E-Payment Systems and Cryptocurrency Technologies

https://course.ie.cuhk.edu.hk/~ftec4004

Prof. Wing C. Lau
wclau@ie.cuhk.edu.hk
http://www.ie.cuhk.edu.hk/~wclau

Acknowledgements

- The slides used in this lecture are mostly adapted from the following sources. The copyrights and contribution of the original authors are hereby acknowledged and recognized:
  - The Electronic Payment Systems course by Prof. Michael Shamos, CMU
  - “Payments 101: Credit and Debit Card Payments,” A First Data White Paper, Oct 2020.
  - “How a Credit Card is Processed”, CreditCards.com, 2013.
  - Matt Davies, “Hot Topics in Payments,” Fedral Reserve Bank of Dallas, Oct 2014
  - Leanne Phelps, “EMV, Tokenization and Apple Pay: The New Landscape,” Oct 2014.
  - Seth Harrington et al, “What’s NOT in your Wallet ?”, Ropes & Gray, #iLAW Summit, Mar 2015.
  - Levente Buttyán, “Electronic Payment Systems,” Lecture Notes on Information Security, 2005, http://www.hit.bme.hu/~buttyan/courses/Revkomarom/e-payments.pdf
  - Richard Martin, “Secure Mobile Payments: getting the balance right, “ Sept 2013.
  - Guido Mangiagalli, “Wave and Pay – Visa Contactless,” Visa Europe, 2005.

Modern E-Payment Systems to be covered in the rest of this course

- Credit Card based Payment system
  - Traditional Credit Card Systems
  - Support of MOTO by Credit Cards
    - The SSL (TLS)-based solution
    - The (failed) SET protocol
    - 3D Secure
- Smartcards
  - Smart-card technologies: Smartcard, NFC, RFIDs
  - EMV (Euro-MasterCard-Visa) initiatives:
    - Chip-and-PIN technology
    - PayWave
  - Other Smartcard-based Stored-Value Facilities (SVFs), e.g. Octopus vs. the (failed) Mondex card
- P2P payment systems, e.g. Paypal

Modern E-Payment Systems to be covered (cont'd)

- Digital Wallets and Mobile Payment Systems
  - Apple Pay, Samsung Pay, Google Pay (Wallet) and Union Pay
  - AliPay and WeChat Pay
- (Failed) Micro-Payment Protocols
- (Failed) Electronic Cash Protocols
- Crypto-currencies and related Technologies
  - Bitcoin
    - Blockchains, Public Distributed Ledger technologies
  - Ethereum
    - Smart Contracts, ICOs, Town Crier
  - Central Bank Digital Currencies (CBDC)

Credit Cards

Credit Cards

- The most expensive ePayment mechanism
- Visa/ MasterCard:
  - online: about $0.30 + 3.5% of transaction value
- A $100 charge costs the merchant $3.80
- Currently, the most convenient method in Developed Countries (e.g. U.S., Europe and even HK), as well as for International (cross-border) payment transactions,
- Advantages:
  - Allow credit => People can buy more than they can afford
  - Well-established Brands and Infrastructure support for both Face-to-Face, and Online Payment transactions worldwide
- Disadvantages:
  - Doesn't work for small amounts (too expensive)
  - Doesn't work for large amounts (too expensive)
  - Considerable Security+Cost concerns due to Wide-spread Frauds (Stolen Credit card numbers, Skimmers, etc) !

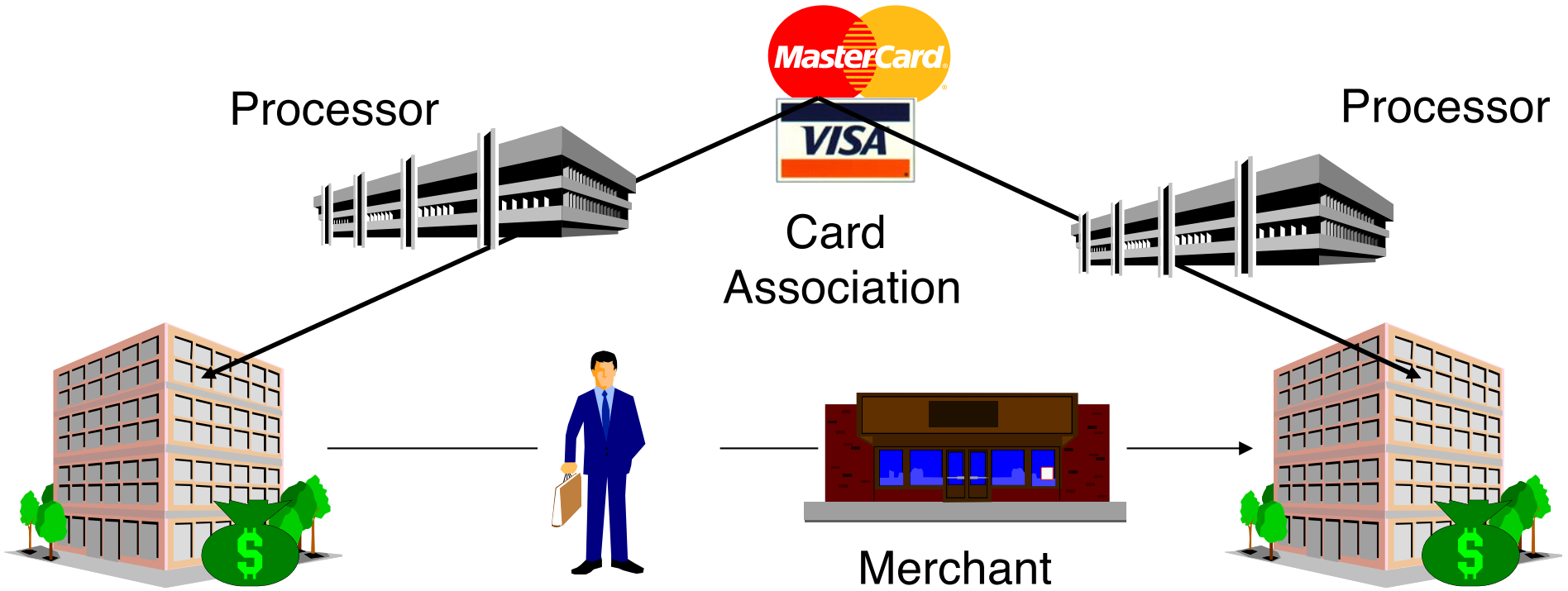
Different Payment Card Types

- Credit Card
  - The customer does not need to pay immediately, not even at the end of the monthly period
  - The bank does not count interest until the end of monthly period
- Debit Card
  - The customer must have a bank account associated with the card
  - Transaction is processed in real-time: the customer's account is debited and the merchant's account is credited immediately.
- Charge Card, e.g. American Express
  - The customer does NOT need to pay immediately but only at the end of the monthly period
  - Is he/she has a bank account, it is debited automatically
  - Otherwise, he/she needs to transfer money directly to the card association.

Brief History of Credit/Payment Cards

- 1950: First card was issued in the US ("Shopping Plate")
  - Initial, a card only work for a specific merchant, e.g. some specific department stores as Charged-card.
- 1950: Diners Club issued the 1st "general purpose" charge card for Travel and Entertainment.
- 1958: Bank of America in California issued the 1st general-purpose credit card that involved a "revolving credit" feature and licensed the card nationally in 1966.
- 1958: American Express Card issued a travel and payment entertainment card
- …: Many card companies have started up and failed
- 1969: Magnet strip standard for Cards adopted and made global via IBM
- 1976: Bank of America spun off BankAmericard and joined with other banks to form (and owned) Visa International.
- 1979: Mastercard came to existence, formerly the InterBank Card Association and Master Charge
- 2006-08: Mastercard and Visa International became publicly traded companies.
- 2015: The EMV (Euro Master Visa) chips become standard to enhance protection against Credit Card Frauds
- Today: 2 major credit card companies: Visa International (60% share of credit and debit purchases) and Mastercard (27%) dominate the world
  - Plus Eurocard in Europe and UnionPay within China

Participants



- Issuing Bank
- Issues card
- Extends credit
- Assumes risk of card
- Cardholder reporting

- Merchant Bank (Acquirer)
- Sets up merchant
- Extends credit
- Assumes risk of merchant
- Funds merchant

PNC

PNC

3 . Acquiring Bank's Processor
- direct connections to MC /VI
- obtains authorization from Issuer
- returns response to merchant
- five digit number that must be stored

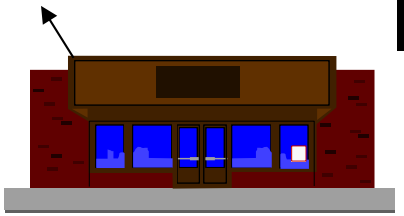
4 . Issuing Bank / Processor
- receives auth request
- verifies available funds
- places hold on funds

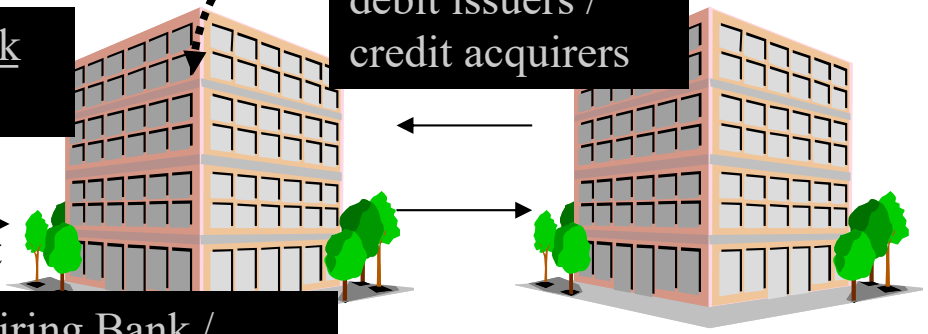
2.Card Authorization
via dial, lease line, satellite

8. MC / VI
debit issuers / credit acquirers

9. Acquiring Bank
funds merchant

Authorizations
Batch Settlement





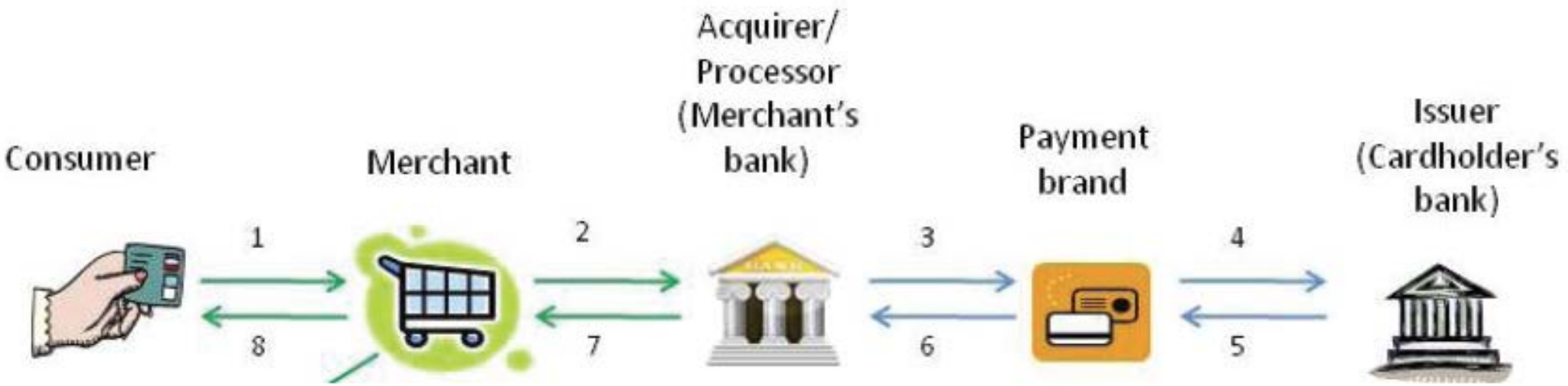
1. Customer
- pays with card
- card swiped
- mag data read
- (get signature)

5. Merchant
- stores authorizations and sales conducted
- captures sales (at end of day)
- submits batch for funding

6. Acquiring Bank / Processor
- scans settlement file
- verifies authorizations match captured data
- prepares file for MC/VI
- prepares funding file
- records txs for reporting

7. Issuing Bank / Processor
- receives settlement file from MC / VI
- funds MC / VI
- matches txs to auths
- post txs to cardholder
- records transactions for reporting

Simplified Transaction Flow for Credit & Signature Debit



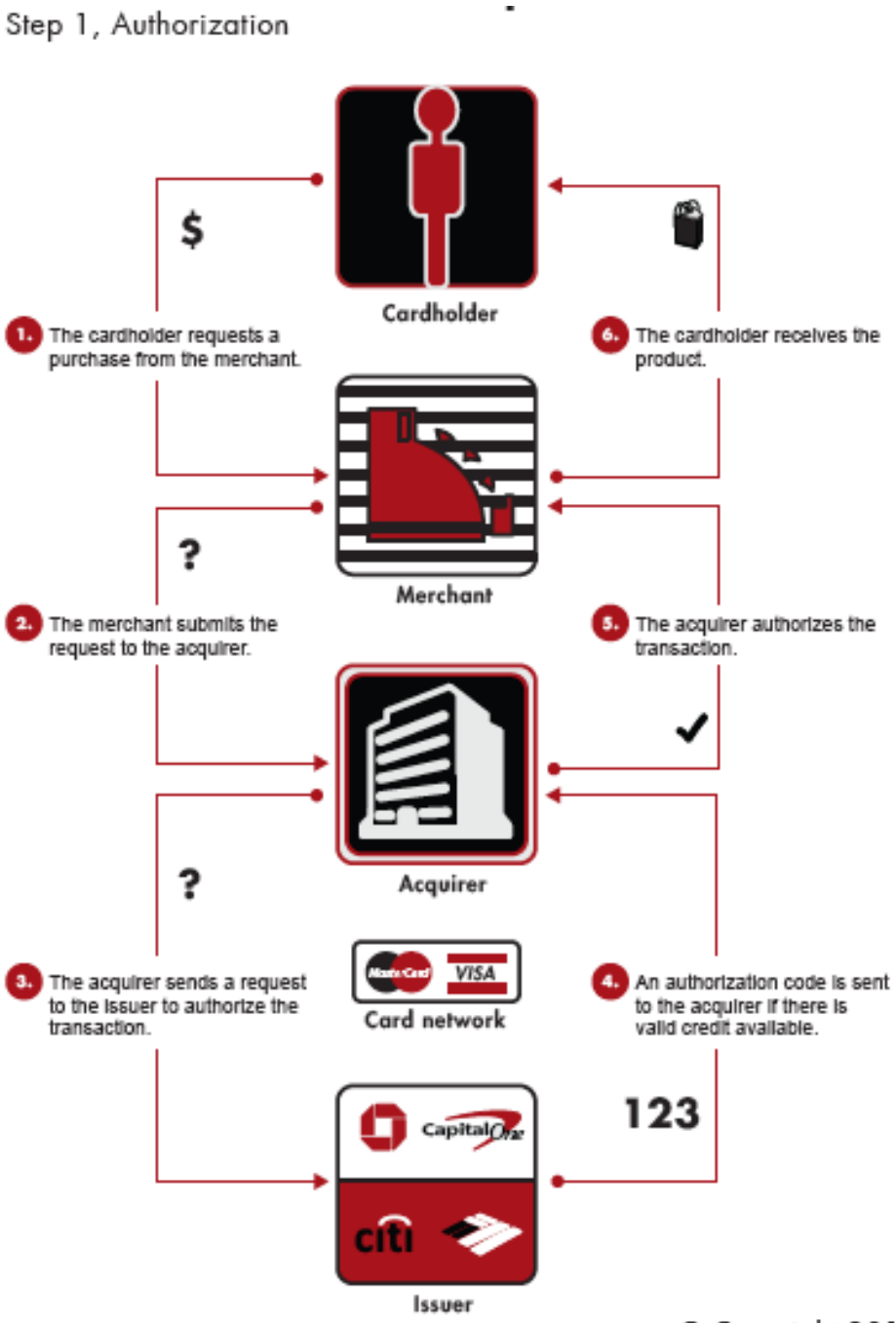
1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

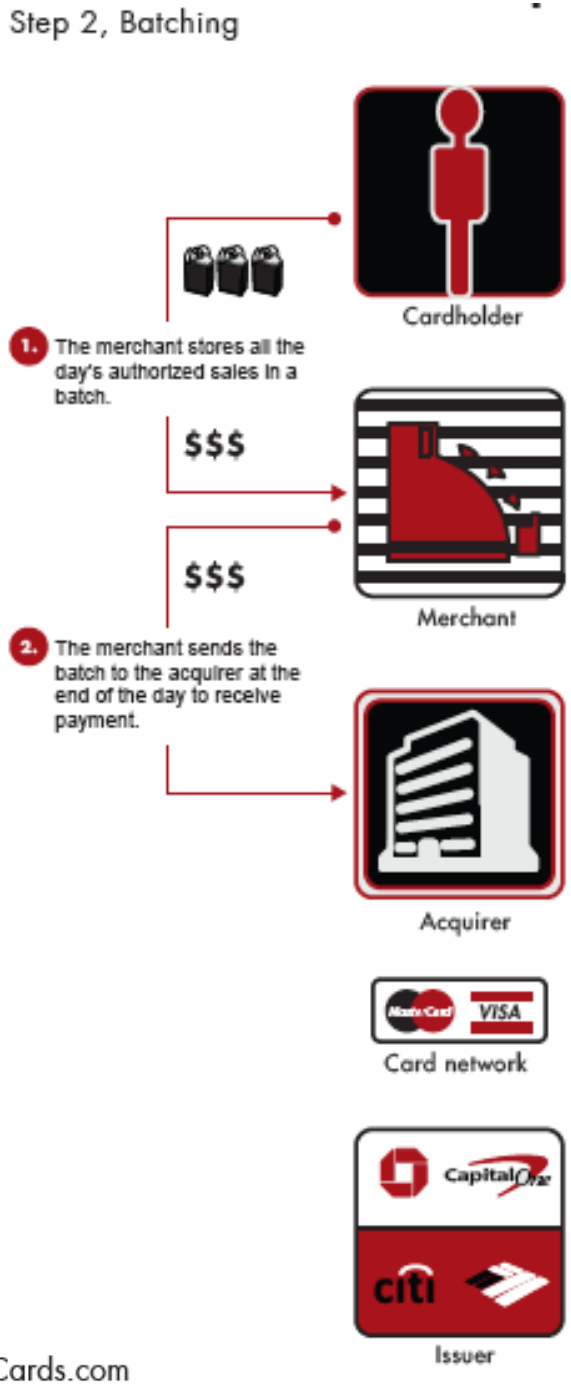
MasterCard Banknet Performance (circa 2017)

- Closed TCP/IP network
- Payment authorization/response time 140msec on avg.
- System Capacity Limit: 3.4 billion transactions per day, 38K+ transactions per second (Vs. Visa's 24K TPS)
- > 210 countries (more than SWIFT!)
- > 25,000 issuing banks
- > 650 service delivery points
  - At least 13 global hubs
  - At least 32 country hubs

