Secure E-Commerce

M. H. Sherif, Ph. D.
AT&T

Outline

- Various aspects of e-commerce
  - Technologies, systems and usage
- Electronic payment systems
- Security of electronic payments
  - Network
  - Transaction
  - Payment
- OSI model for cryptographic security
- Key management
- Certification and privilege management

Outline (continued)

- B2B, EDI and XML
- Payment with Bank cards
  - SSL
  - SET
  - C-SET
- Smart Cards
- Micropayments
  - Face-to-face
  - Remote

Some Definitions of Electronic Commerce

- Trade of good and services in which the final order is placed over the Internet (*John C. McCarthy, Forrester Research*)*
- Similar definition for SEMPER (*Secure Electronic Marketplace for Europe)*
- Sharing and maintaining business information and conducting business transactions by means of a telecommunications network (*Vladimir Zwass*)*
- Web-based applications that enable online transactions with business partners, customers, and distribution channels (*Stephen Cho, Cisco*)*
- Electronic information technology to conduct business between trading partners, through Electronic Data Interchange (EDI) or the Internet (*Mentis*)

* IEEE Comm. Magaz. Sept. 1999

Objectives of E-Commerce

- *Increase efficiency and reduce operating costs*
  - more effective communications with existing business partners and customers
  - less dependence on paper-trail
  - less exposure to inventory risks
- Increase revenues of existing product and services
  - discovery of new suppliers or marketing channels
  - improve communications with existing suppliers and channels
  - improved analysis of customer's and channels information for better prediction and scheduling
- Offer new services (on-line distribution of information)

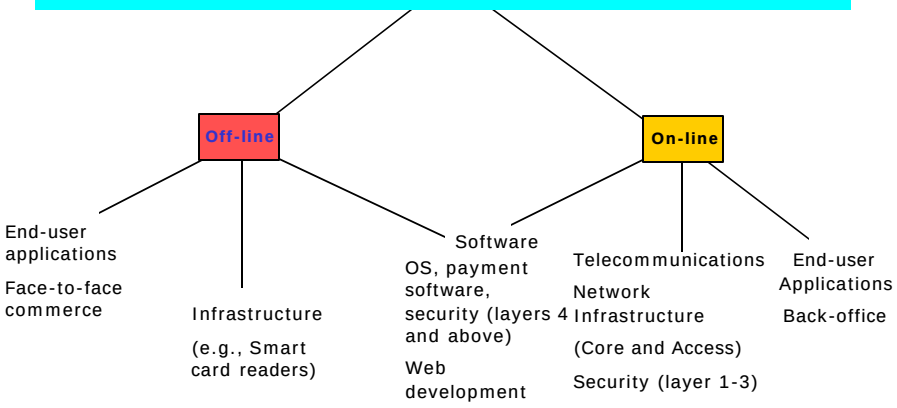
What is sold in Electronic Commerce

- Physical goods
- Virtual goods (software, information, music, books)
- People's profiles (habits or personal details)
  - build contact list of customers
  - sell this list to advertisers
- Non-monetary aspects of the Internet
  - freeware and shareware

Definition Used in This Tutorial

- The set of totally dematerialized relations that economic agents have with each others (French Association for Commerce and Electronic Interchange)
- Covers transactions with Internet, EDI, smart cards, wireless telephony, electronic purses, etc.

Electronic Payments



Components

- Access
  - Modems for dial-up access
  - ADSL
  - ISDN
  - DSL
  - Wireless
- Multiplexing of voice and data
- Server load balancing (including multi-sites)
- Security services
- Servers

Technical Needs for E-Commerce

- Telecommunications Infrastructure needed
- Specialized systems
  - Web servers and other infrastructures, in addition to network servers
  - smart card readers
- System Security
  - Security of on-line transactions including payment
  - Security of computer systems (various attack)
  - Encryption is not security
- System reliability
  - Software development tools are still evolving and changing rapidly
  - Lack of standards may pose incompatibility problems
- Backward compatibility with existing applications and databases

Information Processing

- Storefront
- Payment
- Back-office processing
- Customer Relationship Management (CRM)
  - reduces threats of substitutes and raises barriers to entry through customization and personalization (e.g. electronic fund transfer of checks or electronic bills slows switching from one bank to another)
  - Redefines the role of the sales workforce
- Supply chain management
  - Universal standards lower the barriers to entry and intensify competition within an industry

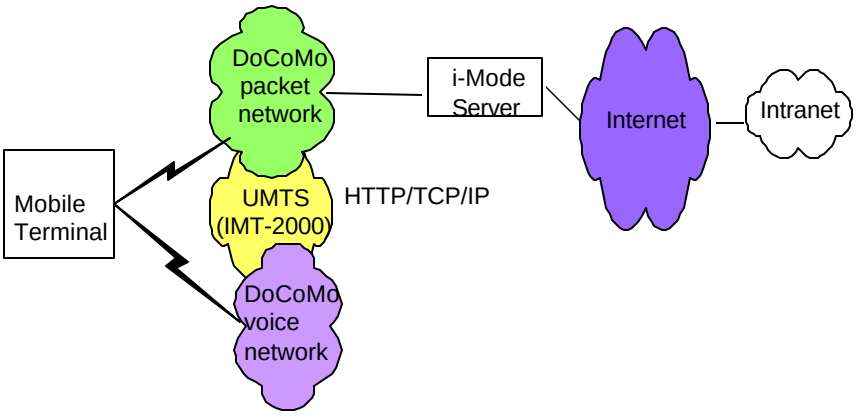
Business-to-Business Electronic Commerce

- Airline reservations, bank clearing and settlement systems, etc.
- Interbank transfers
- Inventory and part replenishments
- Data exchange (automotive, aerospace, airline reservations)
- Brokerage and insurance

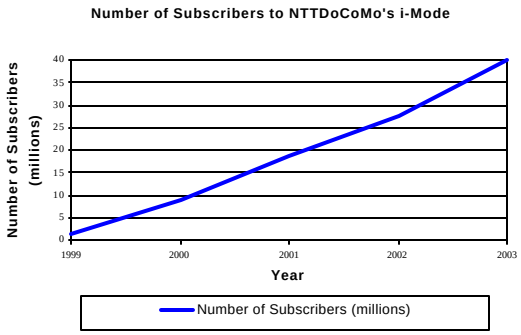
Business-to-Consumer Transactions

- Purchase of goods and services
- Electronic bill presentment
- Games and gambling
- Prepayment cards (telephone, electricity, parking, universities, military bases, Olympic villages, etc.)
- In 2000 and 2001 12.5% to 13% of holiday purchases are from on-line sites. This is equivalent to $13.8 B. Full year 2001 is estimated at $32.2 B (FT, Jan 8, 2002, p.15). However, traffic to U.S site increased by 50% in 2001!
- Wireless services and geolocation

i-Mode Network Architecture

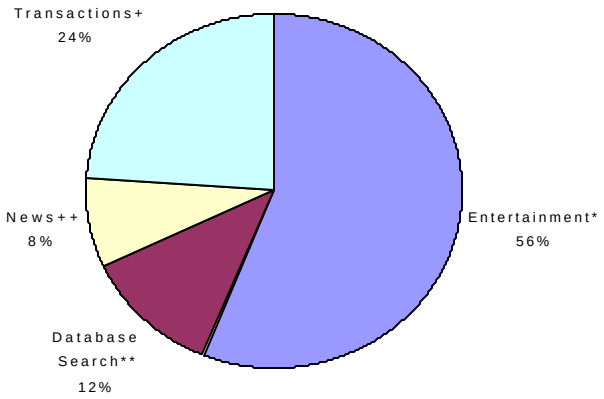


Number of Subscribers to NTT DoCoMo's i-Mode



Source: Meridien Research, NTTDoCoMo

Breakdown of i-Mode Services

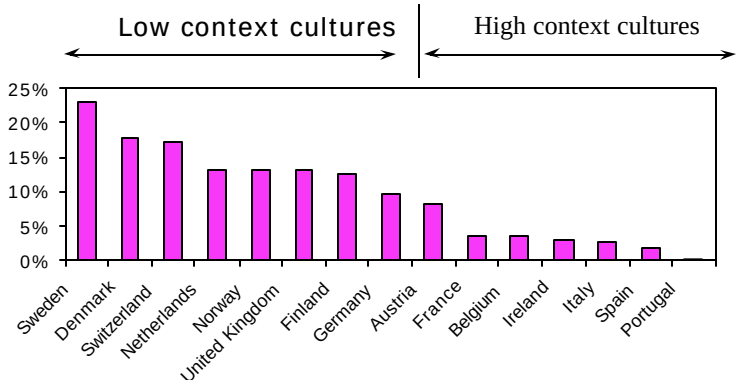


Source: Meridien Research, NTTDoCoMo

Limitations

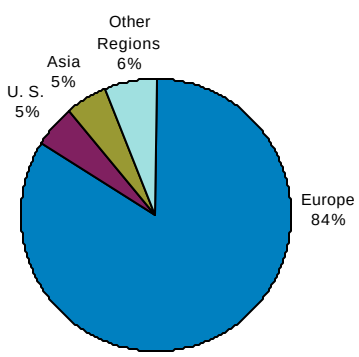
- Technological diffusion
  - Telephone access (50% of the world population has no access to a telephone line)
  - Home penetration of PCs
  - Internet
  - Mobile infrastructure
  - Smart cards
- Dot.com collapse
- Failures of Enron, Marconi, etc.

Internet Usage in Western Europe

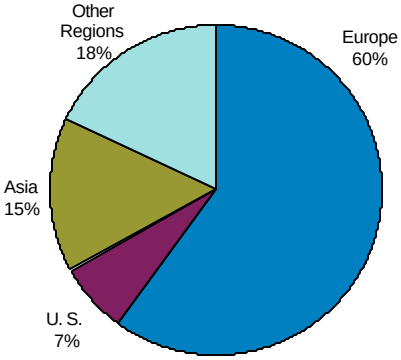


Smart Card Utilization

Source: Celent Communications (Red Herring, Jan. 2002, p. 72

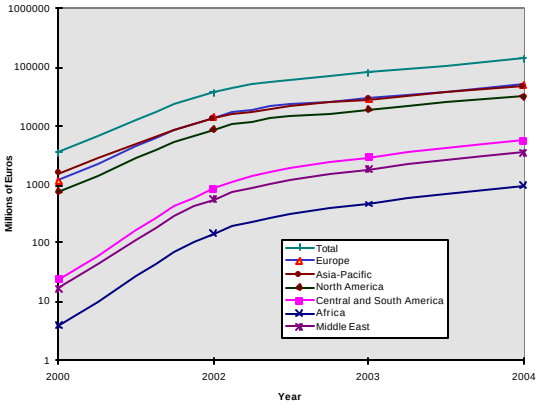


2001: $233 million



2004: $370 million

World-Wide Income from m-Commerce

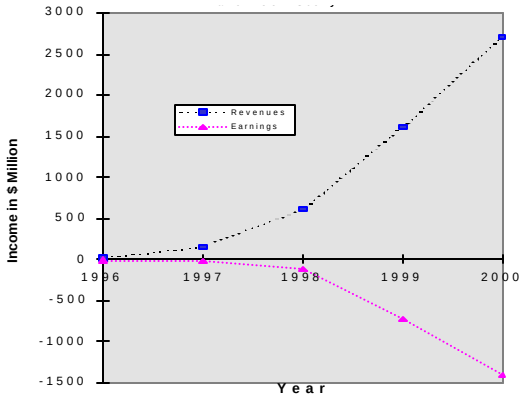


Source: *Ovum*

Obstacles to m-Commerce in North-America

- US is more oriented to PC communications.
- Cellular phone penetration in the US is about 50%.
- Fragmented market:
  - Most mobile phones are still analog (cannot support any financial transaction activity)
  - Multiple terminals, including PDAs and pagers
  - Multiple digital standards
    - CDMA: (IS-95) Sprint
    - TDMA: AT&T Wireless
    - GSM: VoiceStream, Cingular, AT&T Wireless
- Limited rules for free distribution of music

Amazon Story



Other Limitations on E-Commerce

- Cost
  - Complexity of information infrastructure
  - Expenses of maintenance and quality assurance
  - Outsourcing needs to be managed
- Trust
  - Customers do not trust an unknown faceless seller, paperless transactions, and electronic money. So switching from a physical to a virtual store may be difficult.
  - Many unresolved legal issues on a global basis (e.g., lack of consumer protection or privacy protection)

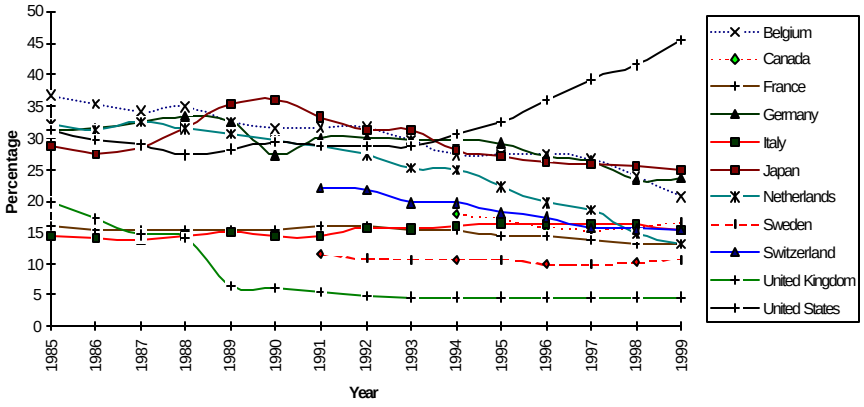
Types of Monies

- Fiduciary money (coins and notes issued by the Central Bank)
- Scriptural money
  - created by a bank
  - a merchant is free to accept or reject
- Private money
  - Tokens
  - Stocks and shares

Instruments of Payment

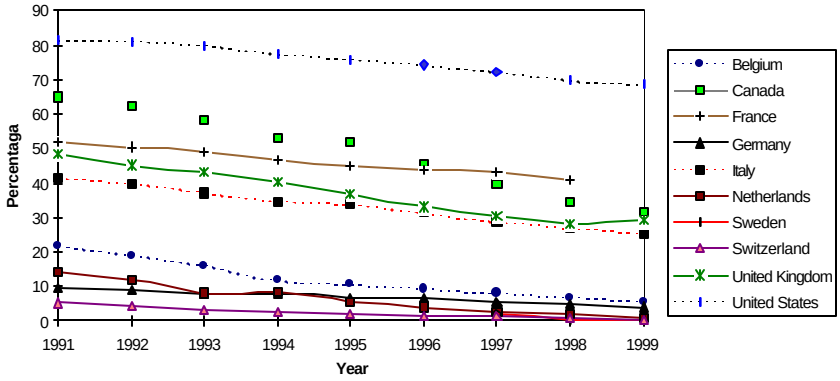
- Payment instruments are used to transfer the power of money from one economic agent to another - Some have a legal status and some are banking inventions
- Cash
  - Checks
  - Credit transfer
  - Direct debit
  - Interbank transfers
  - Bills of exchanges
  - Payment card

