Universidad Carlos III de Madrid

University Carlos III of Madrid

Module 2: Enhanced security service

Secure E-commerce
OpenCourseWare

J. M. de Fuentes, A.I. González-Tablas, A. Ribagorda

Main objective

The development of an enhanced security service to secure customer's transactions.

Module's main tasks

To successfully pass this module, the following tasks are needed:

- **Implement** an enhanced security service described in the following sections.
- **Analyze the security requirements for each entity** involved in the process proposed in this second module.

Module description

Module 2 of laboratory work intends to solve some of the security problems found in Module 1. In particular, a way to improve security would be to allow customers to contact their bank directly to authenticate themselves as the genuine originators of each online transaction.

A new security service will be introduced in our schema: the **"Enhanced Security Service"**. This service is a global agreement amongst all parties involved in the electronic payment in order to enhance the security of electronic transactions. Customers, Merchants and Banks wishing to join the security service scheme must register with the appropriate third party. This **third party** provides with a "***Payment Network***" **or "Payment Schema"** with the functionality described later in this document (this entity could be similar to VISA).

Enhanced Security Service

Components:

1. Directory Server (DS)
2. Access Control Server (ACS)

Functionality

We will consider the procedures of browsing through the Merchant's server and checking-out the same as in Module 1.

Also, it is assumed that entities (consumer, merchant and banks) have already enrolled in the enhanced security service and that the **enrolment is not part of the online transaction process**. In particular, for the customer this means that **a password has been established between the consumer and the bank** to be used during the authentication process.

The new improved service forces us to include new messages into our original scheme. These new messages are described below:

Step 1: The Consumer sends the Merchant a message with "Authorization Data" (refer to Module 1).

The Merchant creates an **"Enrolment Verification Request" (VEreq)** with the data specified in Table 1 (the PAN is taken from the message received from the Consumer).

Table 1.

Enrolment Verification Request	**VEreq**
Personal Account Number	*PAN*
Merchant's bank ID (4 digits)	*BIN*
Merchant's ID (max. 24 char)	*Merchant ID*

The Merchant sends a VEReq message to the **Directory Server.** Upon receiving the VEReq the Directory Server checks:

- Whether the Merchant (identified by its ID) is enrolled in the Enhanced Security Service.
- Whether the Merchant's Bank (identified by the BIN) is also enrolled in the service.

In case of one of these assertions not being true, the Directory Sever sends the Merchant an "**Enrolment Verification Response" (VEres).** In this case, the content of the message is described below:

Table 2.

Enrolment Verification Response	**VEres**
PAN Auth. available	*NO*
ACS URL	*Null*
Error code	*Error code*

However, if both the Merchant and its Bank are enrolled in the scheme, the Directory Server proceeds as follows:

Step 1.2: The Directory Server sends an Enrolment Verification Request (VEreq) to the ACS (Access Control Server) containing:

Enrolment Verification Request	**VEReq**
Personal Account Number	*PAN*
Merchant's bank ID (4 digits)	*Null*
Merchant's ID (max. 24 char)	*Null*

The ACS (that is part of the Consumer's bank) receives the VEreq message from the Directory Server and checks whether the PAN is registered as one of its cards and whether it is enrolled in the Security Service scheme.

Step 1.3: The ACS answers with an **Enrolment Verification Response (VEres).**

If the consumer is enrolled in the Security Service, further authentication checks must be carried out, so the VEres message will include the following data:

Enrolment Verification Response	**VEres**
PAN Auth. available	*YES*
ACS URL	*http://<**server**>:<**port**>*
Error code	*Null*

If the consumer is not enrolled in the service there will be no extra authentication, so the VERes will include the following data:

Enrolment Verification Response	**VERes**
PAN Auth. available	*NO*
ACS URL	*Null*
Error code	*Null*

Step 1.4: The Directory Server sends without any modifications the VERes message received from the ACS to the Merchant.

The Merchant, once received the VERes from the Directory Server checks the field *PAN Authentication available.*

- If the value is *NO*, the schema used in conventional commerce (Module 1) will be used to process the transaction.
- If the field's value is *YES,* an additional authentication step is required (see step 1.5).

