



## Sicherheitsinformationen

Informationen der European American Investment Bank Aktiengesellschaft (nachfolgend „Euram Bank“) zum Schutz Ihrer Daten und sensibler Informationen im Zusammenhang mit der Nutzung von e-Banking.

### Sicheres e-Banking mit PIN

Um einen Missbrauch Ihrer elektronischen Euram Bank Bankverbindung (nachfolgend „e-Banking“) auszuschließen, sichern wir alle Ihre Transaktionen durch unser PIN-Identifikationsverfahren ab.

Bitte beachten Sie folgendes zum **PIN-Identifikationsverfahren**:

- Die PIN darf Zahlen, Buchstaben und Großbuchstaben enthalten.
- Die PIN muss mindestens 5 Zeichen lang sein und mindestens 1 Buchstaben enthalten.
- Speichern Sie Ihre PIN niemals auf Ihrem Gerät.
- Bewahren Sie Ihre PIN stets so auf, dass kein Dritter Zugang dazu hat.
- Geben Sie Ihre PIN niemals an Dritte weiter.
- Melden Sie sich immer ab, sobald Sie Ihr e-Banking beendet haben.

### Freigabe für Transaktionen

Überweisungen und Aufträge können Sie sicher mittels „mTAN“, den Sie von der Euram Bank per SMS erhalten, freigeben.


### Wählen Sie sichere Passwörter



Ein gutes Passwort besteht in der Regel aus mindestens 8 Zeichen - eine Mischung aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen. Auf jeden Fall sollten Sie Eigennamen, wohlbekannte Begriffe, Einträge in Wörterbüchern und Wiederholungen einzelner Zeichen vermeiden. Verwenden Sie bei numerischen Passwörtern keine Abfolgen, die leicht zu erraten sind, wie zum Beispiel Ihr Geburtsdatum oder Ihre Telefonnummer.

Bitte bedenken Sie, dass die Verwendung eines einzelnen Passworts für verschiedene Zwecke problematisch sein kann. Nutzen Sie daher immer unterschiedliche Passwörter je Anwendung. Darüber hinaus ist es wichtig, dass Sie Ihre Passwörter in regelmäßigen Zeitabständen ändern.

### Gesicherte Verbindung zu Ihrem e-Banking

Loggen Sie sich über <https://ebanking.eurambank.com/?lang=de#/> ein.

 <https://ebanking.eurambank.com/?lang=de#/>

 Identified by DigiCert 

Bitte beachten Sie folgendes zur gesicherten e-Banking Verbindung:

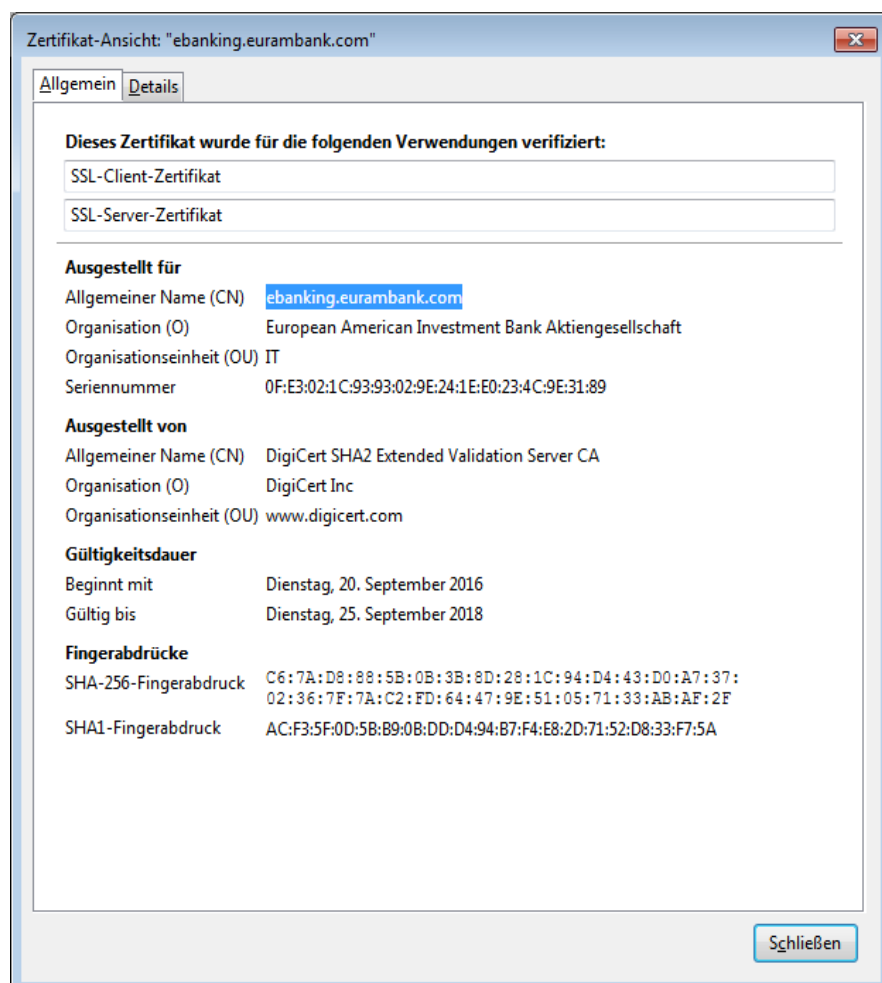
- Die grün hinterlegte Adresszeile (Beispiel zeigt den Internet Explorer 11) und das darin sichtbare Sicherheitssymbol (ein geschlossenes Vorhängeschloss) zeigen die sicheren Verbindungen zu unserem Server an.
- Achten Sie auf die korrekte Adresse in Ihrem Browserfenster, wenn Sie e-Banking starten: <https://ebanking.eurambank.com/?lang=de#/>
- Das Server-Zertifikat können Sie überprüfen, indem Sie das Sicherheitssymbol doppelklicken. Vergleichen Sie die angezeigten Informationen am besten mit den Detailinformationen des Zertifikates der Euram Bank.
- Wir werden Sie niemals auffordern, neue Sicherheitszertifikate auf Ihrem Endgerät zu installieren.