Patterns of Cash Usage in percentage of the M1 aggregate



Patterns of Money Flow

(Percentage of checks in the volume of scriptural transactions)

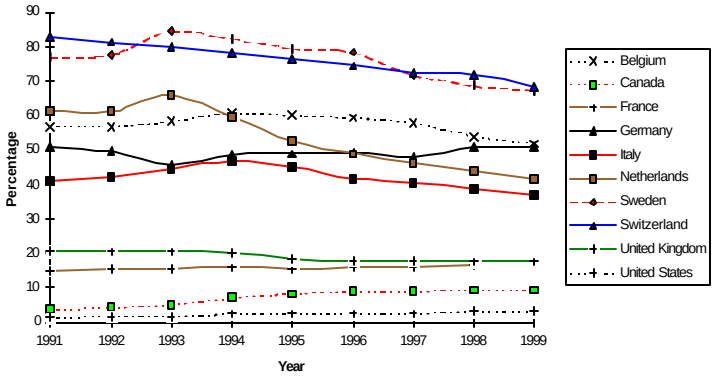


In 2001, the proportion of check in the US went down to 60% (Source: Federal Reserve)

Patterns of Money Flow

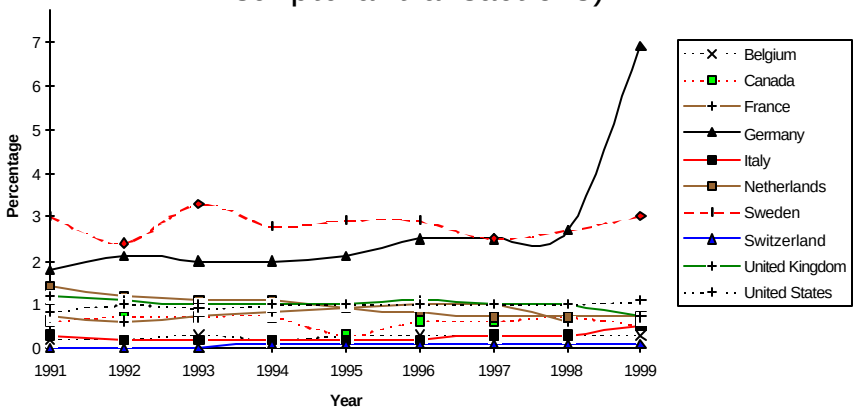
(Percentage of credit transfers in the volume of scriptural transactions)

Since 1/1/99, all payments by the U.S. federal government use credit transfers except for tax refunds



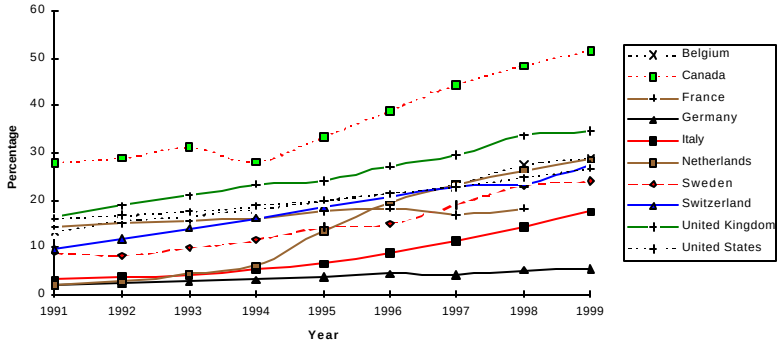
Patterns of Money Flow

(Percentage of debit transfers in the volume of scriptural transactions)

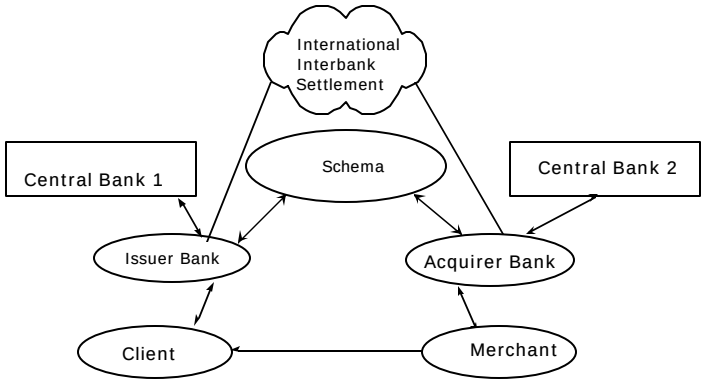


Pattern of Money Flow

(Volume of bank card in scriptural transactions)



Financial Networks



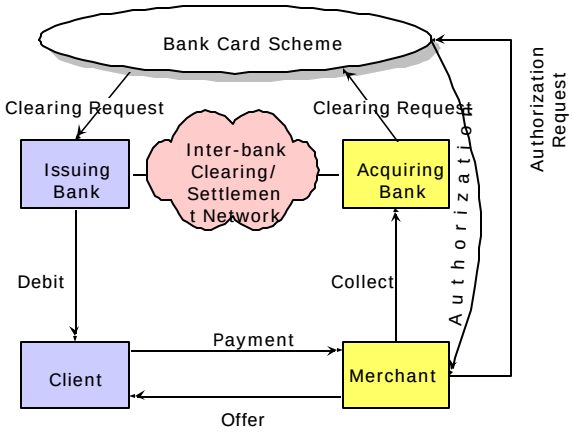
Clearing and Settlement

- Clearing & Settlement refers to the process where banks settle their accounts by exchanging money.
- All bank representatives usually meet every working day in a special *clearing house* and
  - Compare their respective credits in various financial instruments
  - Settle the account by exchanging money
- In electronic Clearing & Settlement, this process is done over computer networks.

Classification of Settlement Networks

- Nature of the processing
  - large value systems
  - mass systems (many transactions of relatively small value)
- Ownership and management of the network
  - public network owned by the central bank
  - private network owned by members of a group of banks
  - private network leased to the banks on a use basis
- The way the settlement is done
  - real-time gross settlement (the same day)
  - netting (consolidation of various transactions to avoid paying settlement charges)

Exchanges during Bank Card Transactions



Emerging Payment Types - Dematerialized Monies

- Electronic money
  - fiduciary money stored in electronic forms
- Virtual money
  - fiduciary money
  - Token (Jeton)
- Digital Money: value stored in the form of algorithms
- Private money (stock options and shares)
  - Cisco acquisitions
  - Zhone Technologies, Inc. with the City of Oakland, CA

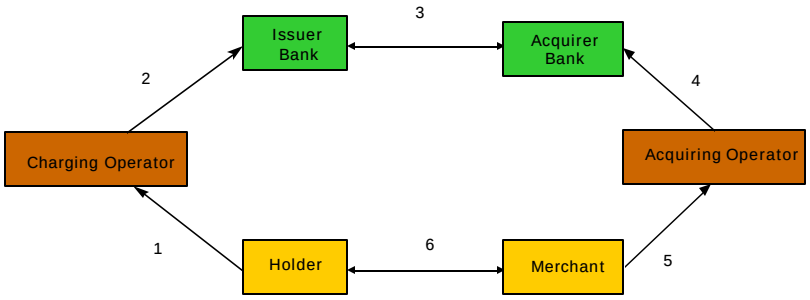
Electronic purses and electronic jeton (token) holders

- Electronic Money within physical support
  - Electronic Purses (Mondex)
  - Electronic Token (Jeton) Holders (Telephone Cards)
- Virtual Money stored in software programs
  - Virtual Purses (Odysseo)
  - Virtual Jeton Holders (Millicent)

Comparison of Money

Type of Money	Nature of Money	Support (the container)	Value Store	Value Representation	Mode of Payment	Means of Payments (Instrument)
Fiduciary	Concrete, material	Paper, piece of metal	Safe, wallet, purse	Bank notes, coins	Face-to-face transaction	Bank notes, coins
Scriptural	Immaterial (an account maintained by a credit institution)	Magnetic, optical, electronic Integrated circuit card Computer	Account maintained by a credit institution Electronic purse Virtual purse (memory allocated by an intermediary	Numerical value	Remote, face-to-face (retail automatic machines)	Check, debit card, credit card, credit transfer Electronic fund transfer

Flows in a Transaction with Protocols for Dematerialized Monies



- charging and discharging of the dematerialized money
- purchasing and payment protocols
- verification protocols (on line, off line, semi-online)
- protocols for collection, acquisition and clearance
- peer-to-peer transfer protocol

Transactional Properties of Dematerialized Currencies

- Atomicity
- Consistency
- Isolation (no interference among transactions)
- Durability (resilience to errors)
- Anonymity (not always)
- Non-traceability: anonymity + two payments by the same person cannot be linked

Security Requirements of Charging Protocols

- The protocols must resist attacks from outside the system:
  - Must resist misappropriation by any one of the participants
  - A 3rd-party non-participant must not be able to intercept the message to manipulate the content, modify orders, or resend valid but old messages.
  - Must resist false charges such as
    - Attributing the charge to a client other than the one identified
    - Attributing an amount different from the requested one
    - Repaying a previously authenticated charge
    - Repudiating a previously correctly executed charge
- Must be robust to return to previous state if there is an error.

Anonymity

- Anonymous plastic support
- Anonymous recharging transaction
- Anonymous payment transaction (cannot be tied to the holder's bank account)
- Anonymity for face-to-face commerce
- Anonymity for remote transactions
- Use of "mix networks" to achieve anonymity and untraceability of the sender (David Chaum)

Basic Idea of Mixes

If the sender wants to establish anonymity, it chooses n mixes (M_1,.., M_N) with addresses A_{M1}, ..., A_{MN} and encrypts the message using the public keys of the successive mixes as well as the end receiver after adding a random blinding factor to prevent replay attacks as follows:

$N_1 = PK_{M1} (A_{M2}, k_1, N_2)$

$N_2 = PK_{M2} (A_{M3}, k_2, N_3)$

...

$N_{n+1} = PK_R(N)$

Extension to Bilateral Anonymous Communications

- Receiver repeats the same steps
- For Web publishing with client and servers remain anonymous
  - use pseudonyms
  - generate session keys for the pseudonym
  - exchange the keys through another channel with dynamically generated addresses to prevent replay attacks
- T. Demuth, Establishing bilateral anonymous communication in open networks, IFIP TC11 17th International Conference on Information Security (SEC 2002)

E-Commerce Security

- Security is an important consideration in EC:
  - Buyers are concerned about sending their private information on the Internet.
  - Sellers are concerned about their systems being compromised and their data being stolen.
- Security of the Internet is an afterthought
- In 1999, half of card payment disputes and frauds in the EU are related to Internet transactions (1% of the turn over) - FT 4/12/99

Security of Electronic Exchanges

- Network Protection
  - Access
  - Routing
  - Service continuity
- Protection of individual transactions
- Protection of the merchandise:
  - physical goods
  - virtual goods: protection of the intellectual property
- Protection of the records
  - legal requirements
  - privacy

Network Security

- Aspects
  - Physical connectivity -> sabotage or outages
  - Availability -> Denial of service attacks
  - Correct routing -> address spoofing
- Encryption is not always necessary (Minitel/i-Mode, First Virtual, micropayments, etc.)
- Encryption is more important in open or decentralized networks co-managed by distinct administrative entities

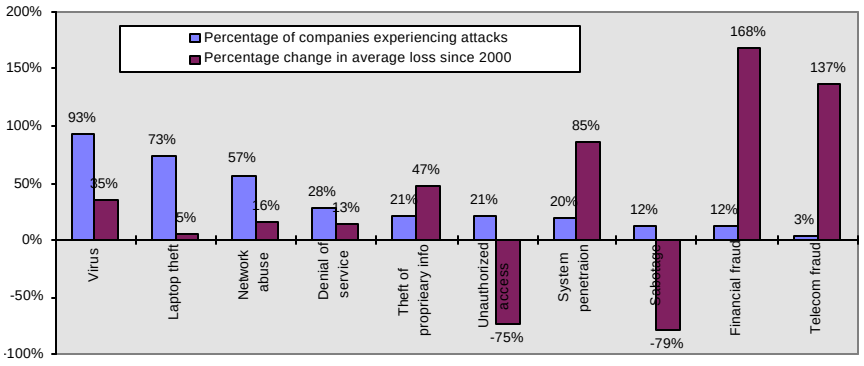
Security of a Transaction

- Verification of person's identity (address) and credit worthiness
- Threshold for calling the authorization server
- Ceiling for allowed expenses or withdrawals
- Fraud detection and management
  - surveillance of activities at the points of sale
  - surveillance of short-term events
  - surveillance of long-term events

Security of Payment Mechanisms

- Security depends on
  - nature of money
  - instrument of payment
  - legal requirements
  - value,
  - support (container) of the value
  - location of the value store
- Architecture of the payment system must reflect the security needs

Cost of Security Breaches



Source: Computer Security Institute - Survey of 500 correspondents

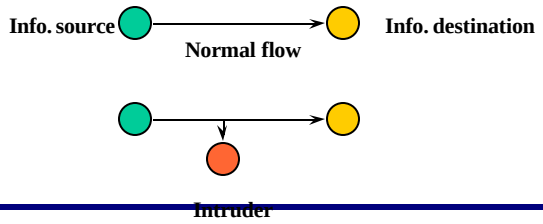
Note: While 344 acknowledged financial losses, only 186 could quantify those losses

Threats and Attacks (X.509 and X.800)

- Passive Attacks (Sniffing or eavesdropping)
  - Interception of identity
  - Data interception
  - Data analysis
- Active Attacks (involve some data alteration or falsification)
  - Masquerading
  - Manipulation of content
- Repudiation of participation

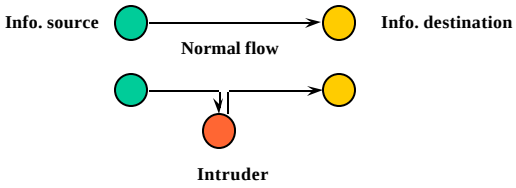
Passive Attacks

- Intruder logs on to the network and tries to gather information by monitoring and copying data transmissions.
- Passive attacks are difficult to detect since they do not involve any alteration of the data.



Active Attacks

- Masquerade and message modification
  - Intruder obtains the user ID and password of a legitimate user and logs on to the network to obtain additional privileges or to modify the data being transmitted.
  - Denial of service (DoS)
  - Rendering a server unavailable to others
  - DoS attacks can be done by flooding a server with multiple bogus connection requests.



