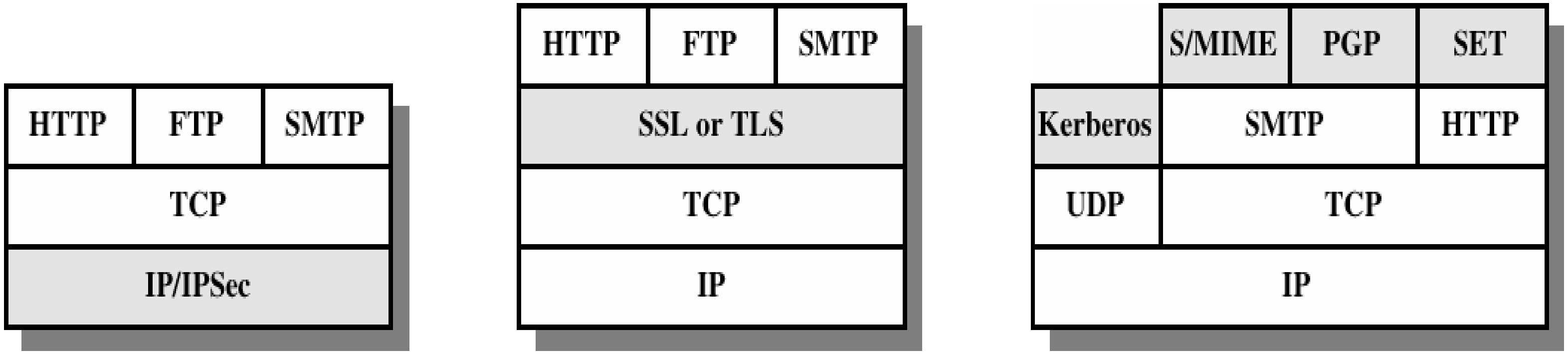
Payment Security

Ola Flygt
Linnaeus University, Sweden
http://homepage.lnu.se/staff/oflmsi/
Ola.Flygt@lnu.se

Outline

- Secure Electronic Transaction (SET)
- 3-D Secure
- PCI DSS
- Electronic money
- Bitcoin
- Apple Pay and Samsung Pay

Security facilities in the TCP/IP protocol stack



(a) Network Level

(b) Transport Level

(c) Application Level

Secure Electronic Transactions (SET)

- An open encryption and security specification
- Protect credit card transaction on the Internet
- Companies involved:
  - MasterCard, Visa, IBM, Microsoft, Netscape, RSA, Terisa and Verisign
- Not a payment system
- Set of security protocols and formats

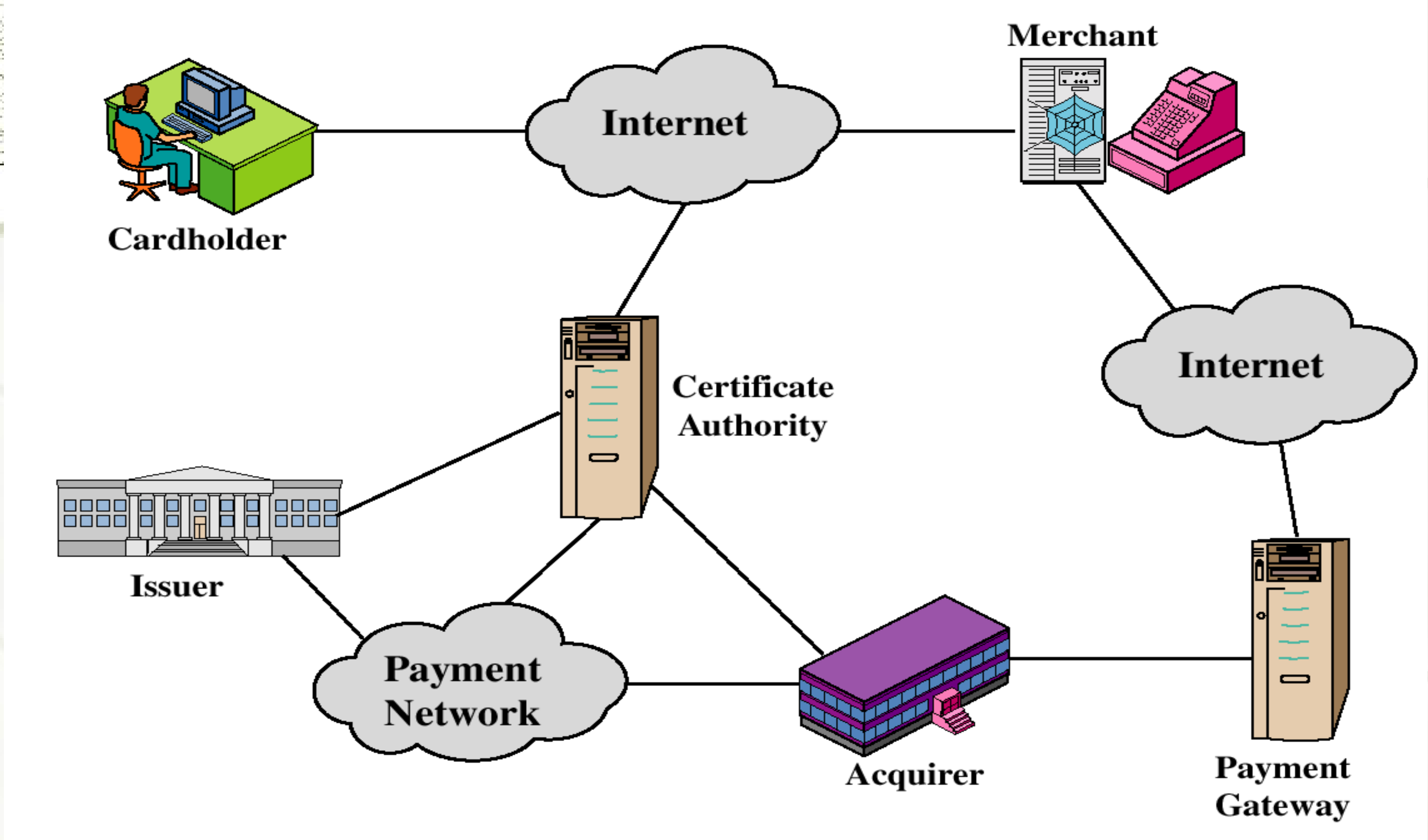
SET Services

- Provides a secure communication channel in a transaction
- Provides trust by the use of X.509 digital certificates
- Ensures privacy

SET Overview

- Key Features of SET:
  - Confidentiality of information
  - Integrity of data
  - Cardholder account authentication
  - Merchant authentication

