المؤتمر العربي الدولي السادس

لتكنولوجيا المعلومات والمعرض المصاحب له

الرباط - المملكة المغربية - 29-31 أكتوبر 2013

تحت شعار

تكنولوجيا المعلومات: وسيلة لمواكبة التطور والإبداع

بسم الله الرحمن الرحيم

Secure Electronic Transaction Protocol in E-Commerce

By
Taroub Issa
Al-Quds Open University-
Palestine
tessa@qou.edu

Outline

- INTRODUCTION
- Encryption Technology
- SET Protocol
- Key Technologies of SET
- Dual Signatures:
- Advanced Models of SET
- 3-D Secure Protocol
- Intermediary-3D Secure
- Conclusion

INTRODUCTION

- **E-commerce was established in 1991; it is selling and buying of products and services by business and consumers via computer network such as internet. It covers a zone of different types of businesses.**
- **It is said that e-commerce is one of the most important sides in the internet to display. From the year 1991 till today, life has faced drastic changes due to technological advancements, but simultaneously they have made our lives more complex. Moreover, e-commerce became a need for development and modifying to protect the data and information from any attack .**

INTRODUCTION

The litany of evolutionary phases in E-commerce masks a number of growing technical challenges, which could be addressed as the following :

- **security and authentication.**
- **content management and publication.**
- **reliable systems, messaging, and data.**
- **complex interactions and transactions.**
- **business model implementation and business process enactment.**
- **distributed processing and distributed data.**

INTRODUCTION

There are two lines of defense for e-commerce which are technology solutions and policy solutions .

- **Encryption Approach**
- **Secure Socket Layer**
- **Secure Hypertext Transfer Protocol (S-HTTP)**
- **Trust Seals Programs**
- **Digital Signature**
- **Secure Electronic Transaction (SET)**
- **And many other solutions……**

Encryption Technology

Encryption is the key security schemes adopted for electronic payment systems, which is used in protocols like SSL and SET. It is a very old technology for keeping messages secret from unauthorized access.

- DES
- RSA

RSA

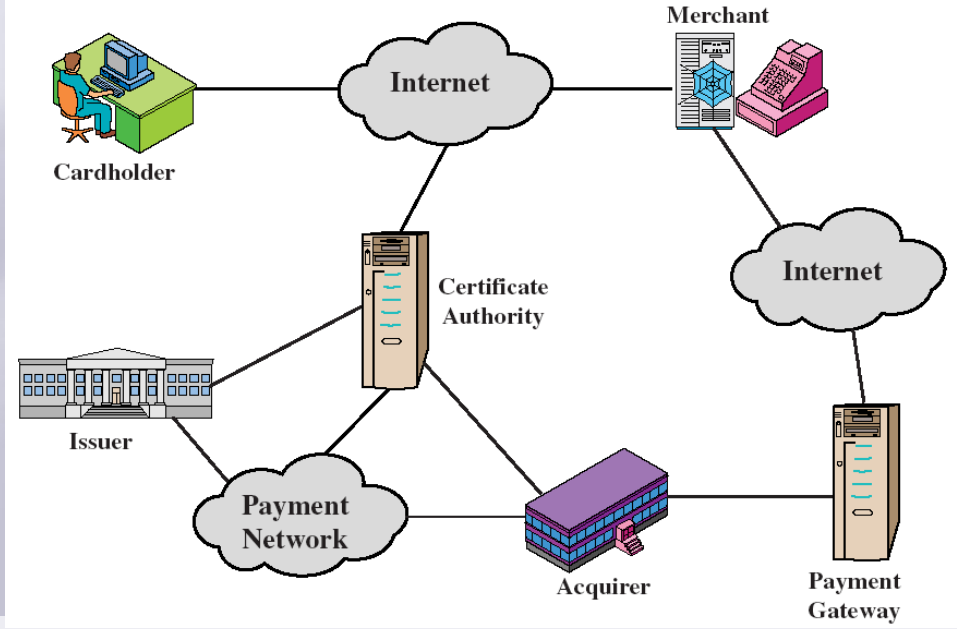
- The RSA Cryptosystem is an asymmetric cryptosystem developed by the trio: Ronald Rivest, Adi Shamir and Leonard Adleman [13]. The RSA cryptosystem is based on the principle that if two large prime numbers are multiplied, the resulting number is hard to factor back to its original numbers. In the RSA cryptosystem the two numbers are keys, namely private and public keys. A private key must be kept secret, while a public key can be revealed to anyone.