OSI Model For Cryptographic Security

- Security Services
  - Confidentiality
  - Identification
  - Authentication
  - Non-repudiation
- For selective protection:
  - network layer

Security Services

- Confidentiality
  - Symmetric cryptography
  - Public key cryptography (for small messages, e.g, symmetric key)
- Data Integrity (through a "fingerprint" or "signature" of the message)
- Blind-signature is a special type of signature of a message without knowing the content (used for digital money)

Security Mechanisms

- Encryption
  - to ensure confidentiality
- Authentication
  - Verification of user's identity
  - Access control lists for authorized access to network resources
  - Dynamic password assignment
- Message Authentication
- Non repudiation
  - Digital signature, time stamping, etc.

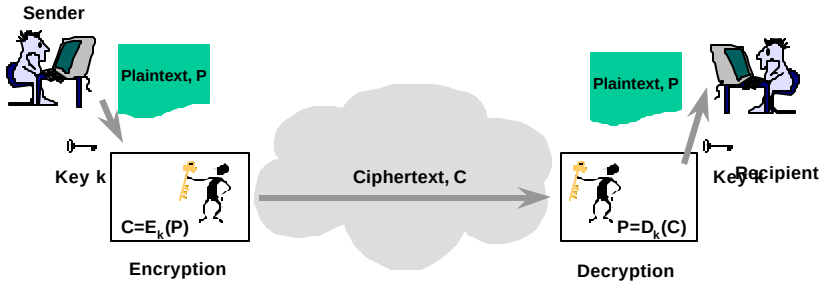
OSI Model for Cryptographic Services

- Physical and Link layers: All traffic is protected. Only confidentiality can be assured (frequency hopping, spread spectrum, etc.)
- Network Layer: bulk protection from one end system to another: Firewalls, IPSEC (RFC 1825)-SKIP-S/WAN-FreeS/WAN)
- Transport Layer: when network is not reliable (SSL) or for protection after a fault
- Application layer (high granularity and non repudiation)
  - SET for Bank Cards
  - EDI Security

Secret-Key (or Symmetric) Encryption

- The same key is used to encrypt and decrypt messages.
- The two sides must coordinate to send an encrypted message, and key security is essential.
- Many algorithms exist:
  - Data Encryption Standard (DES)
  - RC2, RC4, RC5 (from RSA Data Security)
  - IDEA (International Data Encryption Algorithm)
  - AES (Advanced Encryption Standard)

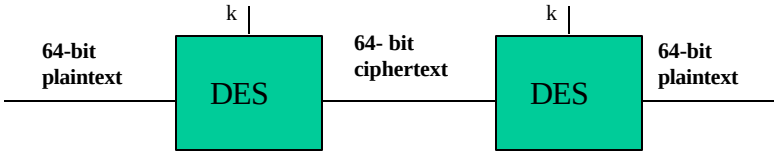
Secret-Key (or Symmetric) Encryption



© M. H. Sherif ISCC 2002 - Sicily, Italy, 4 July 2002

Data Encryption Standard (DES)

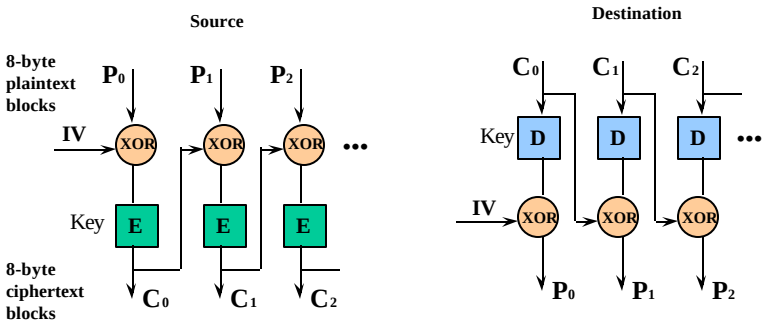
- DES is the most widely used symmetric encryption algorithm.
- DES blocks are 64 bits; the key is 56 bits.
- DES was adopted by NBS (now NIST) in 1977 (FIPS PUB 81) and updated in 1993, for non-military data communication (ANSI X3.92)
- Applying 64-bit ciphertext to a DES block with the same key recovers the 64-bit plaintext.



DES Chaining

- Electronic Codebook Mode (ECB) is susceptible to replay attacks
- DES chaining (Cipher Block Chaining or CBC) breaks the direct relationship between ciphertext and plaintext blocks
- CBC used for non-real time encryption and to calculate message authentication codes (MAC)

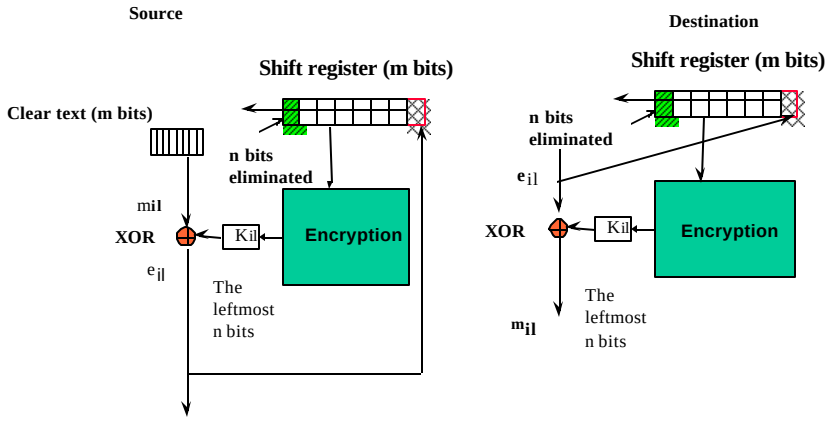
DES Chaining - CBC Mode



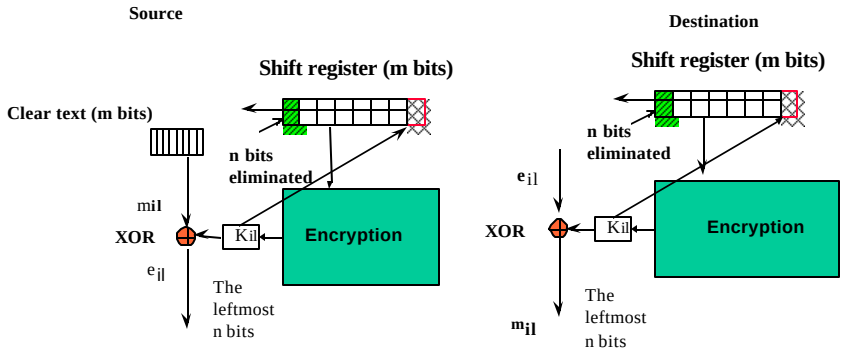
Other DES Chaining Modes

- Cipher feed-back mode (CFB)
  - Encryption of a block of m bits is done in sub-blocks of n bits
  - A new sub-block is combined with the encrypted bits before encryption
  - Used for MAC calculation
- Output feedback mode (OFB)
  - Similar to the CFB but the bits used in the computation are not transmitted
  - Useful in case of transmission errors
  - A mechanism for resynchronization is needed

DES Chaining - CFB Mode



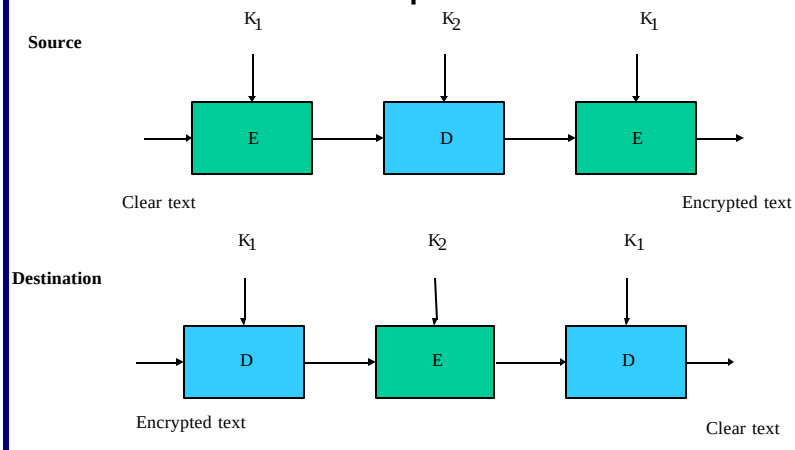
DES Chaining- OFB Mode



Extending DES Useful Life

- DES with 56-bit key is considered insecure (8-byte blocks can be switched).
- Triple DES (3DES) is a 1999 NIST standard for Point-to-Point Protocol (PPP):
  - Runs DES three consecutive times using a different key each time.

Triple DES



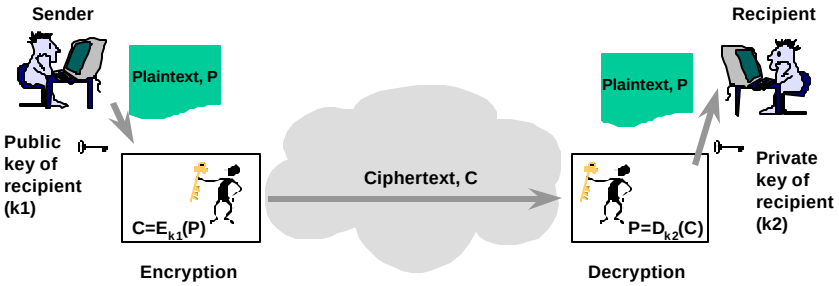
AES (Advanced Encryption System)

- New Federal standard (2001)
- AES offers better security than DES
  - Uses 128-bit secret key; can also use 192-bit and 256-bit keys if necessary
  - Based on Rijndael algorithm which uses a lot of parallelism, making efficient use of processor resources
  - Can be implemented efficiently on smart cards

Public-Key (or Asymmetric) Encryption

- In Public Key encryption, each user has two keys: a *public key k1* and a *private key k2*
- The pubic key is available to anyone but the private key remains a secret know to the user only
- Public-key encryption reduces the problem of key distribution among pairs of communicants

Confidentiality with Public-Key Cryptography



Public Key Cryptography

- RSA (ISO/IEC 9796): patent expired on 9/20/2000
- DSA (FIPS 186)
- PKCS (a series of business specifications based on RSA)
- PGP (RFC 1991)
  - Public key exchange with RSA and MD5 hashing
  - Data compression with ZIP
  - Message encryption with IDEA
  - ASCII "armor" to protect binary messages through the Internet

Characteristics of Public-Key Algorithms

- Algorithms require a trap-door one-way function:
  - a function whose inverse is extremely difficult to compute unless certain “trap-door” information is known.
  - Systems based on the discrete logarithm problem
    - Diffie-Helman
    - El-Gamal
  - Systems based on the factoring problem
    - Rivest, Shamir and Adleman (RSA)
  - Systems based on the elliptic logarithm problem
- Computational load much larger than for symmetric algorithms

RSA Algorithm

Generate two large distinct random prime numbers
p and q

Compute $N = p \times q$. and $\phi(N) = (p - 1)(q - 1)$

Select a random integer e, $1 < e < \phi$

such that $\gcd(e, \phi) = 1$

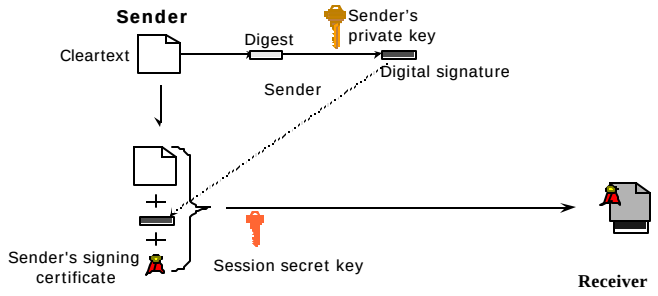
There is a unique integer d such that

$ed \equiv 1 \pmod{\phi}$

Public key is (N, e), private key is d

Suggested values for e in practice are 3 or $2^{16} + 1$

Combination of Integrity and Confidentiality with Public Key and Symmetric Key Encryptions



Elliptic Curve Discrete Logarithm

- Require shorter keys than RSA to achieve the same level of security
- A 160-bit elliptic curve key is roughly equivalent to a 1024-bit RSA key
- Elliptic Curve Digital Signature Algorithm (ECDSA) is standardized ANSI X9.62 and IEEE P1363

Notes on RSA

- A public key of 512 bits is no longer safe (was factored by a team of scientists of the National Research Institute of Mathematics and Computer Science in the Netherlands in 1999)
- Adi Shamir designed a factoring device named TWINKLE to break a 512-bit key within a few days
- For short term security, keys should be at least 768 bits
- For long term security (5 -10 years), 1024 bits should be used
- It is believed that a key of 2048 bits, would last about 15 years
- There are many computational tricks to reduce the decoding time if the keys are available.

