eCommerce
Payment Systems

Access Control for Server Wallets
Separating authentication from the application

Authors: **Jürgen Weiß, Stefan Risto**
Version: **1.0, 2002-02-12**

Abstract:
At the moment, server based wallets are going to be established as the leading architecture within the ePayment area. Because of this, it is very important to deal with the topics identification and transaction release, which are playing a central role for every server wallet. Since there is a wide range of identification and transaction release mechanisms available at the market, it is a difficult decision which of them have to be integrated into a server wallet. Besides from the classic methods, e.g. PIN/TAN and idToken, mobile methods will gain in importance in the near future. That shows the necessity of replacing old identification and transaction release methods and/or integration of new ones. This document describes how server wallet management can be made more efficient and how the flexibility regarding the supported methods can be increased.

Sulzbacher Straße 29-39
65824 Schwalbach am Taunus, Germany
Phone +49 (0) 6196/88289-0
Fax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Germany
Phone +49 (0) 6196/88289-0, Fax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Basics

Currently, server based wallets turn out to be the most powerful architecture within the ePayments area. It is most important to consider the topics authentication and transaction release very carefully since they play a vital role in every server wallet. The main reason for this is the fact that the user and the system are located in different areas.
The security of internet payment transactions is in particular based on three processes:

- Identification
- Transaction release
- Authorization

Identification
As a first step within a secure payment transaction the user has to be identified without any doubt. To achieve this, the user has to prove his identity. Among a large variety of possible methods, the most common are username/password, PIN and idToken. In future, other challenge-response methods such as digital signatures and biometrics will become more important.
The different methods provide different security levels and therefore should be chosen according to the respective application.

Transaction release
Transaction release means the customer's confirmation of the payment transaction. Besides others, the same mechanisms may be used as for the identification. Although possible, the method used for identification should not be used for transaction release again (e.g. entering the same PIN twice) since this would increase a potential attacker's chance to perform a transaction pretending to be someone else. By using a different method (e.g. TAN) for transaction release cheating will be more difficult – the attacker would have to compromise two different mechanisms to perform a transaction. The most common means for transaction release are TAN, idToken and digital signatures. In future new methods using mobile phones will be established.

Authorization
Authorization means the bank's approval of the payment transaction, which normally takes place after the customer has released the transaction using the wallet. The authorization result depends on several checks performed by the bank, e.g. against personal limits or risk management systems.

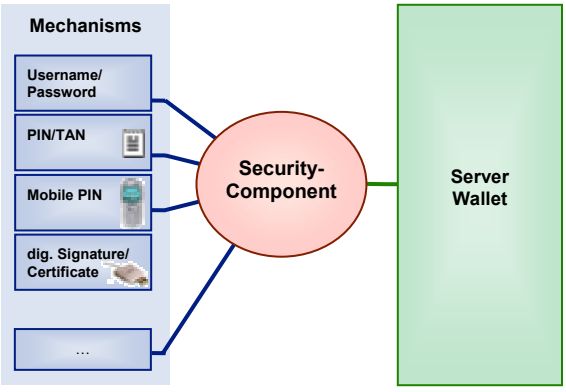
The Server Wallet takes care of the tasks identification and transaction release, whereas the payment authorization is done by the backend systems.
Therefore mechanisms capable of ascertaining the customer's identity need to be implemented as part of every server wallet. The level of certainty required and therefore the variety of applicable methods depends on the application and the regional habits. Not every method is established in every country, e.g. idTokens are very popular in Scandinavia whereas in Germany idTokens are not commonly used.
Before a customer gets access to the server wallet he has to be registered once. For this purpose personal data as well as data required for the payment transactions have to be recorded. After this, the customer receives the access data for the server wallet. These data are required to prove his identity and to release transactions. Depending on the chosen method, these data will differ and may include software and hardware components.
Many server wallets that are already in place are capable of only one mechanism. Especially for large scale and international solutions multiple methods should be offered. In the following section an architecture is described that fulfills this requirement in a well defined and efficient way.

NOVOSEC Aktiengesellschaft
Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Germany
Phone +49 (0) 6196/88289-0, Fax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Approach with separated authentication

Usually providers of large scale server wallets provide a variety of means for identification and transaction release. Since the methods available at the market are further developed continuously an easy and efficient way to integrate new methods or to remove old methods has to be found. The following approach takes this aspect into account.
A server wallet will be much simpler if its functionality is restricted to the mere payment task and does not need to take care of authentication and transaction release. Therefore the wallet is separated from the security mechanisms. A security component placed in front of the wallet will take care of the required authentication and transaction release. The wallet then receives the processed and proven identification and transaction release data from this component.
According to this, the security component is a core element. It has to be implemented such that new methods can be integrated during run time without affecting any mechanism already in place. New methods for mobile transaction release are of special interest, e.g. mobile PIN.

The following figure provides a short overview on the architecture described before:



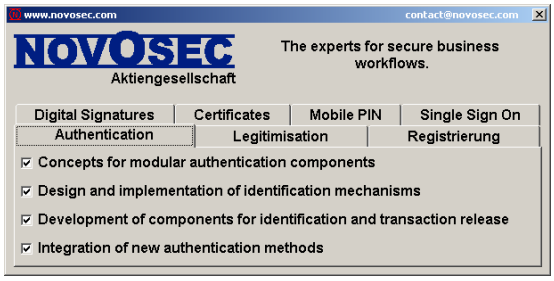
During registration of the customer (either manual or automated) the wallet only receives and stores data required for handling the payment transaction. All data regarding identification and transaction release will be stored by the security component.