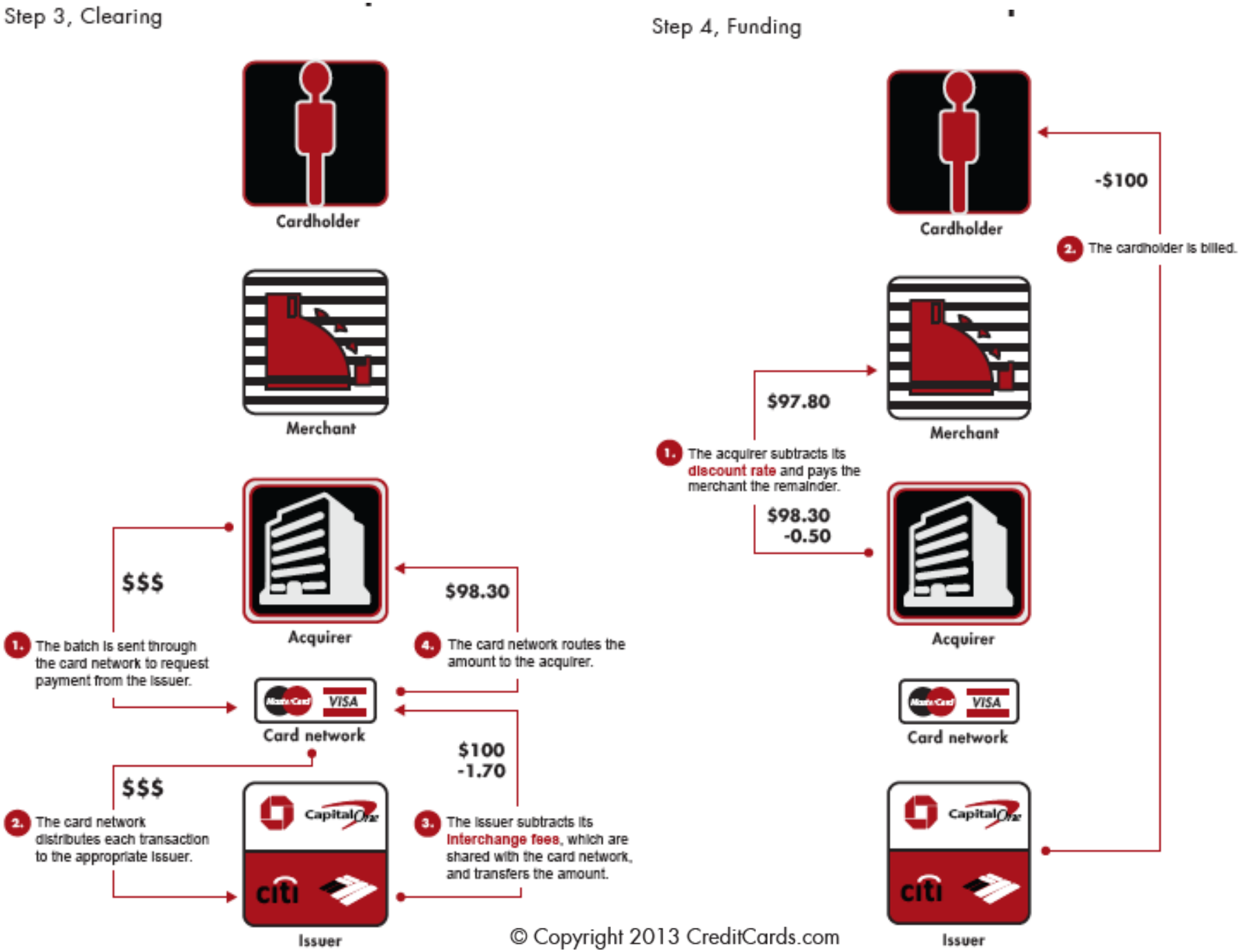
SOURCE: https://www.quora.com/How-many-transactions-do-typical-banks-process-everyday

How a Credit Card transaction is Processed ?





How a Credit Card transaction is Processed ?



Glossary of Credit Card Processing

- **Acquirer**: A bank that processes and settles a merchant's credit card transactions with the help of a card issuer.

- **Authorization**: The first step in processing a credit card. After a merchant swipes the card, the data is submitted to merchant's bank, called an acquirer, to request authorization for the sale. The acquirer then routes the request to the card-issuing bank, where it is authorized or denied, and the merchant is allowed to process the sale.

- **Batching**: The second step in processing a credit card. At the end of a day, the merchant reviews all the day's sales to ensure they were authorized and signed by the cardholder. It then transmits all the sales at once, called a batch, to the acquirer to receive payment.

- **Cardholder**: The owner of a card that is used to make credit card purchases.

- **Card network**: Visa, MasterCard or other networks that act as an intermediary between an acquirer and an issuer to authorize credit card transactions.

- **Discount fee**: A processing fee paid by merchants to acquirers to cover the cost of processing credit cards.

- **Funding**: The fourth and final step in processing a credit card. After receiving payment from the issuer, minus interchange fees, the acquirer subtracts its discount fee and sends the remainder to the merchant. The merchant is now paid for the transaction, and the cardholder is billed.

- **Interchange fee**: A charge paid by merchants to a credit card issuer and a card network as a fee for accepting credit cards. They generally range from 1 to 3 percent.

- **Issuer**: An financial institution, bank, credit union or company that issues or helps issue cards to cardholders.

- **Clearing**: The third step in processing a credit card. After the acquirer receives the batch, it sends it through the card network, where each sale is routed to the appropriate issuing bank. The issuing bank then subtracts its interchange fees, which are shared with the card network, and transfers the remaining amount through the network back to the acquirer.

Key Credit and Debit Concepts

- Discount fee: charged to Merchants by Acquiring banks
- Interchange is a fee
  - Largest component of Discount fee
  - Charged to Acquiring banks
  - Set by the payment brands (Visa, Mastercard, etc)
  - Paid to the Issuing banks
  - Depend on:
    - Payment network used
    - Card-type (Credit vs. Debit, Rewards vs. Standard) ; Signature-based vs. PIN-based less expensive fees than Signature-based Debit Cards
    - How payment was made, e.g., in-person (aka card-presented) vs. over the Internet vs. via phone, etc
    - Industry and size of merchant
    - Region/Country where purchase took place

Key Credit and Debit Concepts (cont'd)

- Chargebacks: When an Issuer charges back the purchase amount to the merchant, generally the result of a customer complaint to the issuer
  - A form of consumer protection, e.g. Against fraudulent transactions, customer dispute, technical payment error (double-charge etc)
  - Merchants, following card payment brand rules can also dispute the charge back via the acquiring bank or processor.
- Compliance
  - Payment Cardholder Industry Data Security Standard (PCI DSS) to protect cardholder information to reduce data theft
  - Security Requirements for Merchants, Acquirers, Processors, Issuers (and their systems/ devices) in order to be eligible to handle card payment transactions
    - e.g. May not store some elements of magnetic-stripe data after an authorization
    - Account (Credit card) numbers must be encrypted anywhere when they are stored etc.
  - Business cost to get certified as PCI DSS compliant

PCI DSS

- Responsibility for privacy and data security of transaction information are typically set by contract.

Payment Card Industry Data Standard ("PCI DSS")

PCI Security Standards Council

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

Legal Landscape

- But increasingly by statute as well.
  - MN, NV, WA statutes incorporate all or part of PCI DSS
    - In 2007, Minnesota enacted a law prohibiting the retention of payment card data.
      - *"**No person or entity conducting business in Minnesota that accepts an access device** in connection with a transaction **shall retain the card security code data**, the PIN verification code number, or the full contents of any track of magnetic stripe data, **subsequent to the authorization of the transaction** or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction."*

      Minn. Stat. § 325E.64 (2014).

Legal Landscape

- In 2009, Nevada required merchants doing business in the state to comply with PCI DSS
  - *If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services,* ***the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard****, as adopted by the PCI Security Standards Council ....*

  Nev. Rev. Stat. § 603A.215 (2014).
- In 2010, Washington enacted a similar statutory provision
  - ***Processors, businesses, and vendors are not liable under this section if*** *(a) the account information was encrypted at the time of the breach, or (b)* ***the processor, business, or vendor was certified compliant with the payment card industry data security standards*** *adopted by the payment card industry security standards council, and in force at the time of the breach. A processor, business, or vendor will be considered compliant, if its payment card industry data security compliance was validated by an annual security assessment, and if this assessment took place no more than one year prior to the time of the breach.*

  Wash. Rev. Code § 19.255.20 (2014).

Legal Landscape

Other laws governing privacy and data security of transactions:

- State data security laws
- State consumer protection statutes
- FTC Act
- Gramm Leach Bliley Act (financial institutions only)

PCI DSS 3.0

PCI 2.0 v. 3.0 Key Themes

- **Education and awareness of security standards** – 3.0 adds clarifications to help organizations better understand the intent of the requirements and proactively implement and maintain controls.
  - Ex. Clarification that sensitive authentication data must not be stored after authorization even if card number is not present.

- **Increased flexibility to address common risks** of weak passwords, authentication methods, malware, and poor self-detection.
  - Ex. flexibility for customized approach to mitigate common risks
  - Ex. rigorous testing procedures such as penetration tests and audit logging requirements

- **Shared responsibility for security** – defined PCI DSS responsibilities when working with different business partners.
  - Ex. Maintain information about which PCI DSS requirements are managed by service providers and which are managed by the entity

MOTO – Mail Order/ Telephone Order

(Non-Internet based scheme of using Credit Cards Remotely

- Credit Card number is sent via phone call or post and then processed in the traditional way (using existing infrastructure)
- No Cardholder Signature !
  - User can deny/ not agree to the purchase later on (limited liability)
  - Merchant (instead of the banks) must handle disputes
  - Some special rules and precautions are applied:
    - Additional information is requested from user (e.g. name, address)
    - Goods are delivered to the address associated with the card
- Fraud is still possible (but hopefully the benefits outweigh the disadvantages
- Still very popular (in the US and Western Europe)

High Risk Merchants

Product	Services	Method of Sale
Illegal goods	Investment opportunities	Outbound telemarketing
Book and record club	Travel agency	Inbound teleservices
Pawn shop	Dating/escort service	Door to door sales
Vitamins	Limousine/taxi service	Future services
Computer software	Bail/bond payments	Out of home sales
Stamp/coin stores	Massage parlors	Nonpermanent locations
Auto rental/leasing services	Employment agencies/collection services	Flea markets/no store front
Water purification	Timeshare/audio text pay per call	Use of third party for product, sales, or delivery

Protocols to Support Credit Card Purchases over the Internet

Credit Cards on the Internet

- Problem: communicate credit card and purchasing data securely to gain consumer trust
  - Authentication of buyer and merchant
  - Confidential transmissions
- Systems vary by
  - type of public-key encryption
  - type of symmetric encryption
  - message digest algorithm
  - number of parties having private keys
  - number of parties having certificates

Credit Card Protocols

- SSL 1 or 2 parties have private keys
- TLS (Transport Layer Security)
  - IETF version of SSL

VERY IMPORTANT. Dominated way to use Credit Cards over Internet to-date

- *i*KP (IBM) i parties have private keys
- SEPP (Secure Encryption Payment Protocol)
  MasterCard, IBM, Netscape based on 3KP
- STT (Secure Transaction Technology)
  VISA, Microsoft

OBSOLETE

- SET (Secure Electronic Transactions)
  - MasterCard, VISA all parties have certificates

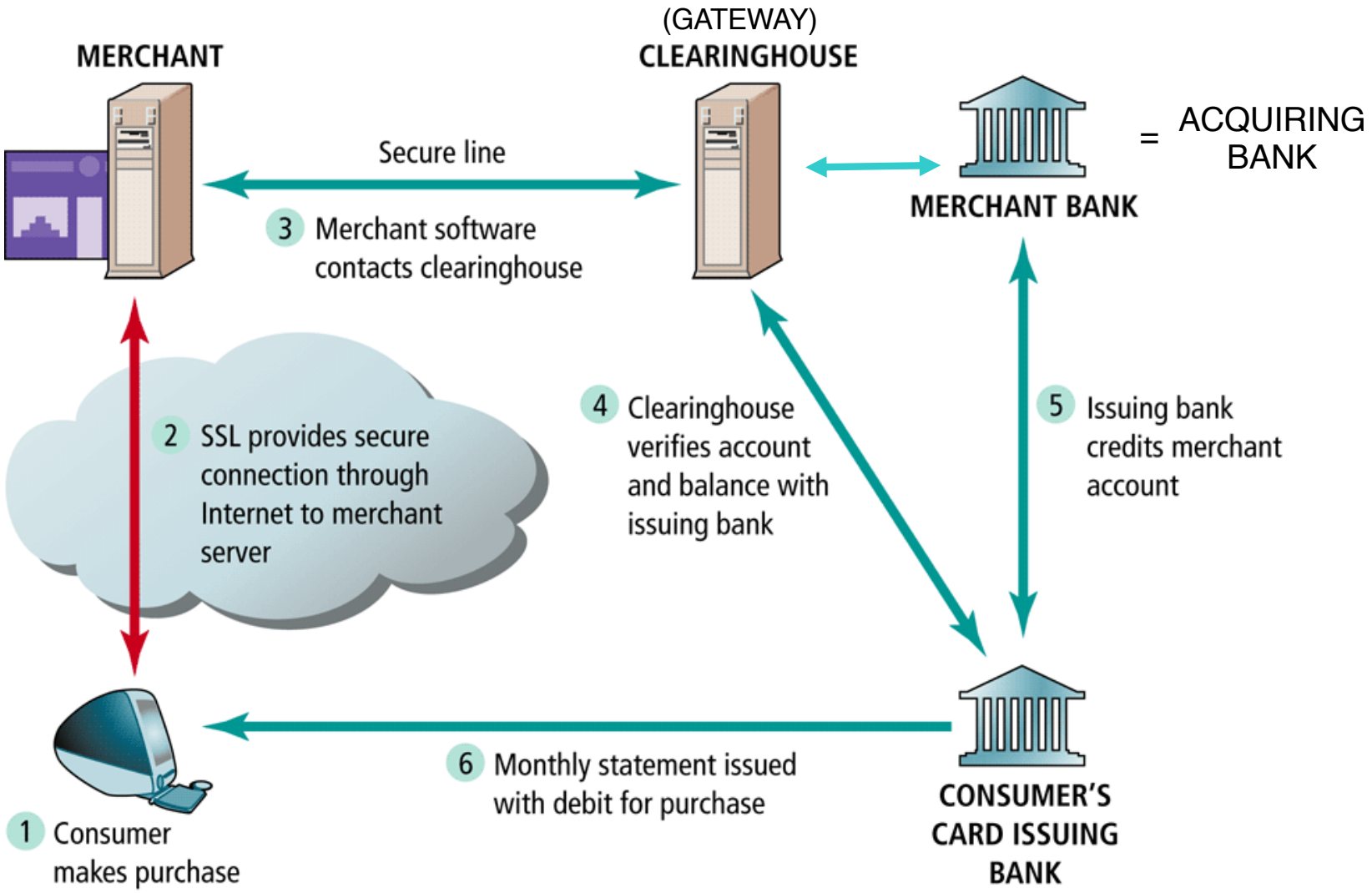
DEAD due to poor acceptance

- 3-D Secure real-time authentication
  - The technology behind "Verified by Visa", and MasterCard SecureCode etc.

RAPID EXPANSION in SOME Countries BUT Not popular in US

- And more in the later part of this course …, CHIP-and-PIN, PayWave, Apple Pay, Google Pay, etc

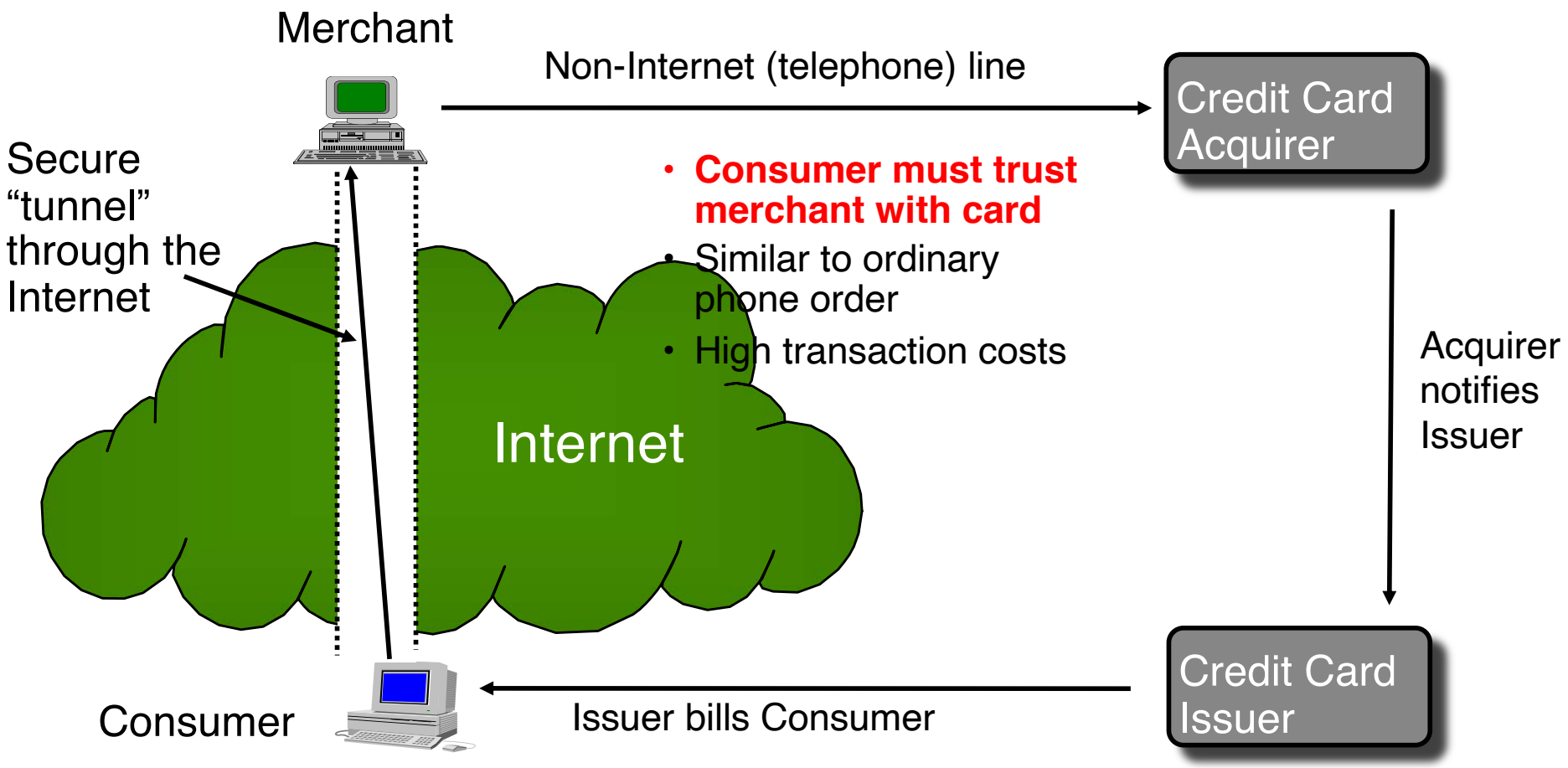
Workflow for Online Credit Card Transaction using SSL/TLS



