

# Liesbeth - Toelichting beveiliging

## 1. Elektronische handtekening

### Inleiding

De beveiliging in Liesbeth maakt gebruik van zowel asymmetrische als symmetrische encryptie. Bij symmetrische encryptie dient het geheime versleutelelement door beide partijen gekend te zijn. Bij asymmetrische encryptie is er sprake van twee complementaire sleutelementen: een geheim gedeelte (= geheime sleutel) en een publiek gedeelte (=publieke sleutel). Hierbij dient het geheim gedeelte enkel gekend te zijn door die éne partij tot wie de sleutel toebehoort, terwijl het publieke gedeelte bij een ruimer publiek kan/mag gekend zijn. Het asymmetrische sleutelbaar heeft de eigenschap dat data geëncrypteerd met het ene sleutelement enkel gedecrypteerd kunnen worden met het complementaire gedeelte.

### Technieken

Een dergelijk asymmetrisch sleutelbaar kan als volgt aangewend worden:

- Indien een partij gebruik maakt van de publieke sleutel van een tegenpartij om data te encrypteren, is enkel de bedoelde bestemming in staat om de data te decrypteren met behulp van zijn/haar eigen geheime sleutel. Op die manier kan de confidentialiteit van een uitgewisseld bericht bewerkstelligd worden.
- Indien een partij gebruik maakt van zijn/haar geheime sleutel om een overeengekomen gegeven te encrypteren, kan de tegenpartij, door decryptie met de publieke sleutel van de afzender, verifiëren dat de ontvangen data met zekerheid afkomstig zijn van de houder van de bijhorende secret key. Op die manier kan de herkomst van een uitgewisseld bericht met zekerheid vastgelegd worden.
- Indien daarenboven het overeengekomen gegeven bestaat uit een berekend extract (=hashwaarde) van een bericht waarbij wijziging van het bericht niet mogelijk is zonder wijziging van het extract, kan men eveneens verifiëren of het bericht, sinds zijn verzending, ongewijzigd is gebleven. Op die manier kan men verzekerd zijn van de integriteit van een uitgewisseld bericht.

### Elektronische handtekening

Het gebruik van een geheime sleutel ter encryptie van een hashwaarde van een bericht, kan aldus als een elektronische handtekening beschouwd worden: de herkomst én de integriteit van het bericht kan immers onmiskenbaar bepaald worden door verificatie met behulp van de bijhorende publieke sleutel.

## 2. Beveiligingsmiddelen Liesbeth

Het Liesbeth Telebankingpakket geeft aan de gebruiker en de abonnee volgende beveiligingsmiddelen ter beschikking:

- De toegang tot het pakket wordt voor elke gebruiker beveiligd met een persoonlijk toegangswachtwoord. De gebruiker is in staat om zelfstandig dit wachtwoord te wijzigen. Aan dit wachtwoord en de toegang tot het pakket zijn een aantal modaliteiten verbonden die toelaten om de beveiliging van de toegang tot het pakket te verhogen zoals: instelbare geldigheidstermijn van het toegangswachtwoord, beperking in tijd van de toegang tot het pakket, enz. Deze modaliteiten kunnen door een gebruiker die optreedt als beheerder van het pakket zelf ingesteld worden. Deze beveiliging is op alle soorten gebruikers van toepassing.
- Het gebruik van het pakket kan voor elke gebruiker ingesteld worden op een vooraf gedefinieerd gebruikersprofiel. Een gebruikersprofiel bepaalt welke modules en functionaliteiten van het pakket voor een gebruiker toegankelijk/beschikbaar zijn. Deze profielen kunnen door een gebruiker die optreedt als beheerder van het pakket toegewezen worden aan een andere gebruiker. De handtekenbevoegdheid kan echter niet ontnomen worden van een gebruiker door een beheerder van het pakket. Deze beveiliging is op alle soorten gebruikers van toepassing.
- Het ontvangen/versturen van data tussen enerzijds een Liesbeth installatie en alle daarin opgenomen abonnementen en anderzijds VDK spaarbank gebeurt op een beveiligde manier gebaseerd op asymmetrische encryptie. Op die manier zijn beide partijen (VDK en de abonnee) verzekerd van de integriteit en de herkomst van de uitgewisselde gegevens. Bovendien wordt tijdens de communicatie ook de confidentialiteit ten aanzien van derden gewaarborgd. Deze beveiliging gebeurt op een transparante wijze waarbij geen tussenkomst van de abonnee of gebruiker vereist is.
- Een groep van verrichtingen die naar VDK ter uitvoering opgestuurd wordt, dient van geldige elektronische handtekeningen voorzien te zijn. Het nodige en voldoende karakter van deze handtekeningen, is bepaald in de volmachtregels die in het abonnement opgenomen zijn.
- Het plaatsen van een elektronische handtekening is enkel mogelijk met behulp van een persoonlijk wachtwoord dat door de gebruiker zelf gekozen wordt bij de creatie van zijn/haar persoonlijke sleutel.