PKCS

- A set of business standards developed by RSA Laboratories in collaboration with others
- Describe the mechanisms for data encryption, message formats, key formats, etc.
- Described in IETF documents but not standardized because they use proprietary algorithms

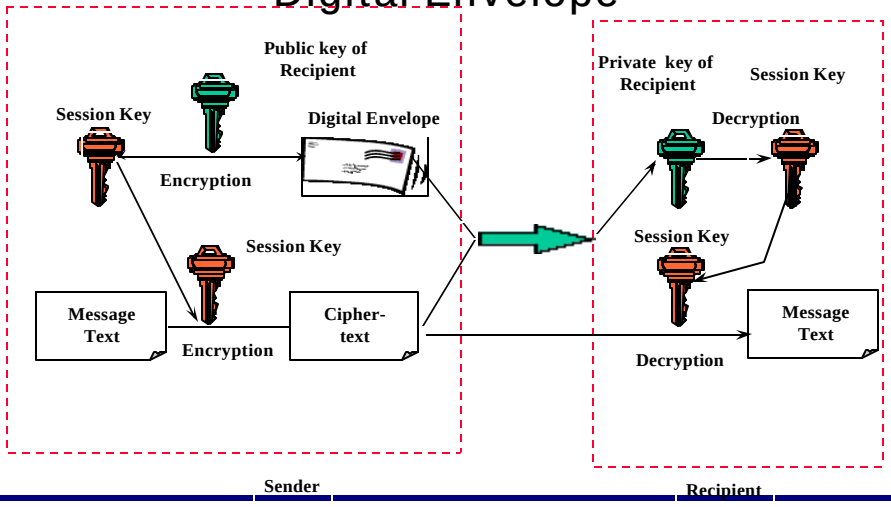
PGP (Pretty Good Privacy)

- Uses RSA with MD5 Hashing
- Data Compression with ZIP
- Message Encryption with IDEA
- Not suitable for large scale applications

Digital Envelope

- Public-key algorithms are slower than secret-key algorithms because of their longer keys.
- A combination of secret and public-key encryption, known as *Digital Envelope*, is used in real-world applications:
  - Public-key encryption is used to create and send a symmetric key to the message recipient.
  - The symmetric key is then used for symmetrical encryption

Digital Envelope



Hash Functions

- One-way function used to calculate the fingerprint or hash or message digest h=H(M)
- It has the following characteristics
  - Given M, h can be easily computed
  - Given h, it is very difficult to find M (impossibility of inversion)
  - Absence of collisions (the probability of obtaining the same value h using two different messages is very small)
  - A small difference between the two messages gives a large difference between the finger prints

Hash Functions in Electronic Commerce

- AR/DFP (German Banks)
- DSMR (ISO/IEC 9796)
- MCCP (ISO/IEC 1116-2)
- MD4 (RFC 1320)
- MD5 (RFC 1321) a 128-bit hash message designed by Rivest
- NVB7.1, NVBAK (Dutch Banking Standard)
- RIPEMD-128,-160 (ISO/IEC 10118-3)
- SHA, SHA-1 (FIPS 180-1, ISO/IEC 10118-3) (Secure Hash Algorithm 1) produces a 160-bit hash for use with the Digital Signature Standard (DSS). Designed by NIST

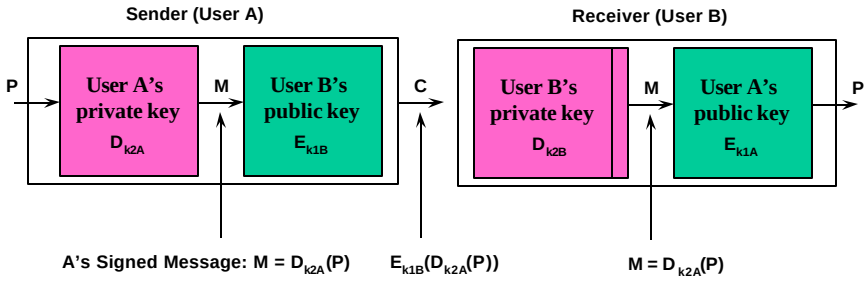
Data Integrity

- Verify that the message content has not been modified, intentionally or accidentally during transmission
- A sequence of bits that depends on the content of the message ("finger print") travels with the message to be protected
- At the destination, the receiver recalculates the value and compares it with what is received. Any difference indicates tampering
- Blind-signature is a special type of signature of a message without knowing the content (used for digital money)

Integrity Verification

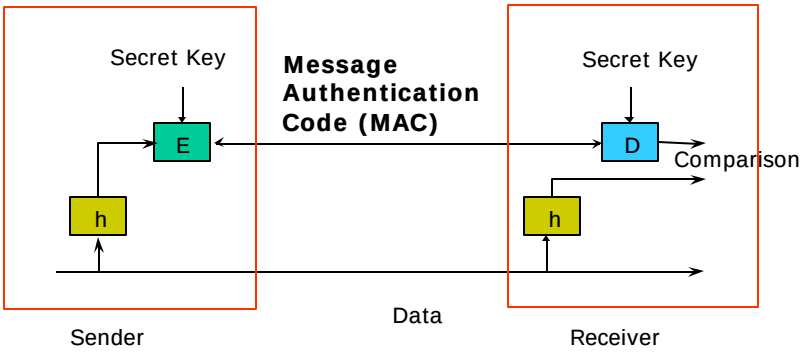
- Symmetric cryptography and hash functions
  - Hash function --> Message Authentication Code (MAC) or Hashed Message Authentication Code (HMAC)
  - Encrypt the MAC with a symmetric algorithm
  - This is called a "signature"
- The legitimate recipient can verify the integrity; others cannot
- With public key cryptography, if the MAC is encrypted with the sender's private key; anyone having the public key can verify the integrity

Verification of Integrity with Public Key



A more common approach is to use the fingerprint (hash) of the message because this reduces the computational load

Verification of Integrity with Symmetric Cryptography



Identification and Authentication

- In one step:
  - with symmetric cryptography
  - with biometric recognition
- In two steps with public key cryptography
- In public cryptography, requires a certification infrastructure

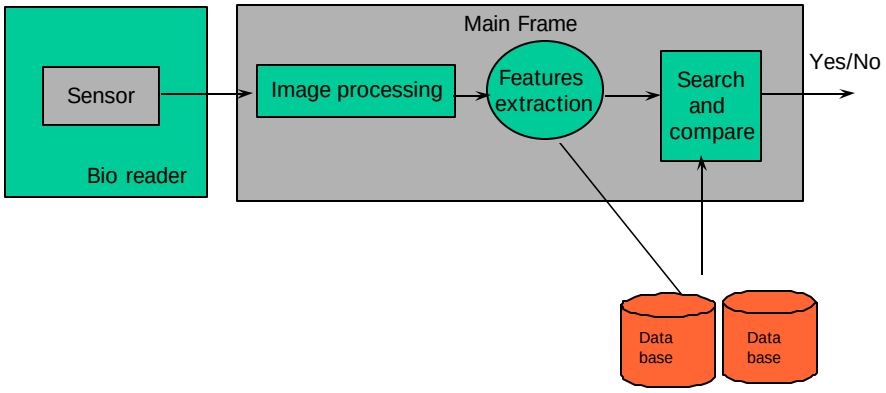
Biometric Identification

- Identification systems
  - centralized data base
  - used with badge, password
- Verification system
  - distributed architecture
  - compare actual data with data stored on a card
  - verify privileges

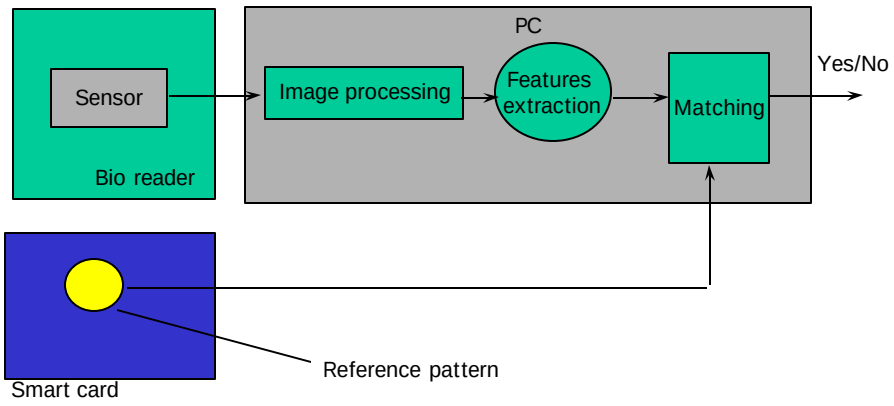
Classification of Biometric Systems

- Characteristics used (acquired vs. innate)
- Identification systems
  - biometric data matches an entry in a database
  - supplement another identifier (password, badge, etc.)
- Verification systems
  - biometric data match what is stored in user credentials (e.g., a smart cart) to verify access privileges

Biometrics Framework for Identification



Biometrics Framework for Verification



Applications and Mode of Operations

- Applications:
  - Face-to-face applications
    - Secure access to physical areas
    - Check cashing
    - Identification of bodies
  - Remote
    - Secure access to networks
    - Telework (telecommuting)
    - Mobile telephony
    - Electronic co
- Mode of operation (on-line, off-line, semi-online)
    - mmerce on the internet

Measures of Accuracy

- Identification systems
  - rate of mix-up of identities
  - percent rejects of authorized identities
- Verification systems
  - rate of false rejects
  - rate of false acceptances

Acquired Biometrics

- Handwritten signature
- Voice
- Keystroke dynamics
- Gait

Innate Biometrics

- Photo image
- Fingerprint
- Iris scan
- Retina
- Dental imprints
- Shape of the hand, the ear, etc.
- DNA

Voice Systems

- Speaker identification vs. speaker verification
- Size of voice prints 1 - 70 K octets depending on algorithm and duration
- Performance depends on ambient noise, network conditions, etc
  - AT&T's text-to-speech algorithm sounds human
  - Bacob and Keyware technologies for electronic commerce (by phone) http://www.keywareusa.com)
  - Motorola/Trintech for mobile commerce
  - ITU SG16: distributed speech recognition and distributed speaker verification systems

Manual Signature Recognition

- Static by comparing to a stored signature
- Dynamic (using a special stylus and pad) to analyze movement dynamics (speed, acceleration, pressure, etc.)
- http://www.wacom.com
- FSTC has a project for signature recognition on checks
- Relatively large rate of false rejects

Keyboard Recognition

- Characteristics of keyboard typing
- Net Nanny Software (http://www.biopassword.com)
- Reference contains at least 8 characters and training requires 8 repetitions.
- Verification requires 15 trials.

Retinal Recognition

- Configuration of blood vessels in the eye
- Descriptor's size 35 octets
- Secure access (military, high security prisons, etc.)
- Enrollment in 60 s but requires an invasive exam
- Verification time is about 5 s for a library of 1500 persons
- Rate of false acceptance claimed to be 1 per million
- EyeDentify, Inc. (http://www.eye-dentify.com) since 1975

Iris Recognition

- Description of iris patterns in 256 octets (2048 bits)
- Less invasive and less complex than retinal scanning
- IriScan, Inc. (http://www.iriscan.com) now Iridian
- Duration of capture claimed to be less than 1 sec.
- Independent verification of performance may be needed.

Face Recognition

- Template from 100 to 800 octets
- A person can be detected from a library of 5 000 to 50,000 images
- Verification lasts 3 to 20 s.
- Affected by other factors (wearing glasses, moustaches, lighting, head inclination, etc.)
- TrueFace™ (from Miros)
- Visionics (www.viisage.com) has implemented FaceIt® from Rockfeller University

Performance of Face Recognition Systems

- US Army Research Laboratory results from 1996 to 1997: the rate of false rejects increase with the time between the reference image and the execution image

Finger Prints or Finger Images

- Performance
  - rate of false rejects in commercial systems (3%)
  - false acceptance (1 in a million)
- Phenomenon used to record the s minutia
  - Capacitance (Infineon, Secugen)
  - Electric field (Authentec, Veridicom)
  - Optical and optoelectronic (Identix, Who?Vision)
  - Temperature (Thomson-CSF)

Hand Geometry

- Used for control access to U.S. entry
- Enrollment takes a few minutes
- Template has a size of 9 octets
- BiomMet Partners (http://www.biomet.ch) and Recognition Systems (http://www.recogsys.com)

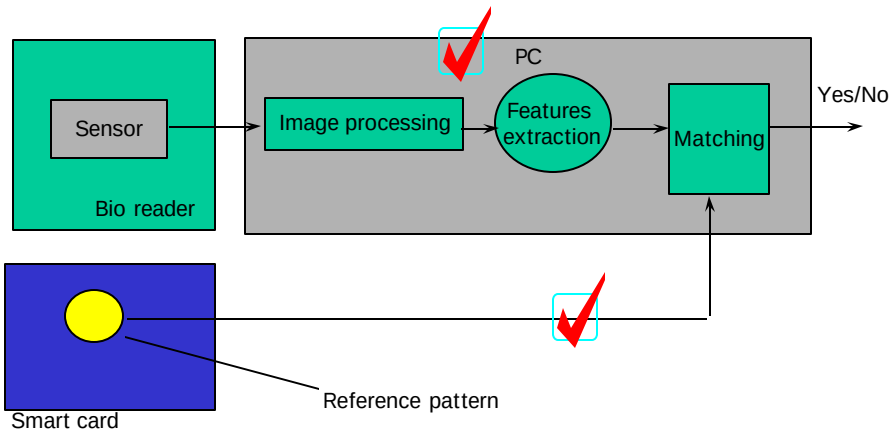
Summary of Biometric Identification

- Acquired characteristics
  - Handwritten signature (500-1000 octets)
  - Voice print (1000-2000 octets)
  - Keystroke dynamics
- Innate characteristics
  - Photo image (100-800 octets)
  - Fingerprint (500-1000 octets)
  - Iris scan(256 octets)
  - Retina (35 octets)
  - Shape of the hand (9 octets)
- BIOAPI

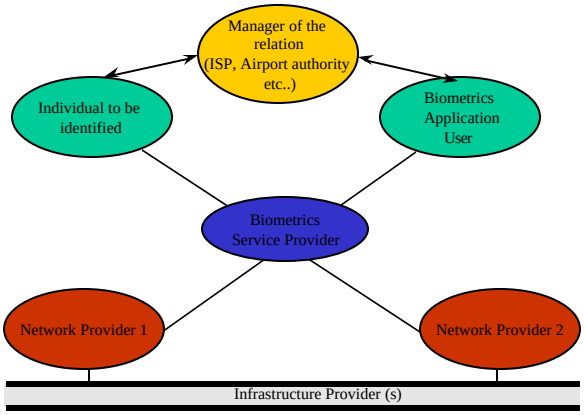
Major Problems for Large Scale Operation

- Systems are not interoperable at any level (hardware, software, architecture, application, etc.)
- Business demands are not focused or strong enough to encourage standardization
- IPR and Patents
- No single place responsible for evaluation and standardization

Biometrics Points of Vulnerability

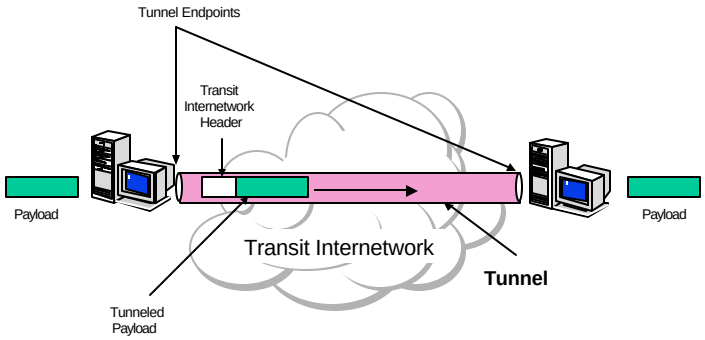


Biometrics in a Networked Environment



Performance depends on the exchange of performance and fault management information across administrative domains

Tunneling

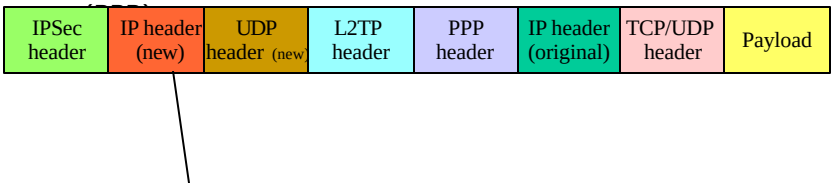


Tunneling Protocols

- Point-to-Point Tunneling Protocol (PPTP), Microsoft's extension to Point-to-Point Protocol (PPP)
- Layer Two Forwarding (L2F, proposed by Cisco)
- IP Security (IPSec): an IETF standard, RFCs 1825, 1826, and 1827
- Layer Two Tunneling Protocol (L2TP), another IETF standard for tunneling over IP, X.25, FR, or ATM networks

Layer 2 Tunneling Protocol (L2TP)

- Used to tunnel data using the point-to-point protocol



IP Security (IPSec)

- IPSec operates below the transport layer (TCP, UDP), therefore transparent to applications and end users
- IPSec provides three security services:
  - *authentication:* with certificates using the AH (Authentication Header) protocol
  - *confidentiality:* encapsulates an IP datagram in a new encrypted packet using the ESP (Encapsulating Security Payload) protocol
  - *key management*: concerned with the secure exchange of keys using the IKE (Internet Key Exchange) protocol

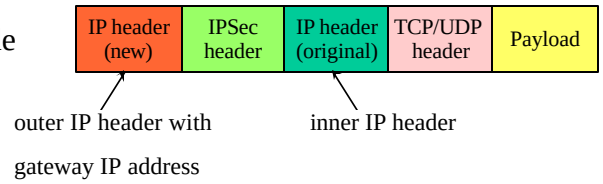
IPSEC Modes

- Transport mode
  - Encapsulates just the payload
  - Typically used for end-to-end communication between two hosts
- Tunnel Mode
  - Encapsulates the whole packet
  - Used when one or both ends of the connection is a security gateway, such as a firewall router.

