E-commerce security: SSL/TLS, SET and others.

4.3

Universidad
Carlos III de Madrid
Grupo SeTI · Dpto. Informática

3-D Secure: Payment Authentication

- Higher chargeback rates for Internet purchase transactions than face-to-face
  - fraud-related
  - cardholders claiming non participation
- Issuers need a means to verify that the person making an e-commerce purchase is an authorized cardholder
  - == “payment authentication”
- Visa has developed payment authentication capabilities to
  - improve transaction performance online
  - accelerate the growth of electronic commerce through increased consumer confidence

3-D Secure: Protocol Features

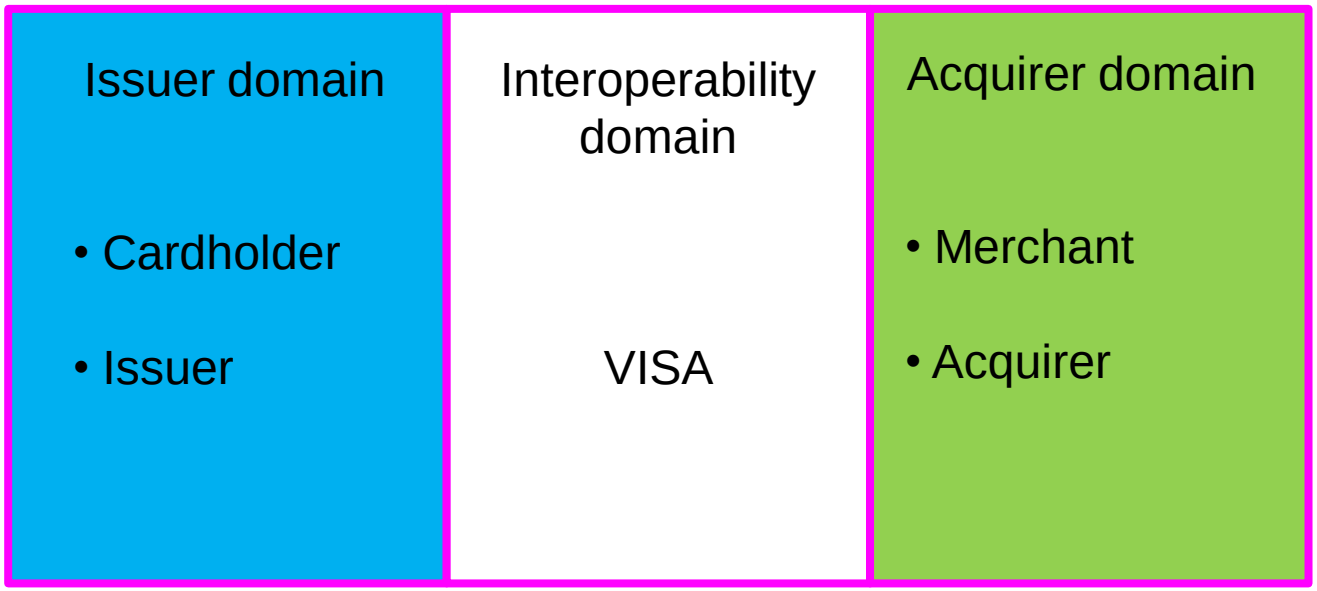
- Global framework for authentication
- Reduced operational expense
- No special hard- or software for cardholder
- Upgradeable by issuer to meet customer requirements
- Extensible to mobile phone, PDA's, digital TV
- Based on globally accepted standards (IETF)
- Centralized archive of payment authentications (for use in dispute resolution)

3-D Secure: Benefits

- Reduces
  - Fraudulent usage
  - Disputes
  - Retrievals
  - Chargebacks
- Increases
  - Consumer confidence
  - Sales
  - Card acceptance
  - Usage facility (no special software for cardholder, easy plug-in for merchant)

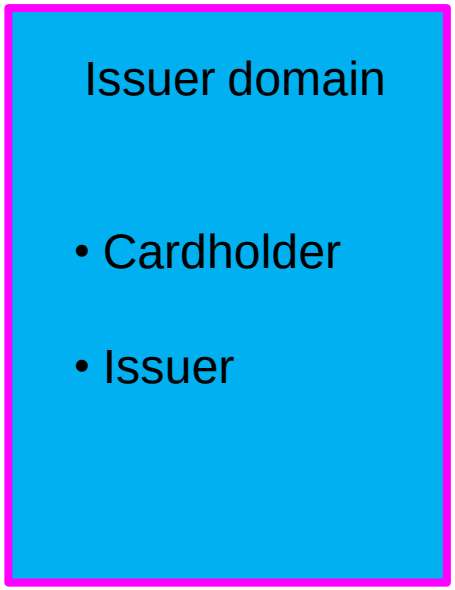
3-D Secure: Three Domain Model

- Uses SSL/TLS and a Merchant Server Plug-in to:
  - pass information and query participants to authenticate the cardholder during an online purchase
  - protect payment card information as it is transmitted via the Internet