Advantages

A great advantage for the wallet provider is the separation of wallet administration from the security component administration. The security component is built modularly and can easily be extended by adding new identification and transaction release methods without affecting the existing methods. In this manner newly introduced methods can coexist with previously installed ones. This enables customers to move smoothly from the old to the new methods. After a transitional period unused methods can be switched off. A convenient side effect of such a security component is the ability to use it for other bank systems as well.
The bank's customer takes advantage of being enabled for new methods as soon as they become available. If desired this can even be done automatically.

Are you interested in these topics? Do not hesitate to contact us:

juergen.weiss@novosec.com



Further documents are available at:
http://www.novosec.com/downloads

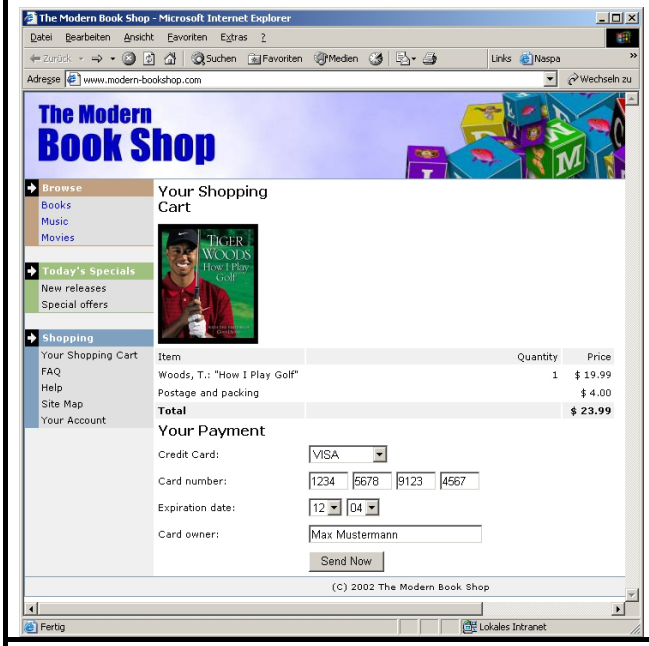
NOVOSEC Aktiengesellschaft

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus, Germany
Phone +49 (0) 6196/88289-0, Fax +49 (0) 6196/88289-11
contact@novosec.com, www.novosec.com

Figure 1 - Credit card payment transaction using authentication method PIN/TAN

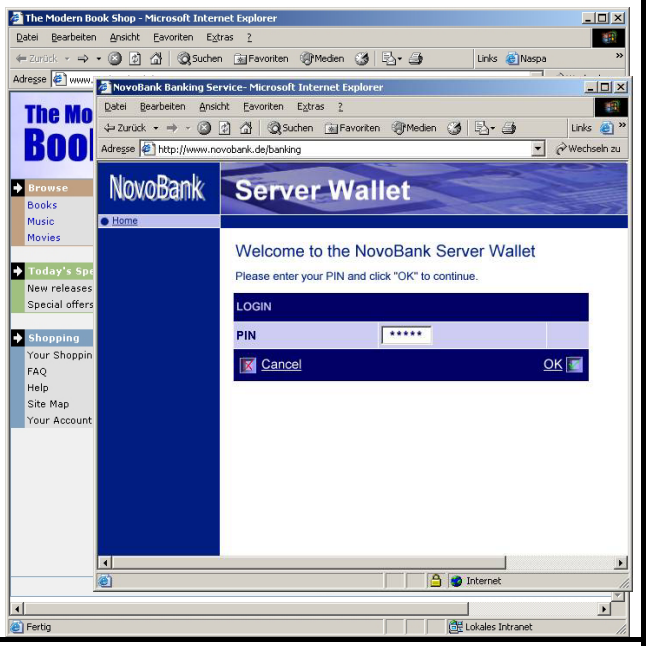
Step 1:

Customer enters Credit Card Information



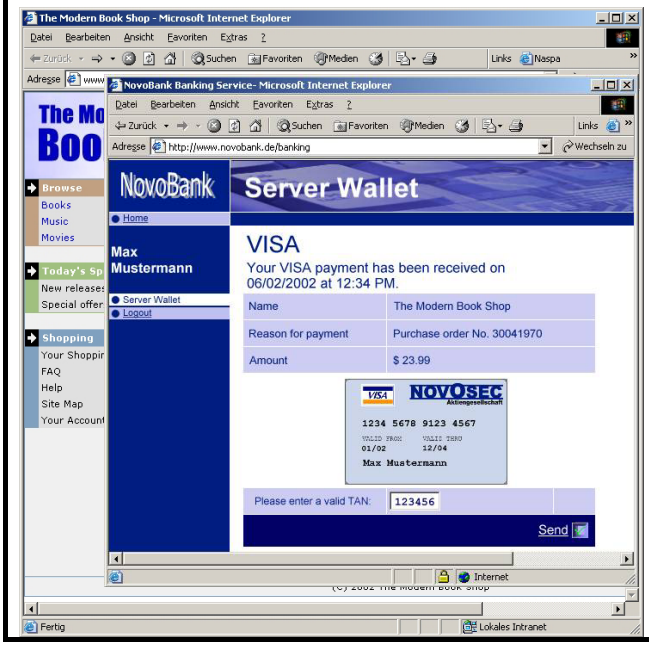
Step 2:

Server Wallet starts automatically and asks customer to enter his PIN



Step 3:

Server Wallet displays transaction data and asks customer to enter TAN



Step 4:

Transaction has been processed successfully