SET Participants

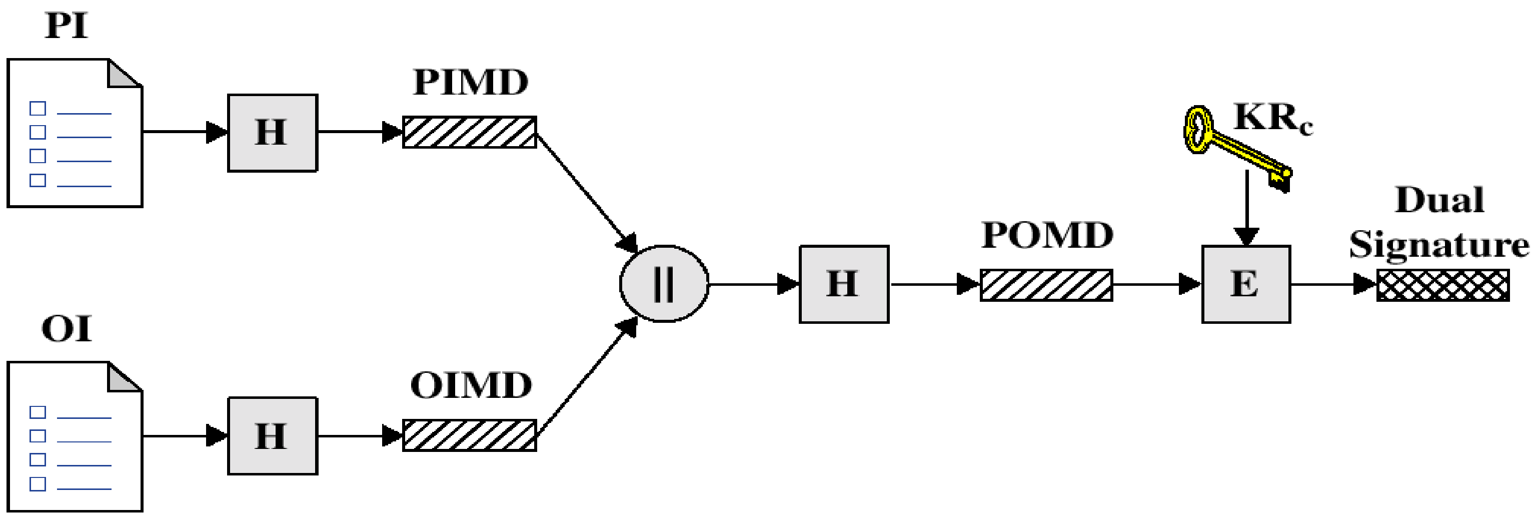


Sequence of events for transactions

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

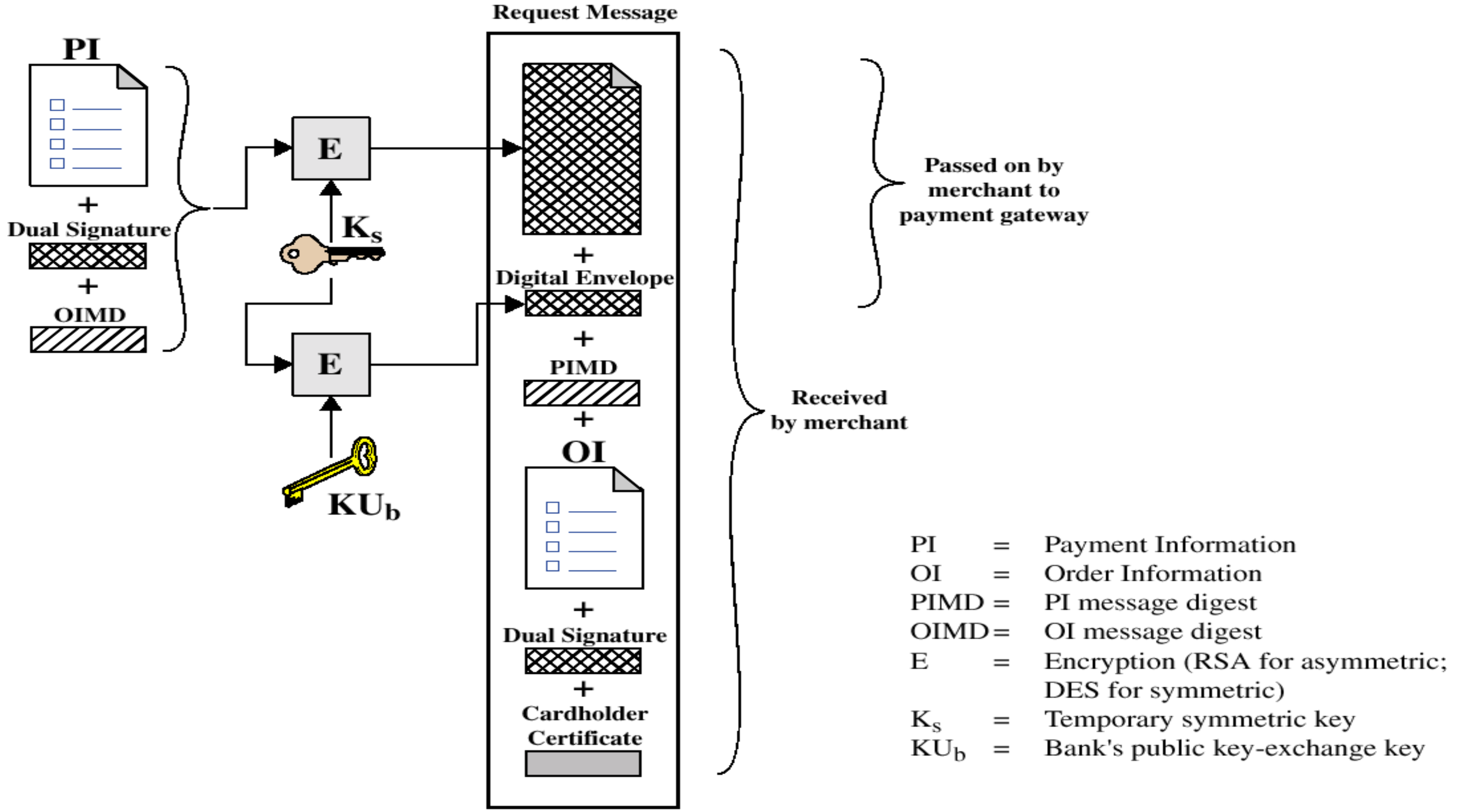
Dual Signature

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



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

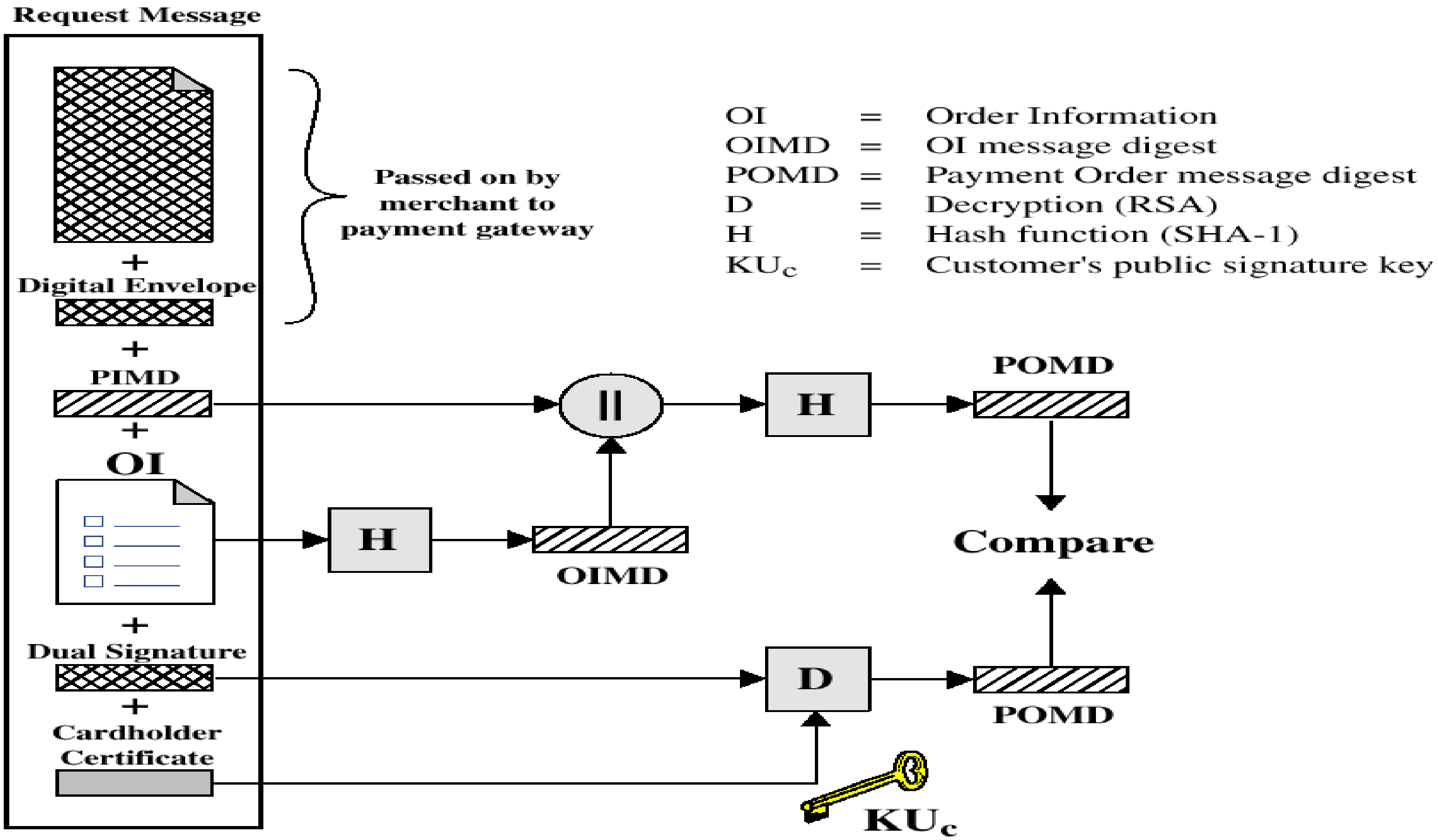
Payment processing



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

Cardholder sends Purchase Request

Payment processing



OI	=	Order Information
OIMD	=	OI message digest
POMD	=	Payment Order message digest
D	=	Decryption (RSA)
H	=	Hash function (SHA-1)
KU$_c$	=	Customer's public signature key

Merchant Verifies Customer Purchase Request

Payment processing

- Payment Authorization:
  - Authorization Request
  - Authorization Response
- Payment Capture:
  - Capture Request
  - Capture Response

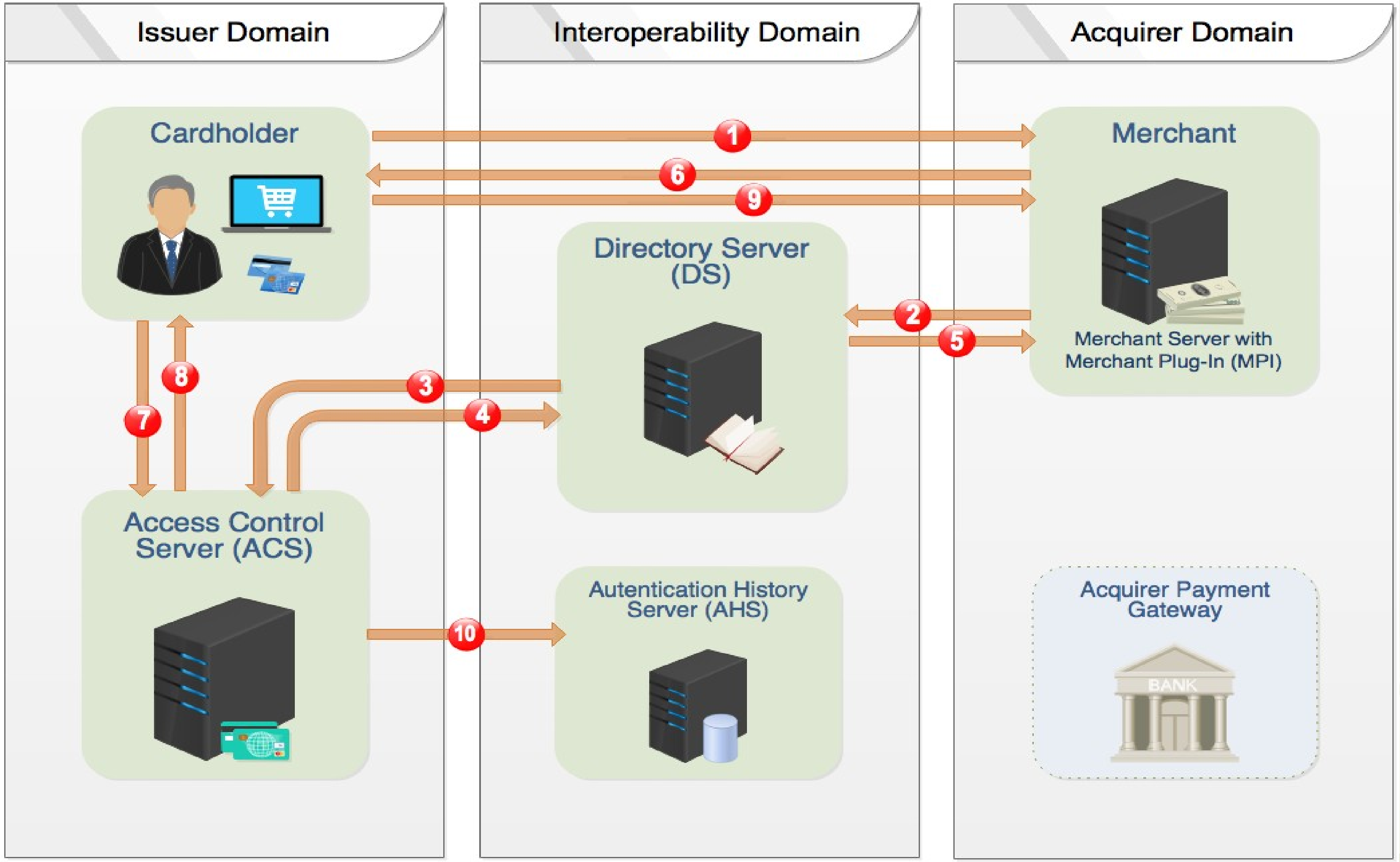
SET today

- Didn’t really take on and is not used anymore
- Main problems
  - Complex and rather costly architecture with many different actors
  - Requires clients to have certificates (was to early to require this) and an client software (e-wallet)

3-D Secure Protocol

- 3-D Secure is an authentication technology that uses Secure Sockets Layer (SSL/TLS) encryption 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 is based on the three-domain model
  - The specifications are currently at version 2.0 (2016) and that version has been rolled out step by step and should be in full use since April 2019.