IPSEC Modes

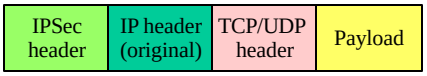
Tunnel mode

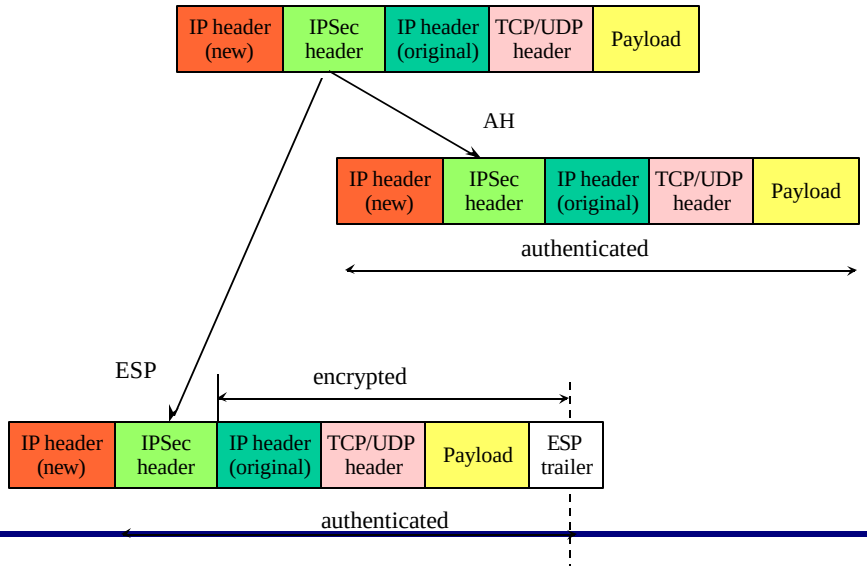
(ESP)



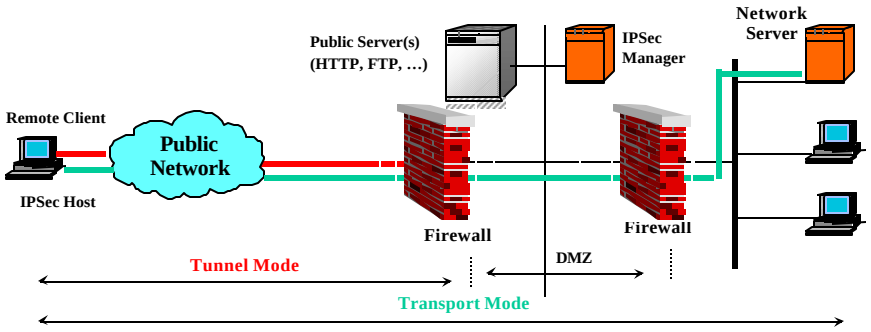
Transport mode

(AH and/or ESP)





IPSec Modes



DMZ: Demilitarized Zone

Non-Repudiation

- This is a legal concept that requires the intervention of a third party
- Non-repudiation at the origin
- Non-repudiation at the destination
- Easier with public key cryptography than with symmetric cryptography
- No backup of private signature key
- Time-stamping and sequence numbers

Technical Aspects of Nonrepudiation (X.813)

- Generation of proofs
- Recording of proofs
- Verification of proofs
- Retrieval and re-verification of the proofs

Digital Certificate

- Issued by a Certification Authority
- Verifies the identity of the holder of a public key
- Structure governed by ITU Recommendation X.509

Basic Content of the X.509 Certification

- Version
- Certificate serial number
- Identifier of the algorithm used to sign the certificate and the parameters used
- Name of the certification authority
- Expiration date of the certificate
- User's references
- Information concerning the public key algorithm of the sender, its parameters and the public key itself

Certification Authority (CA)

- A trusted third party that issues digital certificates
- Individuals or companies apply for digital certificate by sending their public key and identifying information to CA.
- CA verifies the information and creates a certificate containing the applicant's name, public key, and the key's expiration date.
- Each certificate has a unique serial number for identifying it.
- CA uses its private key to encrypt the certificate and sends the signed certificate to the applicant.

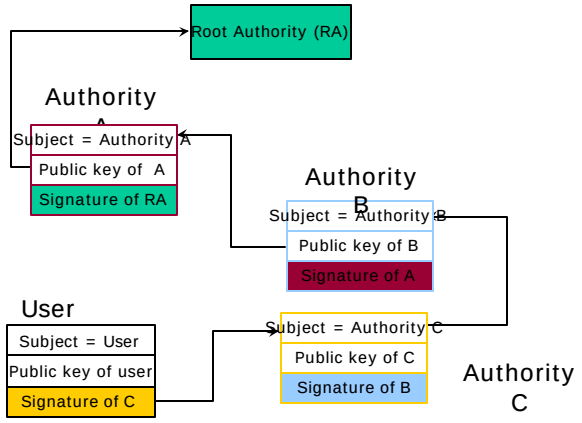
Certification

- X.509/ISO/IEC 9594-1- Four versions
- Directory System is LDAP
- EDIFACT has a different approach- DEDICA
- Certification Path and Recursive Verification
- Cross-certification
- Authorities needed:
  - Certification authorities
  - Naming or Registering authorities
  - Directory

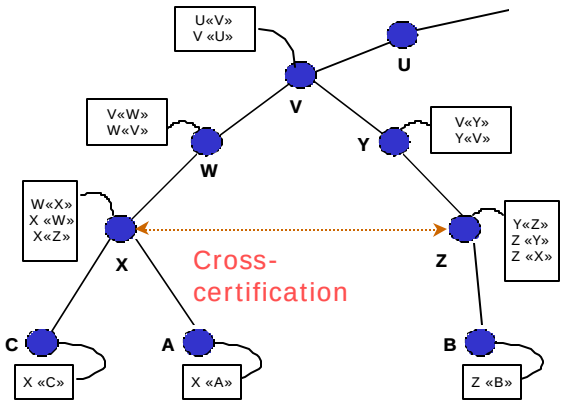
Authentication Steps

- Verify the signature of the certification authority
- Extraction of the requester's public key from the certificate
- Verification of the validity of the certificate by comparison of with the certificate revocation list (CRL)
- Establishment of a certification path between the certification authority and the authority that the server recognizes
- Determination of the privileges that the requester enjoys (e.g., financial data)

Recursive Verification of Certificates



Hierarchical Certification Path X.509

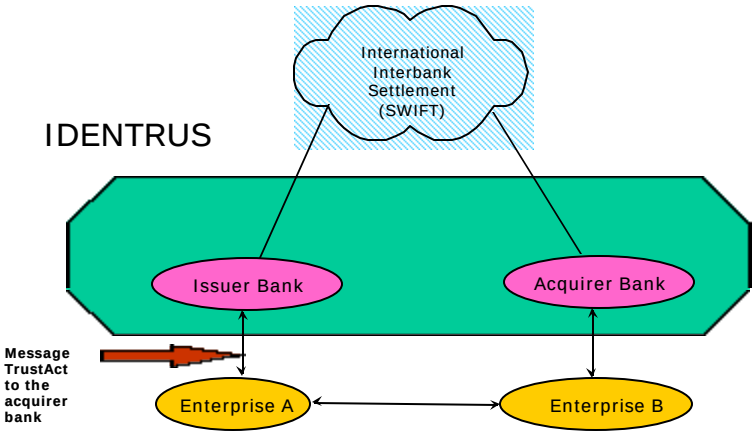


Z «B» = Z certifies B

Digital Certificate Organizations

- Bank-Led Organizations:
  - The Global Trust Authority (GTA) 800 banks
  - IDENTRUS (infrastructure for the TrustAct services from SWIFT)
- Verisign (acquired Thawte Certification)
- Scotiabank (Entrust)
  - North America's biggest bank certification authority
  - 150,000 digital certificates
  - >500,000 online banking transactions

IDENTRUS and TrustAct



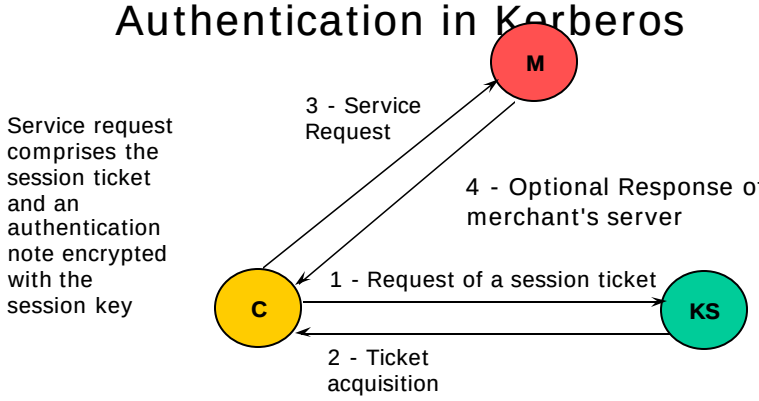
Key Management

- Production
- Storage
- Distribution
- Utilization (Exchange)- Kerberos/Diffie-Hellman
  - ISAKMP- Cisco
  - SKIP- Sun
  - KEA -NSA
- Withdrawal, Replacement
- Deletion
- Back-up and Archival - not of private signature keys

KERBEROS

- Produced by the MIT (ftp://athena-dist.mit.edu/keberos)
- Version 5 currently in use
- Free version called Heidmal (Swedish Institute of Computer Science)
- Public key version used in NetBill (RFC 1510)

Authentication in Kerberos



Message 2 contains a session encryption key encrypted with a common symmetric key between the client and the Kerberos server and a session ticket with information encrypted by the common symmetric key between the merchant and the Kerberos server

Public Key Infrastructure

- Types of Certificates:
  - Identity
  - Privileges or attributes
  - PKIX (IETF) simplifies the X.509 infrastructure and access policies
  - CMP (Certificate Management Protocol): key exchange and cross-certification (Entrust and IBM, as part of PKIX)
- SDSI (Simple Distributed Security Infrastructure)
- SPKI (Simple Public Key Infrastructure): for privileges

Attribute Management

- Grant authority to the holder of the certificate (legal age, sufficient funds availability, payment/shipping guarantees etc.) by reference to an identity certificate
- Allows delegation of privileges
- X.509 v. 4 (2000) defines a framework for attribute certificates
- Useful for banks
  - Scotiabank of Toronto/Canada
  - US Banks: Financial Agent Secure Transaction (FAST)

Access Management

- Rules may be complex (conditional statements)
- Role-Based Access Control (RBAC) restricts access to objects associated with a role
- NIST/OMG are developing a Resource Access Decision (RAD) interface
- (ftp://ftp.omg.org/pub/docs/corbamed/99-03-02.pdf)

Interoperability of Certificates

- MISPC (Minimum Interoperability Specification for PKI Components)- NIST
- GOCPKI (Government of Canada Public Key Infrastructure)
- Internet Council of NACHA (National Automated Clearing House Association)
- Authentication practices must be equivalent
- Independent audits

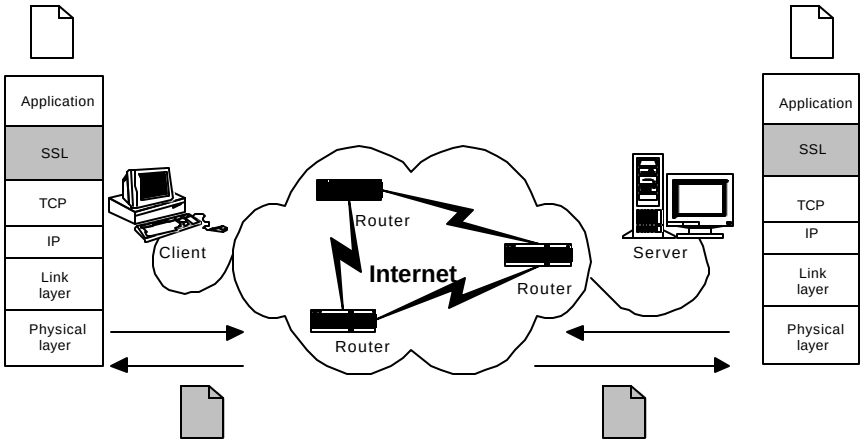
Additional Organizations

- Auditing organizations: American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants
- http://bbbonline.org
- http://www.truste.org (Electronic Frontier Foundation and CommerceNet)
- http://www.aece.org (Spain)

Security in Payment with Electronic Bank Cards

- Required to
  - Authenticate the client and the server
  - Protect message transmission
- The project sponsored by IETF was Secure HTTP (SHTTP, RFC 2660)
- The dominant approach is SSL (Secure Socket Layer), initiated by Netscape, but not an Internet standard
- Standard is TSL (Transport Layer Security) defined in RFC 2246
- Visa and Mastercard jointly developed a more secure protocol, SET (Secure Electronic Transaction)
- WTLS, adapted from SSL, is used in mobile transactions

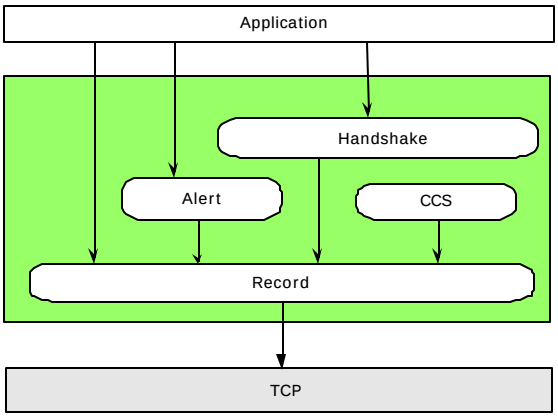
Functional Model of SSL



Main Properties

- Requires TCP => Cannot protect the following protocols:
  - SNMP
  - NFS
  - DNS
  - Voice on IP (H.323)
- For point-to-point only
- Authentication and key exchange
  - RSA
  - Diffie-Hellman
  - SKIPJACK (NSA's algorithm for PCMCIA cards - Fortezza)
- Confidentiality: Many algorithms with key lengths of 128 bits or 40 bits
- Integrity: SHA or MD5