DES

Data Encryption Standard (DES) is the most widely used symmetric cryptography. DES was adopted by NIST (National Institute of Standards and Technology) in 1977 to provide an encryption algorithm to be used in protecting federal unclassified information from unauthorized disclosure or undetected modification during transmission or while in storage.

SET Protocol

- SET is an open standard for encryption and security specification for credit card transactions on the internet [19]. The SET is a set of security protocols and formats that main section are application protocol and payment protocol. The electronic commerce parties based on SET protocols can be illustrated as SHOWN BELOW:

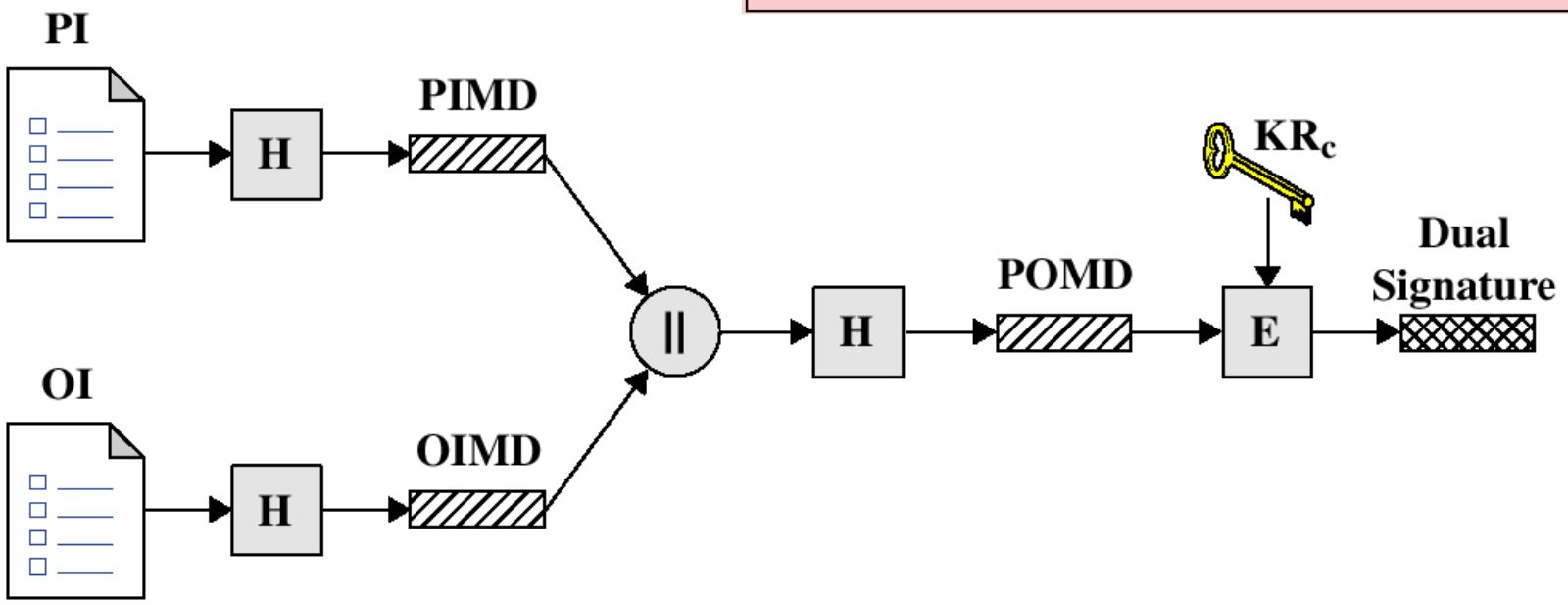


Key Technologies of SET:

- Confidentiality of information: DES.
- Integrity of data: RSA digital signatures with SHA-1 hash codes.
- Cardholder account authentication: X.509v3 digital certificates with RSA signatures.
- Merchant authentication: X.509v3 digital certificates with RSA signatures.
- Privacy: separation of order and payment information using dual signatures.