## Überprüfen Sie das SSL-Zertifikat auf Echtheit

Um das SSL-Zertifikat der Euram Bank zu überprüfen, klicken Sie auf das Sicherheitssymbol in der Adresszeile Ihres Browsers und wählen Sie "Zertifikat anzeigen". Ein Fenster mit verschiedenen Informationen zum Zertifikat wird angezeigt.

- Überprüfen Sie bitte, ob es für die korrekte Webadresse (ebanking.eurambank.com) ausgestellt wurde, und ob es noch gültig ist.
- Vergleichen Sie die Informationen mit den korrekten Detailinformationen (u.a. Fingerprints) des SSL-Zertifikates der Euram Bank.

(Beispiel zeigt Mozilla Firefox)



## **Sicherheitstipps bei der Verwendung von WLAN**

Vermeiden Sie, wenn möglich, öffentliches oder unbekanntes WLAN.

- Verwenden Sie keine sensiblen Informationen in öffentlichen WLAN-Netzen (Bankverbindungen, Kontodaten, Kreditkartendaten etc.).
- Verwenden Sie immer einen aktuellen Virenschutz.
- Nutzen Sie nur verschlüsselte Verbindungen für Ihr e-Banking (beispielsweise https) und prüfen Sie diese auf Authentizität (bei https zum Beispiel das Zertifikat der Website).
- Loggen Sie sich immer aktiv aus dem e-Banking aus, wenn Sie es nicht mehr benötigen.
- Schalten Sie bei mobilen Geräten das WLAN immer aus, wenn Sie es nicht benötigen.

## **Halten Sie die Systeme aktuell und nutzen Sie aktuelle Programm-Versionen**

Nutzen Sie stets die aktuellsten Versionen Ihrer verwendeten Software (Betriebssystem, Browser, Apps). Nur aktuelle Software kann gewährleisten, dass die bis dahin bekannten Sicherheitslücken in diesen Programmen geschlossen sind. Nehmen Sie sich kurz Zeit, bevor Sie Ihr e-Banking durchführen, und aktivieren Sie zusätzliche Sicherheitsmaßnahmen z.B. durch Eingabe eines Passworts beim Starten des PCs. Überprüfen Sie, ob Ihre Anti-Virus-Software aktuell ist.

## **Was sind die technischen Voraussetzungen für die Nutzung von E-Banking?**

Bitte beachten Sie, dass für ein sicheres e-Banking ein aktueller Browser und ein aktuelles Betriebssystem unerlässlich sind. Um das e-Banking der Euram Bank nutzen zu können, benötigen Sie ein aktuelles Betriebssystem und einen aktuellen Browser.

Unterstützte Browser:

- Internet Explorer: IE11
- Google Chrome
- Safari (für Mac)
- Microsoft Edge
- Mozilla Firefox

Unterstützte mobile Betriebssysteme (APPs):

- Android: ab Version 5.0
- iOS: ab Version 9.0

Benutzen Sie veraltete Versionen von Browsern oder benutzen Sie Systeme eines anderen Herstellers, kann es gegebenenfalls zu Sicherheits- oder Darstellungsproblemen kommen.

Bitte beachten Sie:

- Der Microsoft Internet Explorer wird nur mehr in Version 11 unterstützt.
- Für Windows XP werden von Microsoft keine Sicherheitsupdates mehr bereitgestellt. Bitte steigen Sie zu Ihrer eigenen Sicherheit schnellstmöglich auf ein aktuelles Betriebssystem um.
- Der Browser Safari wird unter Windows nicht mehr unterstützt.

