Säkerhet

Anna-Karin Ettik Åsén - 2024-01-12 - Kommentarer (0) - Information till nya användare

Följande tre komponenter nyttjas för att upprätthålla en hög säkerhet i Netmaker Bankgiro Link:

- e-Legitimation (elektronisk identitetshandling) används för att legitimera användaren och för att skydda informationen.
- Genom fullmakt från banken fastställs en länk mellan redovisningsansvarig och bank. Fullmakten specificerar vilka tjänster som kan nyttjas och vilka transaktioner som kan göras.
- Säker kommunikation är en central del avseende elektroniska banktjänster. Vid kommunikation över ett öppet nätverk är kommunikationen säkrad genom olika säkerhetsfunktioner såsom exempelvis kryptering.

Din personliga e-Legitimation

En e-Legitimation kan användas av en person som är kopplad till ett digitalt nätverk som exempelvis Internet.

Genom e-Legitimationen och dess teknologi, juridiska krav och standarder för e-underskrift, kan integritetsnära tjänster utföras online. Din personliga e-Legitimation kan också nyttjas på webbplatser såsom exempelvis Skatteverket (skattedeklaration) och Försäkringskassan (barnomsorg). Antalet webbplatser som tillhandahåller tjänster för användning av e-Legitimation ökar ständigt.

Hur du använder e-Legitimationen

En e-Legitimation är ett standardiserat plastkort med en inbyggd mikroprocessor. Netmaker Bankgiro Link kontrollerar att e-Legitimationen är inte är förfalskad eller spärrad. Precis som med traditionella ID-kort sker distributionen av e-Legitimationen genom en kontrollerad process, och av betrodda parter. Du använder ditt e-Legitimation i en kortläsare och legitimering sker genom angivande av en PIN-kod.

Beroende på vilken bank du har, kommer din e-Legitimation att ha en eller två PIN-koder. Om du enbart har en PIN-kod så skall den användas till både legitimering och underskrift. Om du har två PIN-koder så används den första för legitimering och den andra för underskrift (av de filer du skall sända till Bankgirot).

Observera

Blanda inte ihop dessa två PIN-koder!

Om du använder någon av PIN-koderna fel tre gånger i rad så kommer PIN-koden att bli låst. Kontakta då den organisation som har utfärdat e-Legitimationen för att höra hur PIN-koden kan låsas upp. Instruktioner för att låsa upp PIN-koden är kopplade till den PUK-kod som erhölls i samband med PIN-koderna.

Vid inloggning eller elektronisk underskrift i Netmaker Bankgiro Link kontaktas programvaran BankID som verifierar användarens identitet. Bankgirot kontrollerar att personen som undertecknat har en giltig fullmakt för att attestera.

Hur du skickar en fil säkert med Netmaker Bankgiro Link till Bankgirot:

1. Skapa ett antal betalningar för dina leverantörsfakturor i ditt ekonomisystem och generera en fil med betalningar.
2. Anslut till bankgirot.
3. Kommunikationen mellan dig och Bankgirot är krypterad för att förhindra dataintrång.
4. Öppna din betalfil.
5. Skicka in betalfilen till bankgirot. Det är möjligt att skicka och attestera som en sammanhållen operation
6. Om du ännu inte attesterat filen så attestera den. En fil kan kräva flera attester.
7. Bankgirot kontrollerar med banken att den som har skickat har erforderliga behörigheter.
8. När Bankgirot har fått en bekräftelse på att aktuell person är behörig sker fortsatt hantering av betalinformationen.
9. Du erhåller ett kvitto i Netmaker Bankgiro Link, vilket indikerar att betalningsfilen är godkänd för fortsatt hantering.

Hur du hämtar en eller flera filer säkert med Netmaker Bankgiro Link från Bankgirot:

1. Koppla upp till Bankgirot med hjälp av Netmaker Bankgiro Link. Legitimering sker med hjälp av e-Legitimation via BankID.
2. Bankgirot kontrollerar användarens behörighet och ger denne möjlighet att välja de filer som skall hämtas.
3. Användaren väljer de filer som skall hämtas.
4. Hämtade filer lagras i Netmaker Bankgiro Link och kan nyttjas av användaren.