Dual Signatures:

$$DS = E_{KR_c}[H(H(PI) \| H(OI))]$$



PI = Payment Information
OI = Order Information
H = Hash function (SHA-1)
|| = Concatenation

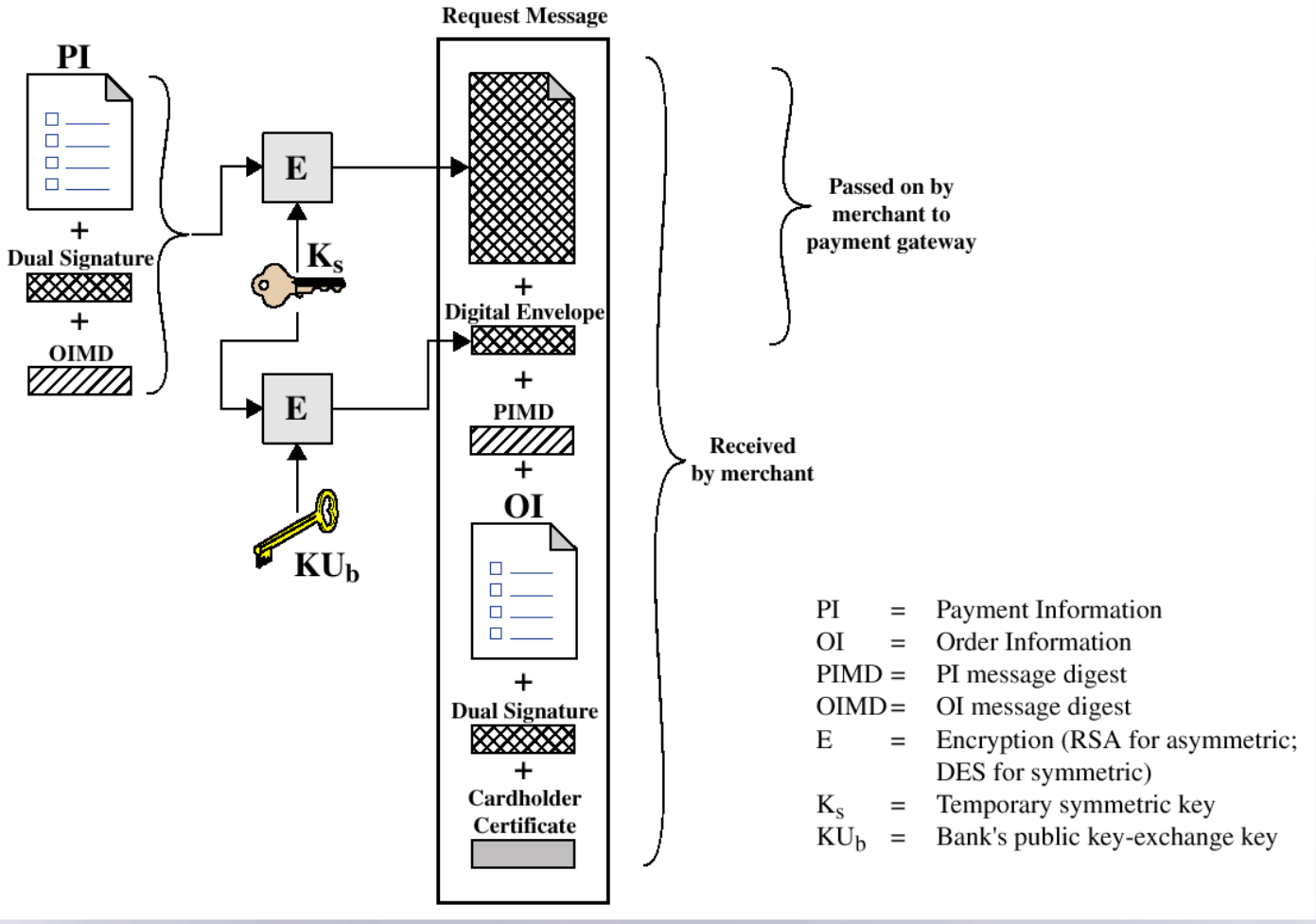
PIMD = PI message digest
OIMD = OI message digest
POMD = Payment Order message digest
E = Encryption (RSA)
KR_c = Customer's private signature key

