Knowledgebase > Information for new users > Security

Security

Anna-Karin Ettik Åsén - 2024-01-12 - Comments (0) - Information for new users

The following three components are used to maintain a high level of security in Netmaker Bankgiro Link:

- e-Legitimation (electronic identity document) is used to authenticate the user and to protect the information.
- Through authorization from the bank, a link is established between the accounting officer and the bank. The power of attorney specifies which services can be used and which transactions can be made.
- Secure communication is a central part of electronic banking services. When communicating over an open network, the communication is secured through various security functions such as, for example, encryption.

Your personal e-Legitimation

An e-Legitimation can be used by a person who is connected to a digital network such as the Internet.

Through e-Legitimation and its technology, legal requirements and standards for e-signature, privacy-related services can be performed online. Your personal e-Legitimation can also be used on websites such as the Swedish Tax Agency (tax return) and the Social Insurance Agency (child care). The number of websites that provide services for the use of e-Legitimation is constantly increasing.

How to use the e-Identification

An e-Legitimation is a standardized plastic card with a built-in microprocessor. Netmaker Bankgiro Link checks that the e-Identification is not forged or blocked. Just as with traditional ID cards, the distribution of the e-Legitimation takes place through a controlled process, and by trusted parties. You use your e-Legitimation in a card reader and identification takes place by entering a PIN code.

Depending on which bank you have, your e-Legitimation will have one or two PIN codes. If you only have a PIN code, it must be used for both authentication and signature. If you have two PIN codes, the first is used for identification and the second for signature (of the files you must send to Bankgirot).

Note

Do not mix up these two PIN codes!

If you use one of the PIN codes incorrectly three times in a row, the PIN code will be locked. Then contact the organization that has issued the e-Legitimation to hear how the PIN code can be unlocked. Instructions for unlocking the PIN code are linked to the PUK code obtained in connection with the PIN codes.

When logging in or electronically signing in Netmaker Bankgiro Link, the Bank-ID software is contacted, which verifies the user's identity. Bankgirot checks that the person who signed has a valid authorization to certify.

How to send a file securely with Netmaker Bankgiro Link to Bankgirot:

1. Create a number of payments for your supplier invoices in your financial system and generate a file with payments.
2. Connect to bankgirot.
3. The communication between you and Bankgirot is encrypted to prevent data breaches.

4. Open your payment file.

5. Submit the payment file to the bankgirot. It is possible to send and certify as a single operation

6. If you have not yet certified the file, certify it. A file may require several certificates.

7. Bankgirot checks with the bank that the sender has the necessary authorizations.

8. When Bankgirot has received confirmation that the person in question is authorized, the payment information will continue to be processed.

9. You receive a receipt in Netmaker Bankgiro Link, indicating that the payment file is approved for further processing.

How to download one or more files securely with Netmaker Bankgiro Link from Bankgirot:

1. Connect to Bankgirot using Netmaker Bankgiro Link. Legitimation takes place using e-Legitimation via Bank-ID.

2. Bankgirot checks the user's authorization and gives him the opportunity to select the files to be downloaded.

3. The user selects the files to download.

4. Downloaded files are stored in Netmaker Bankgiro Link and can be used by the user.