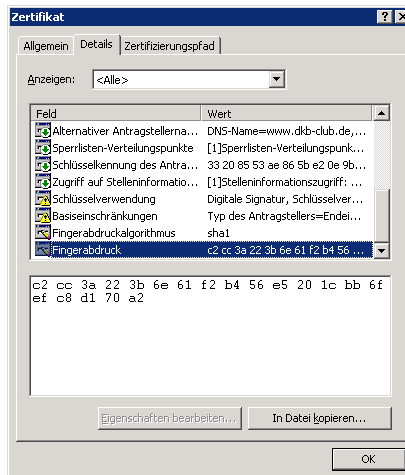
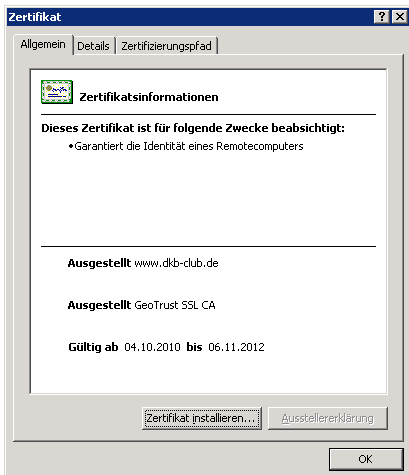
DKB-VISA-Card Verified by Visa und MasterCard® SecureCode™
<https://secure5.arcof.com>



giropay GmbH
<https://giropay.dkb.de> (EV-Zertifikat)

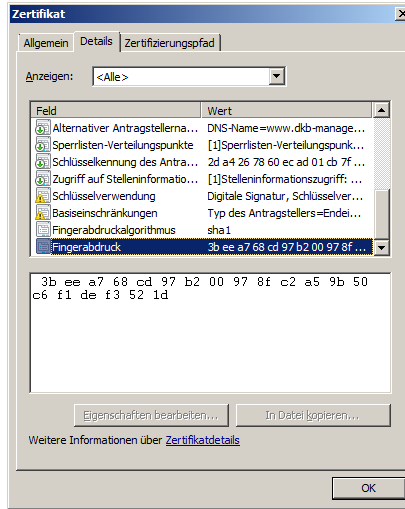
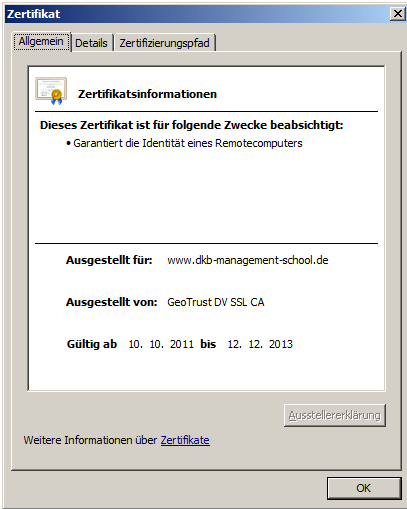


DKB-Club
<https://www.dkb-club.de>



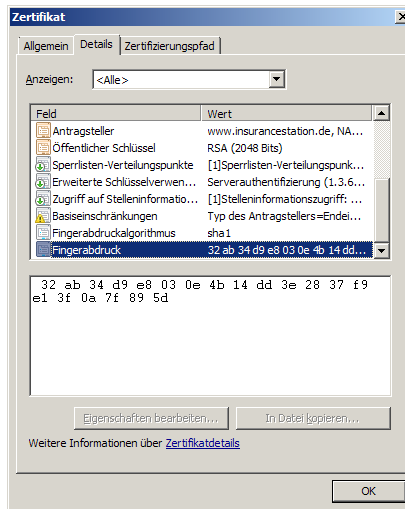
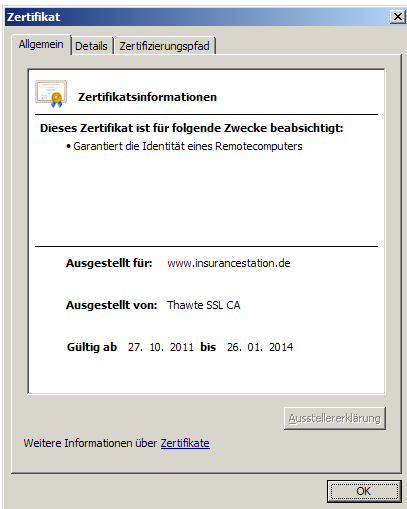
DKB Management School

