

Hinweise zur sicheren Nutzung des KfW-Online-Kreditportals/Online-Banking für Kreditnehmer



Für eine sichere Nutzung bitten wir Sie als Nutzer die nachfolgenden Sicherheitshinweise zu beachten. Sie ermöglichen eine sichere Kommunikation und erleichtern Ihnen die Erkennung von Angriffsversuchen:

Sicherheit geht vor!

- **Die KfW-Bankengruppe versendet Authentifikationsinformationen (PIN/TAN) grundsätzlich nur per Briefpost an die von Ihnen angegebene Anschrift.**
- **Auf KfW-Seiten wird zur Anmeldung niemals eine oder mehrere TAN abgefragt.**
Geben Sie Authentifikationsinformationen (PIN/TAN) nur bei gewohntem Ablauf innerhalb der Online-Kreditportal-Anwendungen ein. Sollte Ihnen etwas merkwürdig vorkommen, beenden Sie bitte die Verbindung und versuchen es erneut. Veränderungen sollten Sie misstrauisch machen.
- **Die KfW-Bankengruppe fordert Sie niemals auf mehrere TAN auf einmal einzugeben.**
- **Die KfW-Bankengruppe fordert Sie niemals per E-Mail oder per Telefon zur Angabe von Authentifikationsinformationen (PIN/TAN) auf.**
Bitte übermitteln Sie keine persönlichen oder vertraulichen Informationen per E-Mail oder Telefon.
- **Die KfW-Bankengruppe versendet ausschließlich Benachrichtigungen ohne Anhänge per E-Mail, wenn Sie diesen Service abonniert haben. Die elektronische Kommunikation erfolgt immer über den elektronischen Postkorb innerhalb ihres Zugangs.**
Bitte seien Sie vorsichtig, wenn in E-Mails Links, Anlagen oder Aufforderungen zu einem Programmdownload enthalten sind.

Was können Sie im Notfall tun?

Haben Sie Ihre Authentifikationsinformationen (PIN/TAN) irrtümlich weitergegeben oder verloren?

- **Sperren Sie bitte ihren Online-Zugang sofort.**
Dies können Sie selbst, z. B. durch 3-malige Fehleingabe der PIN oder über die KfW-Hotline durchführen.
- **Informieren Sie uns bitte so schnell wie möglich.**
Sie erreichen die KfW-Hotline unter **0228 831 9994**.
- Die von Ihnen angeforderten neuen Authentifikationsinformationen werden Ihnen unverzüglich an Ihre Postanschrift zugestellt.
- Sichern Sie ggf. Beweise (E-Mails, Screen-Shots der Internetseiten) und erstatten Sie im Schadensfall Anzeige bei der Polizei.

Falls Sie unsicher sind, ob eine Ihnen zugegangene Information zum Online-Kreditportal (E-Mail, Internetseite) authentisch ist, informieren Sie bitte auch die KfW-Hotline unter der oben genannten Telefonnummer.



Die KfW-Hotline hilft Ihnen auch, wenn Sie Ihr Passwort vergessen haben.

Was können Sie zu ihrem eigenen Schutz beitragen?