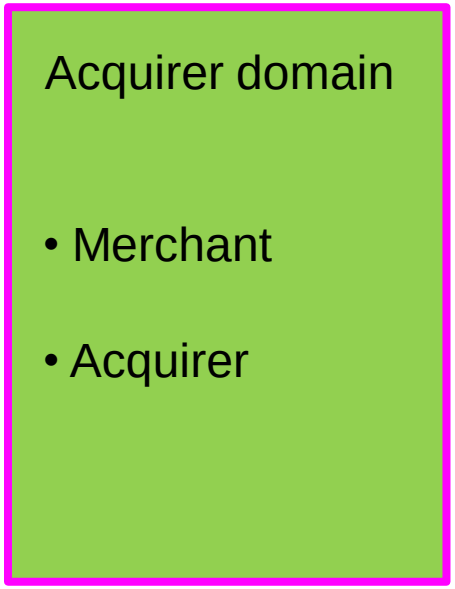
3-D Secure: Three Domain Model

- Issuer domain
  - Cardholder +
    - Cardholder browser
    - Additional components
  - Issuer +
    - Access control server
- The Issuer is responsible for :
  - managing the enrollment of their cardholders in the service
  - authenticating cardholders during online purchases



3-D Secure: Three Domain Model

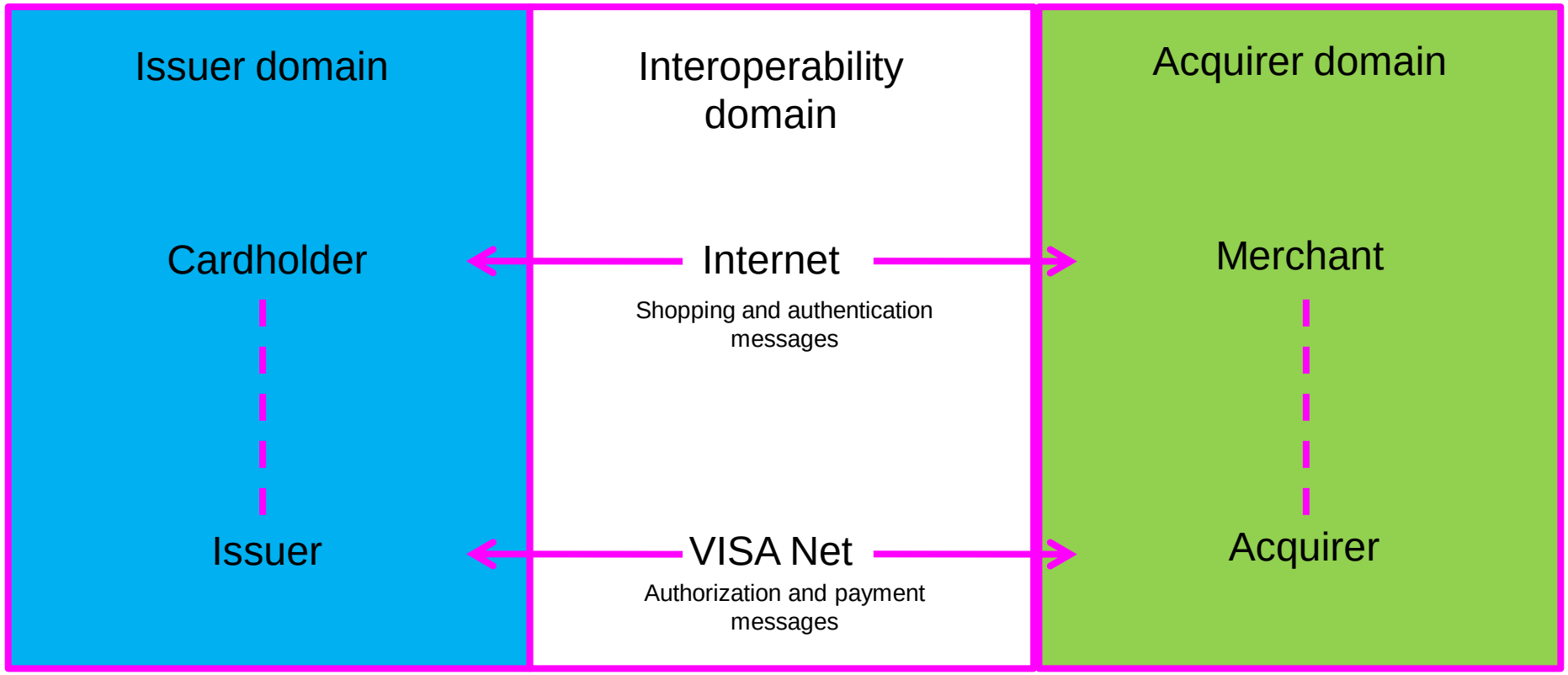
- Acquirer domain
  - Merchant +
    - server plug-in
  - Acquirer
- The Acquirer is responsible for:
  - defining the procedures to ensure that merchants participating in Internet transactions are operating under a merchant agreement with the Acquirer
  - providing the transaction processing for authenticated transactions