## **Vorsicht vor Schadsoftware**

Das Internet wird zunehmend zur Verbreitung von Schadsoftware genutzt, welche sich auf dem eigenen Computer, oftmals leider gänzlich unbemerkt in den Systemtiefen, ablegt.

Das vorrangige Ziel schädlicher Programme ist es, persönliche Daten wie Passwörter und Zugangsdaten abzugreifen und diese Informationen oftmals in Echtzeit zum Missbrauch zu übermitteln.

Bitte beachten Sie:

- Verwenden Sie nur vertrauenswürdige Quellen für die Installation von Programmen und Apps.
- Prüfen Sie Ihre Software regelmäßig auf verfügbare Sicherheits-Updates.
- Nutzen Sie zusätzliche Sicherheitssoftware wie eine Firewall, Antiviren und Anti-Malware-Tools.
- Aktualisieren Sie laufend die Virendefinitionen.
- Fremde PCs wie z.B. in Internet Cafés bergen entsprechende Gefahren, weil man nicht davon ausgehen kann, dass diese PCs frei von Schadsoftware sind.

Sollten Sie eine Aufforderung erhalten, ein Sicherheitszertifikat, einen Virenschanner oder etwas anderes auf Ihrem Computer oder Mobilgerät zu installieren, befolgen Sie diese Anweisungen nicht.

### **Achtung vor Phishing E-Mails**

Immer wieder versuchen Trickbetrüger durch sogenannte Phishing E-Mails mit gefälschtem Absender an Kunden- bzw. Zugangsdaten zu gelangen. In diesen E-Mails wird entweder direkt nach Zugangsdaten (Kundennummer, PIN, TAN) gefragt, oder sie enthalten einen Link, der jedoch nicht auf die Internetseite des vermeintlichen Absenders, sondern auf eine von Betrügern täuschend ähnlich aufgesetzte andere Seite führt. Die dort abgefragten Informationen werden an unberechtigte Dritte weitergeleitet.

Die Euram Bank verschickt niemals E-Mails mit derartigen Fragen oder solche Links an ihre Kunden. Antworten Sie daher nicht darauf, öffnen Sie keinesfalls angehängte Dateien und klicken Sie keinesfalls die enthaltenen Links an. Wenn Sie so ein E-Mail erhalten, informieren Sie bitte Ihren Kundenbetreuer per E-Mail oder telefonisch unter +43 1 512 38 80 0 (während der Geschäftszeiten der Euram Bank).

### **Achtung vor gefälschten SMS Nachrichten**

Gefälschte SMS täuschen eine seriöse Herkunft (Banken, Kreditkartenorganisationen etc.) vor und geben oft eine Rückrufnummer an. Es wird versucht, vertrauliche Informationen von Kunden zu erhalten.

Bitte beachten Sie:

- Sie erhalten von uns ausschließlich SMS Nachrichten, wenn Sie die Autorisierungsmethode mittels mTAN nutzen. Die SMS beinhaltet eine TAN, welche nur für einen begrenzten Zeitraum gültig ist.
- Sollten Sie eine SMS mit der Aufforderung erhalten, sensible Informationen preiszugeben, antworten Sie nicht und rufen Sie nicht zurück.
- Sollten Sie eine SMS mit der Aufforderung erhalten, ein Sicherheitszertifikat, einen Virenschanner oder ähnliches auf Ihrem Computer oder Mobilgerät zu installieren, befolgen Sie diese Anweisungen nicht.
- Falls Sie einen Betrug vermuten, informieren Sie bitte Ihren Kundenbetreuer per E-Mail oder telefonisch unter der Telefonnummer +43 1 512 38 80 0 (während der Geschäftszeiten der Euram Bank).

## **Überprüfen Sie regelmäßig Ihre Kontobewegungen**

Kontrollieren Sie bitte regelmäßig Ihre Konten auf auffällige oder Ihnen unbekanntes Transaktionen. Falls Sie Auffälligkeiten bemerken, informieren Sie bitte umgehend Ihren Kundenbetreuer per E-Mail oder telefonisch unter der Telefonnummer +43 1 512 38 80 0 (während der Geschäftszeiten der Euram Bank).

## **Vorgehensweise bei Verlust oder Diebstahl mobiler Geräte**

Bei Verlust oder Diebstahl Ihres mobilen Endgerätes oder wenn sonstige Umstände vorliegen, die einem unbefugten Dritten Missbrauch ermöglichen können, informieren Sie bitte umgehend Ihren Kundenbetreuer per E-Mail oder telefonisch unter der Telefonnummer +43 1 512 38 80 0 (während der Geschäftszeiten der Euram Bank), um eine Sperre Ihres e-Banking Zuganges zu veranlassen.