SOURCE: LAUDON & TRAVER

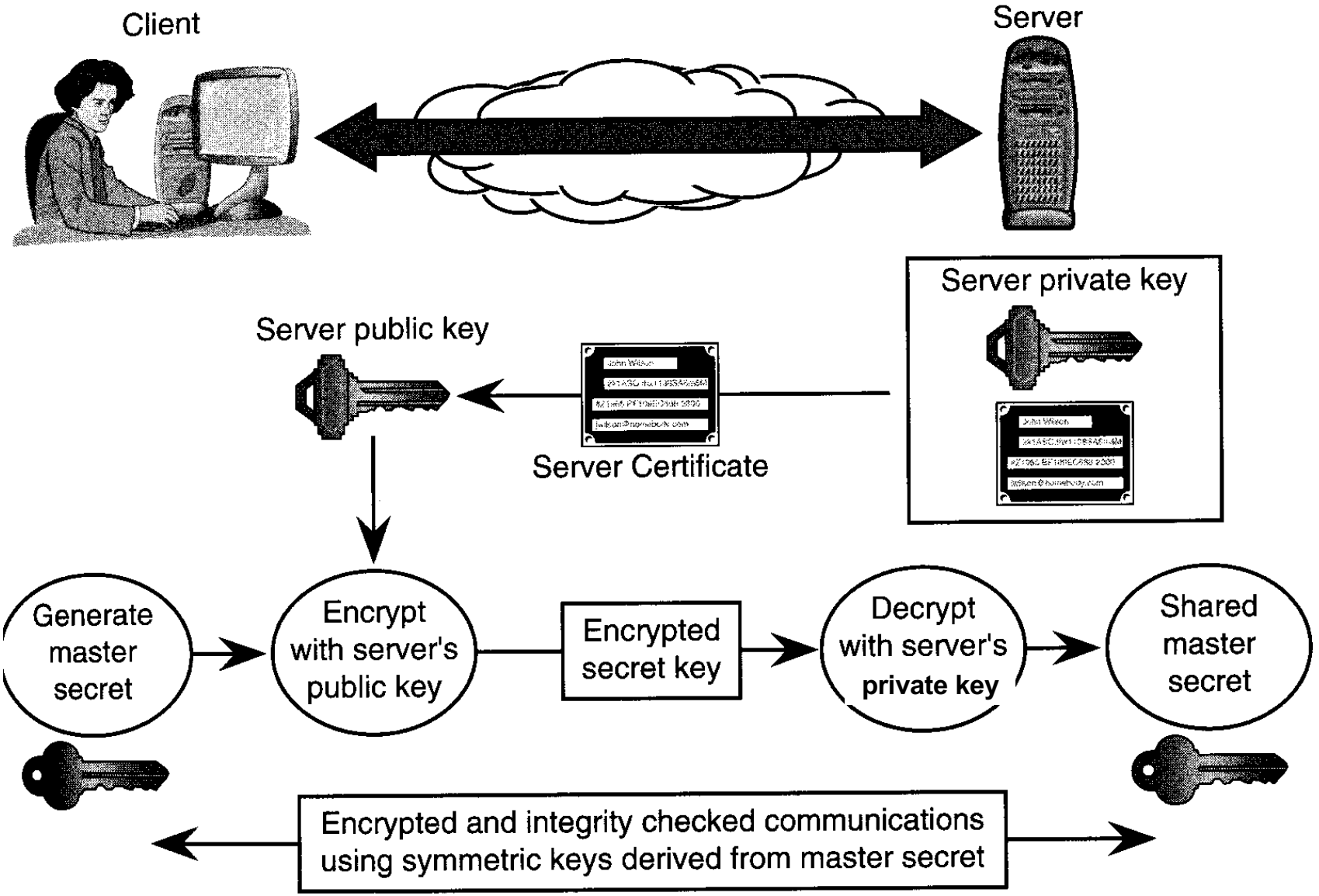
PURPOSE of using SSL/TLS: ALLOW A USER WITHOUT A CERTIFICATE TO SEND SECRET INFORMATION (A CREDIT CARD NUMBER) SECURELY and EFFICIENTLY

SSL (Secure Sockets Layer) Concept

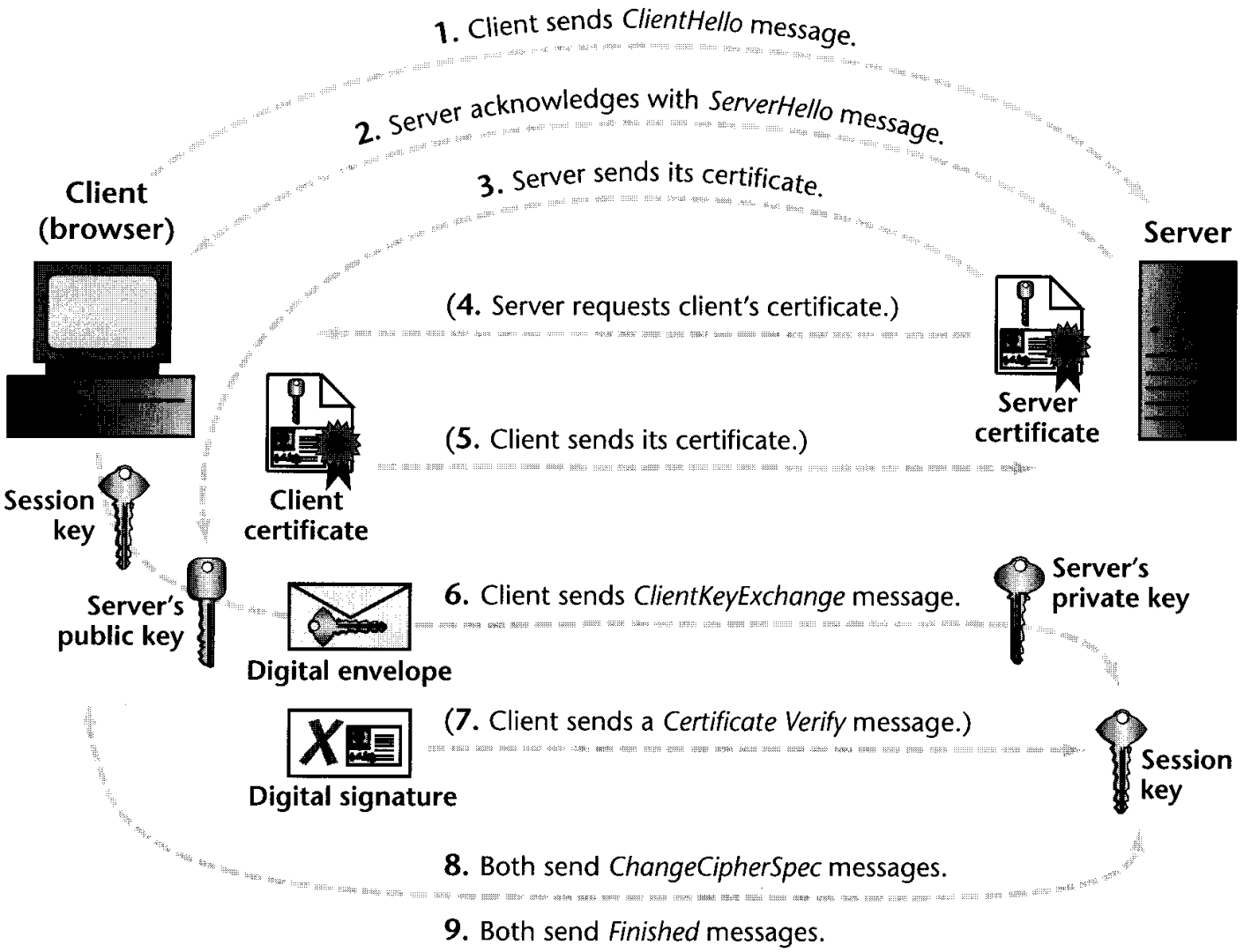


SOURCE: MARVIN SIRBU

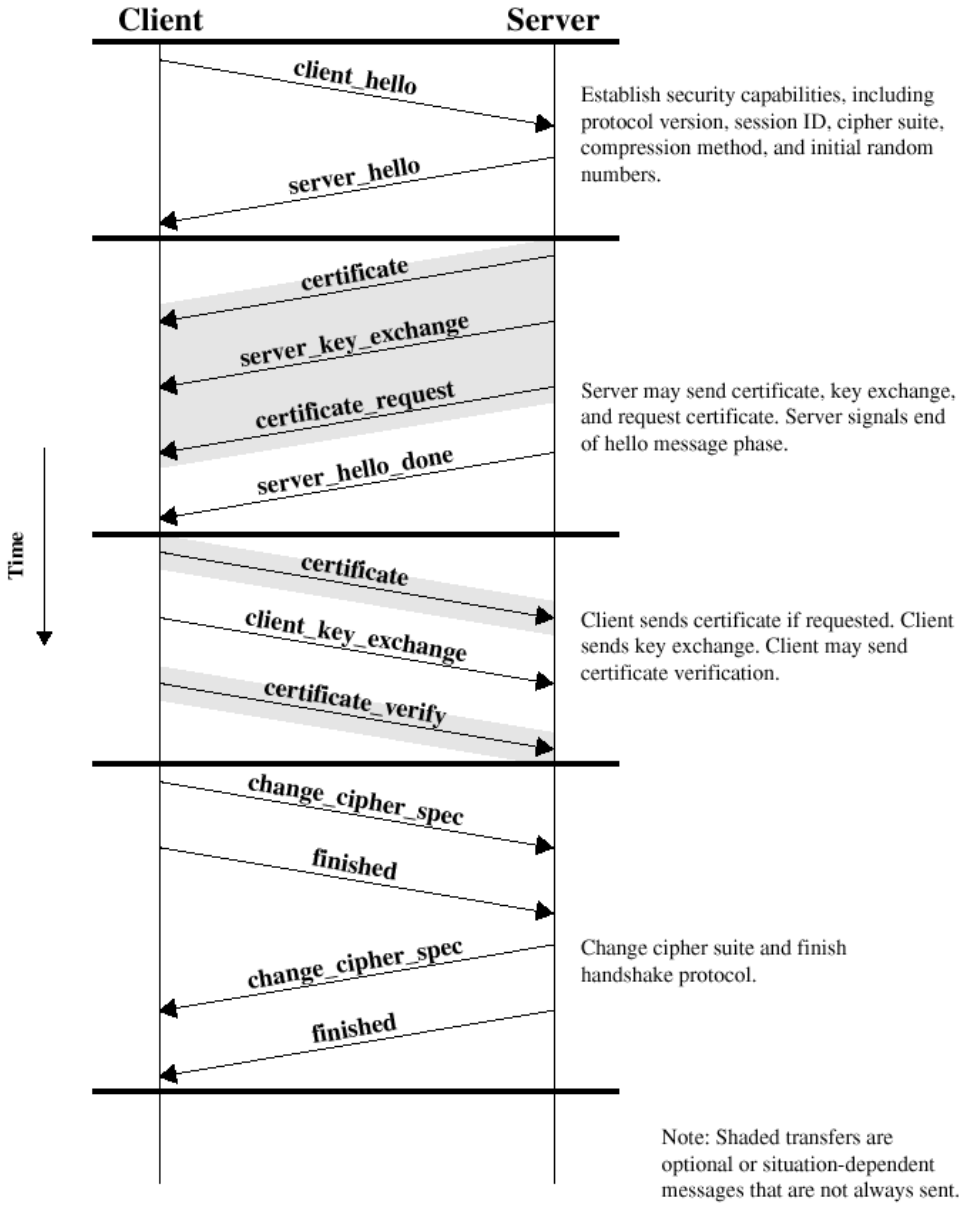
SSL Server Authentication, Encryption and Integrity Checking



A simplified SSL Handshake



Handshake Protocol Action



Transport Layer Security (TLS)

- The same record format as the SSL record format.
- Defined in RFC 2246, 4346, 5246.
- Similar to SSLv3.
- Differences in the:
  - version number
  - message authentication code
  - pseudorandom function
  - alert codes
  - cipher suites
  - client certificate types
  - certificate_verify and finished message
  - cryptographic computations
  - Padding
- RFC 4347,5238, Datagram TLS (DTLS), ``SSL running on unreliable Transport Protocols", e.g. UDP or DCCP"
- TLS v1.3, a new standardized version since v1.2 (released about a decade ago) has been finalized as of March 21, 2018 !!

Major Changes in TLS v1.3

- Support 1-RTT Handshakes
- Also support 0-RTT handshake for previously visited server
  - BUT without replay protection nor Perfect Forward Secrecy (PFS)
- Remove support for weak and lesser-used named Elliptic curves in ECC.
- Remove support for MD5 and SHA1
- Require Digital Signatures even when a previous configuration is used
- Dropping support for many insecure or obsolete features including compression, renegotiation, AES-CBC mode etc
- Prohibit SSL or RC4 negnotiation for backwards compatibility

See Eric Rescoria's talk on TLS1.3 for details:

http://web.stanford.edu/class/ee380/Abstracts/151118.html

The crypto-library developed by Mozilla and used by its Firefox browser enabled TLS 1.3 by default in Feb 2017

SET – Secure Electronic Transactions

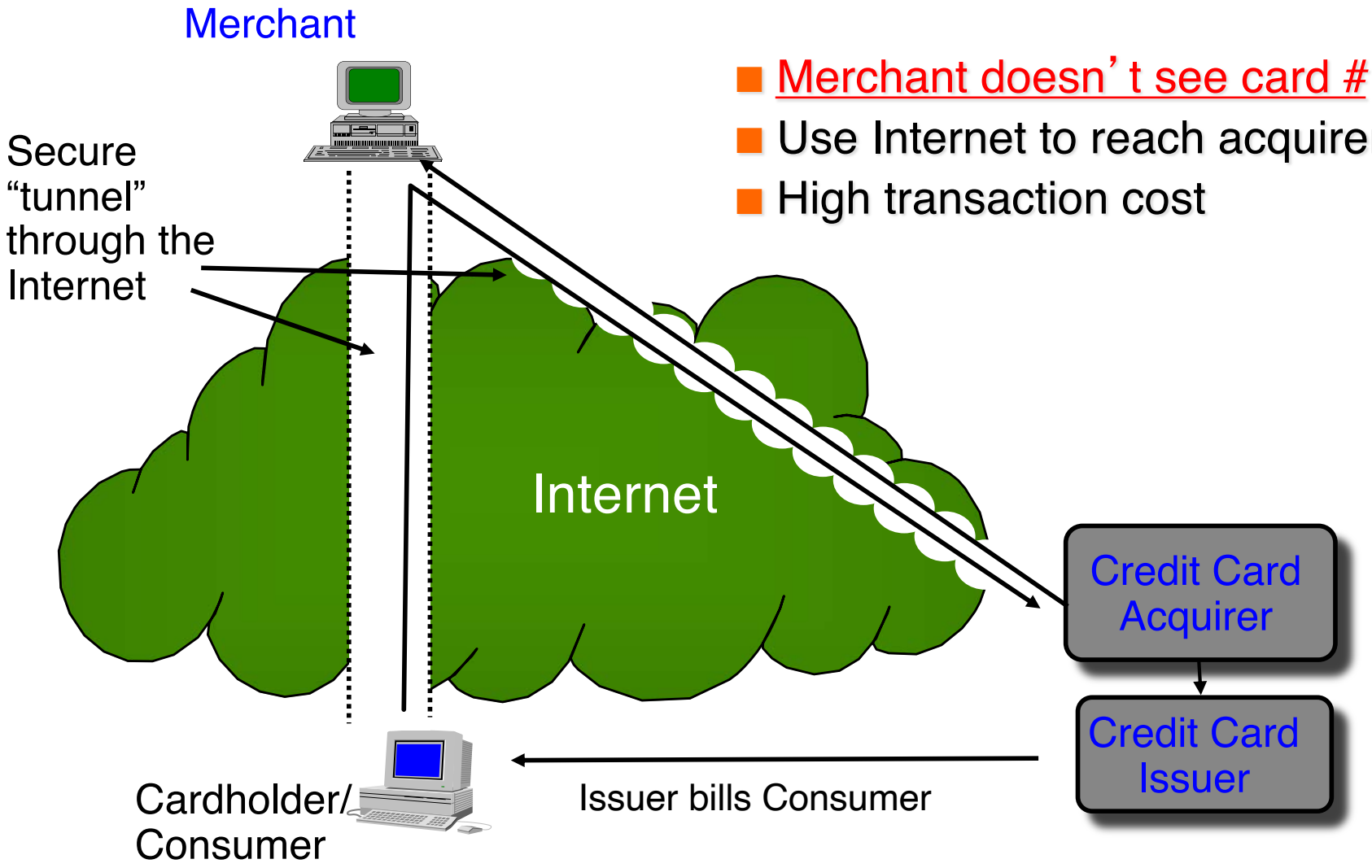
- A protocol specifically designed to protect credit card transactions on the Internet (vs. SSL/TLS is for general Internet communications)
- Initiated and promoted by MasterCard and Visa
  - MasterCard (with IBM) had SEPP (Secure E-Payment Protocol)
  - Visa (with Microsoft) had STT (Secure Transaction Technology)
  - The two proposals converged/ merged into SET
- Many companies were involved in the development of the specifications (IBM, Microsoft, Netscape, RSA, VeriSign, …)

=> It resulted a 1000-page specifications consisted of 3 books:

1. Business Description
2. Programmer's Guide
3. Formal Protocol Definition

- Way Too Complex to be understood and implemented by Laymen !