SSL Sub-protocols



Functions of Record

- Data segmentation
- Data compression (if available)
- Generation of digest (HMAC) to ensure integrity
- Data encryption to ensure confidentiality

SSL Exchanges

- Preliminary phase:
  - Identification of the two parties
  - Negotiation of the cryptographic attributes
  - Generation and sharing of keys
- Establishment of an SSL Session
  - an association of the two entities with a common set of parameters and cryptographic attributes
  - cannot last more than 24 hours
- An SSL Connection uses the principal cryptographic parameters of a session and reinitializes the encryption

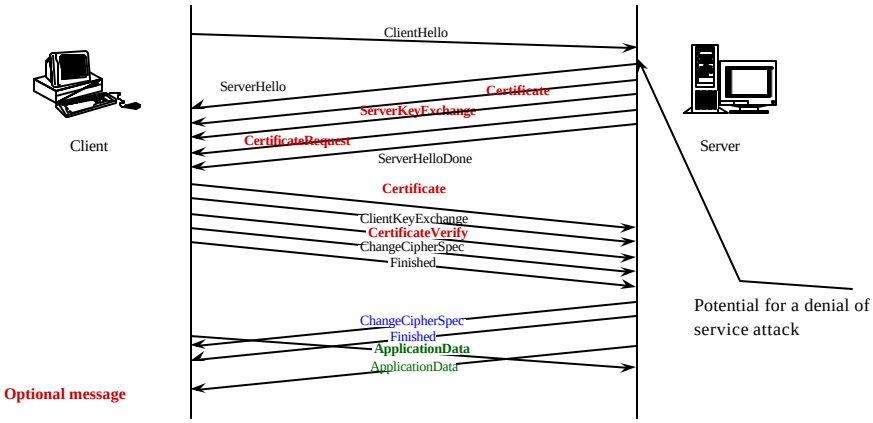
State variables of an SSL Session

- A session ID
- Peer certificate
- Compression algorithm
- A cipher suite (encryption and hashing algorithms and their parameters)
- MasterSecret: 48 octet secret shared between the two sides and used to generate all other secrets
  - calculated at the start-up of a session from a PreMaster secret exchanged with a key exchange algorithm
  - remains constant throughout the session

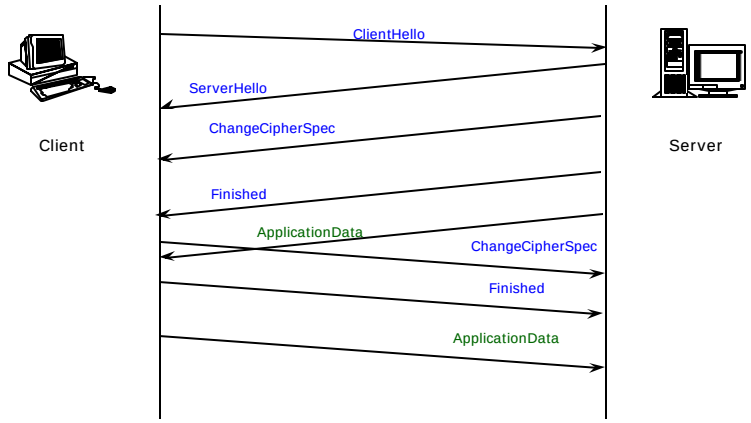
State Variables of a Connection

- Two random numbers of 32 octets (server_random, client random) exchange in the clear
- Two secret keys (one for each side) for HMAC calculations
- Two keys for symmetric encryption (one for each side)
- Two initialization vectors for symmetric encryption
- Two sequence numbers of 8 octets (one on each side)

SSL Exchanges for Session Establishment



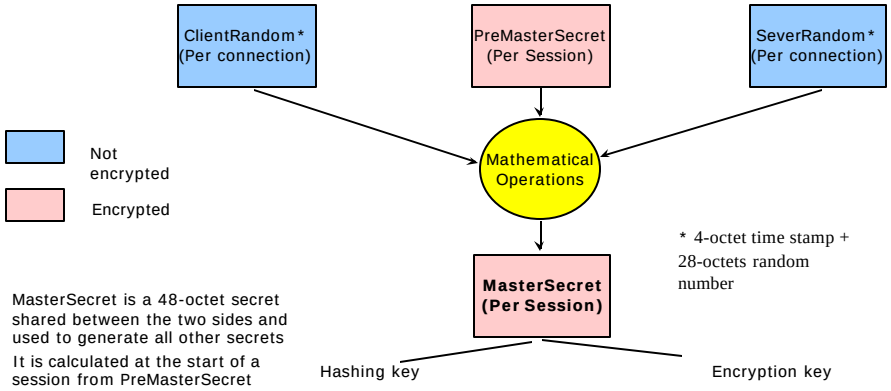
SSL Exchanges for Connection Establishment



Message Contents of an SSL Session

- ClientHello includes:
  - Which method(s) the browser supports for
    - Encryption
    - Hashing
    - Compression
    - client_random
- ServerHello includes:
  - Selected method(s) for
    - Encryption
    - Hashing
    - Compression
    - server_random
- Certificate

Construction of the MasterSecret



- MasterSecret is a 48-octet secret shared between the two sides and used to generate all other secrets
- It is calculated at the start of a session from PreMasterSecret exchanged during the initial handshake

Calculation of the Session Cryptographic Parameters

- Once PreMasterSecret has been exchanged, both the client and server compute MasterSecret
- From MasterSecret, each side calculates
  - the encryption keys
  - the key for hashing with HMAC
  - the initialization vectors
- *Finished* message
  - Includes a hash of all the handshake messages with the cryptographic attributes just negotiated to prevent any man-in-the middle attack.

Practical Considerations

- Low computational load
- Time to establish a session by the client is about 15 % higher than for the server
- Widespread use
  - Used in WAP applications
  - Limited to point-to-point applications
- Many libraries are available (commercial, research and freeware)
- SSL Accelerators

SSL Implementations

- SSLeay is an API distributed free of charge
- OpenSSL Project is a collaborative world-wide effort to develop an Open Source tool kit
- Team from UK, Germany, Denmark, and Sweden
- http://www.openssl.org

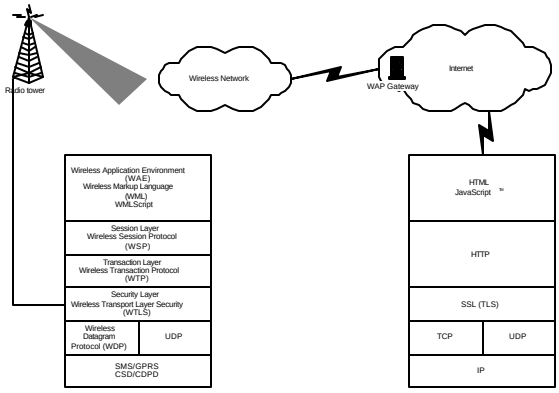
TLS (Transport Layer Security)

- Defined in RFC 2246
- Main differences
  - More additional allert messages
  - Standard method for message authentication: H-MAC algorithm
  - Standard method for key generation
  - Does not include Fortezza

WTLS (Wireless Transport Layer Security)

- Protocol for wireless transcations adapted from SSL
- Can work with interrupted flow due to packet loss
- Can support UDP (transport protocol may be unreliable)
- Can sustain large round-trip delays
- Can be configured to terminals with low processing power and low memory
- Ensures non-repudiation
- Incompatible with SSL
- Optional in WAP 2.0

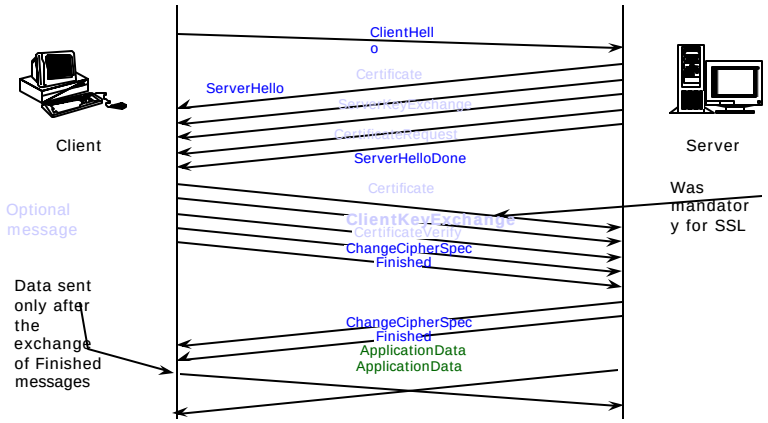
WAP Protocol Stack



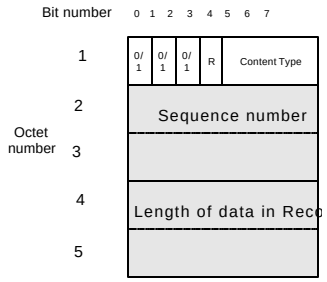
WTLS Services

- Identification
- Authentication
- Confidentiality
- Integrity
- Non-repudiation

WTLS Exchanges for Session Establishment



Header for Record in WTLS



Other Differences between SSL and WTLS

- Several Handshake messages can be consolidated in one message
- Handshake messages can be retransmitted under certain conditions
- New contents for ClientHello, ServerHello, Certificate, ServerKeyExchange, ClientKeyExchange
- Size of variables are different

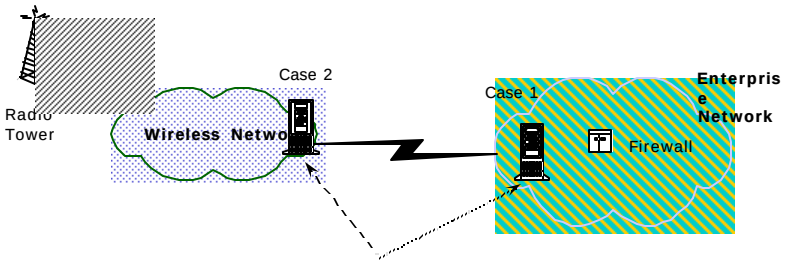
Variables Sizes in Octets

- Symmetric key: 5 to 16 octets inSSL/ 5 to 21 in WTLS
- Client_random: 32 in SSL /16 in WTLS
- Session identifier: 3 in SSL /2 in WTLS
- MasterSecrete: 48 in SSL /30 in WTLS
- Sequence number: 8 in SSL /2 in WTLS
- PreMasterSecret: 48 in SSL / variable (20 for RS) in WTS
- Server_random: 32 in SSL / 16 in WTLS

Position of the WTLS/SSL Gateway

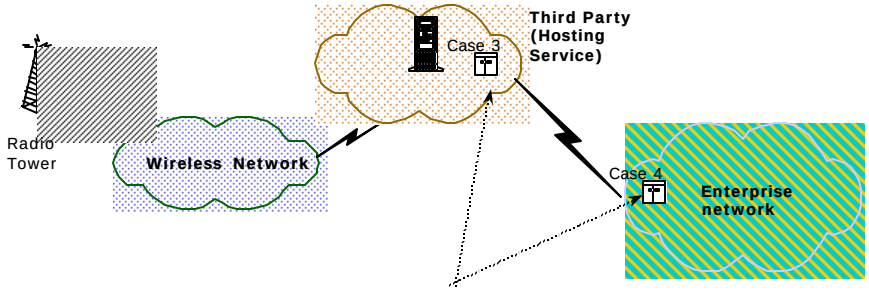
- Within the enterprise network after the firewall
- At the ISP
  - only the radio channel
  - the radio channel and the gateway
  - all applications

Possible Locations of the WTLS/SSL Gateway



Possible positions of the WTLS/SSL Gateway

Possible Locations of the Enterprise Firewall

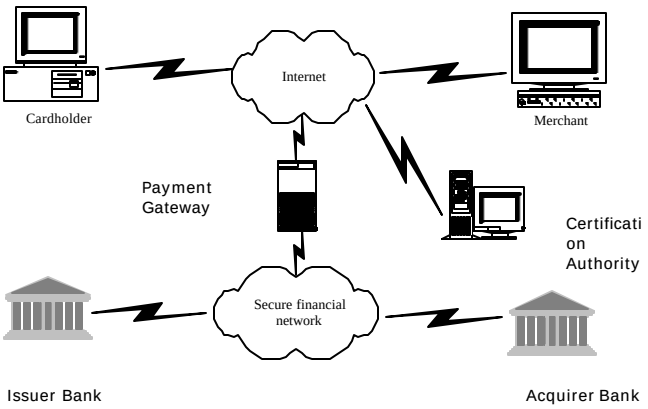


Possible positions of the Firewall

Secure Electronic Transaction (SET)

- Initiated by Visa and MasterCard; supported by IBM, GTE, Verisign, and others
- Provides
  - Registration of Cardholders and Merchant with the certification authority, and delivery of certificates
  - Authentication, confidentiality, integrity, and non-repudiation of purchase transactions
  - Payment authorization and payment capture
  - Message formats, certificate format, and procedures for message exchange
- Uses
  - DES for confidentiality
  - RSA for authentication, identification, and integrity
  - SHA1 for hashing
  - HMAC-SHA1 for keyed hashing

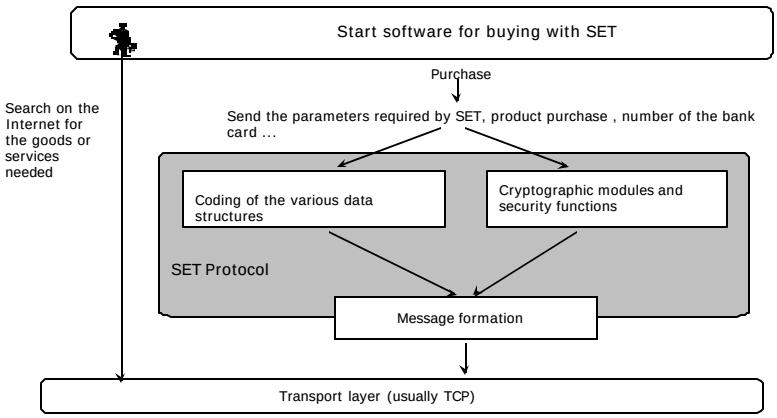
Actors In SET



SET (Secure Electronic Transaction)

