

Security Information

Information by European American Investment Bank Aktiengesellschaft (hereinafter “Euram Bank”) to protect your sensitive data when using e-Banking

Secure banking with a PIN

To prevent misuse of your electronic Euram Bank account (herein after “e-Banking”), we secure all your transactions through our PIN identification process.

Please note the following about the **PIN identification procedure**:

- The PIN may contain numbers, letters and capital letters.
- The PIN must be at least 5 characters long and contain at least 1 letter.
- Never save your PIN on your device.
- Always keep your PIN in such a way that no third party has access to it.
- Never give your PIN to third parties.
- Always log out as soon as you have finished e-banking.

Authorization of transactions

Transfers and orders can be safely authorized by using an "mTAN”, which Euram Bank provides to you via SMS.


Choose secure passwords

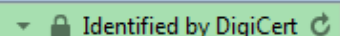
A good password usually consists of at least 8 characters - a mixture of uppercase and lowercase letters as well as numbers and special characters. In any case, you should avoid proper names, well-known terms, dictionary entries, and repetition of single characters. For numeric passwords, do not use sequences that are easy to guess, such as your date of birth or phone number.

Please keep in mind that using a single password for different purposes can be problematic. Always use different passwords per application. In addition, it is important that you change your passwords at regular intervals.

Use a secured connection

Logon on via <https://ebanking.eurambank.com/?lang=en#/>.

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

 Identified by DigiCert

Please note the following for a secured e-Banking connection:

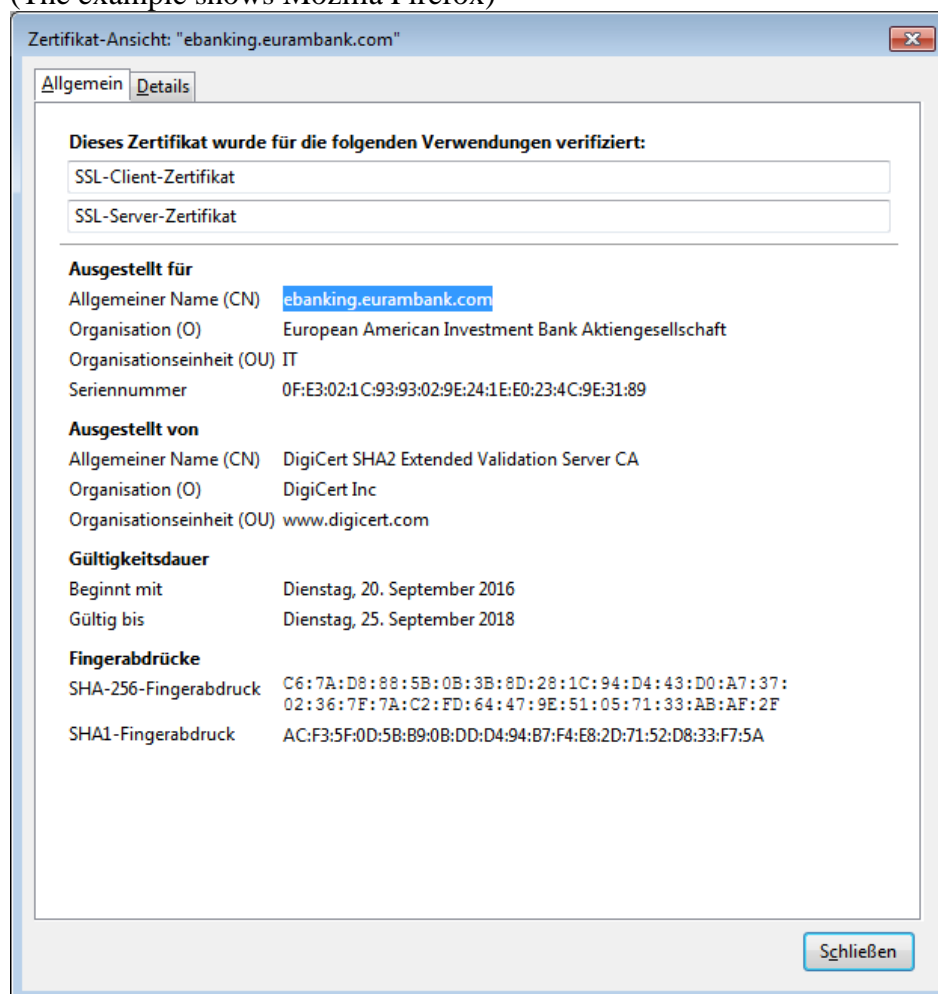
- The green address bar (example shows the Internet Explorer 11) and the security symbol visible inside it (a closed padlock) indicate the secure connection to our server.
- Check for the correct address in your browser window when you start e-Banking:
<https://ebanking.eurambank.com/?lang=de#/>
- You can verify the server certificate by double-clicking the security symbol. Compare the displayed information best with the detailed information of the certificate of Euram Bank.
- We will never ask you to install new security certificates on your device.