Secure Electronic Transactions (SET)



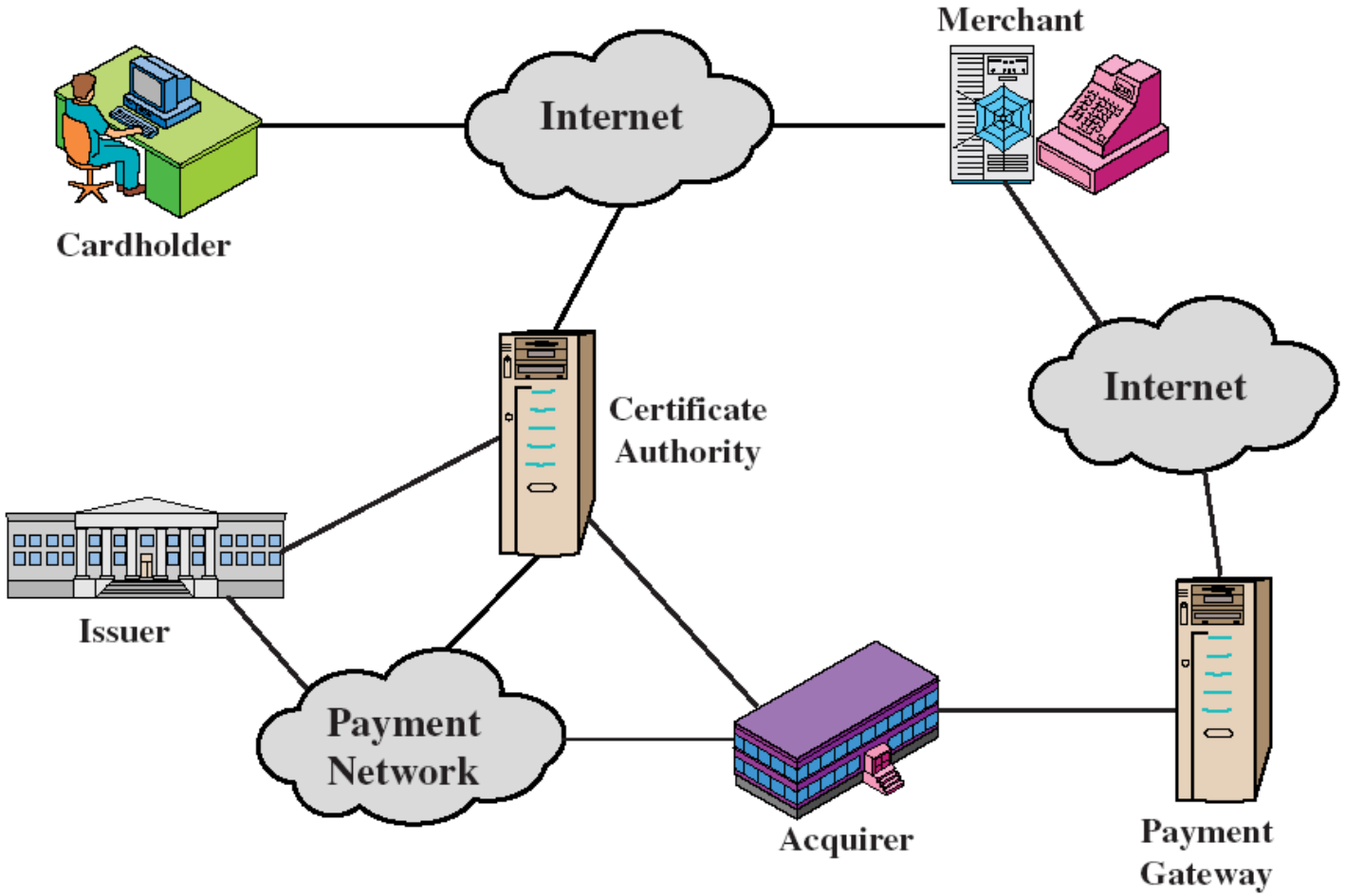
- Merchant doesn't see card #
- Use Internet to reach acquirer
- High transaction cost

SOURCE: MARVIN SIRBU, CMU

Additional Participants:

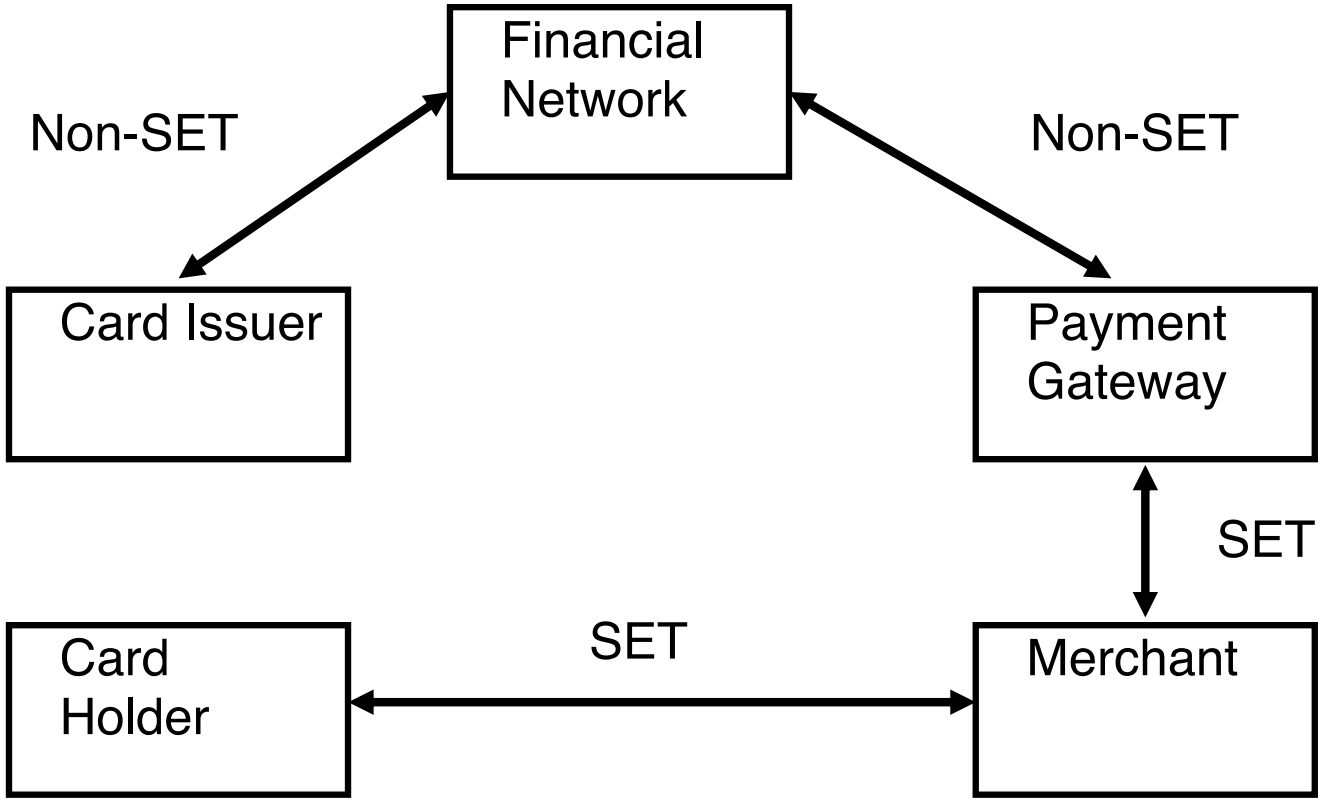
- Payment Gateway – Interface between the Internet and existing Credit-card payment network
- Certificate Authorities (CAs)

Participants in SET



SOURCE: WILLIAM STALLINGS

Framework of SET



SET Objectives

- Confidentiality of payment and order information
  - Encryption
- Integrity of all data (digital signatures)
- Authentication of cardholder & account (certificates)
- Authentication of merchant (certificates)
- No reliance on secure transport protocols (TCP/IP or SSL)
- Interoperability between SET software and network
  - Standardized message formats
- SET is a payment protocol
  - Messages relate to various steps in a credit card transaction

SET Services

- Cardholder Account Authentication
  - Merchant can verify that the client is a legitimate user of the card – based on X.509 certificates
- Merchant Authentication
  - Client can authenticate the merchant and check if it is authorized to accept payment cards – based on X.509 certificates
- Confidentiality
  - Cardholder account and payment information (i.e. her credit card no.) is protected while it travels across the network
  - Credit card no. is hidden from the merchant as well !
- Integrity
  - Messages cannot be altered in transit without being detected – based on digital signatures
- Non-repudiation
  - Client authorizes the transaction using his/her digital signature

  => He/ she cannot this is his/her act

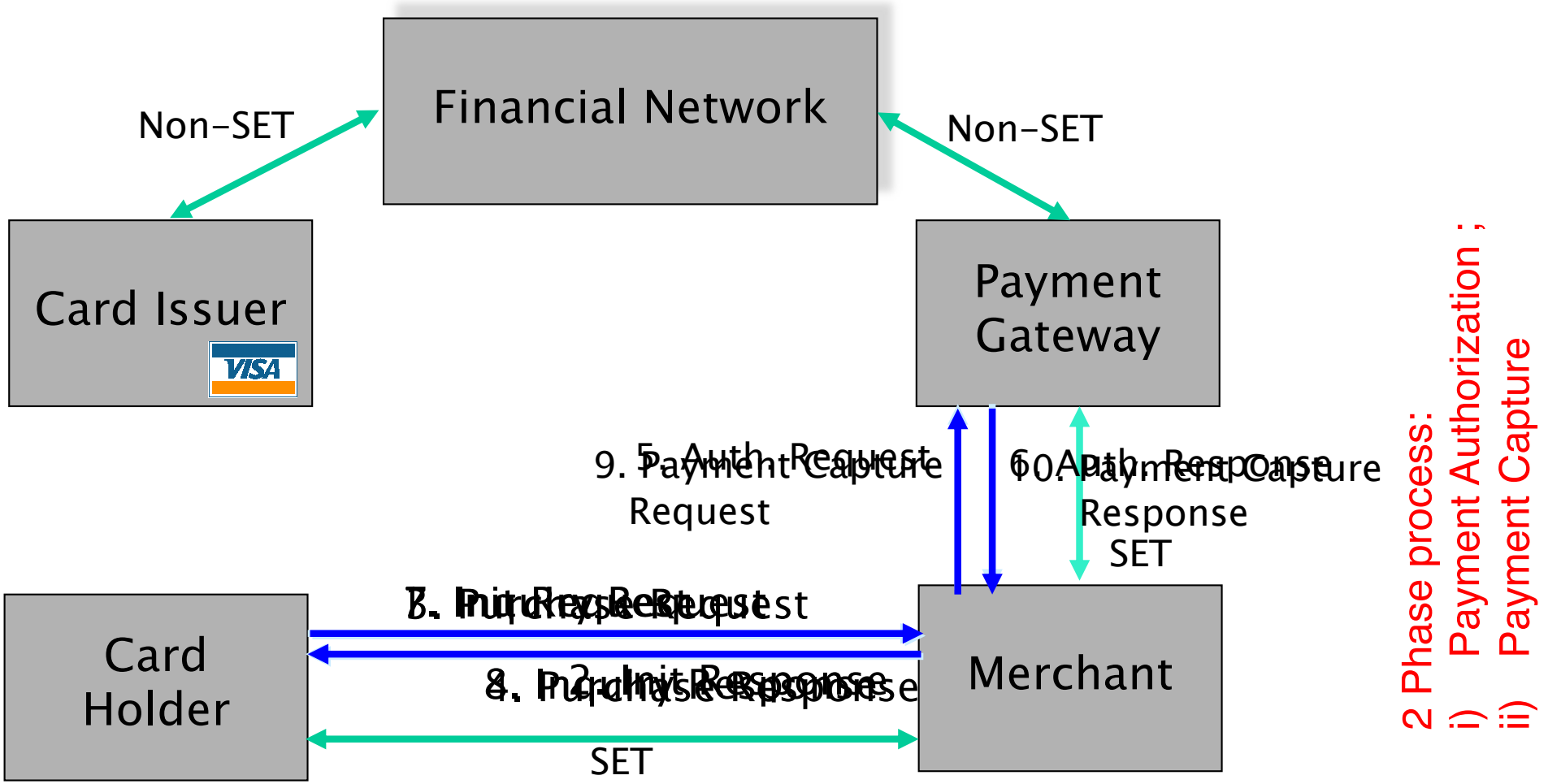
  => the transaction is treated as a Card-Present one

SET in the Transaction Process

1. Browsing
2. Product selection
3. Customer order entry
4. Selection of payment mechanism
5. **Customer sends order and payment instructions**
6. **Merchant requests payment authorization**
7. **Merchant sends order confirmation**
8. Merchant ships goods
9. **Merchant requests payment from bank**

SET PROTOCOL FUNCTIONS:

SET Message Flow



SET Message Flow

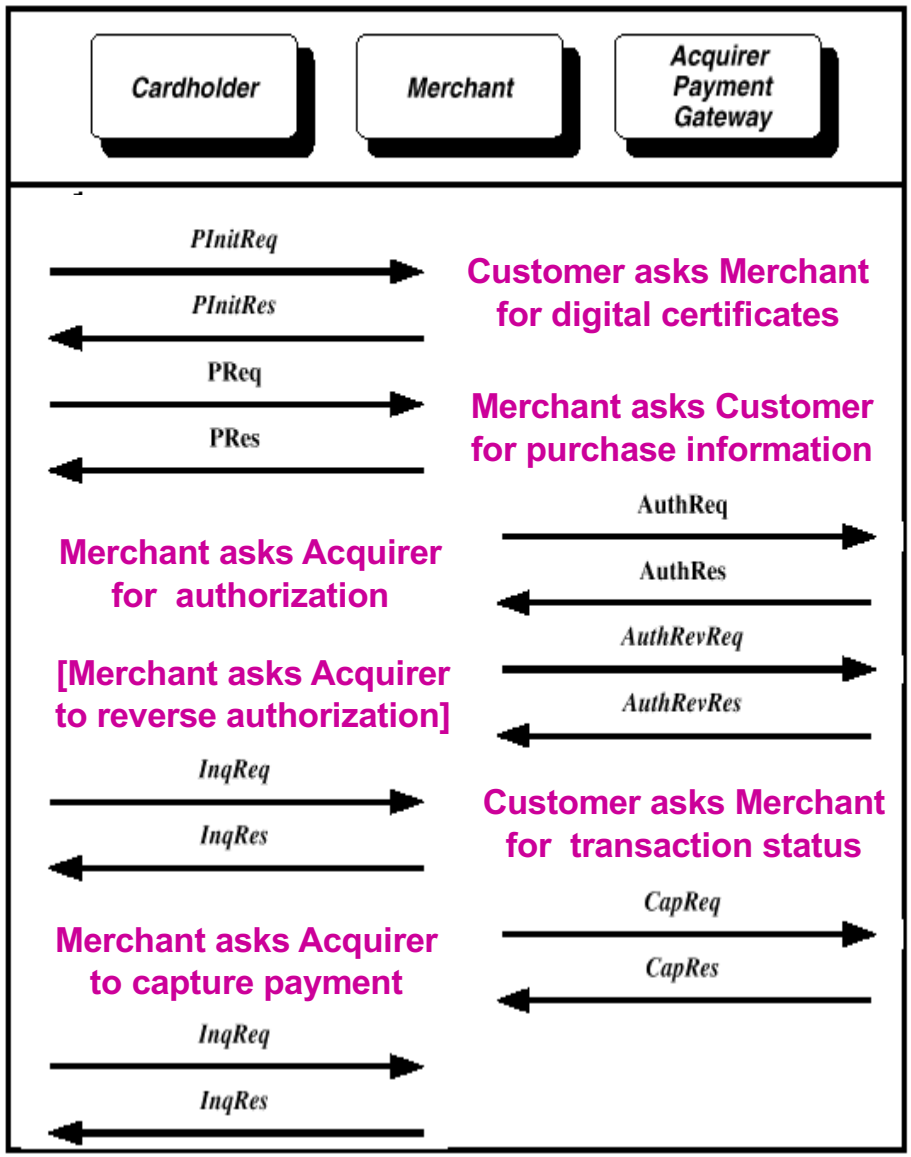
SET messages come in pairs:

Request

followed by

Response

Appropriate cryptography is applied to message wrappers



2 Phase process:

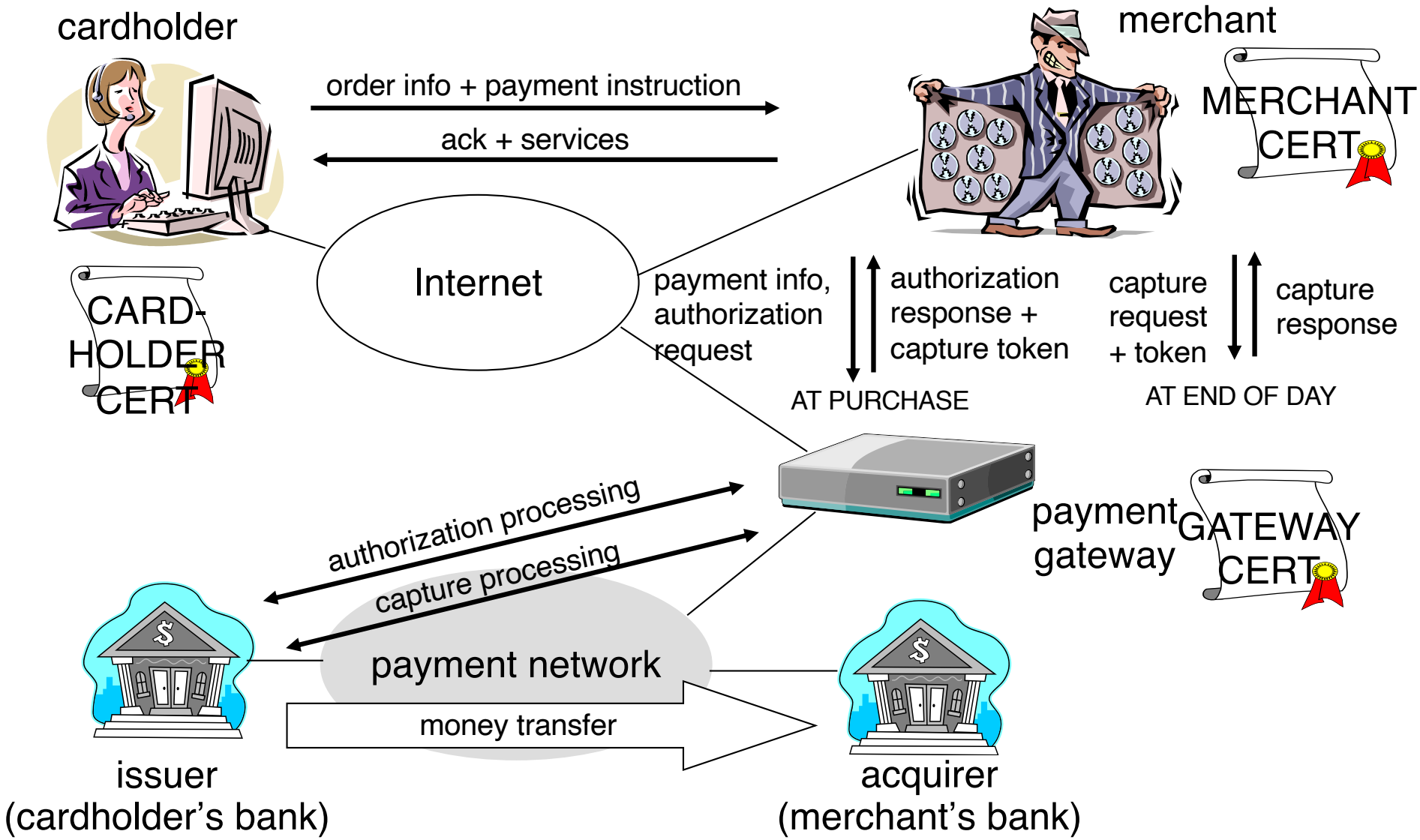
i) Payment Authorization ;

ii) Payment Capture

SET Supported Transactions

- card holder registration
- merchant registration
- purchase request
- payment authorization
- payment capture
- certificate query
- purchase inquiry
- purchase notification
- sale transaction
- authorization reversal
- capture reversal
- credit reversal

