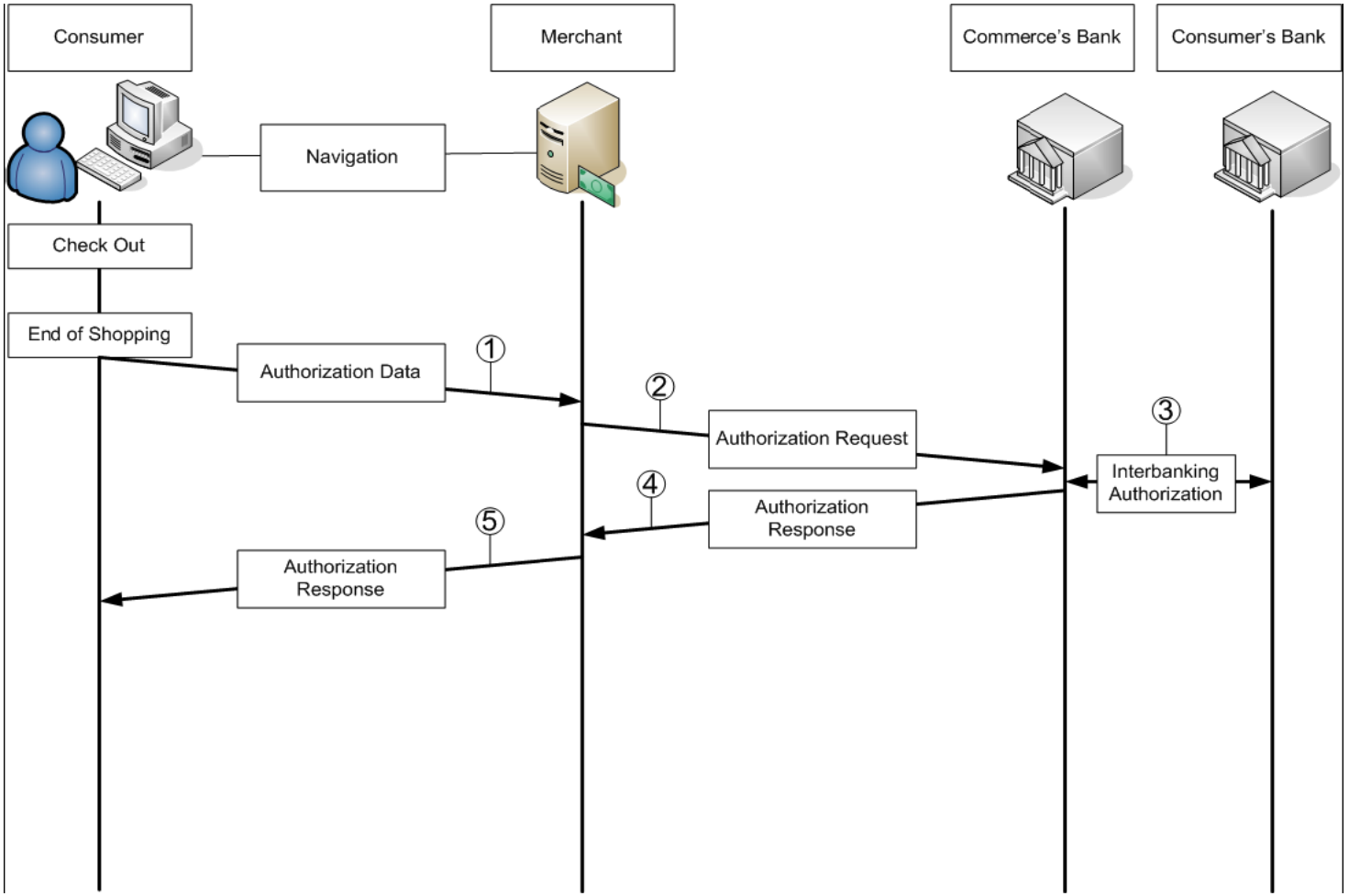
Universidad Carlos III de Madrid

Secure e-commerce
Module 2 - Discussion

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

Module 1. Review of security issues



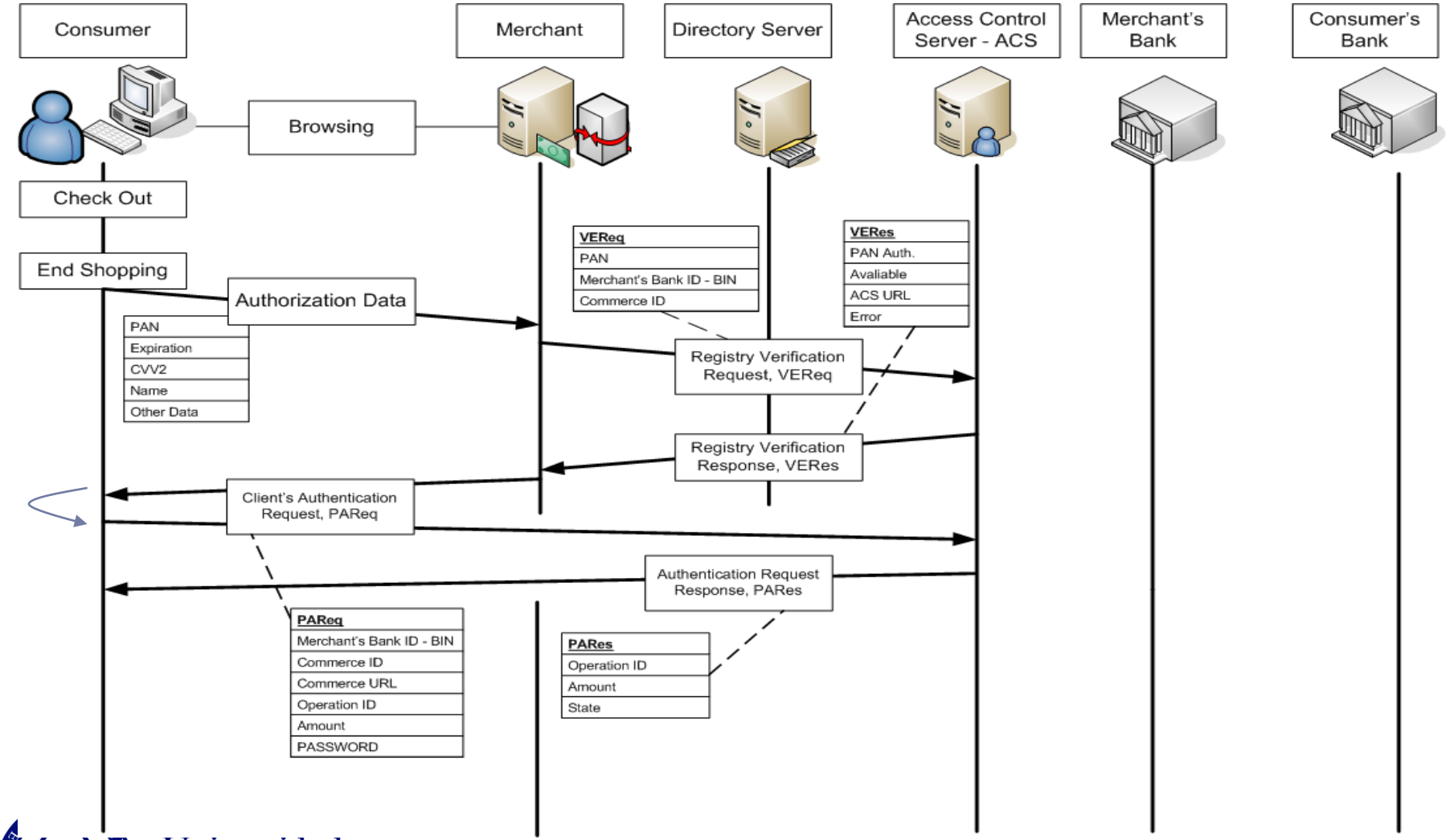
Security discussion

- Merchant´s fraud
  - Mechanisms to solve this:
    - “Data ciphering” (merchant is not able to decrypt them)
    - “Client confirmation”. Pin-alike cards / passwords
    - → Client – Bank direct dialog
- Improvement: **Enhanced security service**
  - Client authentication against its bank