The Three Domain (3-D) Model



Source: http://www.modirumid.com/3dsecure/

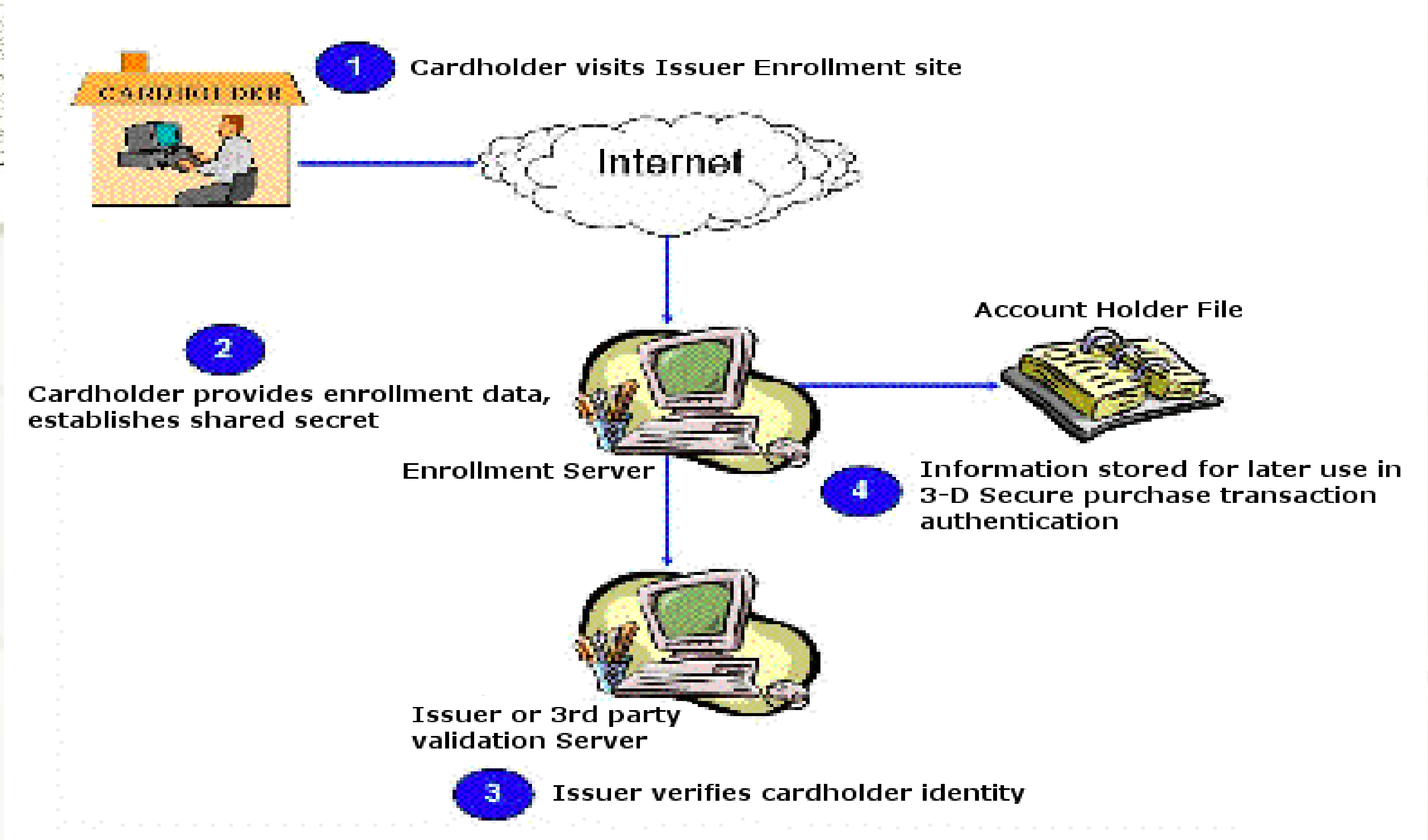
The Three Domain Model

- **Issuer Domain** The Issuer is responsible for:
  - managing the enrolment of their cardholders in the service (including verifying the identity of each cardholder who enrols) and authenticating cardholders during online purchases
- **Acquirer Domain** 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
- **Interoperability Domain**
  - This domain facilitates the transaction exchange between the other two domains with a common protocol and shared services

Implementations

- 3-D Secure Protocol have been implemented by several Credit Card Companies that give similar services:
  - Verified by Visa
  - MasterCard SecureCode
  - J/Secure
  - American Express SafeKey

Enrolment



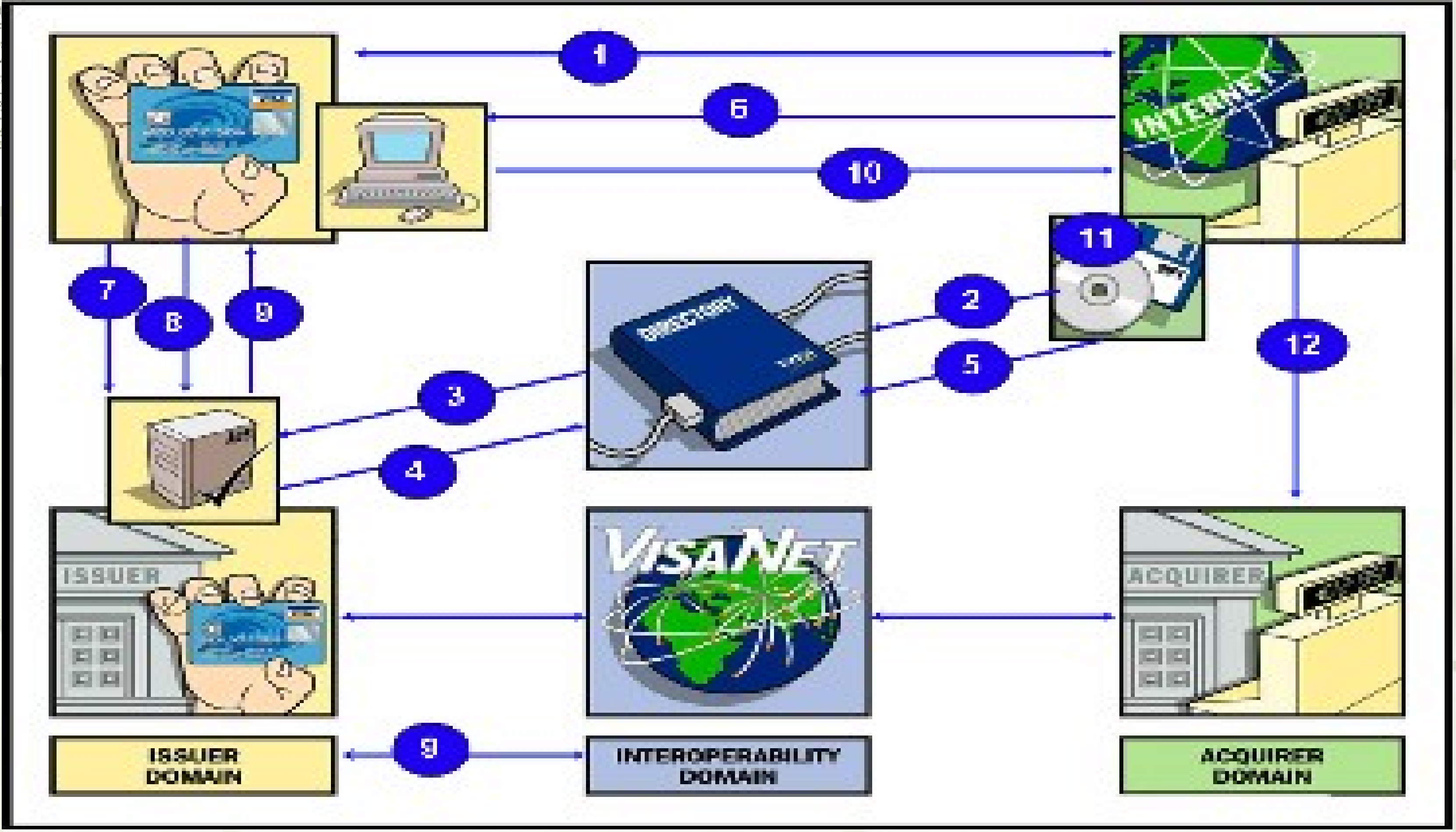
1 Cardholder visits Issuer Enrollment site