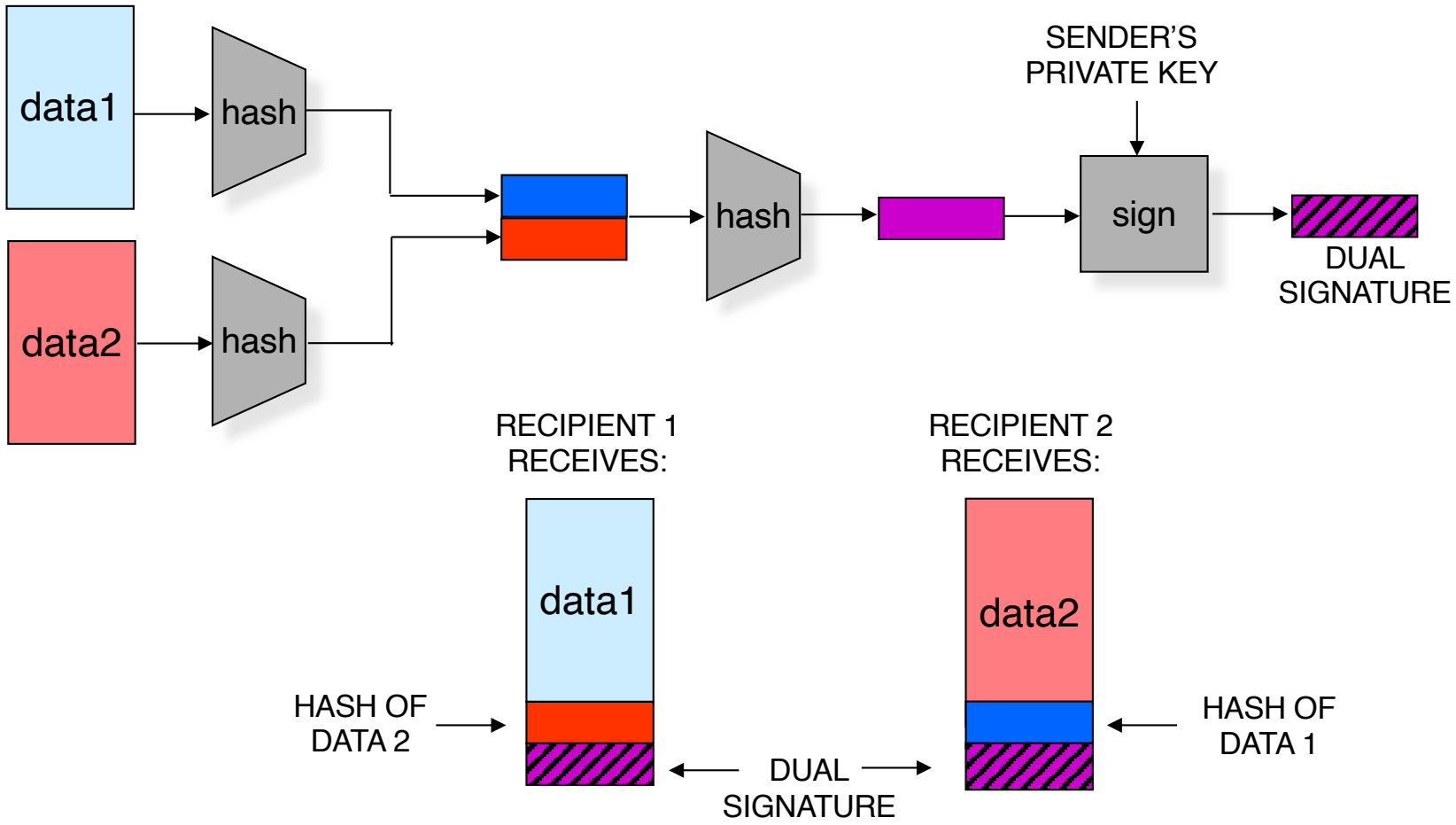
SET Operation Flow



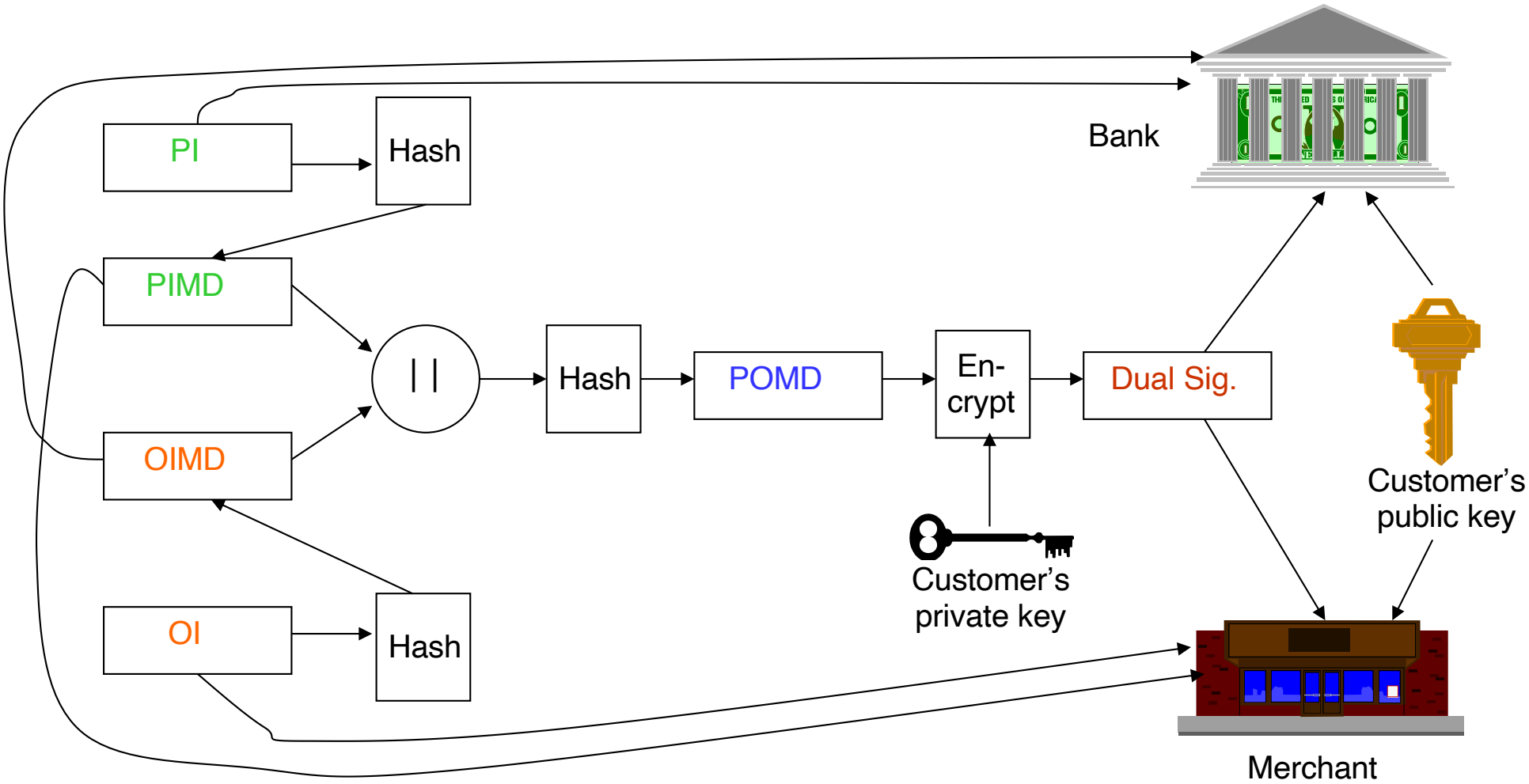
Dual Signature – Basic Concept

Goal

- Links two messages intended for different recipients in a secure manner (e.g. order info and payment instructions in SET) but only one party to read each.
  - Link may need to be proven in case of disputes



Conceptual Use of the Dual Signature



PI: Payment Information
OI: Order Information
MD: Message Digest
PO: Payment+Order

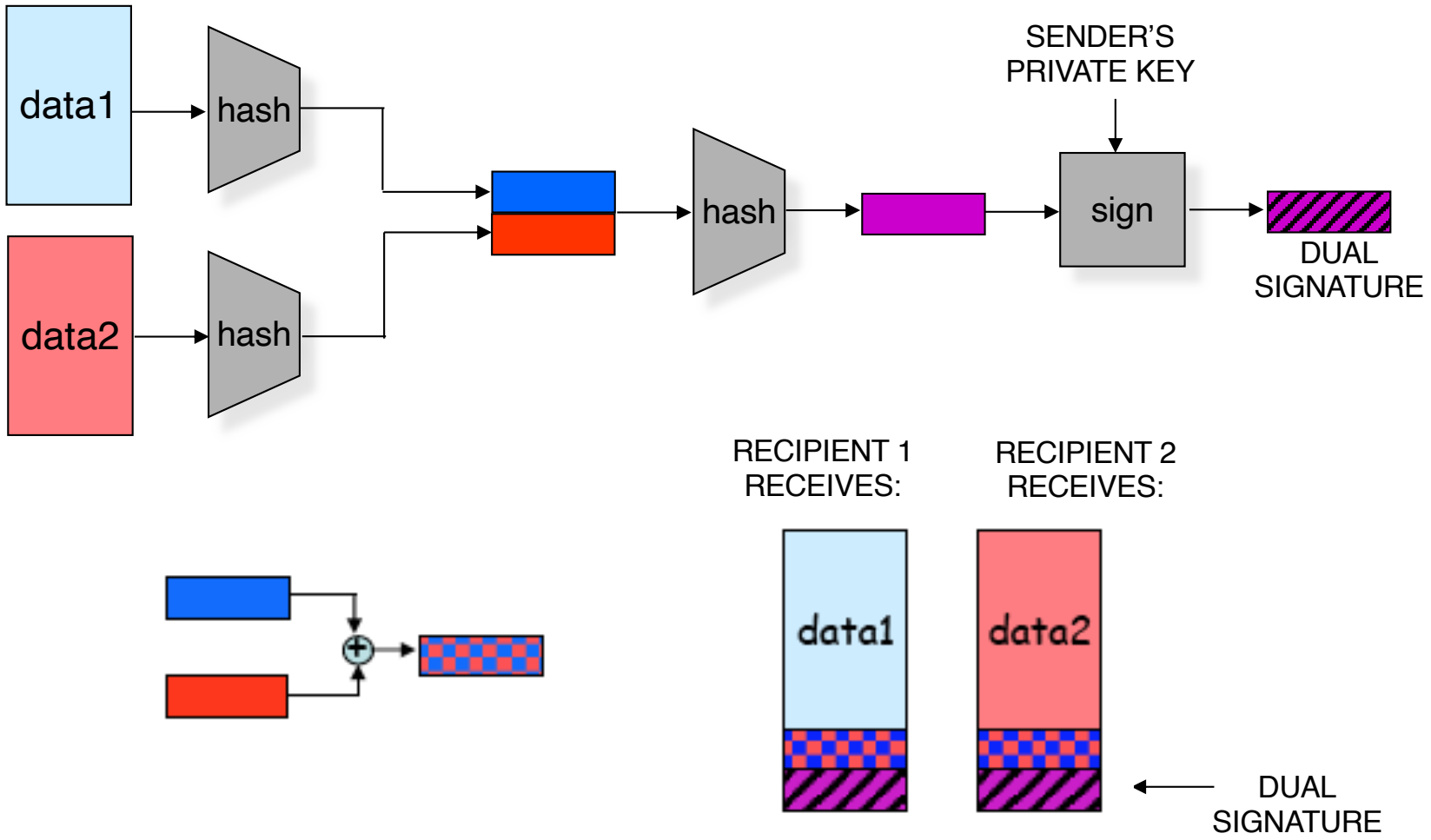
SOURCE: RICHARD STANLEY

Conceptual use of Dual Signatures on Plaintext

- Alice wants to send Message 1 (aka Order Info) to Bob and Message 2 (aka Payment Info) to Carol in plaintext
- Bob can't see Message 2; Carol can't see Message 1
- Both Bob and Carol must be convinced that the messages are linked and unaltered
- Alice sends Bob { Message 1, Digest 2, Dual Signature}
- Bob hashes Message 1, concatenates with Digest2 and hashes
- Bob decrypts the dual signature with Alice's public key
- If the new hash and the decrypted signature match, all is OK
- Now Bob can send Carol Digest 2 and ask if she got the message corresponding to it!
- (Carol got { Message 2, Digest 1, Dual Signature})

Dual Signature in SET

- Same as the Basic Case of Dual Signature EXCEPT that both recipients will get the same XOR version of the 2 Message Digests

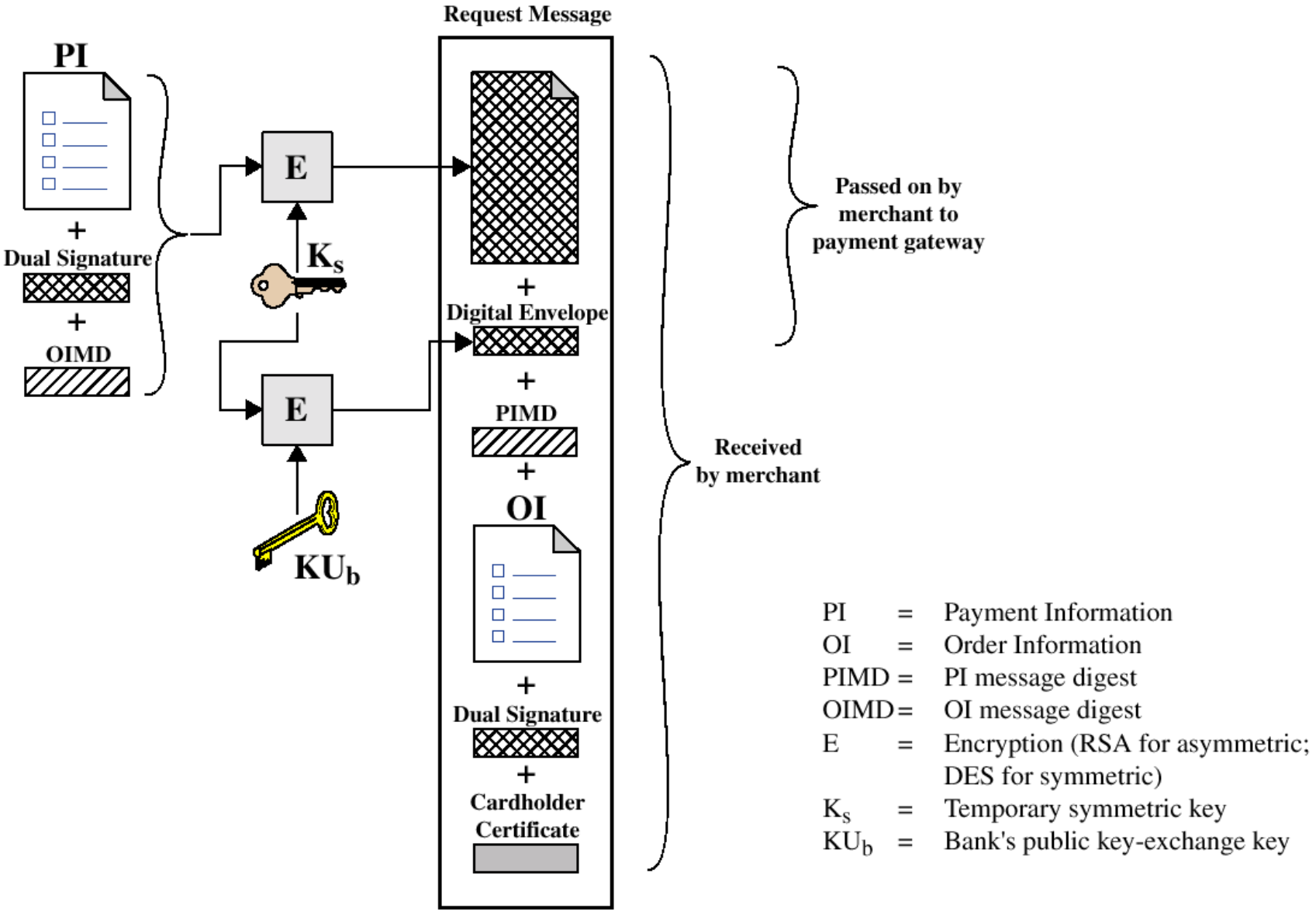


Conceptual Use of Dual Signatures with Encrypted Messages

- Alice wants to send Message 1 (protected by encryption) to Bob and Message 2 (protected by encryption) to Carol
- Message 1 is order info; Message 2 is payment info
- Both Bob and Carol must be convinced that the messages are linked and unaltered
- Alice encrypts Message 1 with Bob's public key; Message 2 with Carol's public key
- Alice sends { PK_{BOB}(Message 1), PK_{CAROL} (Message 2), DualSig} to both Bob and Carol
- Bob hashes PK_{BOB}(Message 1), concatenates with

  the hash of PK_{CAROL}(Message 2), and hashes these 2 pieces of info together again to give the Dual Hash
- Bob decrypts the DualSig with Alice's public key
- If the Dual Hash and the decrypted DualSig match, all is OK

The SET Cardholder Purchase Request



PI = Payment Information
OI = Order Information
PIMD = PI message digest
OIMD = OI message digest
E = Encryption (RSA for asymmetric; DES for symmetric)
K_s = Temporary symmetric key
KU_b = Bank's public key-exchange key

SOURCE: HENRIC JOHNSON

SET Message Flow

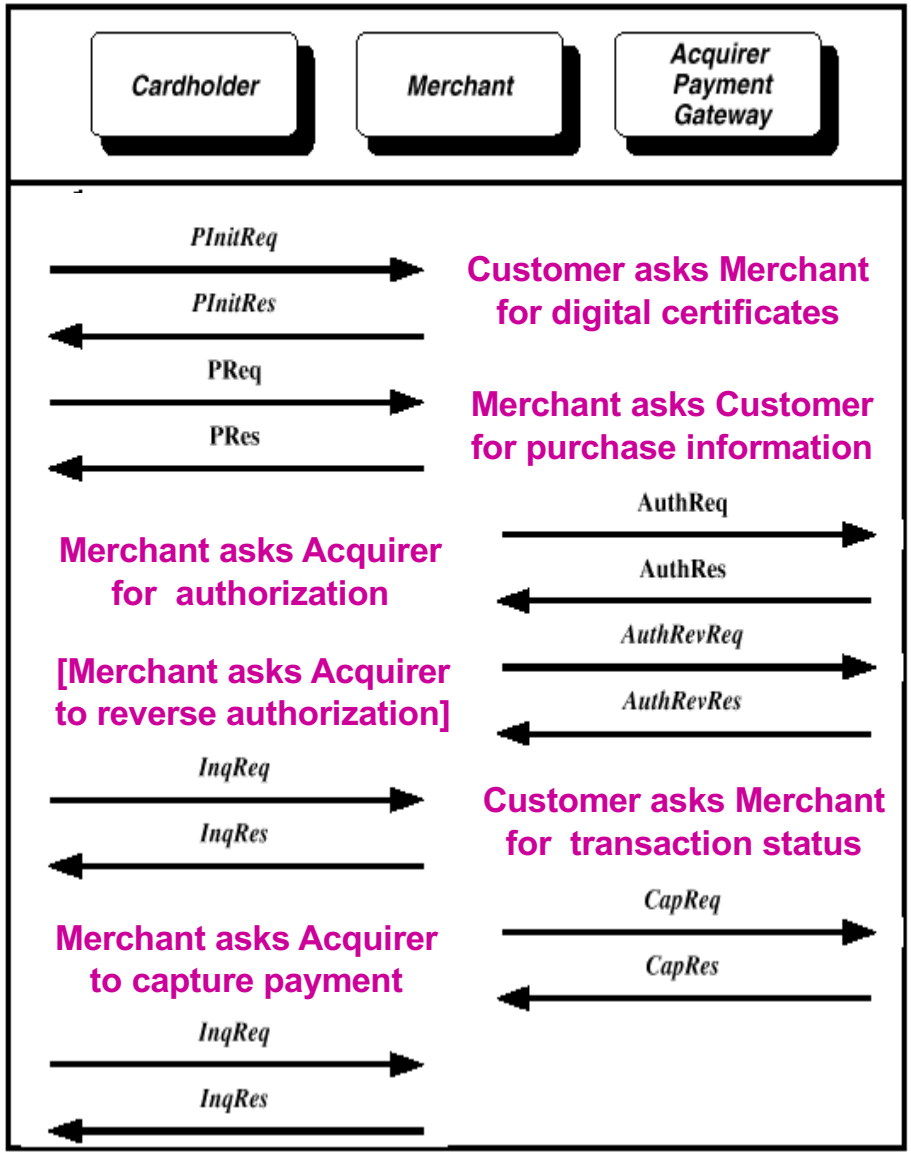
SET messages come in pairs:

Request

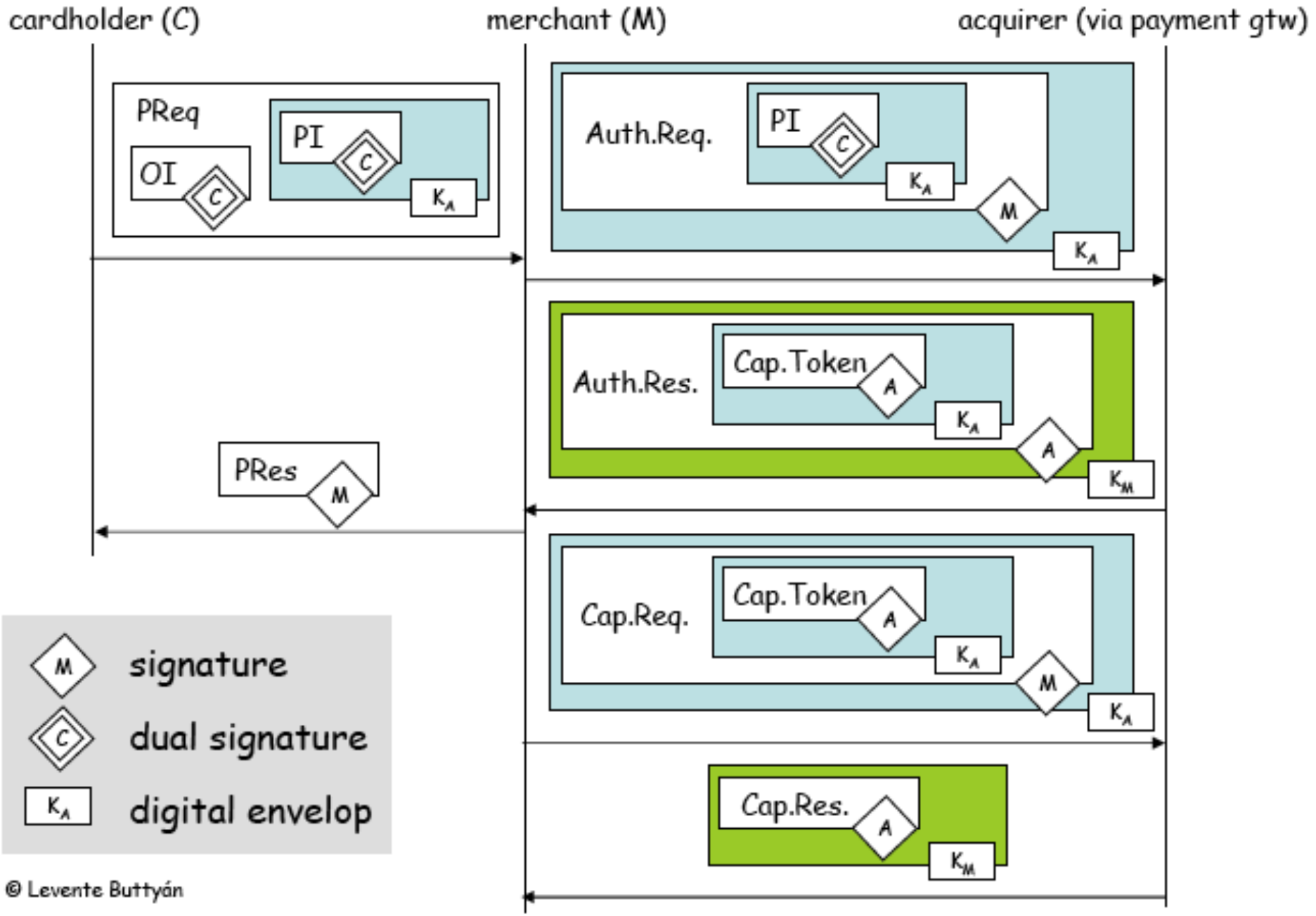
followed by

Response

Appropriate cryptography is applied to message wrappers



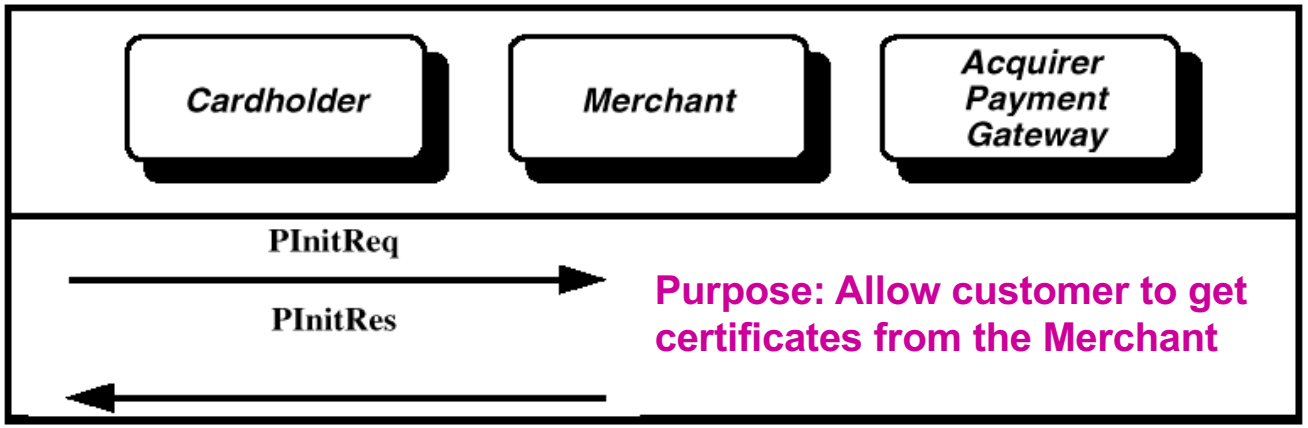
More on SET messages Protection Mechanism



SET Process Steps (Simplified)

1. Merchant sends invoice and unique transaction ID (XID)
2. Merchant sends merchant certificate and (the acquiring) bank certificate (encrypted
   with CA's private key) to the Customer
3. Customer decrypts certificates, obtains public keys
4. Customer generates order information (OI) and payment info (PI) encrypted with different session keys and dual-signed
5. Merchant sends payment request to bank encrypted with bank-merchant session key, PI encrypted by the Customer using Bank's public-key, digest of OI and merchant's certificate
6. Bank verifies that the XID matches the one in the PI
7. Bank sends authorization request to issuing bank via card network
8. Bank sends approval to merchant
9. Merchant sends acknowledgement to customer

SET Payment Initialization



Customer's Language

Card Brand (VISA, MC, etc.)

Bank ID #

PInitReq: { RRPID, Language, LID_C, [LID_M], Chall_C, BrandID, BIN, [Thumbs]}

Request/Response Pair ID

Customer's local ID

Merchant's local ID

Customer's challenge salt to Merchant's signature freshness

Thumbnails (hashes) of of certificates known to Customer

Security Fields in Order Information

OIData	**{TransIDs, RRPID, Chall-C, HOD, ODSalt, [Chall-M], BrandID, BIN, [ODExtOIDs], [OIExtensions]}**
TransIDs	*Copied from* **PInitRes**, *if present; see page 33*
RRPID	*Request/response pair ID*
Chall-C	*Copied from corresponding* **PInitReq**; *see page 72*
HOD	**DD(HODInput)** *Links* **OIData** *to* **PurchAmt** *without copying* **PurchAmt** *into* **OIData**, *which would create confidentiality problems.*
ODSalt	*Copied from* **HODInput**
Chall-M	*Merchant's challenge to Cardholder's signature freshness*
BrandID	*Cardholder's chosen payment card brand*
BIN	*Bank Identification Number from the cardholder's account number (first six digits)*
ODExtOIDs	*List of object identifiers from* **ODExtensions** *in the same order as the extensions appeared in* **ODExtensions**
OIExtensions	*The data in an extension to the* **OI** *should relate to the Merchant's processing of the order.* *Note: The order information is not encrypted so this extension must not contain confidential information.*

TRANSACTION IDs: CUSTOMER, MERCHANT, GLOBALLY UNIQUE

REQUEST/RESPONSE PAIR ID

CARDHOLDER'S CHALLENGE TO MERCHANT SIG FRESHNESS

HASH OF ORDER DATA

ORDER DATA SALT (TO GUARD AGAINST DICTIONARY ATTACK ON ORDER DATA HASH!

MERCHANT'S CHALLENGE TO CARDHOLDER SIG FRESHNESS

DD(x) means data +a hash of the data per PKCS #7

SOURCE: SET STANDARD

SET Security

- Digital envelopes, nonces
- Two public-private key pairs for each party
  - One for digital signatures; one for key exchange messages
- 160-bit message digests
- Statistically globally unique IDs (XIDs)
- Certificates (5 kinds)
  - Cardholder, Merchant, Acquirer, Issuer, Payment Gateway
- Hardware cryptographic modules (for high security)
- Idempotency (message can be received many times but is only processed once)
- Complex protocol. Over 600 pages of detail
- Dual signatures

Visibility of SET Transaction Data

Party Watching

Data Element

	Seller	Buyer	Date	Amount	Item
Seller	full	partial	full	full	full
Buyer	partial	full	full	full	full
Bank	full	full	full	full	none
Observer	none	none	full	none	none

SET achieves:

money atomicity
consistency
durability
authentication
security
secrecy
non-repudiation
scalability

SET does not achieve:

goods atomicity
isolation
economy
interoperability

SET Overhead

Simple purchase transaction:

- Four messages between merchant and customer
- Two messages between merchant and payment gateway
- 6 digital signatures
- 9 RSA encryption/decryption cycles
- 4 DES encryption/decryption cycles
- 4 certificate verifications

Scaling:

- Multiple servers need copies of all certificates
- Compaq sells SET software equipped for 5,000,000 certificates
- NO ONE USES SET. WHY?
- Visa used to list all SET-enabled merchants on its website. No more.

SET Software Requirements

- **Cardholder wallet software (Customer)**
  - Point-and-click interface on customer's PC
  - Communicates with merchant's SET software
  - Verifies merchant's certificate
  - Administers and maintains cardholder's digital certificates
- **Merchant software (Merchant)**
  - Communicates securely with cardholders and banks
  - Exchanges digital certificates prior to a sales transaction
- **Payment Gateway server software (Bank, card organization)**
  - Mediates the payment process
  - Decrypts payment instructions from cardholders
  - Translates SET transaction data to/from different formats

SET Software Requirements

- **Certificate Authority software (Bank)**
  - Financial institutions will use this software to enable cardholders and merchants to register their respective account agreements for secure electronic commerce
  - Issues and administers digital certificates for cardholders and merchants

SET in Practice

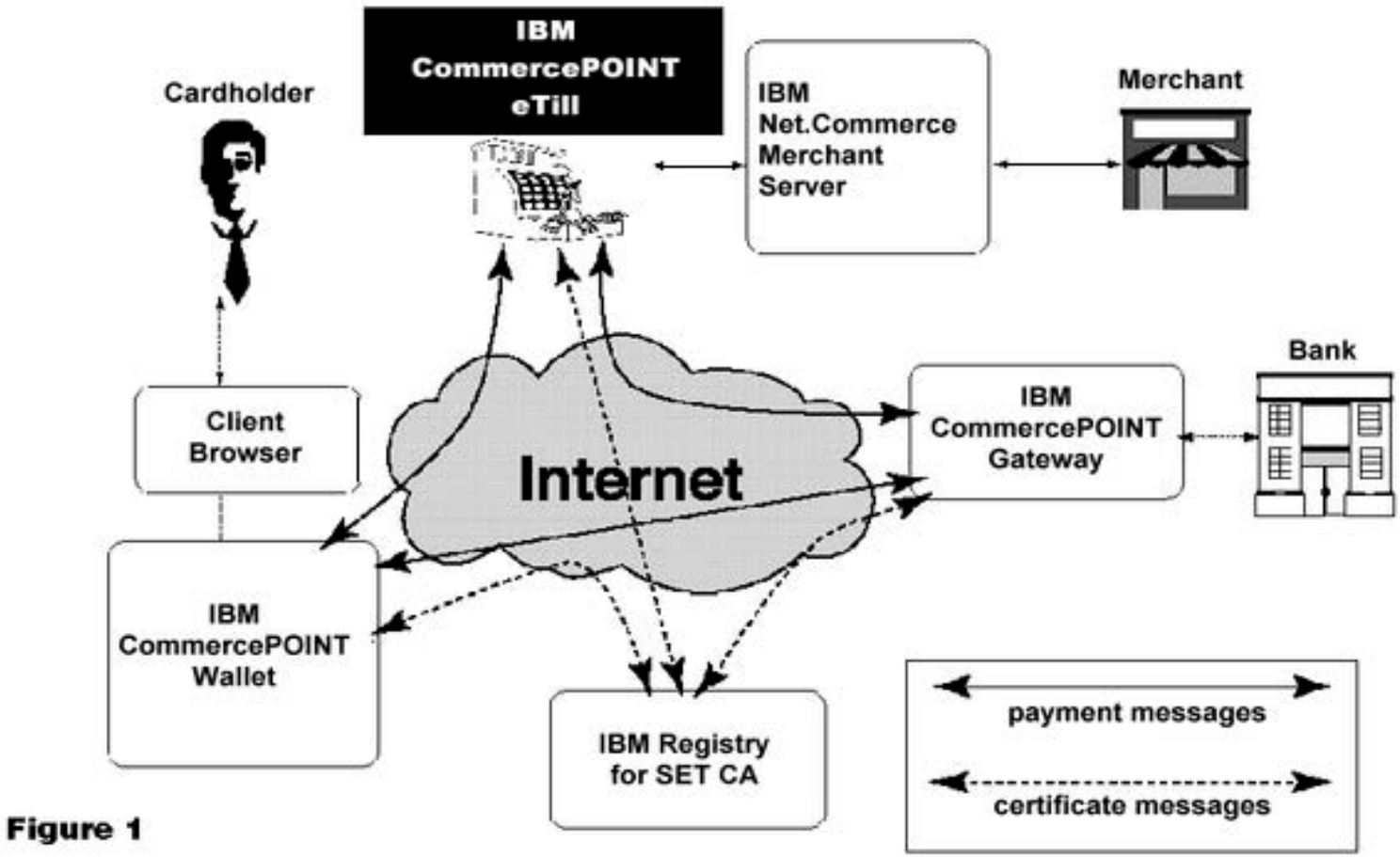


Figure 1

SOURCE: http://www.software.ibm.com/commerce/payment/specsheetetill.html

eCashPad

- Convert a “Card Not Present” transaction into “Card Present” by adopting SET

- Installed in guest rooms at Arizona Holiday Inn

Why did SET fail ?

- Less benefits than expected
  - Merchants like to collect credit card numbers (they use it as indexes in marketing databases)
  - Optionally, SET allows the merchant to get the credit card number from the acquirer

  =>Security improvements of SET are negated
- Too High Costs
  - SET requires PKI
- No advantages for the Customers
  - The idea was that SET transactions would be handled as "Cardholder Present" transactions (due to Digital Signature of the cardholder)
  - Customers prefer MOTO-like systems where they can freely reverse a transaction if they are unhappy (not only in the case of fraud) => by using SET, Customers were much worse off !
  - SET requires the download and installation of special software and obtaining a public-key certificate by the Merchant AND the Cardholder !!

3-D Secure

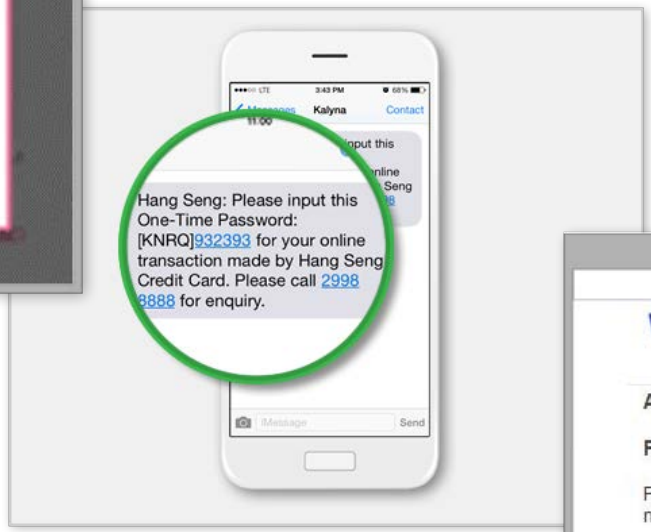
- Idea: Authenticate user without a certificate
- Requires the user to answer a challenge in real-time
- Challenge comes from the Issuing Bank, not the Merchant
- Issuing Bank confirms User identity to Merchant

3-D Secure from the User's Perspective

Invoked during the Checkout Process:

Step 1: Enter Credit card Info of User

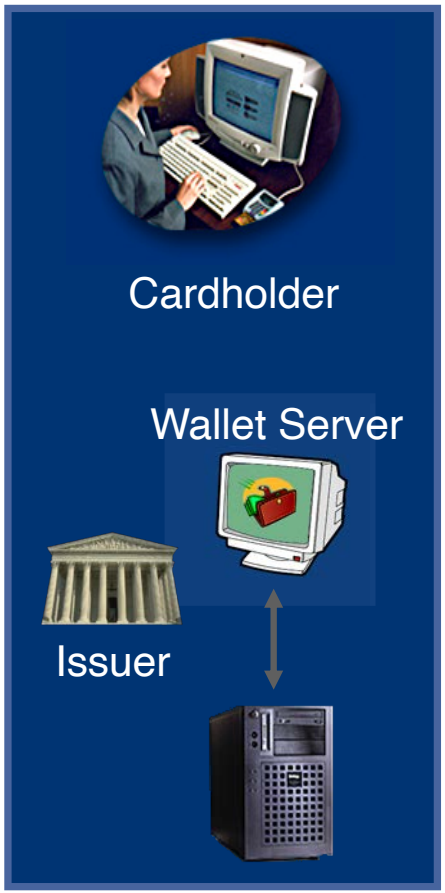
Step 2: User receives One-Time-Password (OTP) from Issuing Bank via a separate channel, e.g. SMS



