



### Toelichting

Wanneer een consument aankopen bij een webwinkel wil afrekenen kan hij veelal kiezen uit een aantal betaalinstrumenten. Indien hij kiest voor een betaling vanaf zijn bankrekening, wordt de consument doorgeleid naar de internetbankierentoepassing van zijn bank en wordt een directe beveiligde “end-to-end” verbinding tussen de PC van de consument en zijn bank gerealiseerd. Als de verbinding echter verloopt via een tussenliggende betaaldienst wordt de veilige “end-to-end” verbinding doorbroken. Omdat de tussenliggende dienst vanuit de consument gezien voor de betaaldienst van zijn bank komt, is sprake van een overlay betaaldienst. Het is voor de consument niet altijd duidelijk dat hij kiest voor een overlay betaaldienst.

Een overlay betaaldienst simuleert als tussenliggende partij richting de bankcliënt de toegang tot de bank en richting de bank de handelingen van de cliënt. Op de website van de bank moeten persoonlijke gegevens worden ingevuld, gegevens die de cliënt ten behoeve van een veilig internetbankieren geheim moet houden. De bankcliënt verstrekt deze gegevens nu aan de overlay betaaldienst die deze gegevens weer invult op de website van de bank. Het bedrag van de transactie wordt rechtstreeks overgeschreven van de rekening van de klant naar de rekening van de webwinkelier, waardoor de overlay betaaldienst een betaalgarantie kan afgeven aan de webwinkelier. Een dergelijke betaaldienst kan worden gerealiseerd zonder samenwerking met de banken. De overlay betaaldienst verricht de handelingen namens de bankcliënt bij zijn bank en vraagt daartoe de benodigde geheime gegevens aan de bankcliënt. De aanbieder van de overlay betaaldienst beschikt hierdoor over deze geheime gegevens. Afhankelijk van de bancaire toepassing kan de aanbieder deze gegevens gebruiken om -op een ander moment- toegang te verkrijgen tot de internetbankierentoepassing van de cliënt bij zijn bank zonder medeweten van deze cliënt. Of daarbij ook transacties kunnen worden verricht, hangt af van de opzet van de toepassing bij de bank. Wanneer daartoe éénmalige transactiecodes zijn vereist, is veelal medewerking van de cliënt nodig omdat daarbij de bankpas, PIN-code en calculator of TAN-code of -lijst nodig zijn.

De banken kunnen niet eenvoudig bepalen of de cliënt zelf dan wel een overlay betaaldienst toegang heeft tot de internetbankierentoepassing en de transacties uitvoert. Daarnaast kunnen fraudeurs ook gebruik maken van dezelfde methodiek. De banken hechten dan ook grote waarde aan de veiligheid van het internetkanaal tussen de internetbankierentoepassing op de webservers bij de bank en de webbrowser op de pc van de cliënt, waarbij een door versleuteling beveiligd “end-to-end” kanaal over Internet wordt gebruikt. Daarnaast mag de cliënt zaken als wachtwoorden, bankpassen, PIN-codes, TAN-codes en -lijsten niet aan derden verstrekken. Alleen als aan deze voorwaarden wordt voldaan kunnen banken de veiligheid van internetbankieren in voldoende mate waarborgen.

Het veiligheidsaspect voor de internetbankierentoepassingen vormt het belangrijkste risico van overlay betaaldiensten. De opzet van dergelijke diensten maakt het voor bankcliënten lastiger onderscheid te maken tussen bonafide en malafide diensten en maakt het onderscheid onduidelijk tussen diensten waarbij geheime gegevens aan derden worden verstrekt, dan wel rechtstreeks aan de eigen bank. De opzet ondermijnt ook de maatregelen van banken om het internetbankieren veilig te houden.

DNB staat in beginsel positief tegenover nieuwe internetbetaaldiensten, omdat daarmee de efficiency van het betalingsverkeer kan worden bevorderd. Nieuwe betaalinstrumenten dienen echter wel veilig te zijn en de veiligheid van bestaande betaaldiensten niet te ondermijnen. Bij de hier bedoelde overlay betaaldiensten wordt de veiligheid van de bestaande internetbankierentoepassingen ondermijnd. Voor DNB weegt dit veiligheidsaspect zwaar.