Step 1.5: The consumer must authenticate directly with the ACS. In order to achieve this, the merchant will redirect the consumer to the URL found in message VERes received, accompanying the redirection with a PAReq message shown below:

PAN Authentication Request	PAReq
Merchant's Bank ID (4 digits)	*BIN*
Merchant's ID (max. 24 chars)	*ID_merchant*
Merchant's URL	*http://<server>:<port>*
Operation ID	*As defined in module 1*
Amount	*XXXx€*
PASSWORD	*Null*

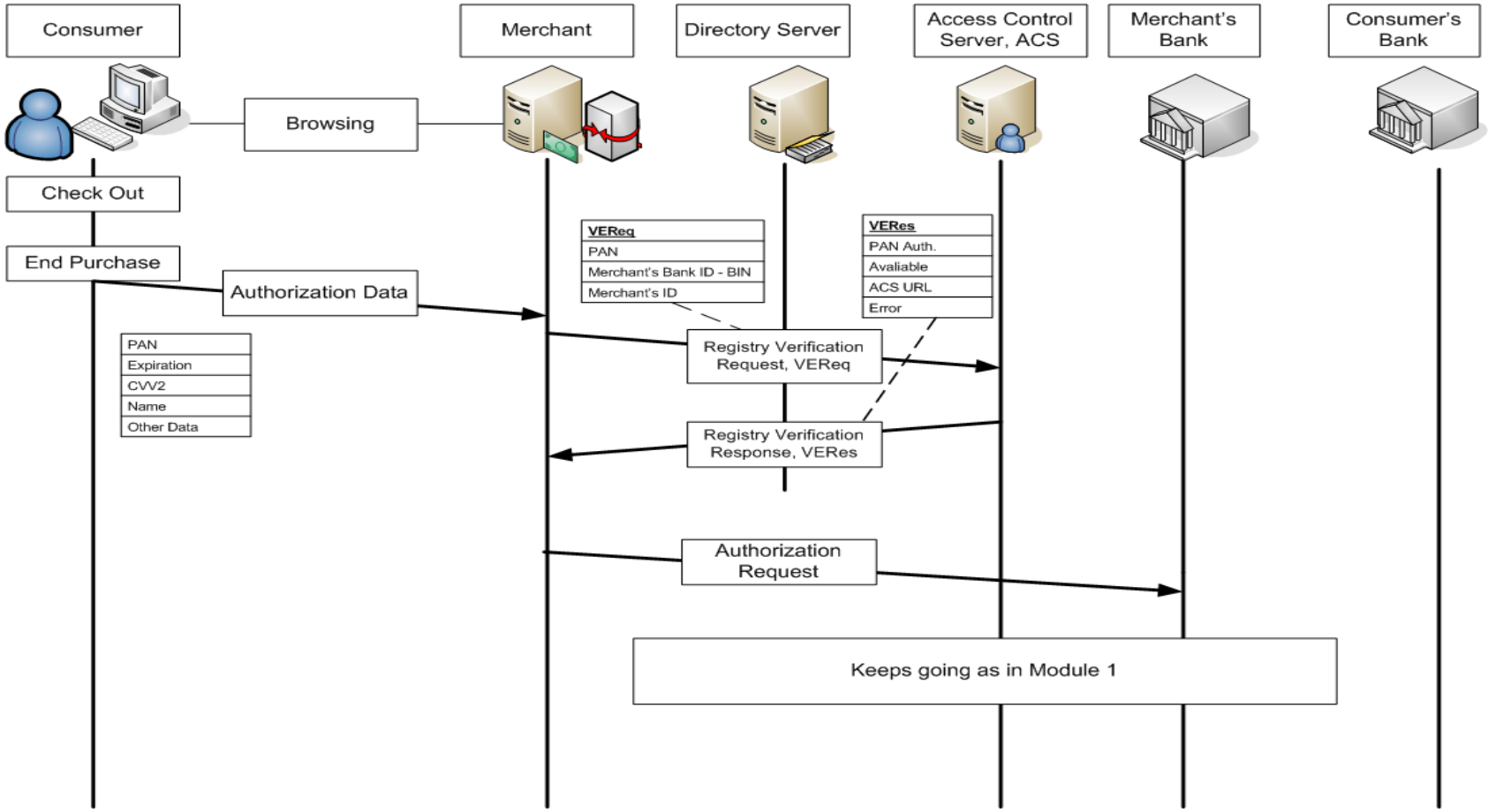
Step 1.6: The consumer sends the PAReq message (with the password obtained from the bank in the enrolment process) to the ACS, so the ACS can then authenticate the origin of the transaction.