<https://www.dkb-management-school.de/>



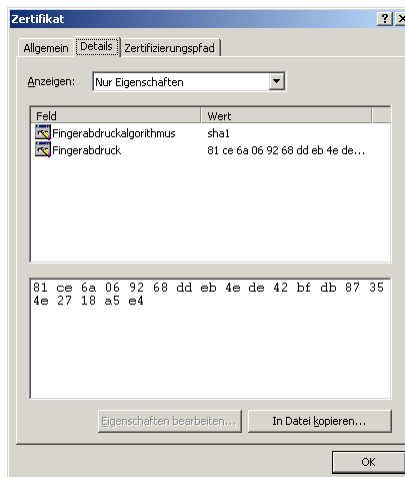
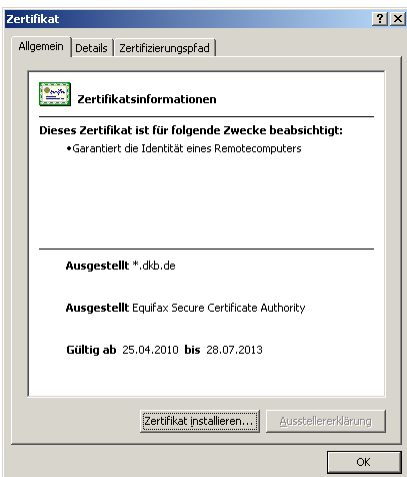
DKB-KFZ-Rechner

https://www.insurancestation.de/makler/pages/kfz/schnellberechnung/default.asp?domain=dkb_kfz_rechner



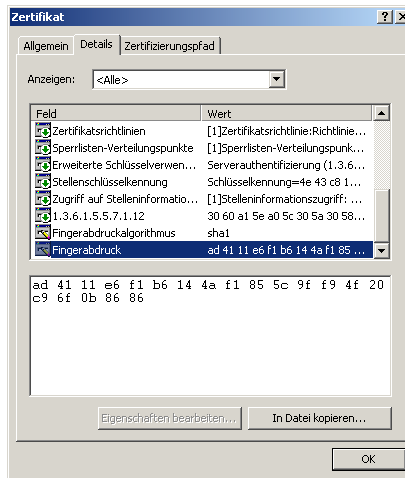
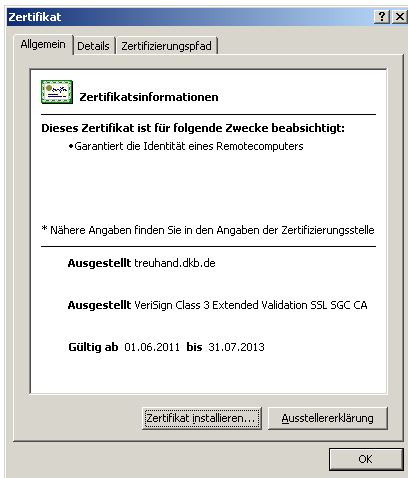
Vermittlerplattform

<https://vermittler.dkb.de> (Wildcardzertifikat)



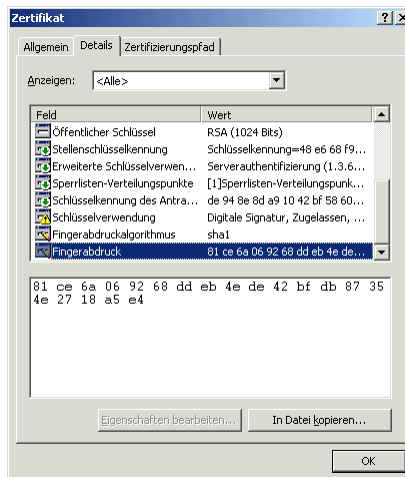
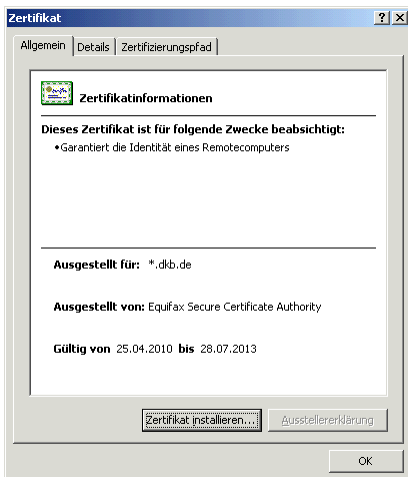
Treuhänderplattform