Dual Signature Model

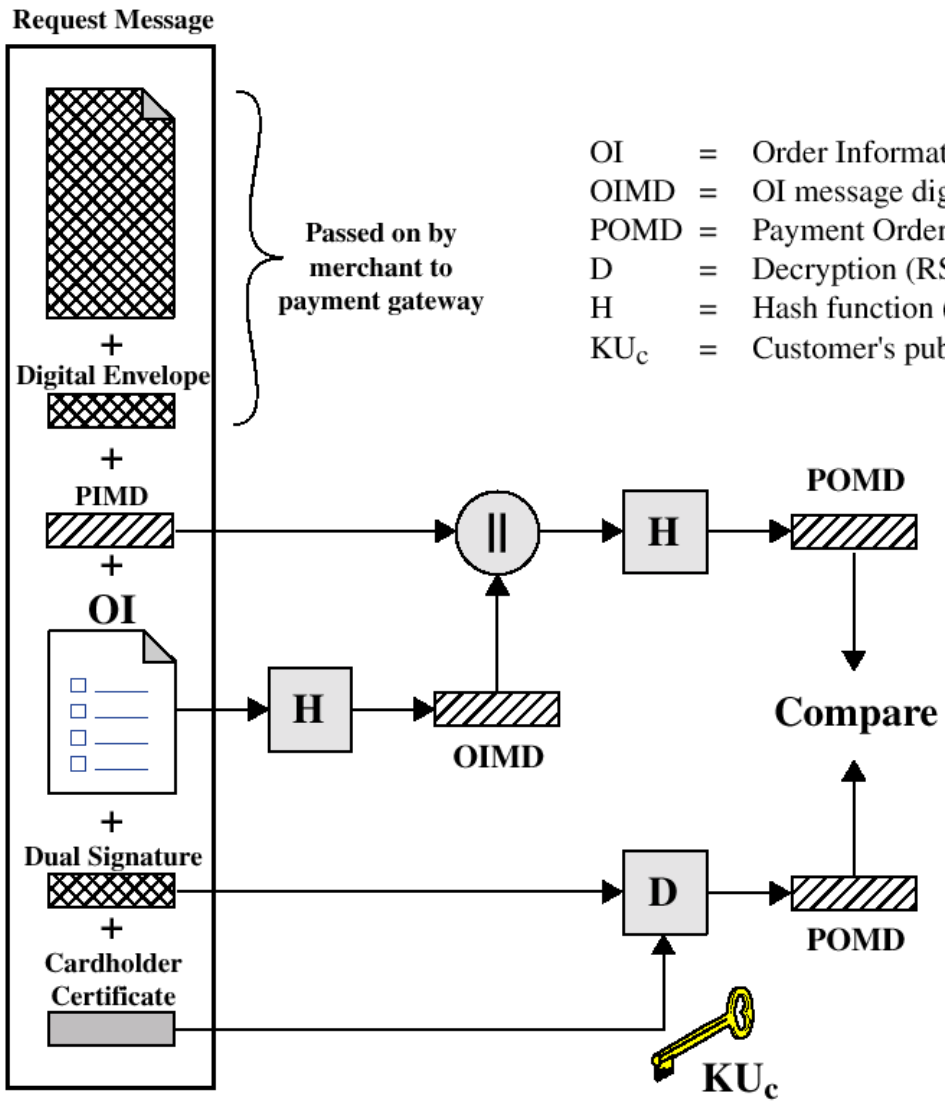
Sequence of events for transactions is SET protocol ar

1. The customer opens an account.
2. The customer receives a certificate.
3. Merchants have their own certificates.
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant request payment authorization.
8. The merchant confirm the order.
9. The merchant provides the goods or service.
10. The merchant requests payments.