3-D Secure: Three Domain Model

- Interoperability domain
  - VISA directory server
  - Commercial certificate authority
  - VISA certificate authority
  - Authentication history server
  - VISA Net
- This domain facilitates the transaction exchange between the other two domains with a common protocol and shared services

3-D Secure: Three Domain Model



3-D Secure: 2 Sub - Protocols

1. Enrollment
    1. Supply payment card number, identity information and password
    2. Validate information
    3. Storage of information for online authentication
2. Payment Authentication
    1. Cardholder purchase
    2. Request to VISA directory server
    3. Cardholder authentication
    4. Payment processing

3-D Secure: Enrollment

Step 1 The cardholder visits the issuer's 3-D Secure Enrollment Web page.

Step 2 The cardholder supplies payment card number and provides other enrollment information with the Enrollment Server that will enable the issuer to validate cardholder identity, and establish any required shared secret, such as a password.

Step 3 The issuer or third party validates the information provided in Step 2 to verify that the cardholder is entitled to use the payment card being enrolled. In the case of a Visa smart card, the verification process also establishes that the cardholder has physical possession of the card at the time of enrollment.

Step 4 Information is stored for validation during authentication processing. The cardholder is informed of success (or failure) of enrollment. The cardholder is ready to go shopping as soon as enrollment is confirmed.

3-D Secure: Authentication

Step 1 Shopper browses at a merchant site, selects items, and then finalizes the purchase. (Note: The merchant now has all the necessary data, including card number and user device information.)

Step 2 The Merchant Server Plug-in (MPI) sends the PAN (Personal Account Number, and user device information, if applicable) to the Visa Directory Server

Step 3 Visa Directory Server queries the appropriate Access Control Server (ACS) to determine whether authentication is available for the PAN and device type. (If an appropriate ACS is not available, the Visa Directory Server creates a response for the MPI and processing continues with Step 5.)

Step 4 The ACS responds to the Visa Directory Server, indicating whether authentication is available for the card number.

3-D Secure: Authentication

Step 5 The Visa Directory Server forwards the ACS response (or its own) to the MPI.

If no authentication is available, the merchant, acquirer, or payment processor submits a traditional authorization request.

Step 6 The MPI sends a Payer Authentication Request (PAReq) to the ACS via the shopper's device.

Step 7 The ACS receives the PAReq.

Step 8 The ACS either authenticates the shopper by using processes applicable to the card number (password, chip, PIN, etc.). The ACS then formats the PARes message with t the appropriate values and signs it.

3-D Secure: Authentication

Step 9 The ACS returns the PARes to the MPI via the shopper's device. The ACS sends selected data to the Authentication History Server (AHS).

Step 10 The MPI receives the PARes.

Step 11 The MPI validates the PARes signature (either by performing the validation itself or by passing the message to a separate Validation Server).

Step 12 If appropriate, the merchant proceeds with the authorization exchange with its acquirer.

Following Step 12, the acquirer processes the authorization request and returns the authorization response to the merchant.

3-D Secure: Different Perspectives

- Merchant perspective
  - Must integrate a Merchant Server Plug-in (MPI)
  - Exchange of messages with VISA Directory and Access Control Servers for authentication of shopper
  - Pass authentication data to acquirer for processing into VISA Net
- Acquirer perspective
  - Responsible for contracting with merchants to offer the 3-D Secure service
  - Possibly provides implementation and processing support to merchants
  - Assigns and manages merchant ID's, passwords, or certificates needed to authenticate merchants

3-D Secure : Different Perspectives

- Cardholder perspective
  - Enrol through web site operated by Issuer
  - Asked for identity information and password (= shared secret between Issuer and cardholder)
  - 3-D Secure transaction not substantially different from ordinary e-commerce transaction
  - No special software required using a magnetic stripe card. In case of using a smart card, chip card reader + software required.
- Issuer perspective
  - Responsible for enrolling cardholders into the system and authenticating them during transactions
  - Information exchange with the Access Control Server for authentication