Universidad Carlos III de Madrid

University Carlos III of Madrid

Module 3: Enhanced security module (part II)

Secure E-commerce
OpenCourseWare

José María de Fuentes, A. I. González-Tablas, A. Ribagorda

Main objective

The development of an enhanced security service to secure customer's transactions. **Continuation of Module 2.**

Module description

Module 3, as well as module 2, 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 on-line transaction.

In Module 3, a new step 1.7 will be defined.

At the end of Module 2, if both the Merchant and the cardholder were enrolled in the scheme, the consumer received from the merchant the following message together with a particular URL (different from MERCHANT'S URL) to which the consumer will have to access in order to authenticate the transaction:

(Step 1.5 in Module 2): ACS's URL +PAReq

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 in Module 2): The consumer had to send the PAReq message just received (with the password obtained from the bank in the enrolment process) to the ACS, so the ACS could then authenticate the origin of the transaction.

(Step 1.7 in Module 2): As a result of the authentication process, in the last message defined in Module 2, the ACS answered the consumer with a PAN Authentication Response (PARes). The content is specified below:

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

MODULE 3 WILL REDEFINE STEP 1.7 PROPOSING THE FOLLOWING ENHANCEMENTS:

New Step 1.7 -- Redefines step 1.7 in Module 2):

Once the consumer has been authenticated to the ACS, the ACS proceeds with the following messages:

- It sends the Consumer's Bank notification of the transaction. The specific content of this message is to be decided by the student as it will depend on the Bank's initial database description.
- It also generates a new PARes message extending the previous one described in step 1.7. The new message will include the MD5 hash value (see sample code available.)

PAN Authentication Response	**New PARes**
Consumer's Bank ID (6 digits)	*BIN*
Merchant's ID (máx 24 chars)	*Merchant's ID*
PAN	*pan*
Operation ID	*As defined in module 1*
Amount	*XXXx€*
Auth result	*OK/ NO_OK*
Date and Time of MD5 hash	*Optional format*
MD5 hash value of message New PARes	*128 bits*

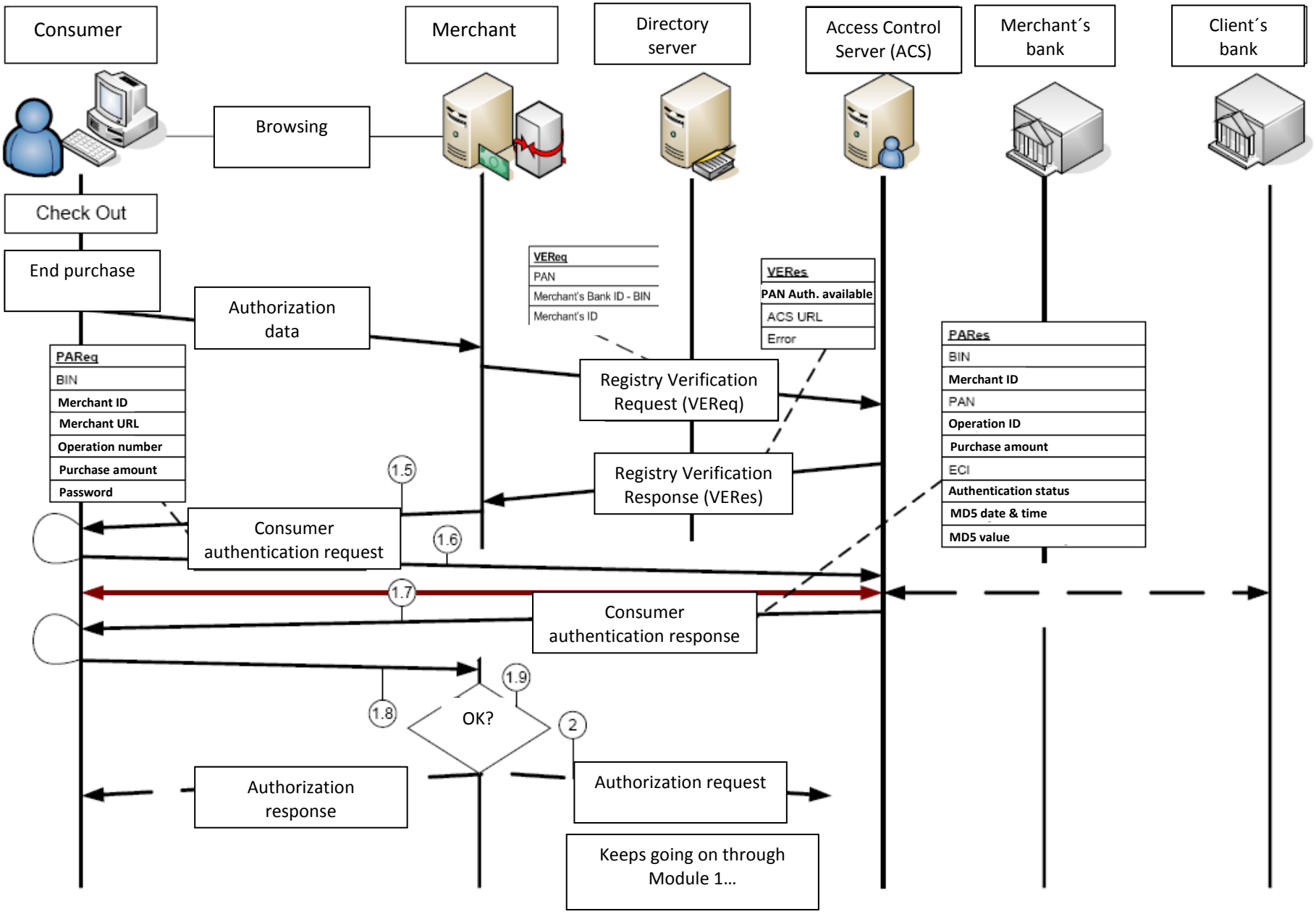
Step 1.8 in Module 3:

Once the consumer has received the new message PARes from the ACS, the consumer relays this message onto the merchant using the URL that the merchant specified in message PAReq (step 1.5 of module 2, Merchant's URL.)

Step 1.9 in Module 3:

When the merchant receives the new message PARes, it carries on the following actions:

- It checks the integrity of the message by verifying that the MD5 value is correct. (In real scenarios the digital signature of such a message would serve to authenticate the ACS who originated it.)
- If the verification is successful, the transaction processing carries on with message Auth Request as specified in Module 1.
- If the verification is not successful, the merchant responds to the consumer with a message Auth Response (module 1, message 5) in which authorization Status is set to NOT_OK. This will abort the transaction as it was not possible to authenticate the consumer's real identity.


Consumer
Merchant
Directory server
Access Control Server (ACS)
Merchant´s bank
Client´s bank
Browsing
Check Out
End purchase
Authorization data
VEReq
PAN
Merchant's Bank ID - BIN
Merchant's ID
VERes
PAN Auth. available
ACS URL
Error
PAReq
BIN
Merchant ID
Merchant URL
Operation number
Purchase amount
Password
Registry Verification Request (VEReq)
Registry Verification Response (VERes)
PARes
BIN
Merchant ID
PAN
Operation ID
Purchase amount
ECI
Authentication status
MD5 date & time
MD5 value
1.5
1.6
1.7
1.8
1.9
2
Consumer authentication request
Consumer authentication response
OK?
Authorization response
Authorization request
Keeps going on through Module 1...