- Sponsored by Visa and MasterCard with IBM, GTE, Verisign, etc.
- Focuses on payments
- Software-oriented
- Multi-party architecture
  - cardholder
  - merchant's server
  - payment gateway
  - certification authority
  - banks

Position of SET on top of TCP/IP



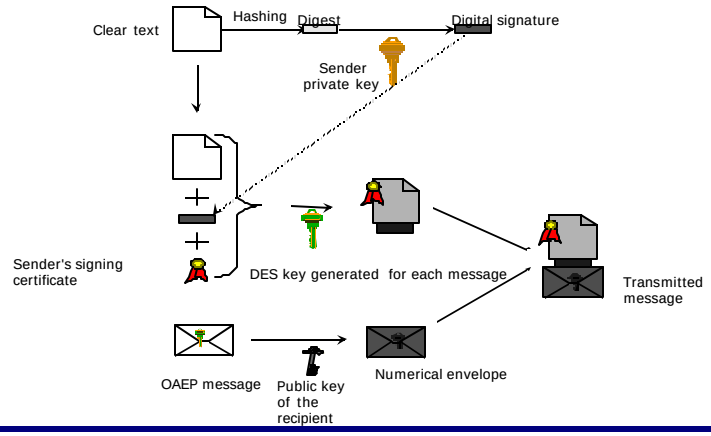
SET Security Services

- Registration of the cardholders and merchant with the certification authority and delivery of certificates
- Authentication, confidentiality and integrity of purchase transactions
- Payment authorization and payment capture
- Offers technical means for nonrepudiation services
- Each transaction has a unique transaction number that is encrypted (prevents replay attacks)

Cryptographic Algorithms in SET

- DES for confidentiality
- Optimal Asymmetric Encryption Padding to increase resistance to attacks
- Use of Dual Signature
- RSA for authentication, identification and integrity
- SHA1 for hashing
- HMAC-SHAI for keyed hashing
- Uses of PKSC #7 structures for *SignedData, EnvelopedData*, *DigestedData* and *EncryptedData*

Cryptographic Processing of SET Messages



Dual Signature in SET

- The SET protocol
  - hides the customer's credit card information from merchants
  - hides the order information from banks
- This scheme is called *dual signature.*
- Suppose the client wants to send two messages:
  - *m1* to the merchant with purchase order
  - *m2* to the payment gateway via the merchant
- The client forms *m3*, a concatenation of digests of *m1* and *m2*:

$$m3 = H(m1) \mid H(m2)$$

- The client applies the hashing function to *m3*, to obtain H(m3)

Dual Signature (Cont.)

- Message sent from client to merchant:

  $m1, H(m1), \{m2, H(m2)\}PK_g, \{H(m3)\}SK_c, H(m1) \otimes H(m2)$
- Message sent from merchant to payment gateway:

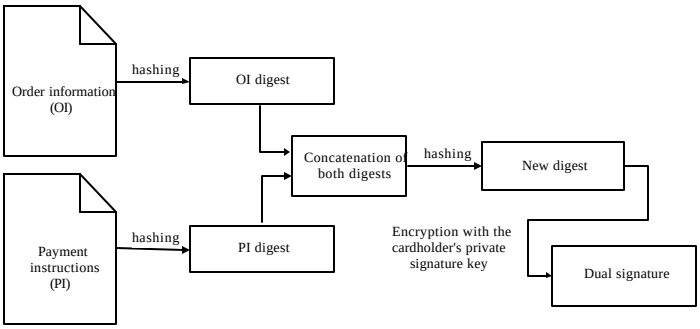
  $\{m2, H(m2)\}PK_g, \{H(m3)\}SK_c, H(m1)$

  where PK_g = public key of the gateway, SK_c = private key of the client
- Merchant can extract H(m2) and verify the integrity of *m3* by calculating H(m3) from H(m1)|H(m2) and comparing it with the value extracted with the public key of the client
- Similarly, the payment gateway can verify the integrity of *m1* without its contents
- Gateway is sure that the merchant has accepted to honor the purchase
- The sale is effective only when the bank approves the payment instruction

Dual Signature - Viewpoints

- Merchant's View Point
  - If the client is certified,
    - Merchant keeps the order information signed with the client's private key
    - Merchant has a copy of the client's certificate
  - Merchant does not have the details of the client's account.
  - Merchant retains the response of the gateway signed with the private key of the gateway
- Cardholder's viewpoint
  - Cardholder receives a response to the purchase order signed with the merchant's private key
  - Cardholder receives a copy of the merchant's certificate
- Gateway viewpoint
  - Gateway has the financial details of the transaction without knowing the subject of the transaction

Dual Signature of the Preq Message



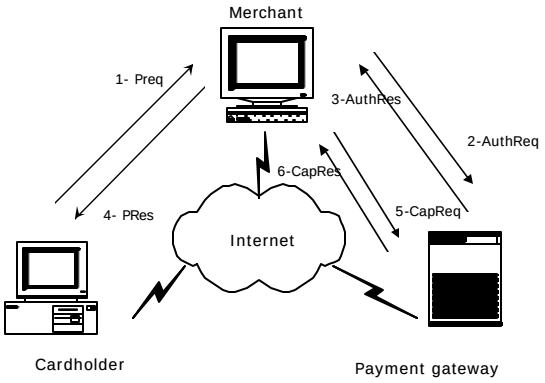
Hierarchy of Certification Authorities

- Root authority (CertCo & Digital Trust Company)
- Brand certification authorities
- Geopolitical authorities (optional)
  - cardholder certification authority
  - merchant's certification authority
  - payment certification authority
- Merchant and Payment gateways have 2 certificates one for signing and one for encryption
- Cardholder has one certificate for signing

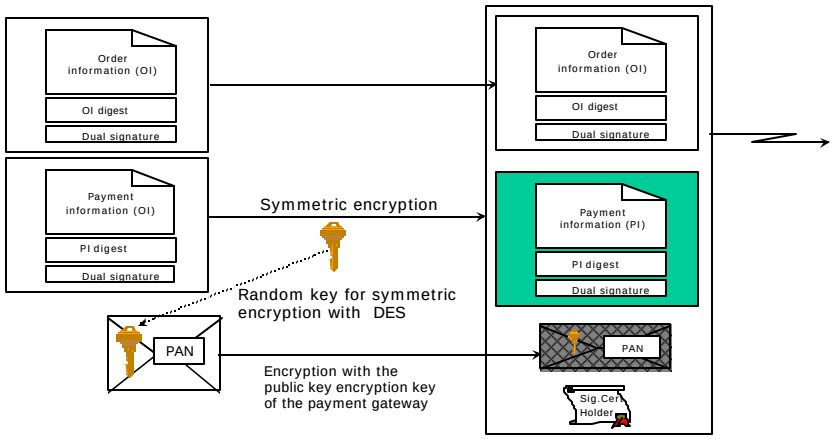
SET Messages

- Certification
- Payment
  - Mandatory
  - Optional
- Certificates renewed according to a given schedule

SET Mandatory Payment Message



Construction of Preq Message



Other Procedures in SET

- Modification or cancellation of previous authorizations
- Modification or cancellation of a capture
- Refund of the cardholder
- Cancellation of a Refund
- Grouped settlement of a batch of capture requests...

Implementations Issues

- Secrets on cardholder side are stored on the computer hard disk: may be a security risk
- Requires legislation that allows encryption
- SETREF is a reference implementation
- Uses BSAFE (was under export control)
- Trintech: First company to have a certified implementation

Comparison of SET and SSL

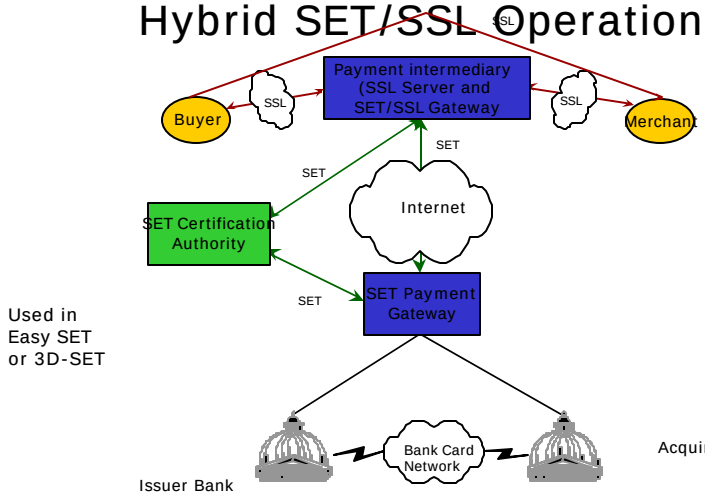
SSL

• SS is mature, simple, and widely used.
• SSL is for general-purpose secure message exchanges (order taking, queries)
• A part of SSL is available on customers' browsers.
• It authentication at the beginning of each session
• SSL does not use a payment gateway: the merchants need to receive both the ordering and credit card information.
• SSL does not have a root certification authority.

SET

• SET is a complex, comprehensive security protocol.
• It provides for privacy, authenticity, integrity, and non-repudiation.
• It is tailored to the credit card payment to the merchants.
• SET authenticates at each request/response pair
• It requires *digital wallet* by the user.
• SET uses dual signature to hide information from those who have no need to know.
• It may be abandoned if it is not simplified.

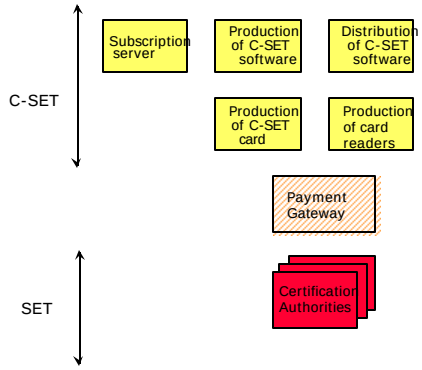
Hybrid SET/SSL Operation



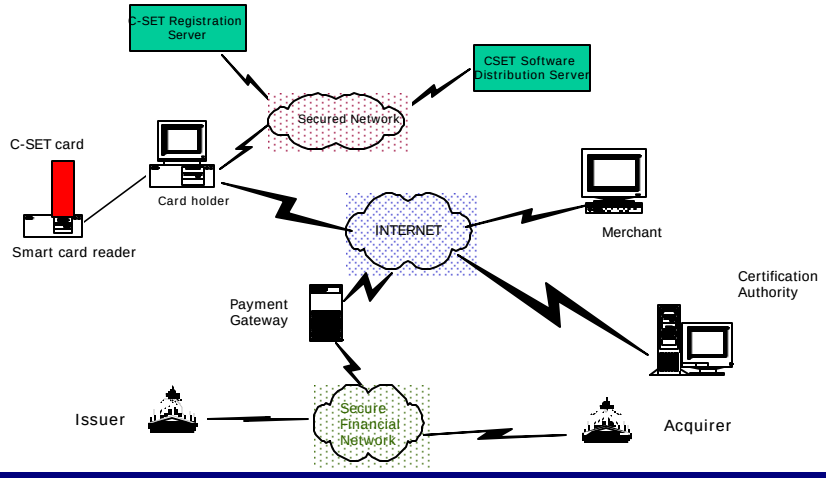
C-SET/Cyber-COMM

- Integration of SET with smart cards by French Banks
- Requires the following parties:
  - secure card reader
  - C-SET registration server (to award C-SET certificates)
  - C-SET distribution center
- C-SET payment gateway acts as:
  - an agent of the acquirer banks
  - C-SET/SET converter

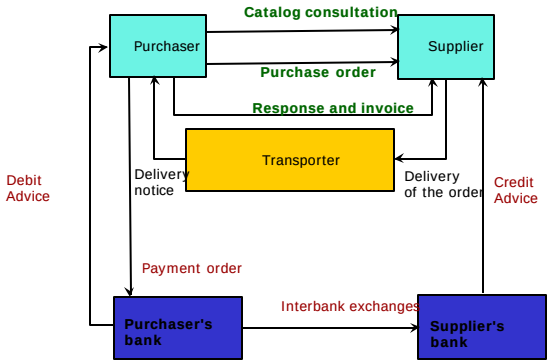
Secure Components of C-SET and SET



C-SET/Cyber-COMM Architecture



Typical Exchanges in a Purchasing Transaction



Key Entitities

- Buying company (procurement management)
- Selling company (marketing, distribution)
- Electronic intermediaries:
  - Marketplace or exchange
  - Application Service Provider (ASP) (hosting, directory service, fullfillment, etc.)
  - Network platform such as the Internet, VAN, intranet and extranet
- Feight delivery of physical goods
- Banks and Payment Processors

Problem Statement

- Sales -> scheduling -> manufacturing -> distribution (flexible manufacturing and Just-in-Time production)
  - automated monitoring and tracking
  - tailor products to markets and individuals
- Interbusiness transactions are complex
  - 51% of the US labor force is involved in interactions among companies
  - In some industries, the rate and number of interactions is high (electronic manufacurers process 200,000 orders/month)
  - Order fulfillment is very complicated because of exception conditions (backorders, partial shipment, returns, substitute products, incorrect orders, etc.)
- Business structures built on partnerships rather than on control (outsourcing, alliances, joint ventures)

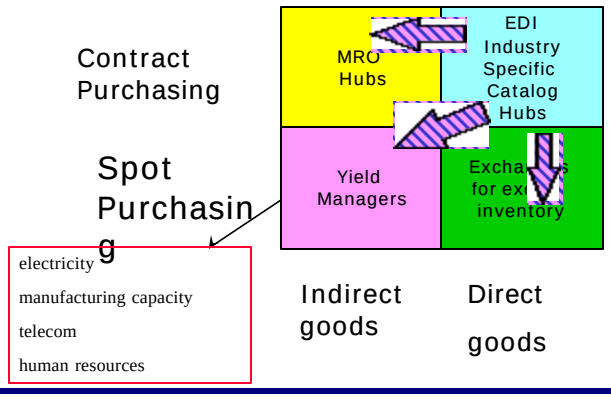
Solution

- Co-operation across organizational boundaries
  - Enterprise Resource Planning (ERP)
  - Supply Chain Management (SCM)
  - Customer Relationship Management (CRM)
  - Collabortive Freight Management (CFR)
- Increased response speed and reduce operational expenses by 20-30%:
  - Less entry errors (40% of manual orders have to be reworked because of errors or missing data)
  - Reduction of warehousing costs
  - Automatic reconcialiation of invoices and accounting

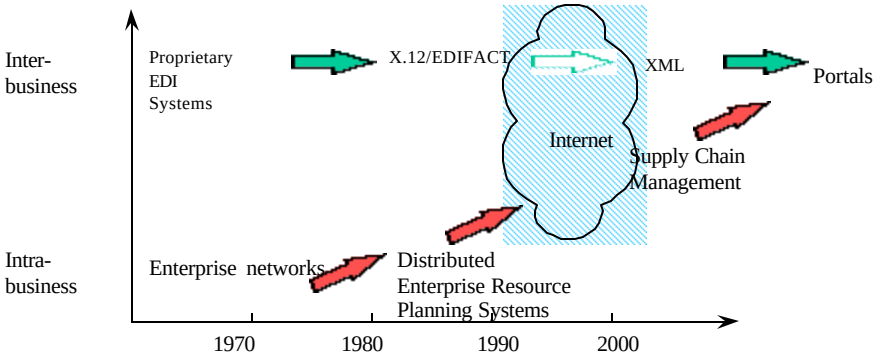
Implementation

- Software solutions must be integrated into business processes.
  - This involves organizational changes and not only automating existing processes.
  - Requires uniform or compatible back-office systems along the entire chain.
- Cost of implementation
  - Cost of software ($1 M to $2 M)
  - Cost of integration with existing systems (x 5)
  - Cost of training and reorganization
- Some legal requirements needed
- Vulnerable to interruptions

Modeling of Supply Chains



Evolution of Business Commercial Networks



Adapted from Rainer Alt and Elgar Fleisch, "Business networking systems : Characteristics and lessons learned", *International Journal of Electronic Commerce* 5(2) :7-27, Winter 2000-2001.