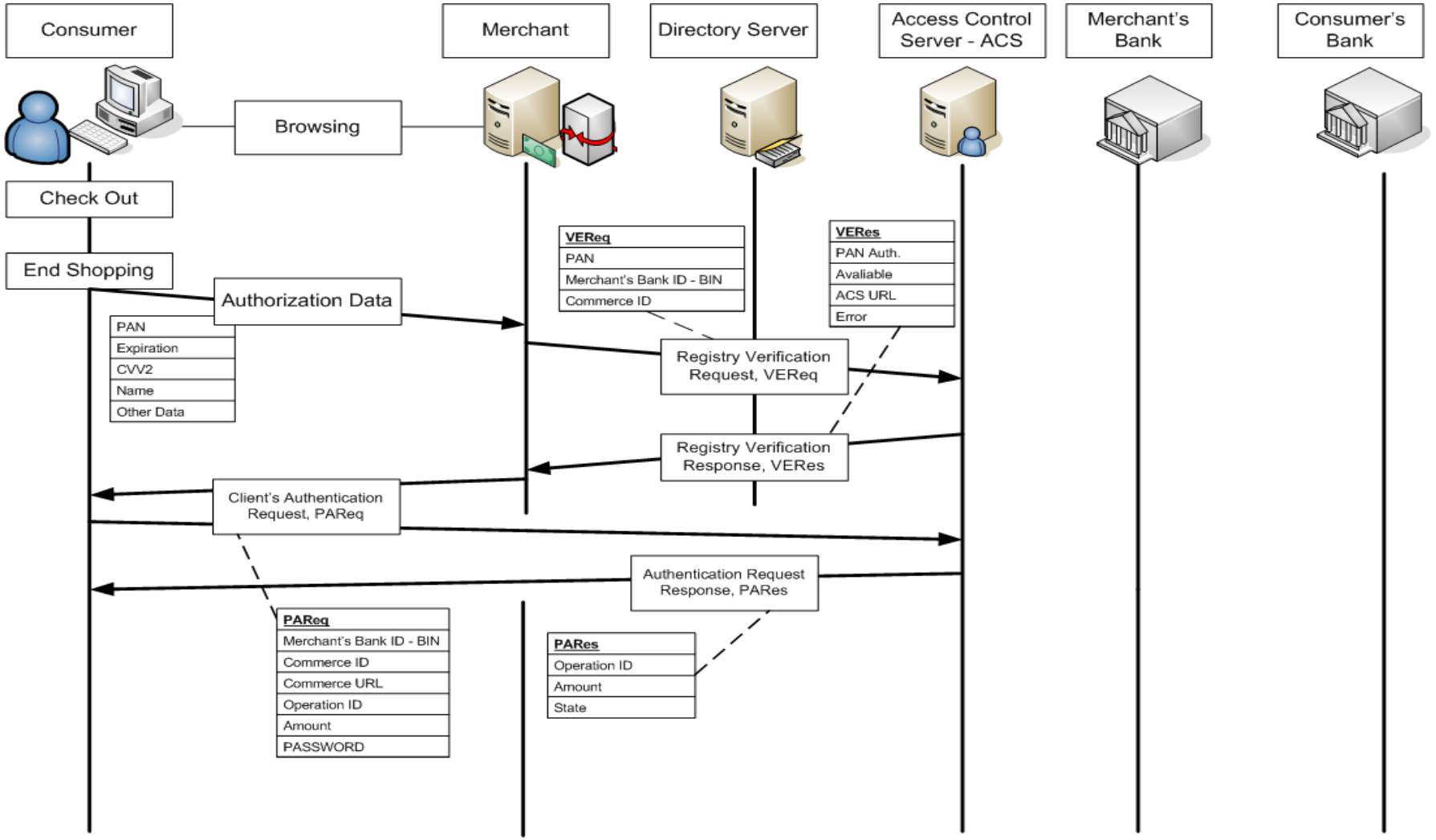
Step 1.7: As a result of the authentication process, the ACS answers the consumer with an PAN Authentication Response (PARes) with the content specified below:

PAN Authentication Response	PARes
Operation ID	*As defined in module 1*
Amount	*XXXx€*
Auth result	*OK/ NO_OK*

Module 2 will stop at this point, without any more messages.

Figure 2 shows the scheme when the consumer can perform the extra security checks authenticating with the ACS. By contrast, Figure 1 represents a scheme in which the ACS cannot directly authenticate the customer.


Consumer
Merchant
Directory Server
Access Control Server, ACS
Merchant's Bank
Consumer's Bank
Browsing
Check Out
End Purchase
Authorization Data
PAN
Expiration
CVV2
Name
Other Data
VEReq
PAN
Merchant's Bank ID - BIN
Merchant's ID
VERes
PAN Auth.
Avaliable
ACS URL
Error
Registry Verification Request, VEReq
Registry Verification Response, VERes
Authorization Request
Keeps going as in Module 1


Consumer
Merchant
Directory Server
Access Control Server - ACS
Merchant's Bank
Consumer's Bank
Browsing
Check Out
End Shopping
Authorization Data
PAN
Expiration
CVV2
Name
Other Data
VEReq
PAN
Merchant's Bank ID - BIN
Commerce ID
VERes
PAN Auth.
Avaliable
ACS URL
Error
Registry Verification Request, VEReq
Registry Verification Response, VERes
Client's Authentication Request, PAReq
Authentication Request Response, PARes
PAReq
Merchant's Bank ID - BIN
Commerce ID
Commerce URL
Operation ID
Amount
PASSWORD
PARes
Operation ID
Amount
State