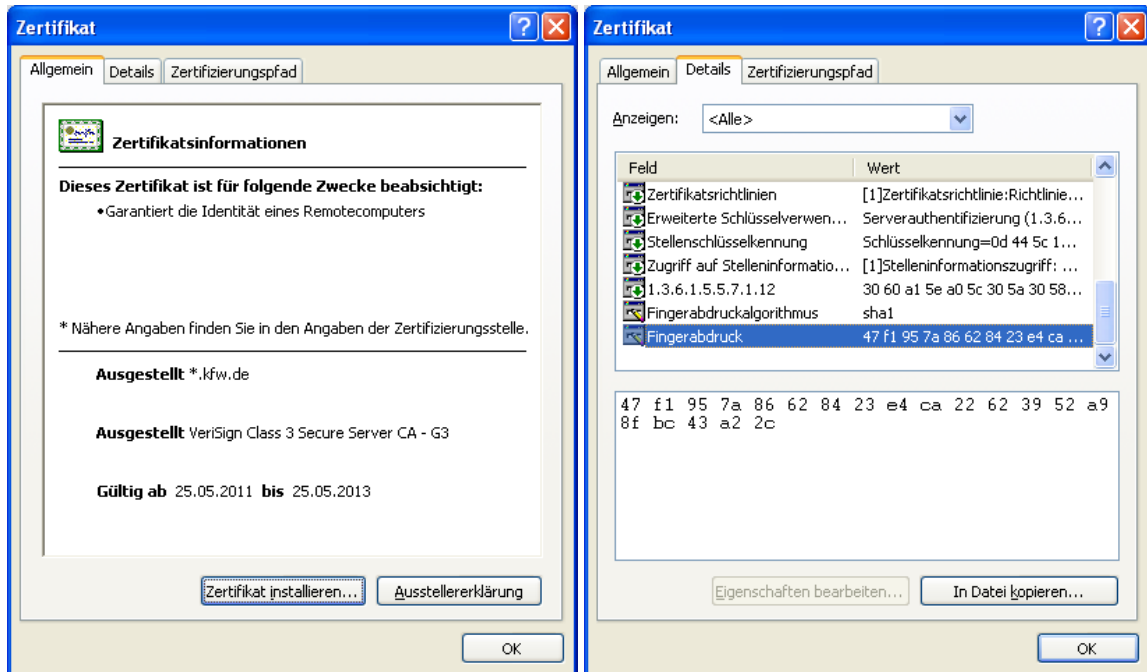
- Bewahren Sie bitte Ihre **Zugangsinformationen** (Benutzernamen, PIN, TAN) gesichert auf, d. h. verzichten Sie z. B. auf die Speicherung dieser Daten auf Ihrem PC.
- Melden Sie sich bitte nur über die **KfW-Homepage** (aktuell: <http://www.kfw.de>) am Online-Kreditportal an. D. h. verwenden Sie bitte z. B. keine Links aus E-Mails zur Anmeldung.
- Kontrollieren Sie bitte die Internetadresse der Anmeldeseite zum Online-Kreditportal:

- o Adresse muss mit "https://onlinekreditportal.kfw.de/..." beginnen.

Adresse  https://onlinekreditportal.kfw.de/

- o Das geschlossene Schloss-Symbol muss zu sehen sein.   Internet

- o Achten Sie bitte auf das richtige **Verschlüsselungs-Zertifikat des Online-Kreditportals**. Machen Sie bitte hierzu einen Doppelklick auf das Schloss-Symbol. Es erscheint ein Fenster mit Informationen zum "Zertifikat", dort finden Sie unter "Details" den Fingerabdruck:



Abhängig vom verwendeten Browser kann die Darstellungsweise des Fingerabdruckes unterschiedlich sein (z. B. Groß-/Kleinschreibung, 2er- oder 4er-Gruppen ...).

- Prüfen Sie bitte regelmäßig Ihren **Kontostand** und die **Kontobewegungen**. So können Sie bei ungewollten Aktionen schnell reagieren.
- Beenden Sie bitte die Online-Sitzung immer durch **korrektes Abmelden**. Ein Schließen des Browserfensters alleine ist nicht ausreichend.
- Wechseln Sie bitte vor der Abmeldung nicht auf eine andere Internet-Seite.
- **Prüfen** Sie bitte eingehende **E-Mails** immer kritisch, da Angriffsversuche häufig über E-Mails erfolgen. Bei dieser Prüfung sollten Sie wissen, dass:
 - o die Absenderadresse von E-Mails gefälscht sein kann;
 - o die E-Mail Viren, Trojaner und andere Schadfunktionen (z. B. manipulierte Bilder) enthalten kann;
 - o Links enthalten sein können, die unabhängig vom angezeigten Linkziel zu einer völlig anderen Seite führen (Phishing-Mails; Näheres zum Thema Phishing finden Sie u. a. auf der Internetseite <http://www.phishing-info.de/>);
 - o Sie in E-Mails unter verschiedenen Vorwänden zur Eingabe von vertraulichen Informationen (z. B. PIN und TAN) aufgefordert werden könnten;
- Nutzen Sie bitte auf Ihrem PC einen **Virens scanner inklusive Spyware-Erkennung und ein Firewall-Produkt**. Halten sie diese per Update-Funktion immer aktuell.

- Prüfen Sie bitte regelmäßig die von Ihnen eingesetzte Software (besonders Betriebssystem und Browser) auf vorhandene Sicherheitsupdates und installieren Sie diese umgehend.
- Nutzen Sie Wireless-LAN (WLAN) und Funktastaturen bitte nur dann für Online-Banking, wenn eine sichere Verschlüsselung aktiviert ist.
- Benutzen Sie möglichst keine ihnen unbekanntem Computer (z. B. in Internetcafes) für das Online-Banking. Auf den Systemen könnte Software installiert sein, die ihre Eingaben (z. B. PIN/TAN) protokolliert oder andere unerwünschte Funktionen ausführt. Auch könnten aus den zwischengespeicherten Informationen (Browsercache) Ihre persönlichen Informationen gewonnen werden.