2 Cardholder provides enrollment data, establishes shared secret

3 Issuer verifies cardholder identity

4 Information stored for later use in 3-D Secure purchase transaction authentication

Purchase Transaction



Purchase Transaction, cont.

- Step 1 Shopper browses at merchant site, adds items to shopping cart, then finalizes purchase. Merchant now has all necessary data, including PAN (Primary Account Number) and user device information.
- Step 2 Merchant Server Plug-in (MPI) sends PAN (and user device information, if applicable) to Directory Server.
- Step 3 Directory Server queries appropriate Access Control Server (ACS) to determine whether authentication (or proof of authentication attempt) is available for the PAN and device type. If no appropriate ACS is available, the Directory Server creates a response for the MPI and processing continues with Step 5.
- Step 4 ACS responds to Directory Server.

Purchase Transaction, cont.

- Step 5 Directory Server forwards ACS response (or its own) to MPI. If neither authentication nor proof of authentication attempt is available, 3-D Secure processing ends, and the merchant, acquirer, or payment processor may submit a traditional authorization request, if appropriate.
- Step 6 MPI sends Payer Authentication Request to ACS via shoppers device. The Payer Authentication Request message may be **PAReq** (for cardholders using PCs) or **CPRQ** (for cardholders using mobile Internet devices - see 3-D Secure: Protocol Specification - Extension for Mobile Internet Devices).
- Step 7 ACS receives Payer Authentication Request.
- Step 8 ACS authenticates shopper using processes applicable to PAN (password, chip, PIN, etc.). Alternatively, ACS may produce a proof of authentication attempt. ACS then formats Payer Authentication Response message with appropriate values and signs it. The Payer Authentication Response message is **PARes** if **PAReq** was received, or **CPRS** if **CPRQ** was received. (**CPRS** is created using values from the **PARes**.)

Purchase Transaction, cont.

- Step 9 ACS returns Payer Authentication Response to MPI via shoppers device. ACS sends selected data to Authentication History Server.
- Step 10 MPI receives Payer Authentication Response.
- Step 11 MPI validates Payer Authentication Response signature (either by performing the validation itself or by passing the message to a separate Validation Server).
- Step 12 Merchant proceeds with authorization exchange with its acquirer. Following Step 12, acquirer processes authorization with issuer via an authorization system such as VisaNet, then returns the results to merchant.

Issues with 3-D Secure

- There are a number of concerns about the security and applicability of 3-D Secure
  - When you authenticate a purchase, a new window or frame opens up. This might be used for phishing attacks since it is difficult to see if the window is legitimate or not.
  - Mobile devices do not always work.
  - From 1 February 2015, EU requires strong authentication for Internet payments. That led to the development of 3-D Secure 2.0
  - Merchants are reluctant to use it since they fear the added steps to authenticate a purchase may defer customers

EMV® 3-D Secure

- To reflect current and future market requirements, the payments industry recognised the need to create a new 3-D Secure specification that would support app-based authentication and integration with digital wallets, as well as traditional browser-based e-commerce transactions
- This led to the development and publication of the EMV® 3-D Secure – Protocol and Core Functions Specification, currently at version 2.3 (building on the 3-D Secure 2.0 standard)
- Also support devices like Gaming consoles and Smart speakers

Payment Services Directive (PSD)

In 2007 EU adopted PSD with the intention to “increase pan-European competition with participation also from non-banks, and to provide for a level playing field by harmonizing consumer protection and the rights and obligations for payment providers and users”

On 8 October 2015, the European Parliament adopted the European Commission proposal to create safer and more innovative European payments (PSD2). The current rules aim to better protect consumers when they pay online, promote the development and use of innovative online and mobile payments such as through open banking, and make cross-border European payment services safer.

An important element of PSD2 is the requirement for strong customer authentication on the majority of electronic payments.

PSD2 went into full effect on 14 September 2019, but due to delays in the implementation, the European Banking Authority allowed for a time extension of the strong customer authentication until 31 December 2020.

The Payment Card Industry (PCI) standard

- The Payment Card Industry (PCI) standard is a set of requirements designed to ensure that **ALL** organizations that store, process, or transmit cardholder data do so in a secure environment.
- Organizations that handle these data need to comply with the standards and are reviewed to check that they do.

Evolution of PCI

PCI Security Standards Council was founded in 2006 by the major card brands:

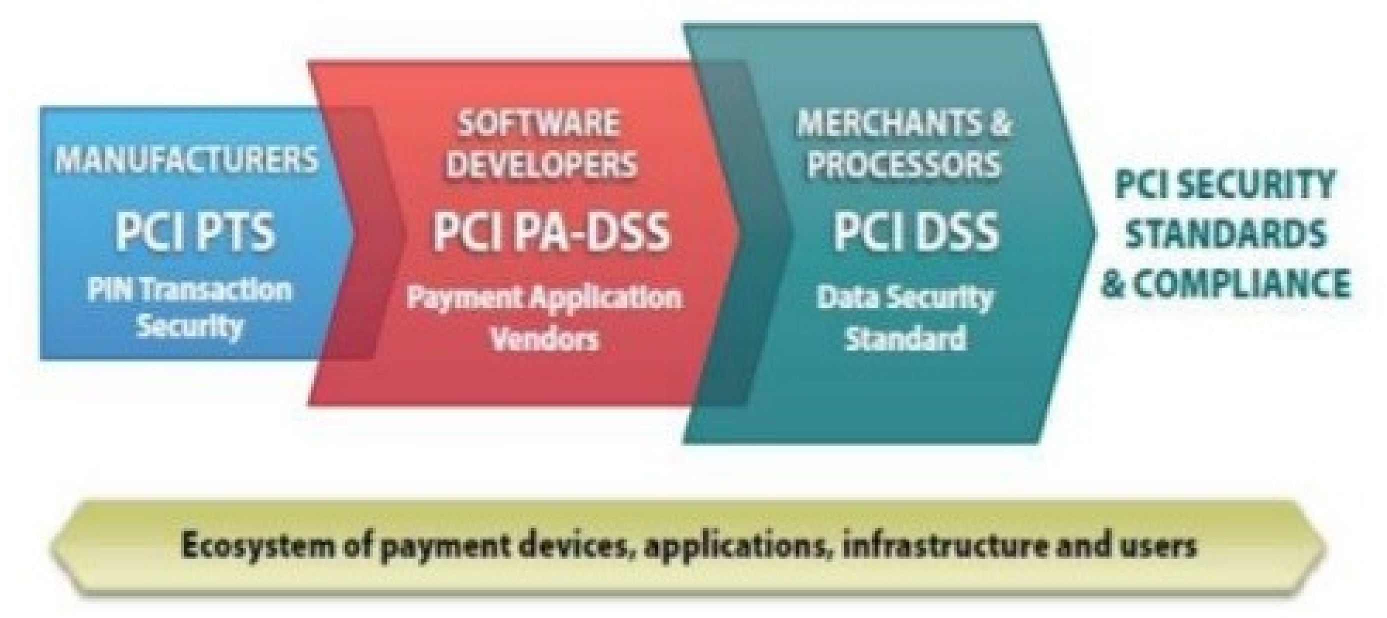
- Visa
- MasterCard
- Amex
- Discover
- JCB