<https://treuhand.dkb.de> (EV-Zertifikat)



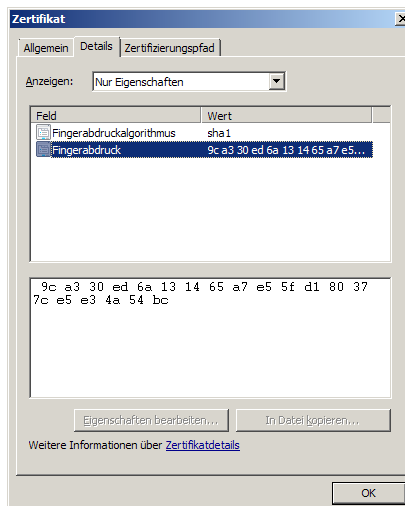
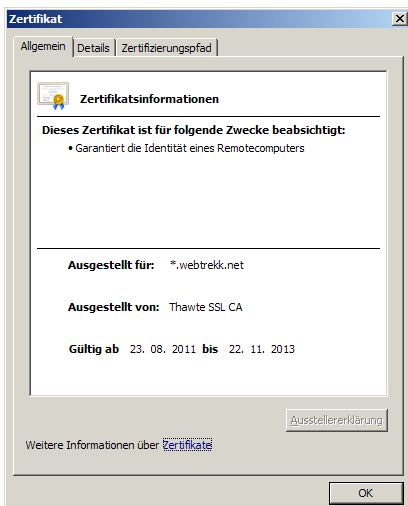
interne Statistik

<https://event.dkb.de> (Wildcardzertifikat)



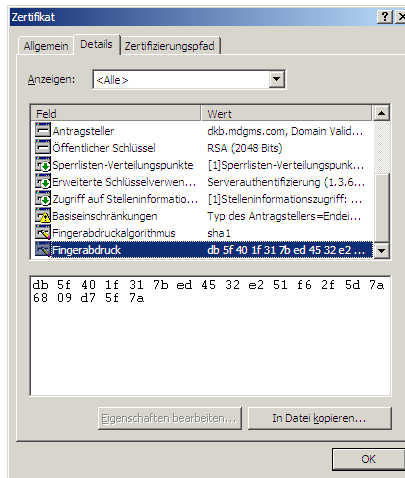
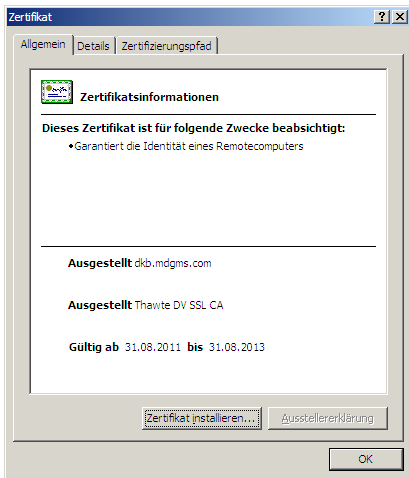
Webtrekk Statistik

<https://dkb01.webtrekk.net>



DKB-Marktüberblick

<https://dkb.mdgms.com/MIS/?id=0107980>



Hinweis zur Browserunterstützung

Firefox 2: Die erweiterte Anzeigemöglichkeit von Extended-Validation-SSL-Zertifikaten ist in Firefox 2 nur über die Erweiterung VeriSign EV Green Bar Extension möglich.

Firefox 3: Die erweiterten Funktionen der Extended-Validation-SSL-Zertifikate werden von Firefox 3 standardmäßig unterstützt. Der linke Teil der Adressleiste wird grün eingefärbt.

Internet Explorer 7: Extended-Validation-SSL-Zertifikate werden standardmäßig unterstützt. Die gesamte Adressleiste wird grün eingefärbt.

Opera 9.5: Extended-Validation-SSL-Zertifikate werden standardmäßig unterstützt. Der rechte Teil der Adressleiste wird grün eingefärbt und das Schloss-Symbol hat zusätzlich ein Häkchen.

Safari 3.2: Extended-Validation-SSL-Zertifikate werden standardmäßig unterstützt. Der Organisationsname wird in grün neben dem Schloss-Symbol angezeigt.