### 3. Certificatieprocedure gebruiker Liesbeth met handtekenbevoegdheid

Alvorens een persoon een rechtsgeldige elektronische handtekening kan plaatsen met behulp van een asymmetrisch sleutelpaar, dient men de identiteit van die persoon én de link met het sleutelpaar, ondubbelzinnig vast te leggen.

Daar de gebruikers van Liesbeth met handtekenbevoegdheid enkel reeds gekende cliënten van VDK kunnen zijn waarvan de identiteit a priori reeds door de bank is gekend, dient in het Liesbeth systeem enkel de toewijzing van een sleutelpaar aan een VDK cliënt vastgelegd te worden. Hiervoor wordt gebruik gemaakt van onderstaande certificatieprocedure:

#### 1. Aanmaken van een sleutelpaar

De gebruiker is zelf verantwoordelijk voor het aanmaken van een asymmetrisch sleutelpaar. Dit is voor de gebruiker mogelijk in het Liesbeth pakket zelf. Hierbij wordt de gebruiker gevraagd een wachtwoord op te geven als toegangsmiddel tot zijn/haar sleutelpaar. De gebruiker geeft dit wachtwoord in telkens als hij/zij zijn/haar elektronische handtekening wenst te plaatsen. De gebruiker is ten allen tijde in staat om in het pakket de toestand van zijn/haar persoonlijke sleutel op te volgen. Hiertoe wordt in het pakket een berekende identificatiewaarde weergegeven welke éénduidig zijn sleutelpaar identificeert.

#### 2. Versturen publieke sleutel naar VDK

Het publieke gedeelte van een sleutelpaar dient naar VDK verstuurd te worden om op een later tijdstip verificatie van een elektronische handtekening geplaatst met behulp van het sleutelpaar, mogelijk te maken. De gebruiker dient in het Liesbeth pakket zelf, enkel een verbinding te maken met VDK om de publieke sleutel naar VDK te versturen.

#### 3. Ontvangst van certificeringbrief

Na ontvangst van de publieke sleutel van een gebruiker door VDK, stuurt VDK een certificeringbrief persoonlijk gericht aan de betrokkene waarin de inhoud van zijn/haar publieke sleutel vermeld is. Daarnaast wordt ook de berekende identificatiewaarde vermeld. Hiermee dient de gebruiker te verifiëren of de publieke sleutel welke verstuurd werd naar VDK overeenstemt met de publieke sleutel vermeld in de certificeringbrief. **De gebruiker verleent zijn elektronische handtekening geplaatst binnen het kader van het Liesbeth Telebankingspakket, dezelfde bindende kracht als een handmatig aangebrachte handtekening door akkoordverklaring met de certificeringbrief.**

#### 4. Certificering gebruiker

Na ontvangst van een gehandtekeningde certificeringbrief door VDK wordt het sleutelpaar door VDK geactiveerd en bruikbaar binnen Liesbeth om een bindende handtekening te plaatsen. De gebruiker is vanaf dat moment gecertificeerd. In het pakket zelf dient een connectie met VDK gemaakt te worden om de activering van het sleutelpaar te ontvangen.

### 4. Beveiligingsprocedures Liesbeth

Om de effectiviteit te waarborgen van de beveiligingsmiddelen welke in het Liesbeth Telebankingspakket ter beschikking gesteld worden, dienen de abonnee en de gebruikers volgende beveiligingsprocedures in acht te nemen:

- Het persoonlijke toegangswachtwoord van een gebruiker wordt geacht geheimgehouden te worden door de gebruiker. De gebruiker is hiervoor zelf verantwoordelijk en zal daarom op geregelde tijdstippen zijn persoonlijk toegangswachtwoord wijzigen, in het bijzonder bij een vermoeden van schending van het geheim ervan. Door de abonnee en de in zijn naam optredende gebruikers kunnen wijzigingen van de modaliteiten met betrekking tot de toegang van het pakket doorgevoerd worden. De abonnee is hierbij zelf verantwoordelijk voor de wijzigingen aangebracht aan de hem toegewezen beveiligingsmiddelen.
- Het gebruik van Liesbeth is beperkt tot de in het abonnement opgenomen gebruikers en volgens het hem/haar toegewezen gebruikersprofiel. Het staat de abonnee en de in zijn naam optredende gebruikers vrij om hieraan nieuwe gebruikers met bijhorend gebruikersprofiel toe te voegen, en/of gebruikersprofielen van bestaande gebruikers te wijzigen. Deze nieuw toegevoegde gebruikers hebben geen handtekenbevoegdheid. De abonnee is hierbij zelf verantwoordelijk voor de wijzigingen aangebracht aan de hem toegewezen beveiligingsmiddelen.
- Het plaatsen van een elektronische handtekening wordt beveiligd met behulp van een persoonlijk ondertekeningswachtwoord. Dit wachtwoord wordt geacht geheimgehouden te worden door de gebruiker. De gebruiker is hiervoor zelf verantwoordelijk en zal het daarom op geregelde tijdstippen wijzigen, in het bijzonder bij een vermoeden van schending van het geheim ervan.
- De gecertificeerde gebruiker kan eveneens overgaan tot een wijziging van het asymmetrische sleutelpaar waarop zijn/haar elektronische handtekening gebaseerd is. Indien een telematicabericht met een dergelijke wijziging van een persoonlijk sleutelpaar VDK bereikt, en vergezeld is van een geldige elektronische handtekening gebaseerd op het vorige sleutelpaar van de gebruiker, wordt het nieuwe sleutelpaar automatisch verwerkt en toegewezen aan de gebruiker. De gebruiker blijft hierbij gecertificeerd en verleent hierbij automatisch een elektronische handtekening gebaseerd op het nieuwe sleutelpaar dezelfde bindende kracht als een handmatig aangebrachte handtekening. Een dergelijke wijziging van het asymmetrische sleutelpaar wordt ondersteund binnen het Liesbeth pakket zelf en vereist kennis van het ondertekeningswachtwoord. Indien een gecertificeerd gebruiker zijn ondertekeningswachtwoord niet meer kent of vermoedens heeft dat de veiligheid en integriteit van zijn sleutelpaar geschonden is, kan hij/zij overgaan tot de creatie van een nieuw asymmetrisch sleutelpaar. Hierbij dient de certificatieprocedure opnieuw doorlopen te worden. De creatie van een nieuw asymmetrisch sleutelpaar wordt ondersteund binnen het Liesbeth pakket zelf. De gebruiker dient hierbij VDK voorafgaandelijk op de hoogte te brengen.

- De beveiliging van de uitgewisselde gegevens tussen een installatie van het Liesbeth Telebankingpakket en alle daarin opgenomen abonnementen enerzijds en VDK anderzijds is gebaseerd op een asymmetrisch sleutelbaar toebehorend aan de/het installatie/abbonement. De gebruiker met voldoende rechten krachtens een hem/haar toegewezen gebruikersprofiel kan overgaan tot een wijziging van het asymmetrische sleutelbaar toebehorend aan de/het installatie/abbonement, mocht die gebruiker dit, om welke veiligheidsredenen dan ook, nodig achten.

Indien een telematicabericht met een dergelijke wijziging van een sleutelbaar VDK bereikt, en vergezeld is van een geldige elektronische handtekening gebaseerd op het vorige sleutelbaar van de/het installatie/abbonement, wordt het nieuwe sleutelbaar automatisch verwerkt en toegewezen aan de/het installatie/abbonement. De beveiliging van de uitgewisselde gegevens blijft hierbij gehandhaafd. Een dergelijke wijziging van het asymmetrische sleutelbaar wordt ondersteund binnen het Liesbeth pakket zelf en gebeurt volledig transparant naar de gebruiker toe. Indien een gebruiker met voldoende rechten krachtens een hem/haar toegewezen gebruikersprofiel, vermoedens heeft dat de veiligheid en integriteit van het sleutelbaar toegewezen aan de/het installatie/abbonement geschonden is, kan die gebruiker overgaan tot de creatie van een nieuw asymmetrisch sleutelbaar. De creatie van een nieuw dergelijk asymmetrisch sleutelbaar wordt ondersteund binnen het Liesbeth pakket zelf. De gebruiker dient hierbij VDK voorafgaandelijk op de hoogte te brengen.

De abonnee houdt toezicht op alle hem door het Liesbeth Telebankingpakket ter beschikking gestelde beveiligingsmiddelen en aanvaardt de volledige verantwoordelijkheid voor het gebruik dat de door hem gemachtigde gebruikers ervan maken.