ardholder sends Purchase Request



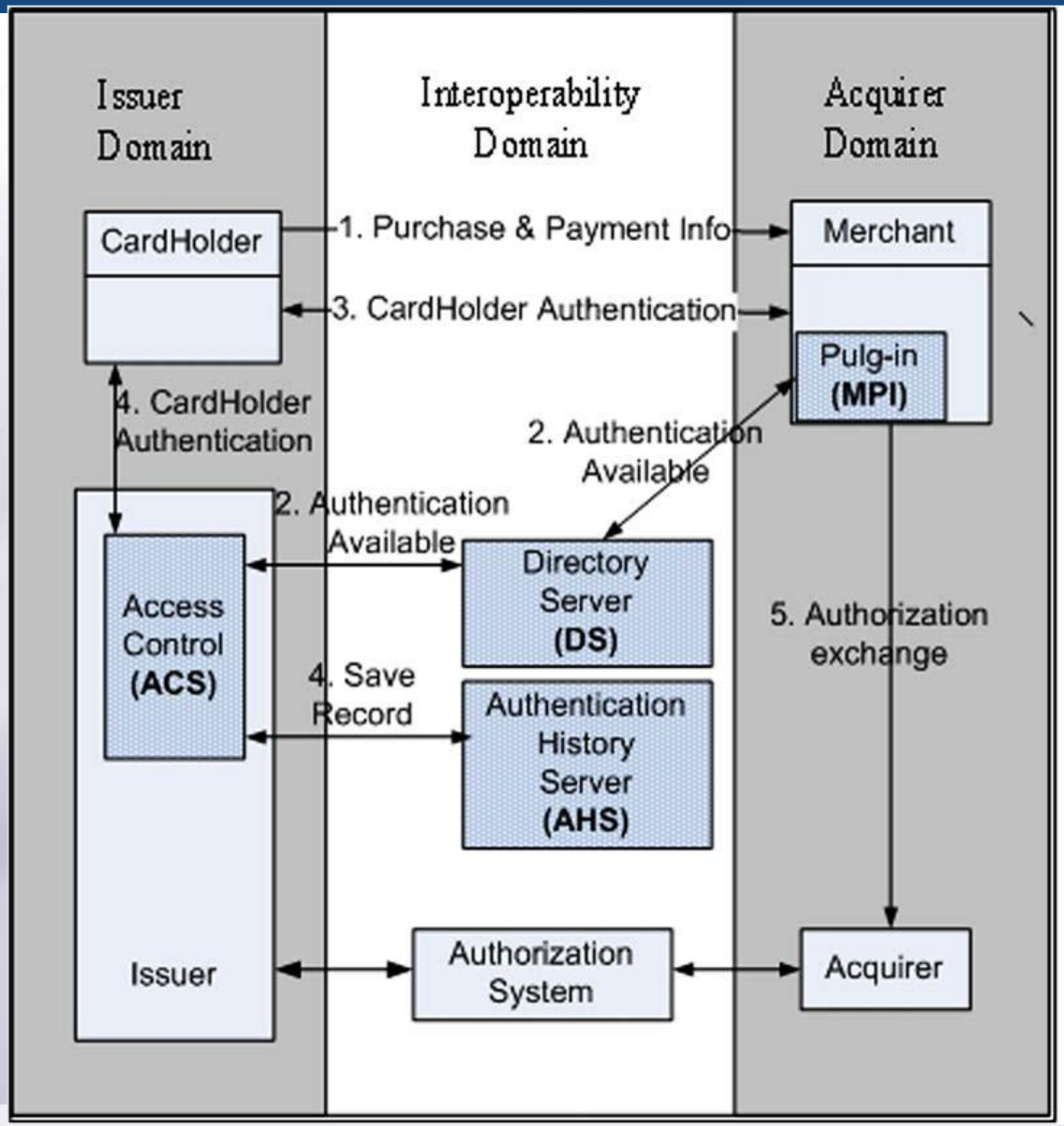
Merchant Verifies Customer Purchase Request



Advanced models of SET
3-D Secure Protocol:

- The three-Domain Secure (3-D Secure) model of VISA provides the issuers with the ability to authenticate cardholders during an online purchase. This reduces the fraudulent use of credit cards and increases traceability of the transaction. The model divides the payment system into:
- Issuer Domain,
- Acquirer Domain
- and Interoperability Domain

