

### Background

When paying for purchases from an online store, a consumer may often choose from a few payment options. If he opts for payment from his bank account, the consumer is directed to his bank's internet banking application and a direct, secure "end-to-end" connection between the consumer's PC and his bank is brought about. However, if the connection runs through an intervening payment service, the secure "end-to-end" connection is interrupted. From the consumer's perspective, the intervening service is positioned before that of his own bank, meaning that the arrangement can be regarded as an overlay payment service. It is not always clear to the consumer that he is choosing an overlay payment service.

As an intermediate party, an overlay payment service simulates the access to the bank vis-à-vis the bank customer and the customer's actions vis-à-vis the bank. Personal details must be entered on the bank's website, details which the client must keep confidential to ensure secure online banking. The bank customer now provides these details to an overlay payment service which then enters them on the bank's website. The transaction amount is transferred directly from the customer's account to the webstore's account, enabling the overlay payment service to issue a payment guarantee to the webstore. Such a payment service can be realised without cooperation with the banks. The overlay payment service carries out the actions on behalf of the bank customer, requesting the required confidential details from him. The provider of the overlay payment service hence has these confidential details at its disposal. Depending on the banking application, the provider could use these details to access the customer's online banking application with his bank at another time, without the customer knowing. Whether transactions may be carried out depends on the structure of the application at the particular bank. If the application requires one-off transaction codes, the customer's cooperation is usually required because such codes are generated using a bank card, PIN and calculator, TAN or TAN list.

The banks cannot easily determine whether the customer himself or an overlay payment service is accessing the internet application and carrying out transactions. Moreover, fraudsters could also use the same method. The security of the internet channel between the internet banking applications on the bank's webserver and the customer's PC, using an encrypted "end-to-end" connection, is thus of prime concern to banks. In addition, the customer is required not to pass on matters such as passwords, bank card, PINs, TANs and TAN lists to third parties. Banks can only adequately safeguard the security of online banking if these conditions are met.

The security aspect of the internet banking applications is the main risk attached to overlay payment services. The structure of such services makes it more difficult for customers to distinguish between bona fide and mala fide services and blurs the distinction between services that provide confidential details to third parties and those that provide them directly to the bank. The structure undermines the banks' measures to keep online banking secure.

DNB is in principle well-disposed to new internet payment services because they can promote the efficiency of payment transactions. However, new payment instruments must be secure and must not undermine the security of existing payment services. In the case of the overlay payment services referred to here, the security of the existing internet application is undermined. DNB takes this security issue very seriously.