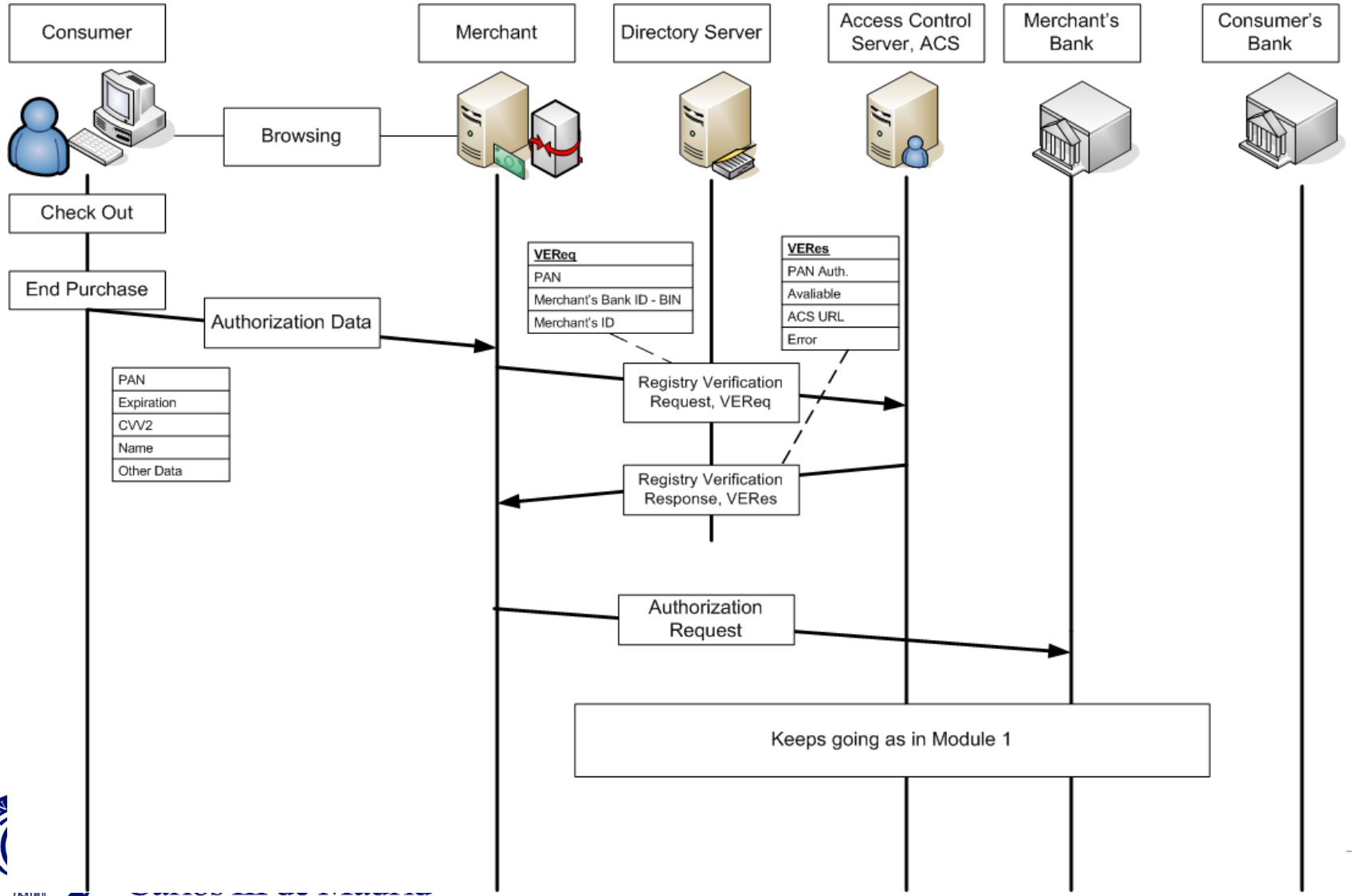
Enhanced security service?