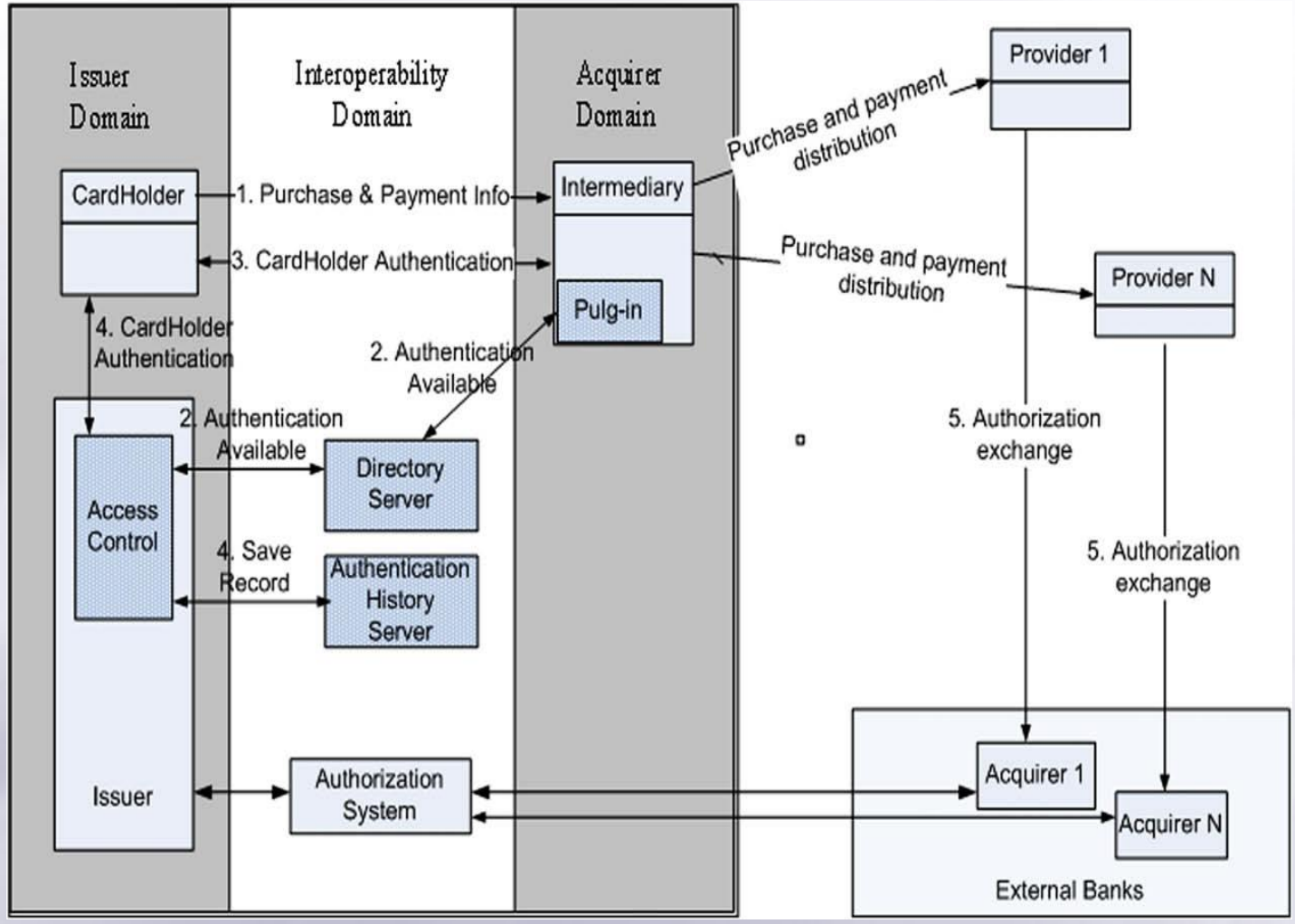
The following figure represents the Domain model of VISA and the principal flows in the payment protocol.



Intermediary-3D Secure

- Mildrey Carbonell & elt. proposed a multiparty electronic commerce protocol in which the intermediary plays the role of a payment mediator. This intermediary helps the customer to make purchases and payments with many providers simultaneously as a single payment transaction. They proposed model decreases the number of customer operations in the traditional multiparty payment process.
- In this multiparty electronic commerce model, the intermediary plays the role of payment mediator between one customer and many providers as illustrated IN THE FIGURE NEXT

3D Secure_ protocol with intermediary



Conclusion

- Electronic payment solutions are mostly focused on traditional two party business models. However, many business models involve some intermediary entities to help negotiation. Mildrey Carbonell & elt. proposed a multiparty electronic commerce protocol in which the intermediary plays the role of a payment mediator. This intermediary helps the customer to make purchases and payments with many providers simultaneously as a single payment transaction. Even though, these proposed models solved many problems of previous one, they still suffer many gaps in the payment process.
- We expect to see other advanced models in the near future that overcome all the disadvantages of the previous protocols and models.

Finished

شكرا لكم