Check the SSL certificate for authenticity

To check the SSL certificate of Euram Bank click on the security symbol in the address bar of your browser and select "Show certificate". A window with various information on the certificate is displayed.

- Please check if it has been issued for the correct web address (ebanking.eurambank.com) and if it is still valid.
- Compare the information with the correct detailed information (including fingerprints) of the SSL certificate of Euram Bank.

(The example shows Mozilla Firefox)



Safety tips when using WiFi

If possible, avoid public or unknown WiFi.

- Do not use sensitive information in public wireless networks (bank details, account details, credit card details etc.)
- Always use the latest virus protection.
- Only use encrypted connections for your banking (e.g. https) and check them for authenticity (e.g. the https certificate for the website).
- Always log out of banking actively when you no longer need it.
- For mobile devices, always turn off the WiFi, when you no longer need it.

Keep your systems up to date and use current programs

Always use the latest versions of the software used (operating system, browser, apps). Only up-to-date software can ensure that previously known security leaks in these programs are closed. Take some time before starting e-Banking and enable additional security measures, e.g. by entering a password when starting the PC. Always check if your anti-virus program is up to date.

What are the technical requirements for the use of e-Banking?

Please note that for secure e-banking, a current browser and a current operating system are essential. In order to use Euram Bank's e-Banking, you need a current operating system and a current supported browser.

Supported browsers:

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

Supported mobile devices operating systems:

- Android: from Version 5.0
- iOS: from Version 9.0

If you are using outdated versions of these operating systems or browsers, or if you are using third-party systems, you may experience security or display issues.

Please note:

- Microsoft Internet Explorer is only supported in version 11.
- Microsoft does not provide security updates for Windows XP. For your own safety, please upgrade to a current operating system as soon as possible.
- The Safari browser is no longer supported on Windows.

Beware of malware

The internet is increasingly being used to spread malicious software, which on your computer often goes unnoticed at system depths. The primary target of malicious programs is to retrieve

personal information such as passwords and access data, and often provide that information for misuse in real time.

Please note:

- Use only trusted sources for installing programs and apps.
- Check your software regularly for available security updates.
- Use additional security software such as a firewall, antivirus and anti-malware tools.
- Keep updating the virus definitions.
- External PCs such as in Internet Cafés pose dangers, because one cannot assume that these PCs are free of malicious software.

If you receive a request to install a security certificate, virus scanner or something similar on your computer or mobile device, do not follow these instructions.

Beware of phishing e-mails

Fraudsters often try to get access to customer data through so-called phishing e-mails from a fake sender. These e-mails either ask directly for access data (customer number, PIN, TAN) or contain a link that does not lead to the supposed sender's website, but to a page deceptively similar. The information requested there will be forwarded to unauthorized third parties.

Euram Bank will never send mails with such questions nor the respective links to you. Thus do not answer such mails, do not open attached files or click on the links provided.

If you receive such an e-mail, please inform your client advisor by e-mail or by calling +43 1 512 38 80 0 (during Euram Bank's business hours).

Beware of fake SMS

Fake SMS pretend to be of serious origin (banks, credit card organizations etc.), and often suggest to call back. This way, fraudsters try to obtain confidential information from customers.

Please note:

- You will only receive SMS messages by Euram Bank if you use the authorization method via mTAN. The SMS contains a TAN, which is only valid for a limited period.
- If you receive an SMS asking you to disclose sensitive information, never reply nor call the phone number provided.
- If you receive a text message asking you to install a security certificate, virus scanner, or something else on your computer or mobile device, do not follow these instructions.
- If you suspect fraud, please inform your client advisor by e-mail or by calling +43 1 512 38 80 0 (during Euram Bank's business hours).

Check your accounts regularly

Please check your accounts regularly for any unusual or unfamiliar transactions. If you notice any such transactions, please notify your client advisor immediately by e-mail or by calling +43 1 512 38 80 0 (during Euram Bank's business hours).

Procedure in the case of loss or theft of mobile devices

In the event of theft or loss of your mobile device or any other circumstances, that might lead to a potential misuse by a third party, please notify your client advisor immediately by e-mail or by calling +43 1 512 38 80 0 (during Euram Bank's business hours) to block your e-banking access.