- Two new entities:
  - Access control server (ACS)
    - Part of the client´s bank!
  - Directory server
    - *Payment network, payment scheme, interoperability domain*
    - Global agreement between all stakeholders
      - ✓ Client
      - ✓ Merchant
      - ✓ Merchant´s bank
      - ✓ Client´s bank
    - Subscription → Reliability

Module 2: Process if checks are correct

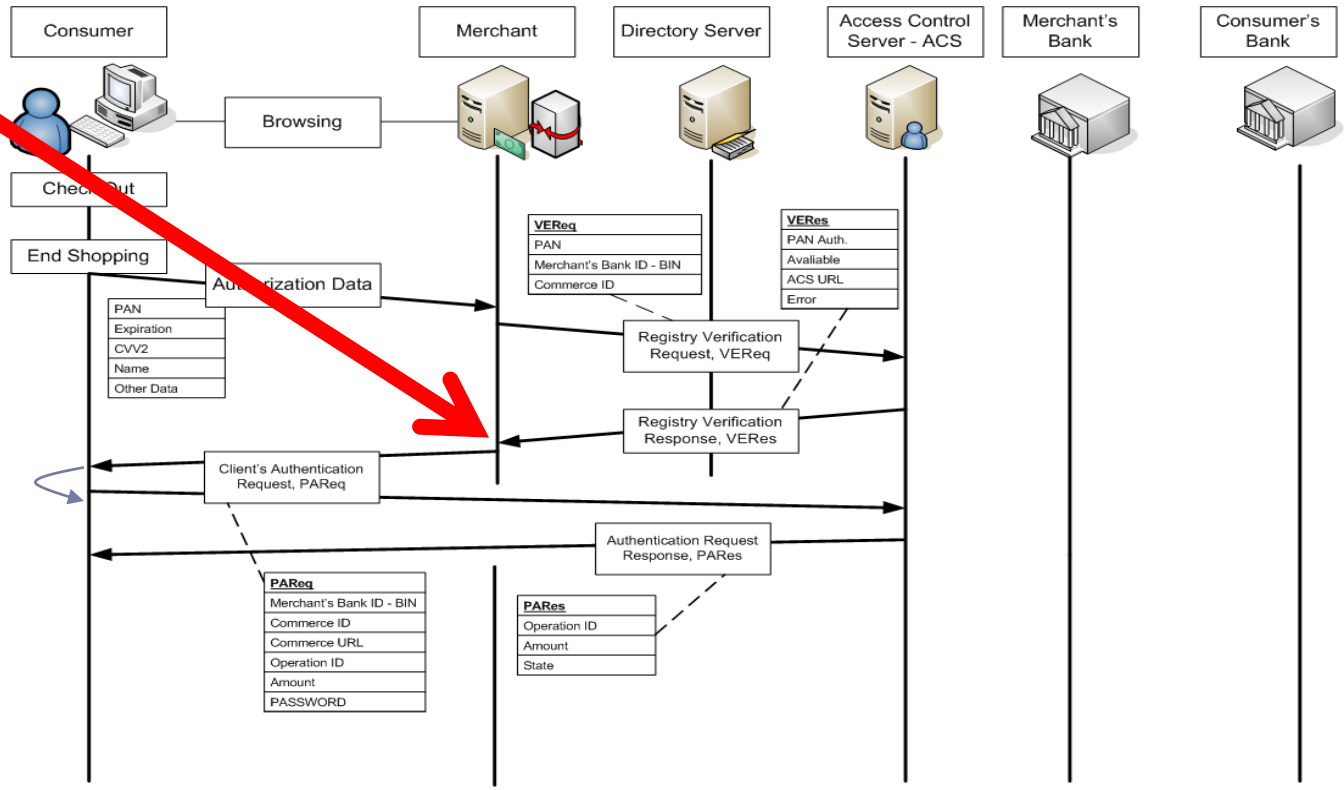


Module 2: Process if checks are **not** correct



Security discussion of module 2 (Result: ☹ ☹ ☹)

PHISHING



- ***Absolute* delegation in the client. Absolute?**

Implementation issues

- Enrollment process has been previously done
- Merchant → Client message should be implemented with TWO messages
  - Redirect header
  - The rest of the message

Universidad Carlos III de Madrid

Secure e-commerce
Module 2 - Discussion

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