Step 3: Enter OTP to complete the payment

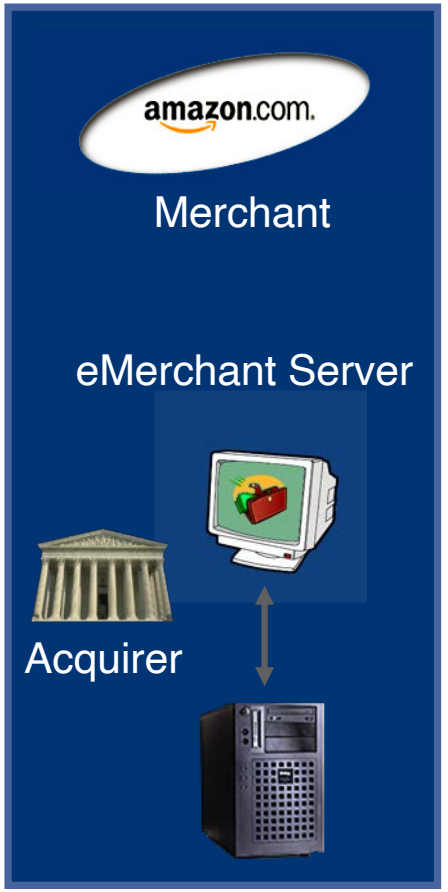
SOURCE: HangSeng.com

3-D (3-Domain) Model



Issuer Domain

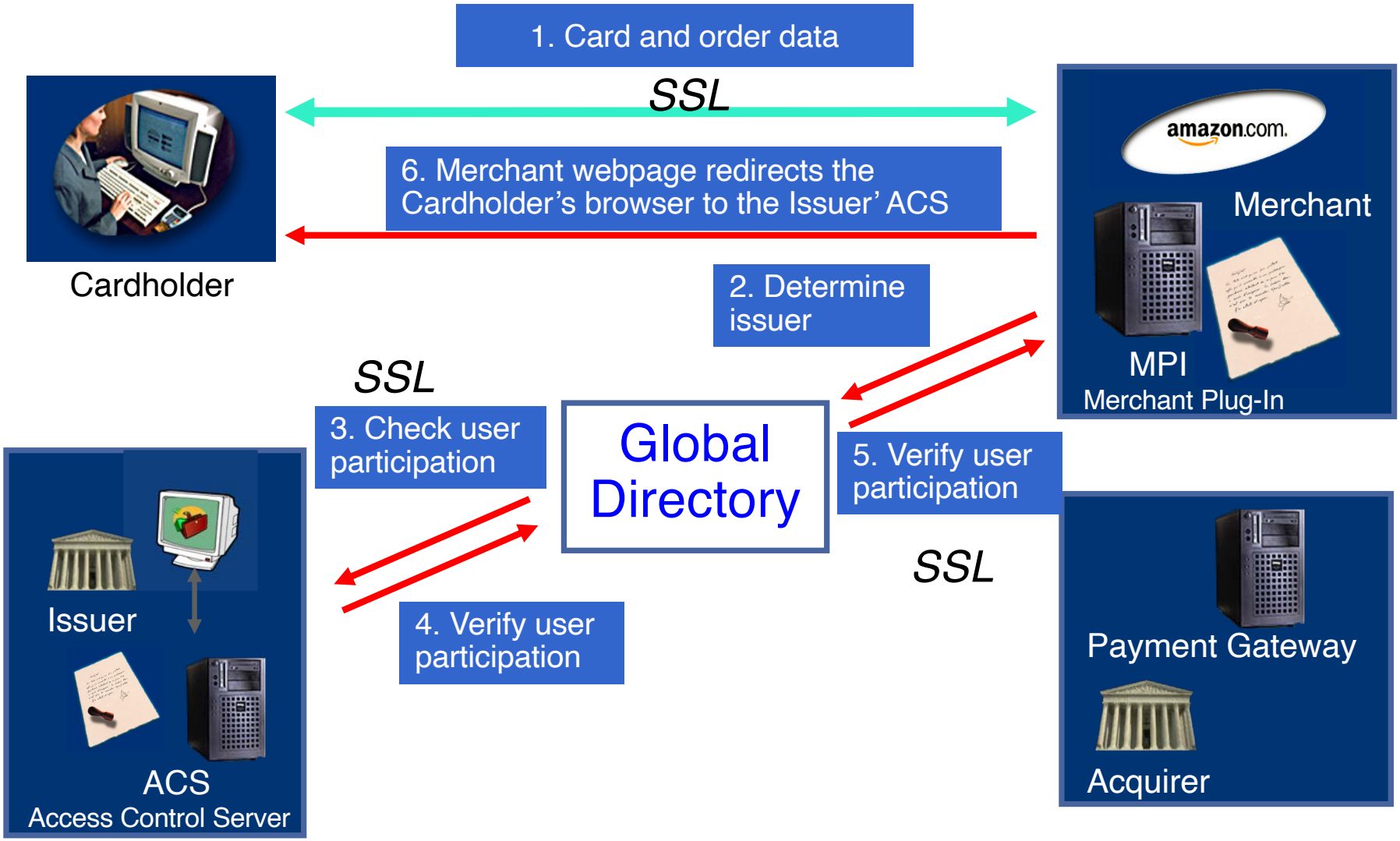
Interoperability Domain



Acquirer Domain

SOURCE: MASTERCARD

3-D Secure Process Flow



3-D Secure Process Flow

Cardholder

10. Payer Authentication Response

SSL

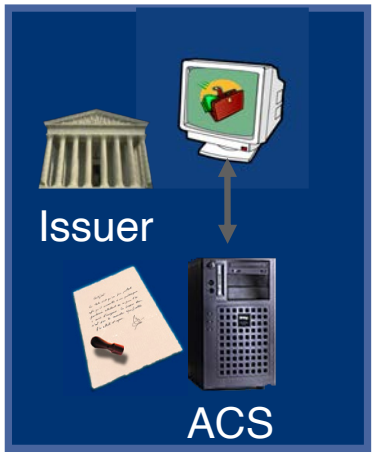
7. Payer Authentication Request

8. Cardholder Authentication

9.Payer Authentication Response

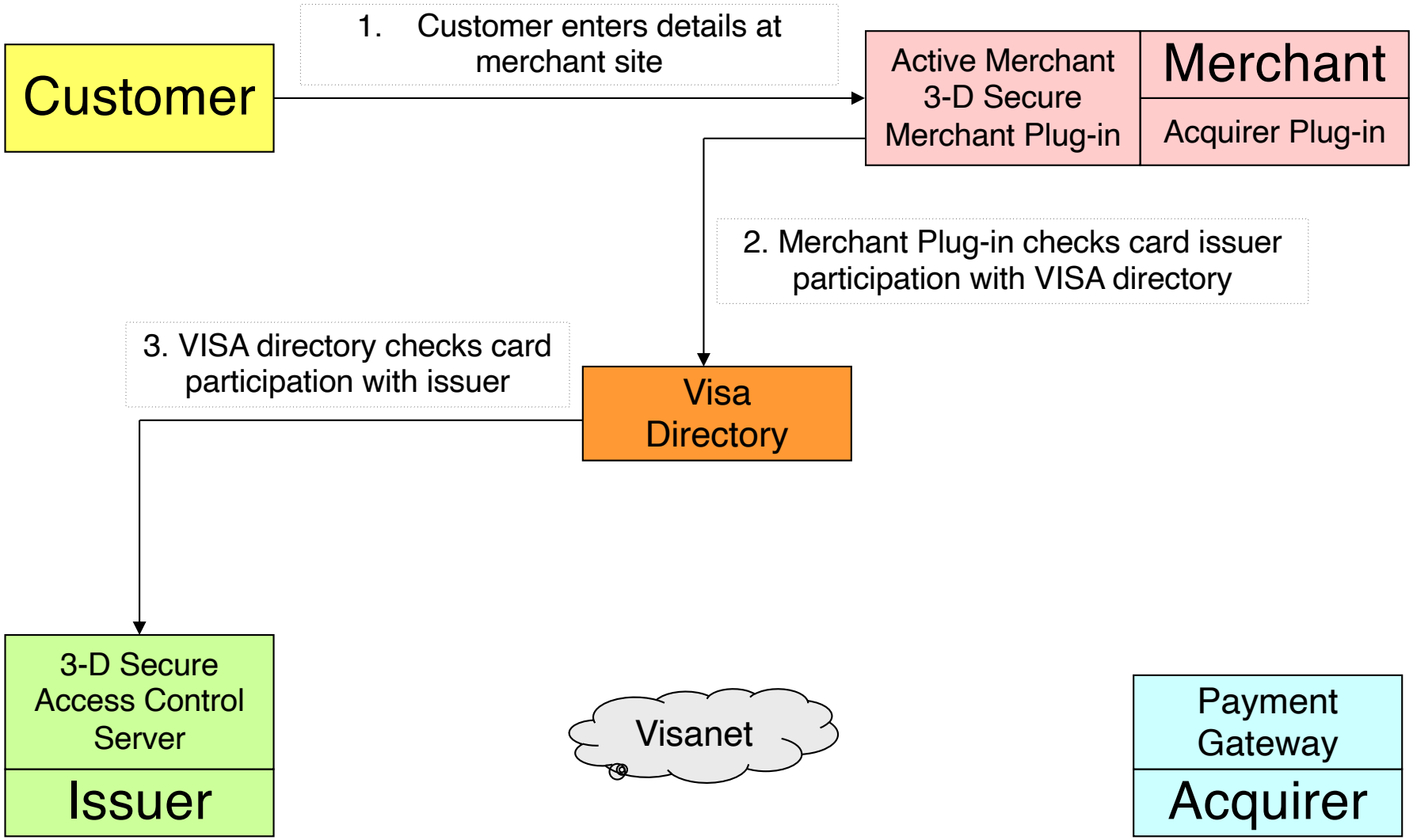
11. Normal Transaction

Global Directory



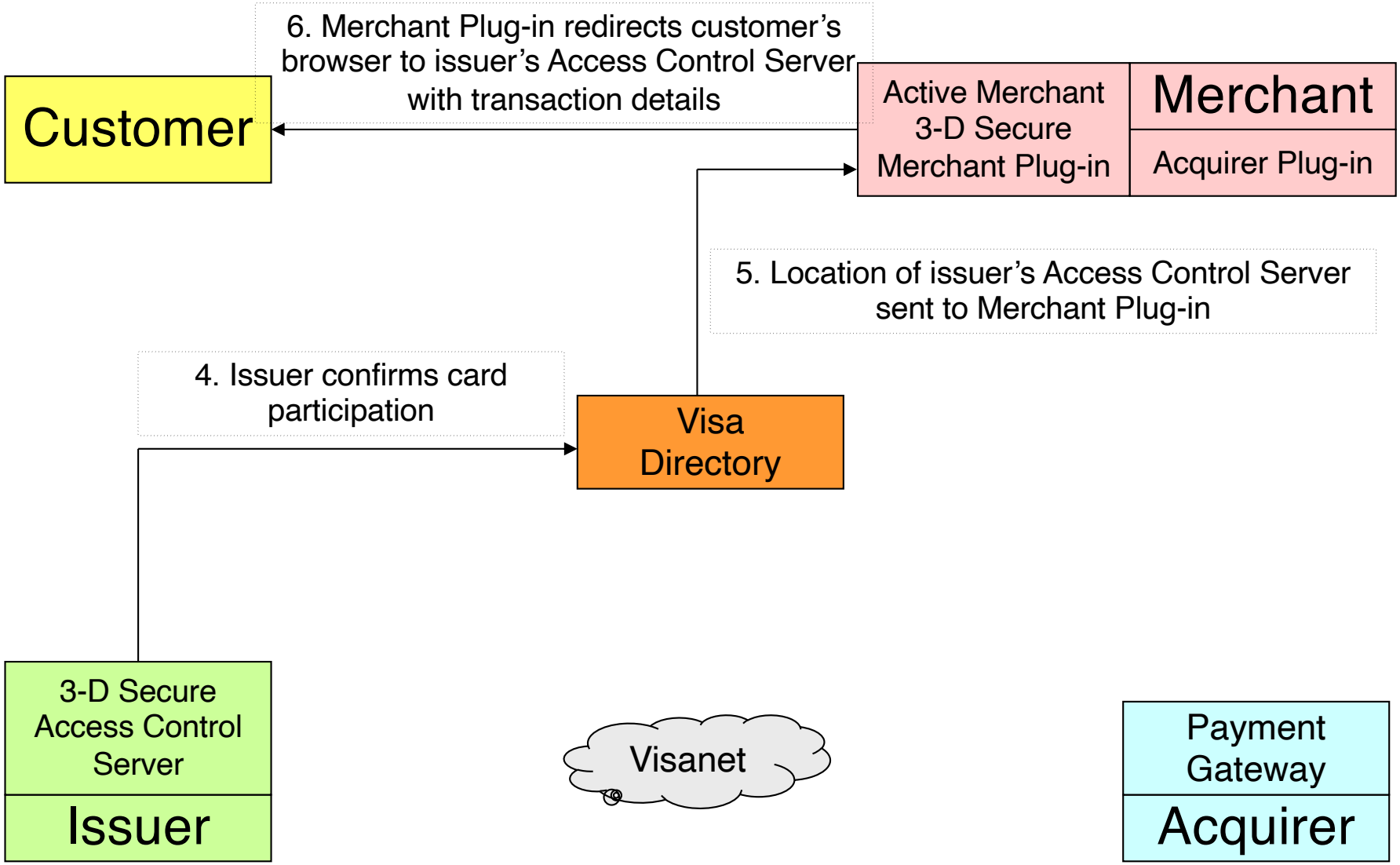
12. Normal Authorization Process

3D Secure (1)



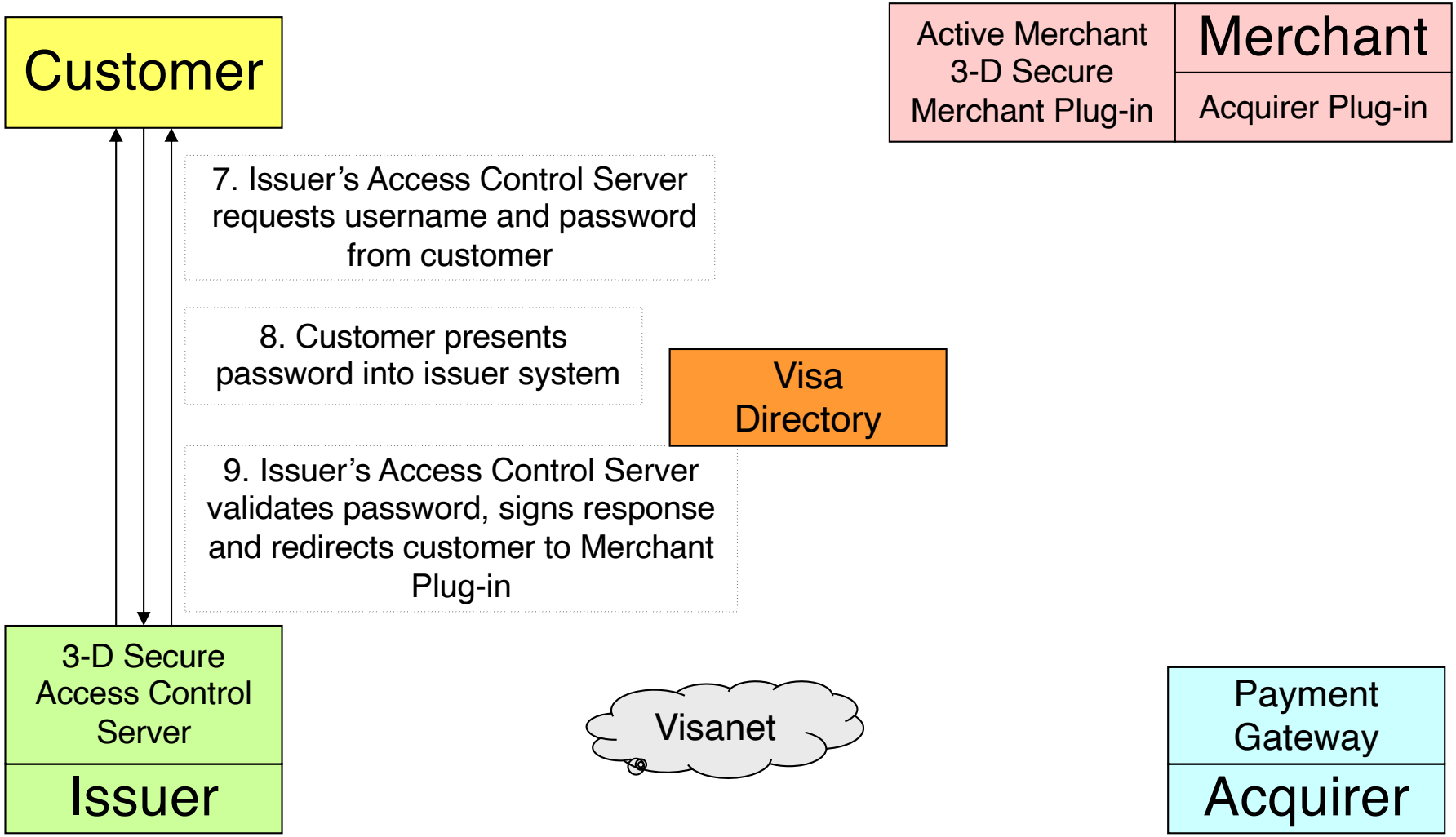
SOURCE: KMIS

3D Secure (2)



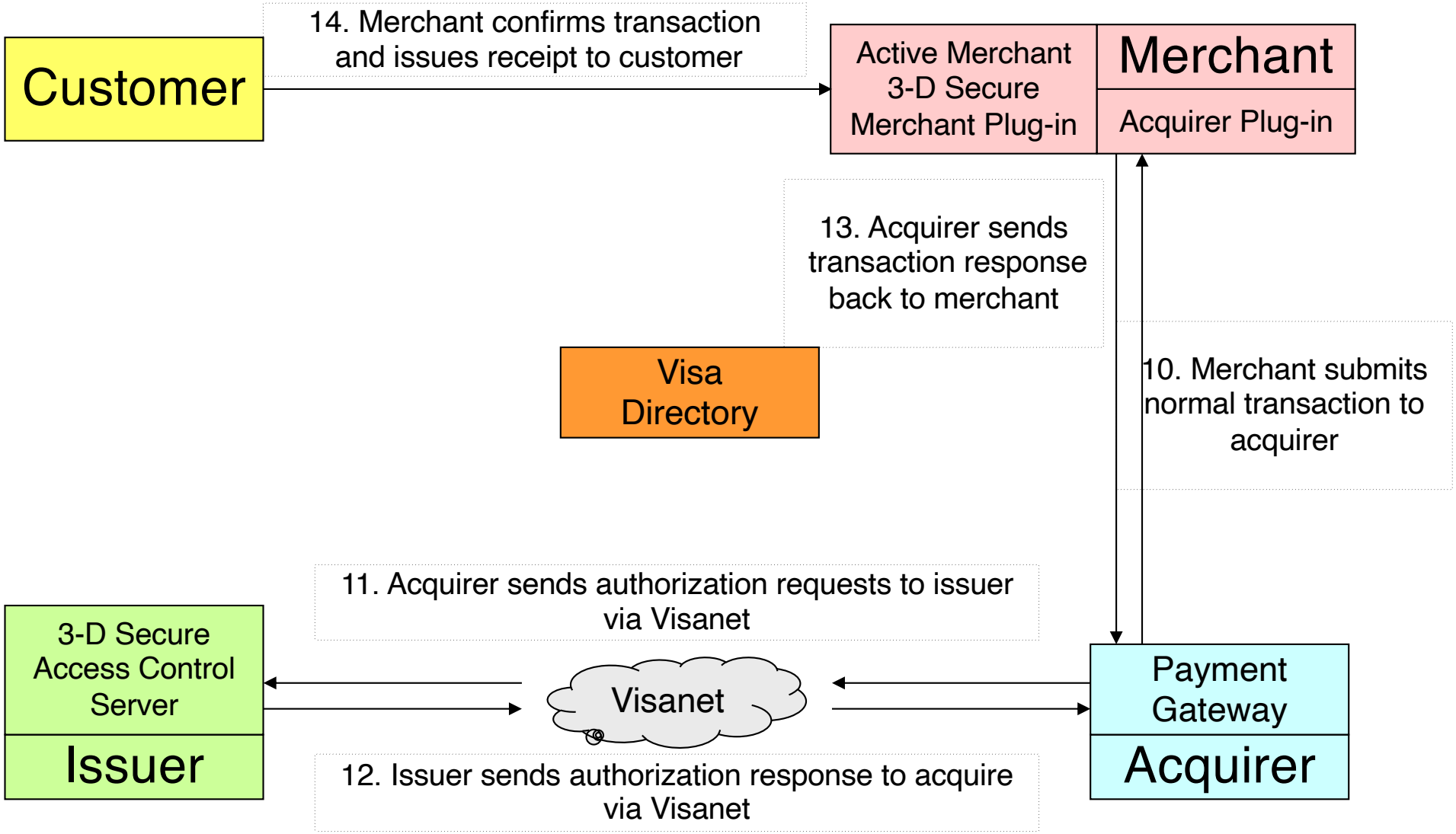
SOURCE: KMIS

3D Secure (3)