Each card brand has input into the guidance provided by the Council.

Architecture of PCI

PCI Security Standard Council is responsible for the oversight of the PCI Standards, which include guidance relative to the following:

- PCI DSS
- PA-DSS
- PTS


MANUFACTURERS
PCI PTS
PIN Transaction Security
SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors
MERCHANTS & PROCESSORS
PCI DSS
Data Security Standard
PCI SECURITY STANDARDS & COMPLIANCE
Ecosystem of payment devices, applications, infrastructure and users

PCI DSS

- Set of 12 best security practices broken down into 6 categories, as follows:
    1. Build and maintain a secure network
    2. Protect cardholder data
    3. Maintain a vulnerability management program
    4. Implement strong access control measures
    5. Monitor and test networks
    6. Maintain an information security policy

PCI DSS today

- The current active version of PCI DSS is v4.0 (from 31 March 2022)
- Some US states have made parts of PCI into law, but primarily it is an agreement between card companies and dealers
- Many organisations avoid having to live up to the rules by using a Payment Service Provider

Electronic Currency & Its Impact

What is Money?

- Physical or Electronic Tokens or Commodities that can be have the following properties:
  - **Unit of Account → defined value**
  - **Medium of Exchange → acceptability**
  - **Store of Value → non-perishable**

Overview: Early Money

- **Early Intermediary Tokens of Exchange**
  - Commodities or Objects of Perceived Worth
- **Minted Coins** → standardized units of metal
  - Code of Hammurabi: legal debt payment
- **Trade Bills** → credit certificate for production
  - Led to Local Merchant Banks for redemption
- **Goldsmiths** → demand deposits & promissory notes

Beginnings of Modern Money

- **Private Bank Notes**
  - Loans based on deposits on account
  - Beginning of Fractional Reserve Banking (loaning out N times what has been deposited)

- **National Currencies**
  - from Central Reserve Banks
  - backed by Gold or Silver
  - Could be used for general payments

Different Types of Money

- **Private Currency** → free banking
- **Community Currency**→ local acceptability
- **World Currency** → trade reference
  - **Hard Currency** eg. US dollar, Euro and Swiss franc (U.S. dollar enjoys status as the world's foreign reserve currency, the reason it is used in 70% of international trade transactions)
  - **Soft Currency** less solid countries

Private Currency

- **Free Banking → No Central Reserve Bank**
  - Free entry into banking industry
  - Freedom to issue notes, accept deposits, and collect checks for payment
  - Freedom to borrow money on term deposit
  - Freedom to lend money & invest assets
  - **Bank Secrecy Act of 1970**
    - Informal Value Transfer Systems IVTS required to cooperate in Anti-Money Laundering efforts
    - Patriot Act enforcement

Community Currency

- **Ithaca HOURS**
  - Ithaca, NY
  - Around 1995

- **BerkShares**
  - Berkshire, MS
  - 2006-

- **Toronto Dollar**
  - Toronto, Ontario
  - 1998-2013

5
TORONTO
FIVE TORONTO DOLLARS
www.torontodollar.com
10% of every Toronto Dollar purchased supports community groups

World Currency

- Global Trade Reference
  - Gold, British Pound, US Dollar, Euro, Yen
  - Private Complementary Currency efforts
- International Monetary Fund (IMF)
  - Special Drawing Rights (SDR)
  - Supplementary Reserve Assets

Modern Fiat Money

Currency which derives its value from government regulation or law

- World War 1 & end of gold standard
  - Scarcity of gold reserves with enlarging circulation
  - Bank notes no longer redeemable for gold
  - Floating value in exchange market
- Money by Decree of Government
  - Backed by issuers ability to repay debts
  - Susceptible to public distrust
  - Possible uncontrolled inflation or deflation
- In Sweden, the state, via the central bank (Riksbanken), has had a monopoly on issuing notes and coins since 1904 (until 1931 is was backed by gold)

What is Electronic Money?

- **Narrow View** of Term:
  - Tokens of Exchange transacted *Only* electronically
  - Examples: Facebook Gold, Digital Gold Currency, Bitcoin, Terra TRC, and other electronic currencies
- **Broad Usage** of Term includes Both:
  - Electronic Payment Authorization → Credit cards
  - Value Holding Electronic Tokens

Bitcoin

- Created by “Satoshi Nakamoto” – initially an anonymous developer. In 2016 Craig Steven Wright claimed he is behind the pseudonym, but it is still debated if it is correct.
- Debuted in 2009
- Used in peer-to-peer transactions in which participating parties recognize its value
- No central bank or clearing house, no financial regulator, not tied to any currency (or anything else substantial)
- Bitcoin are stored and sent through e-wallets and traded/exchanged through online virtual currency exchanges
- One of many Digital currencies; Ethereum, SwiftCoin, Ripple etc.