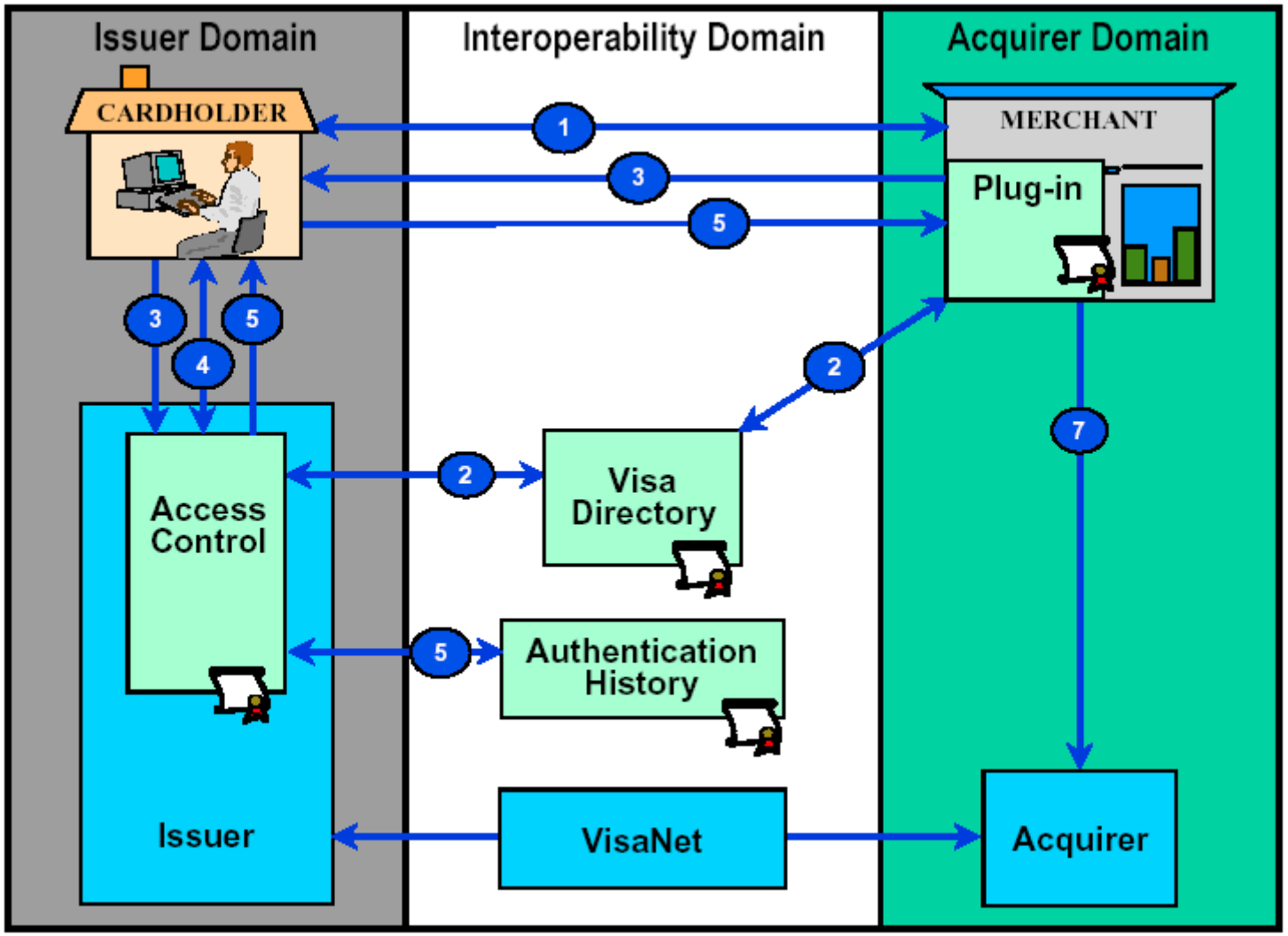


SOURCE: KMIS

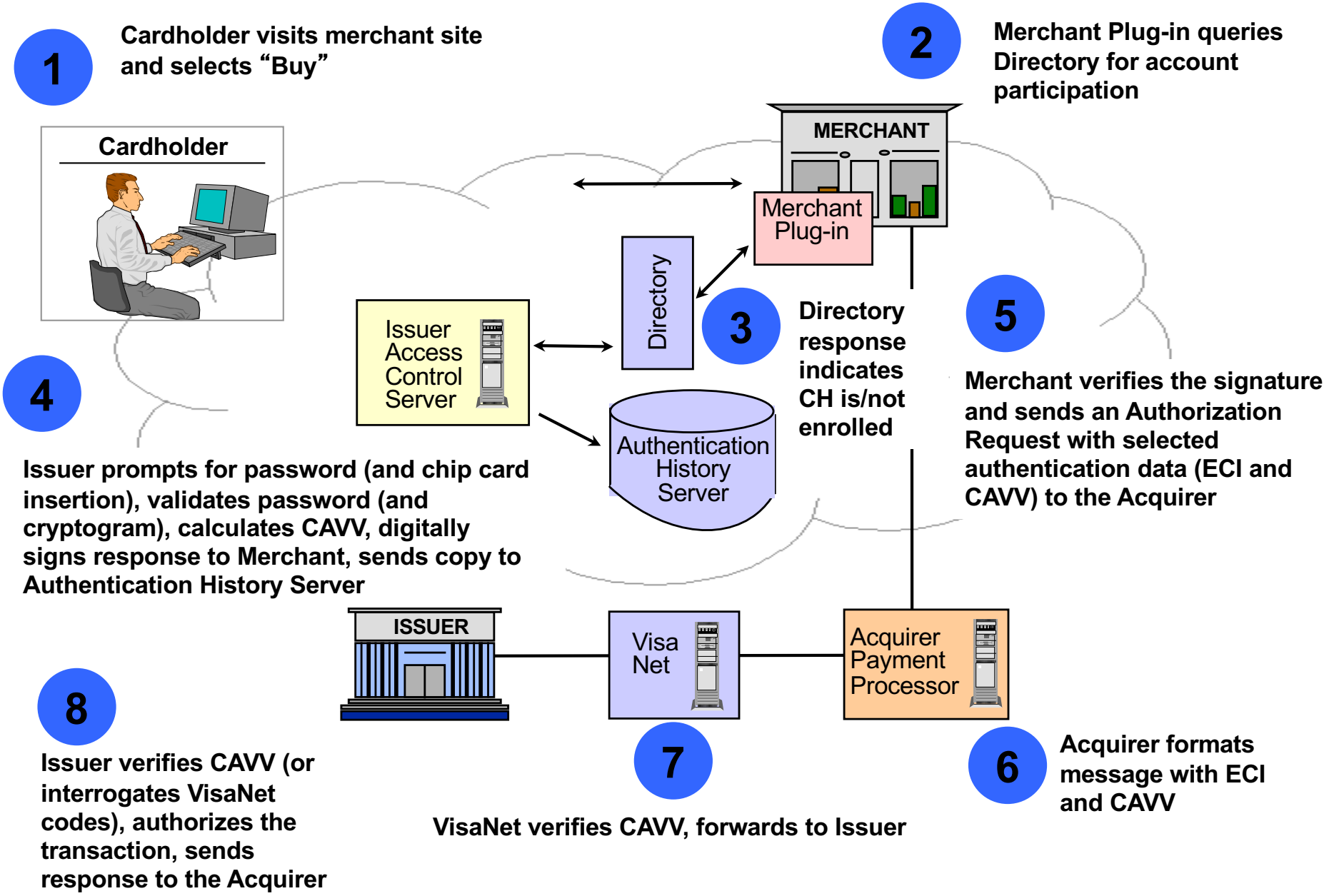
3D Secure (4)


Customer
14. Merchant confirms transaction and issues receipt to customer
Active Merchant 3-D Secure Merchant Plug-in
Merchant
Acquirer Plug-in
13. Acquirer sends transaction response back to merchant
Visa Directory
10. Merchant submits normal transaction to acquirer
11. Acquirer sends authorization requests to issuer via Visanet
3-D Secure Access Control Server
Issuer
Visanet
Payment Gateway
Acquirer
12. Issuer sends authorization response to acquire via Visanet

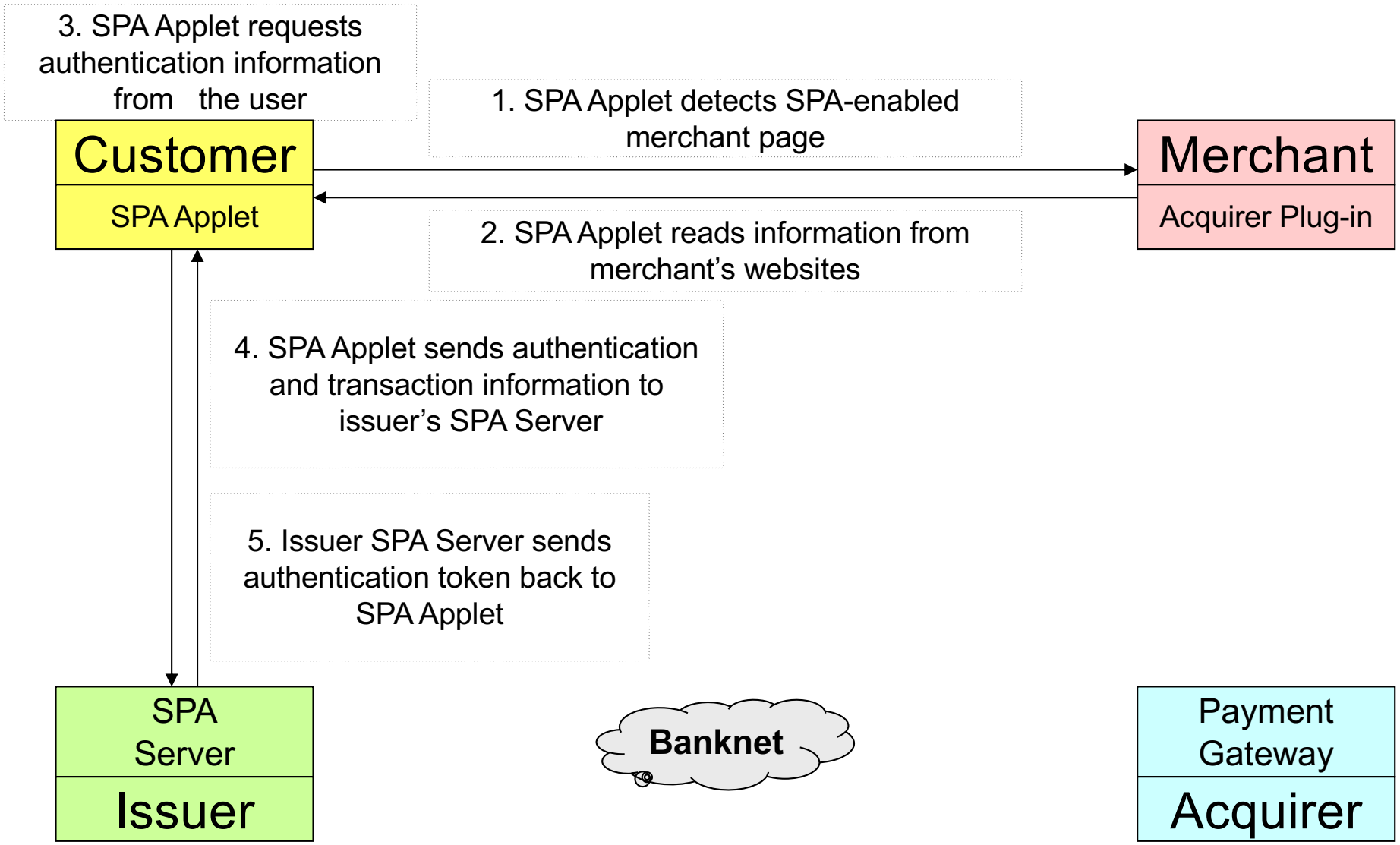
3-D Secure



SOURCE: VISA

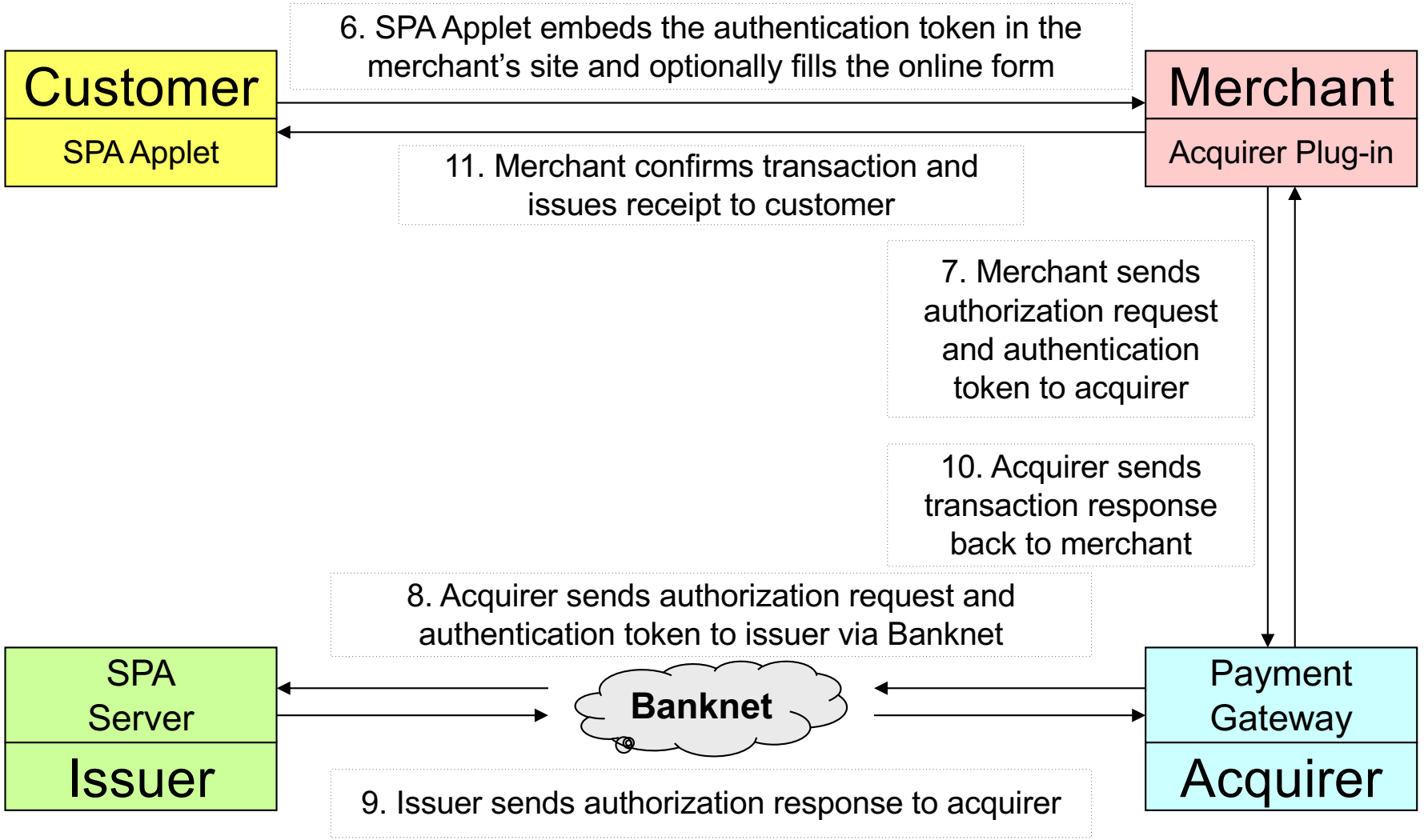

1
Cardholder visits merchant site and selects "Buy"
Cardholder
2
Merchant Plug-in queries Directory for account participation
MERCHANT
Merchant Plug-in
Directory
3
Directory response indicates CH is/not enrolled
Issuer Access Control Server
Authentication History Server
4
Issuer prompts for password (and chip card insertion), validates password (and cryptogram), calculates CAVV, digitally signs response to Merchant, sends copy to Authentication History Server
5
Merchant verifies the signature and sends an Authorization Request with selected authentication data (ECI and CAVV) to the Acquirer
ISSUER
Visa Net
Acquirer Payment Processor
6
Acquirer formats message with ECI and CAVV
7
VisaNet verifies CAVV, forwards to Issuer
8
Issuer verifies CAVV (or interrogates VisaNet codes), authorizes the transaction, sends response to the Acquirer

SPA (1)



SOURCE: KMIS

SPA (2)


6. SPA Applet embeds the authentication token in the merchant's site and optionally fills the online form
Customer
SPA Applet
Merchant
Acquirer Plug-in
11. Merchant confirms transaction and issues receipt to customer
7. Merchant sends authorization request and authentication token to acquirer
10. Acquirer sends transaction response back to merchant
8. Acquirer sends authorization request and authentication token to issuer via Banknet
SPA Server
Issuer
Banknet
Payment Gateway
Acquirer
9. Issuer sends authorization response to acquirer

Major Ideas

- Credit cards are used because of convenience
- But the processing cost is high
- SSL, TLS are general secure message protocols, not payment protocols
- SSL requires the merchant (vendor) to have a certificate ; customer side certificate is optional only
- SET is a payment protocol
- SET requires all parties to have certificates
- SET uses dual signatures
- 3-D Secure provides authentication without certificates