Bitcoin mining

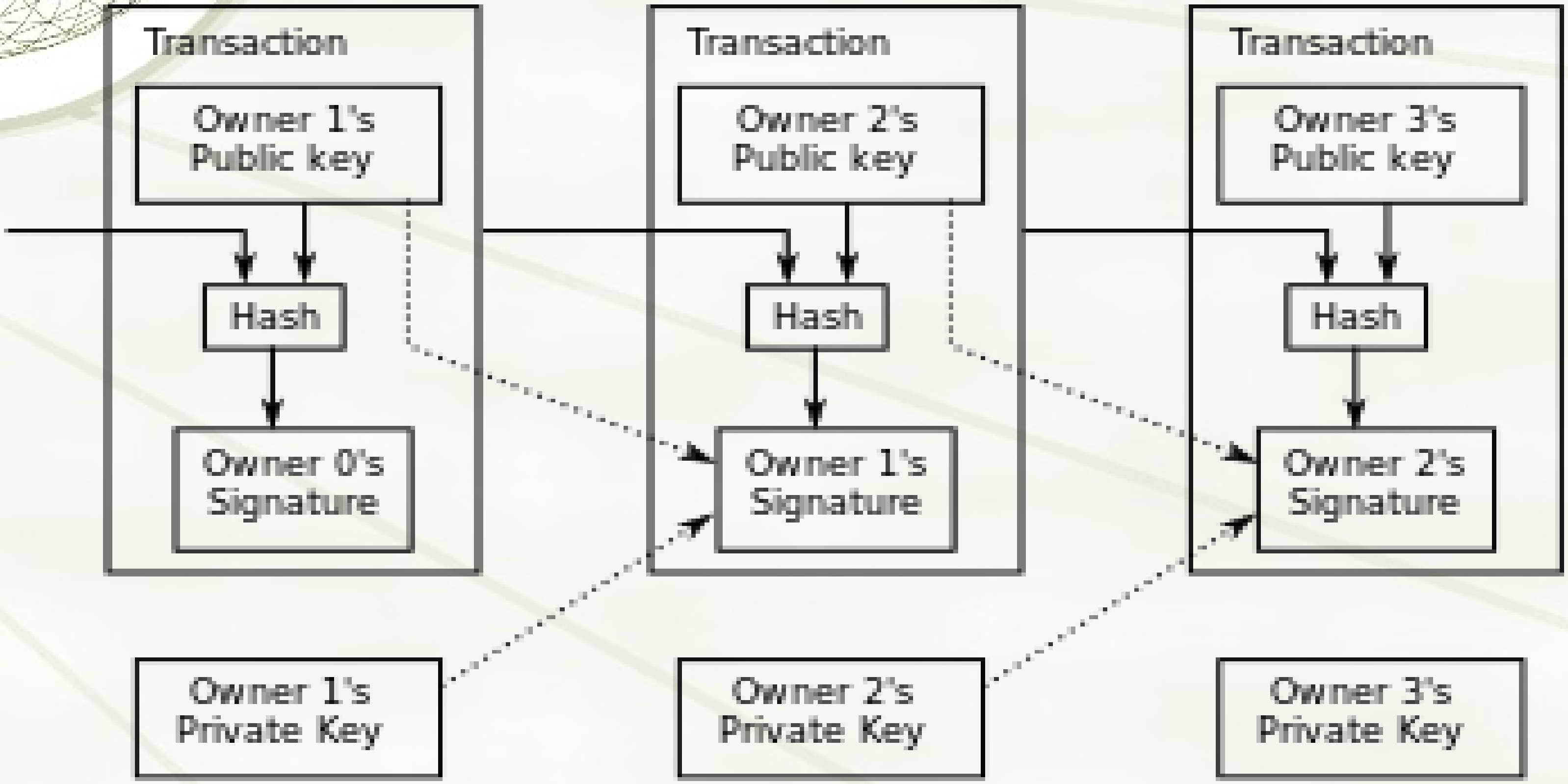
- “Miners” – supply Bitcoin network with computing power needed to maintain the security of the block chain (a distributed technology that acts as Bitcoin’s ledger, keeping track of all transactions)
- Miners are rewarded with “blocks” of issued bitcoins (a “block” currently contains 6.25 bitcoins); this is how currency is issued
- Approximately 18.5 million Bitcoin have been mined (September 2020)
- In total there exist 21 million Bitcoin and it is expected to take around 100 years to mine them all

Reference: https://www.investopedia.com/bitcoin-4689766

Bitcoin and public key cryptography

- A bitcoin address is a cryptographic public key - a human-readable string of numbers and letters around 33 characters in length, beginning with the digit 1 or 3
  - 175tWpb8K1S7NmH4Zx6rewF9WQrcZv245W
- The matching private key is often stored in a digital wallet or mobile device and protected by a password or other means of authentication. Each bitcoin transaction is signed by the private key of the user initiating the transaction.

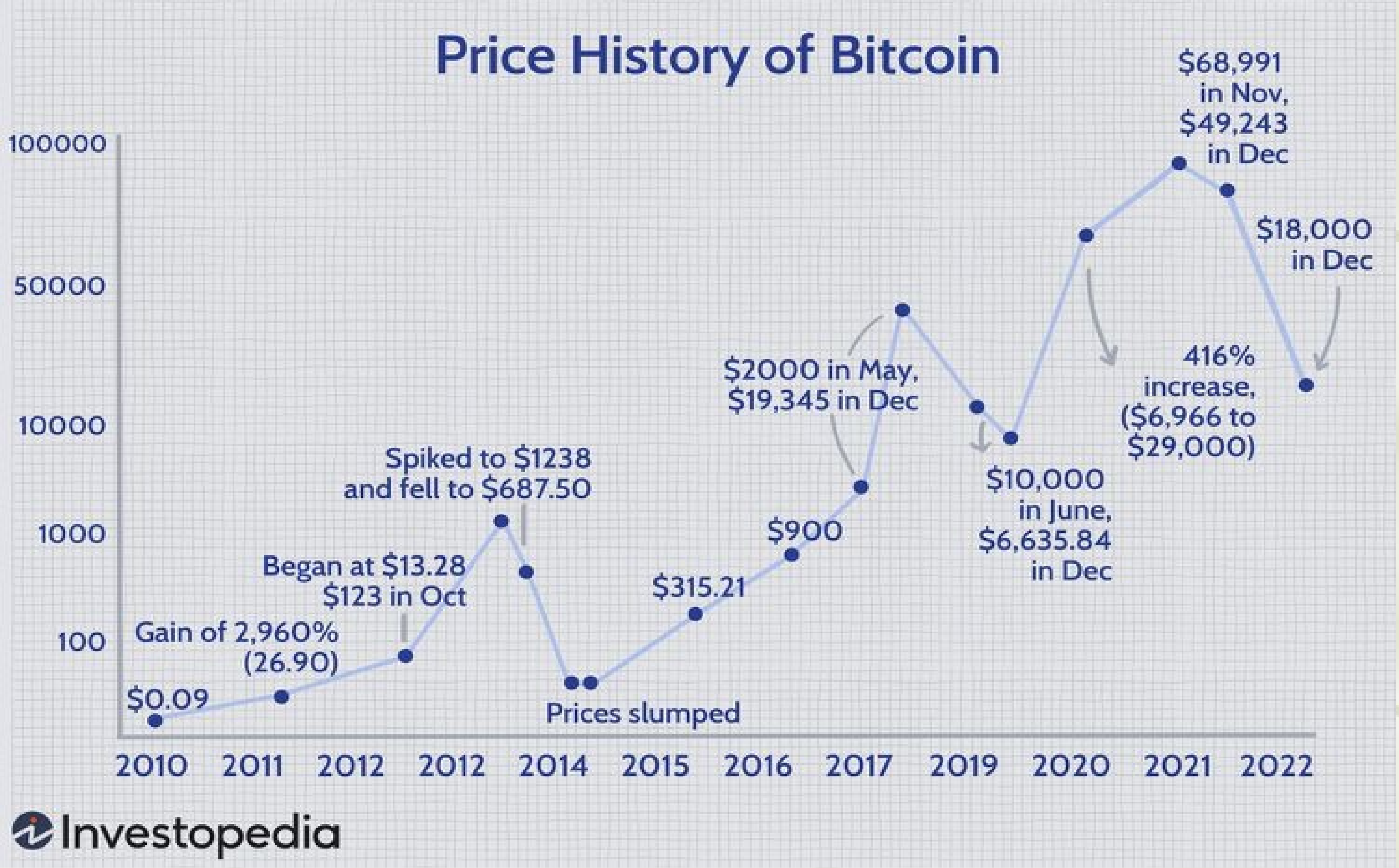
Bitcoin transactions



Bitcoin transactions

- Every single Bitcoin carries the entire history of the transactions it has undergone, and any transfer from one owner to another becomes part of the code
- Bitcoin is stored in such a way that the new owner is the only person allowed to spend it.
- Price of Bitcoin fluctuates wildly. As of 8 May 2023, 1 Bitcoin is worth about $28,176 with is peak value being app. $69,000 (November 2021)

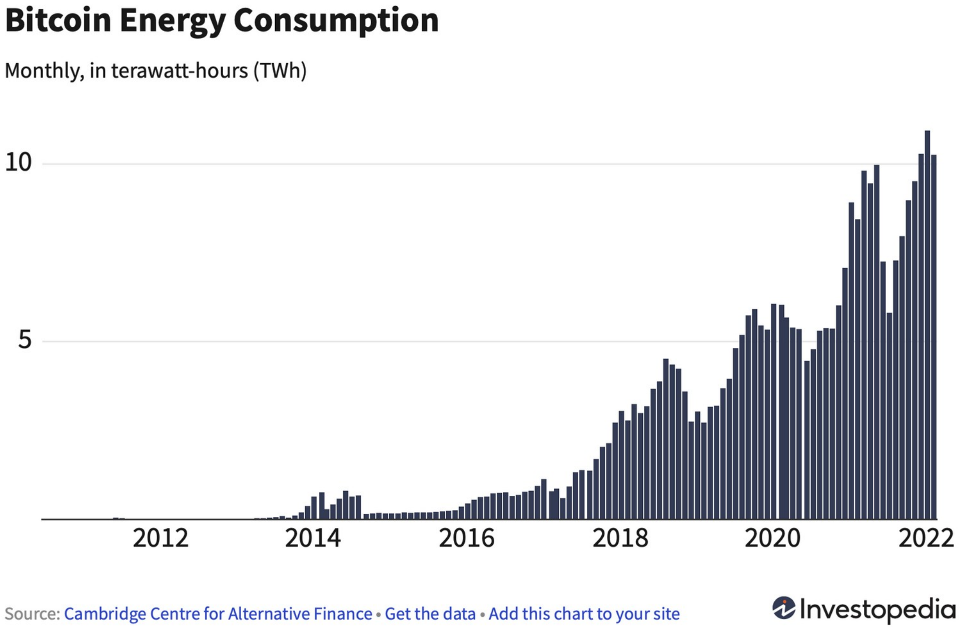
Bitcoin value



Source: https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp#bitcoin-price-history

Bitcoin criticism

- bitcoins have been associated with illegal online activity such as money laundering and ransomware
- bitcoin's volatile exchange rate
- relatively inflexible supply
- high risk of loss
- minimal use in trade
- Lately, also the energy consumption



Bitcoin Energy Consumption

Monthly, in terawatt-hours (TWh)

Source: Cambridge Centre for Alternative Finance • Get the data • Add this chart to your site

For more information

- What is Bitcoin http://www.weusecoins.com/en/

- The truth about Bitcoin http://www.youtube.com/watch?v=w4HGVJjqDVk

Other blockchain systems

- Ethereum is a more recent blockchain system than Bitcoin with an attached crypto currency, ether.
- Ethereum also support other types of application like smart contracts
- Lately similar systems with advantages like faster transaction time have been launched. Examples are EOS and Tron that have gained a high percentage of the market in a short time
- The market is very active and new solutions are offered on a regular rate

e-krona

- Sweden is in the process of replacing or complement its physical banknotes and coins with a digital currency. The Riksbank is investigating digital currency issued by the central bank.
  - The first question is whether e-krona should be booked in accounts or whether the e-krona should be some form of digitally transferable unit that does not need an underlying account structure, roughly like cash.
  - Another important question is whether the Riksbank should issue e-krona directly to the general public or go via the banks
  - Other questions will be addressed like interest rates, should they be positive, negative, or zero?
  - Tests are conducted with different technical solutions but no final decision has been made.

Source: https://www.riksbank.se/en-gb/payments--cash/e-krona/

Mobile payments

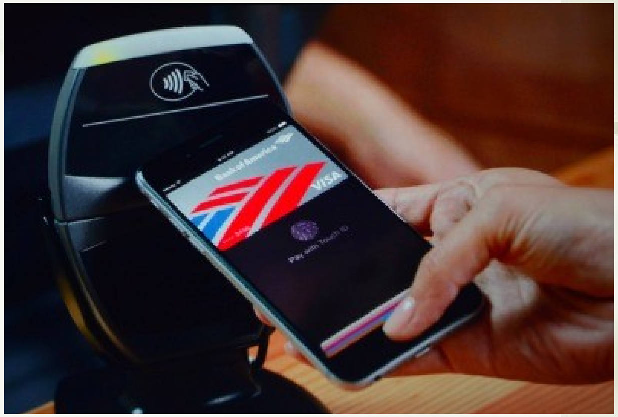
- In recent years using your smartphone as a digital wallet have gained a lot of attention.
- Some announced systems
  - Apple Pay (2014)
  - Google Wallet (2009, re-launched in 2015)
  - Samsung Pay (2015)
  - Android Pay (2015)

Apple Pay

- Apple Pay is a mobile payment and digital wallet service by Apple Inc. that lets users make payments using Apple devices. It was launched in the United States in October 2014 for the iPhone 6 and iPhone 6 Plus, and Apple Watch-compatible devices
- Today (May 2023) available in above 78 countries
- It digitizes and replaces the credit or debit magnetic stripe card card transaction at credit card terminals

Look for this icon at checkout.

Apple Pay Security



- Devices communicate wirelessly (using NFC) with point of sale
- An dedicated chip stores encrypted payment information
- Authorization is done with biometric methods (fingerprint or Face id)
- The service keeps customer payment information private from the retailer and Apple claims that they will not track usage

Samsung Pay

- Introduced in Sweden in March 2017
- Compared to Apple Pay, more types of terminals are supported (even magnetic stripe terminals)
- Except credit cards, also gift cards and customer cards can be digitized
- Security seems to be on the same level as Apple pay

Mobile payments without credit cards

- In many countries services are now established to pay with your phone without involving credit cards
- You use a phone app to move money directly from one bank account to another
- In Sweden we have Swish, in China they have several like WeChat Pay and Alipay

European Mobile Payment Systems Association (EMPSA)

- EMPSA is the name of a organization that is now formed to support mobile payment across Europe. The mobile payment solutions included are, besides Swedish Swish, also Belgian Bancontact Payconing Company, German Bluecode, Finnish and more. In total 17 countries (May 2023)
- In total, the services will unite millions of mobile payment users, more than one million merchant acceptance points and hundreds of European banks
- A stated goal of the collaboration is to enable international mobile payments