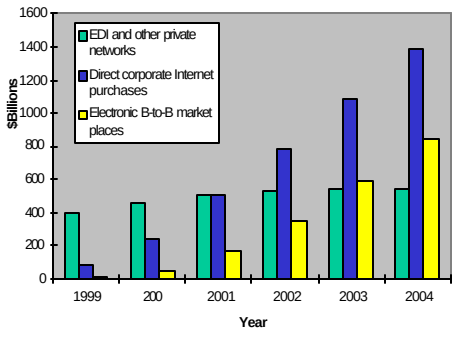
Electronic Data Interchange (EDI)

- Relates to business-to-business exchanges :
  - consultation of catalogues
  - purchasing transactions
  - shipment notices
  - receipts
  - financial data flowing within the banking network
- Reorganization of activities around the information flow and not the flow of materials
- Tracking of containers in automated warehouses
  - MITL (Multi Industries Transport Label)
  - SSCC (Serial Shipment Container Code)

Examples of EDI

- Pre-Internet
  - Automotive Industry
  - Chemical Industry
  - Airline (SITA)
  - Banking (SWIFT)
- With Internet (Many other industries and SMEs)

Electronic Data Interchange (EDI)
EDI - The Infrastructure for B2B

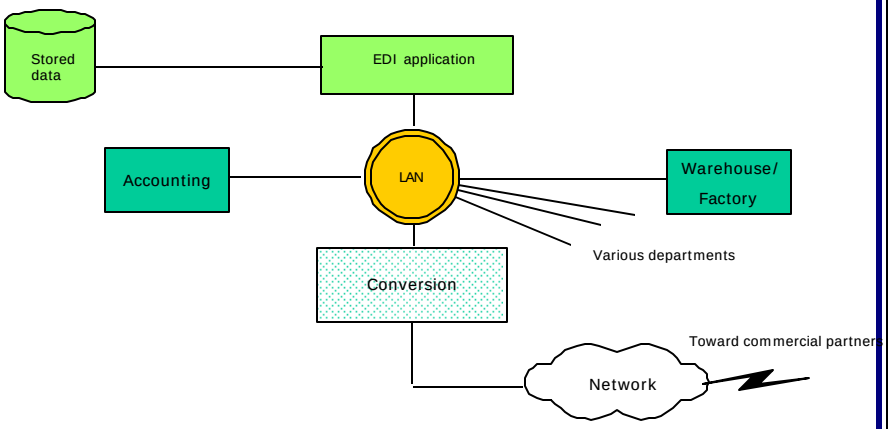


- Usage data from Yankee Group (WSJ, May 21, 2001, p. R18)
- Gartner group (2000)
  - IP-based invoicing is about 8.6 % of B2B electronic billing
  - EDI 56%

Telecommunications Brokerages

- A transaction platform for centralized trading and switching of network capacity expressed in minutes of available calling time for international and domestic long-distance switched voice or in terms bandwidth for data network
- Companies that trade bandwidth can be network providers, ISPs or any other companies that have excess bandwidth in its private network.
- Physical delivery of traded capacity is made automatically through the exchanges switches that are connected to the various carriers networks.
- Single point of contact for planning, provisioning, installation, network management, carrier relations and billing
- Examples:
  - Arbinet
  - Band-X
  - InterXion
  - MVX
  - RateXChange
  - Universal Access

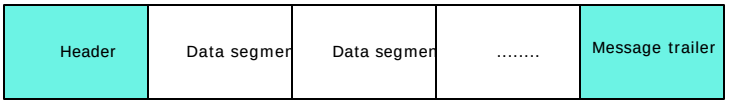
Components of an EDI System



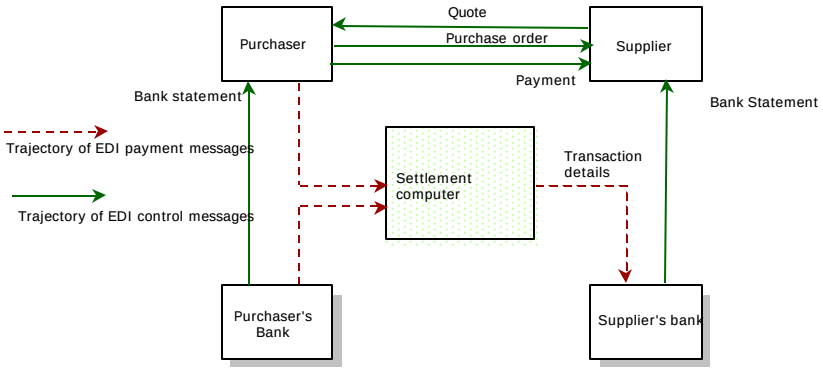
EDI Components

- Transmission and reception of structured data
  - Alphanumeric structuring of the data
    - ANSI X12
    - EDIFACT
  - XML
- Management of distribution
  - VAN
  - X.400
  - MIME/SMTP
- Management of Security

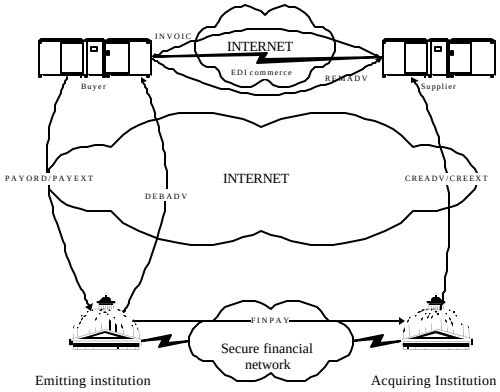
Structure of an EDI Message

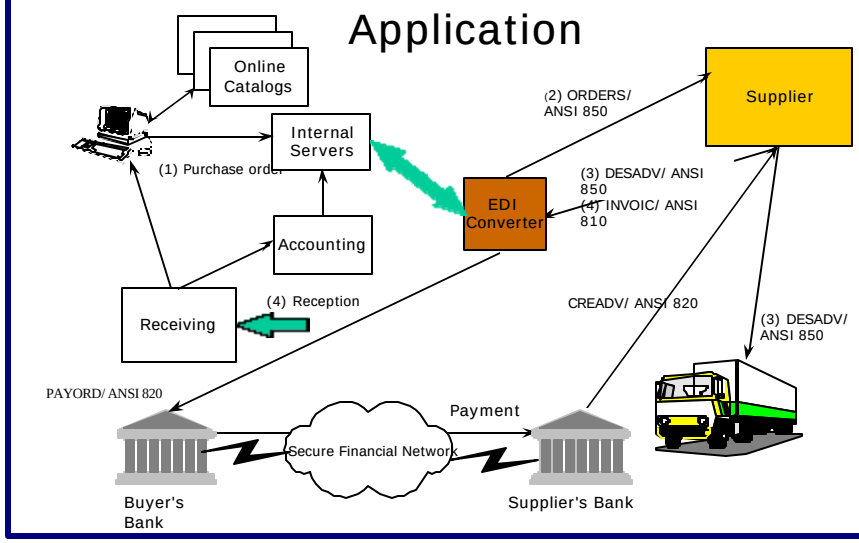


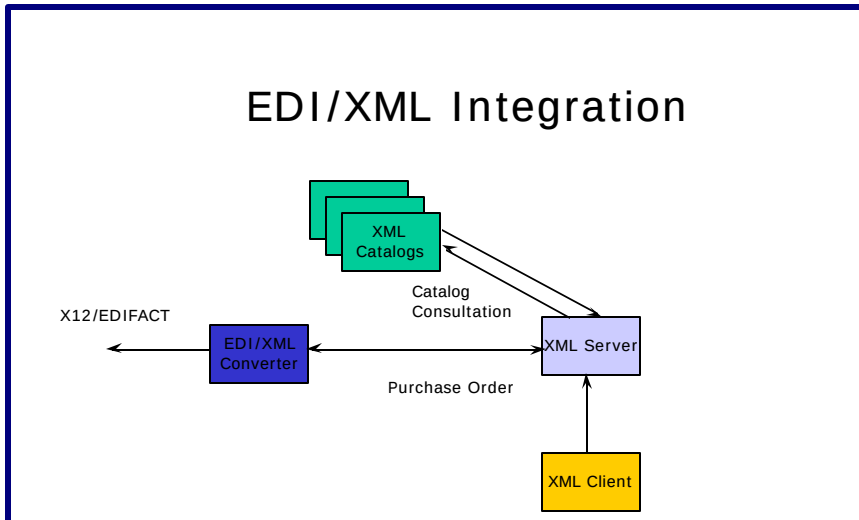
EDI Financial and Electronic Commerce



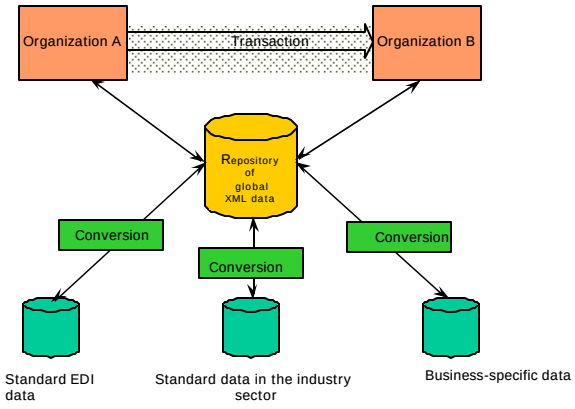
Credit Transfer




Application
Online Catalogs
Internal Servers
(1) Purchase order
(2) ORDERS/ ANSI 850
Supplier
EDI Converter
(3) DESADV/ ANSI 850
(4) INVOIC/ ANSI 810
Accounting
Receiving
(4) Reception
CREADV/ ANSI 820
(3) DESADV/ ANSI 850
PAYORD/ ANSI 820
Payment
Secure Financial Network
Buyer's Bank
Supplier's Bank


EDI/XML Integration
XML Catalogs
Catalog Consultation
X12/EDIFACT
EDI/XML Converter
XML Server
Purchase Order
XML Client

Exchanges in XML/EDI Integration



RosettaNet

- Used for the supply chain in the electronic industry
  - Manufacturers (Cisco, Compaq, HP, IBM, Intel, Siemens, Toshiba)
  - Financiers (Deutsche Financial)
  - End-Users (ABB, AMEX, GSA)
  - Resellers/ SI (CompUSA, Computacenter,EDS, Insight, MicroAge)
  - Shipper (FedEx, UPS)
  - Software Publishers (Microsoft, Netscape,Oracle, SAP 4)
  - Wholesale distributors (C2000, CHS, Ingram Micro,Marshall Industries,Tech Data, Tech Pacific)
  - Technologists (GEIS, pcOrder)
- DTD (Document Type Definition) to define the structure of the XML exchange
- PIP= Partner Interface Process is a special DTD defined by RosettaNet(text coupled with object and data models)

Commercial Offers

- Products
  - Commerce Server (Microsoft)
  - NetCommerce (IBM)
  - SmartCommerce (Bull)
- BizTalk:SOAP +QoS (Microsoft)

UDDI (Universal Description, Discovery and Integration)

- Similar to a DNS service but for businesses
- Answers the following questions
  - Who has the product (*availability*)?
  - Who makes the product (*procurement)*?
  - Do prices vary by geography or by order size (*pricing*)?
  - Is there a substitute or alternative product (*substitution*)?
- Business registers Web services

UDDL Information Services

- Three information models
  - White pages for business names and descriptions
    - WSDL (Web Services Description Language)
  - Yellow pages for categorisation by industry and geograhy
  - Green pages for business processes, service descriptions and bindings
- Registry is distributed over sites that share updates on a daily basis

Electronic Payment Market

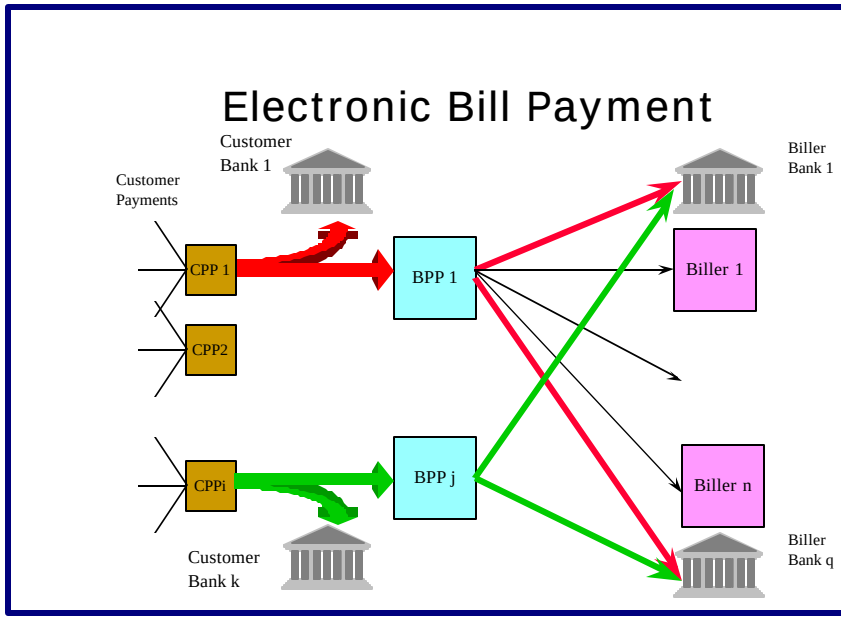
- Front-end services (online bill aggregation, payment)
- Back-end bill consolidation and presentment, payment processing and interfaces to financial instutions
- Front-end may be accessible through banks
- Software providers
  - BCE Emergis
  - Bottomline Technologies
  - Avolent

Service Providers

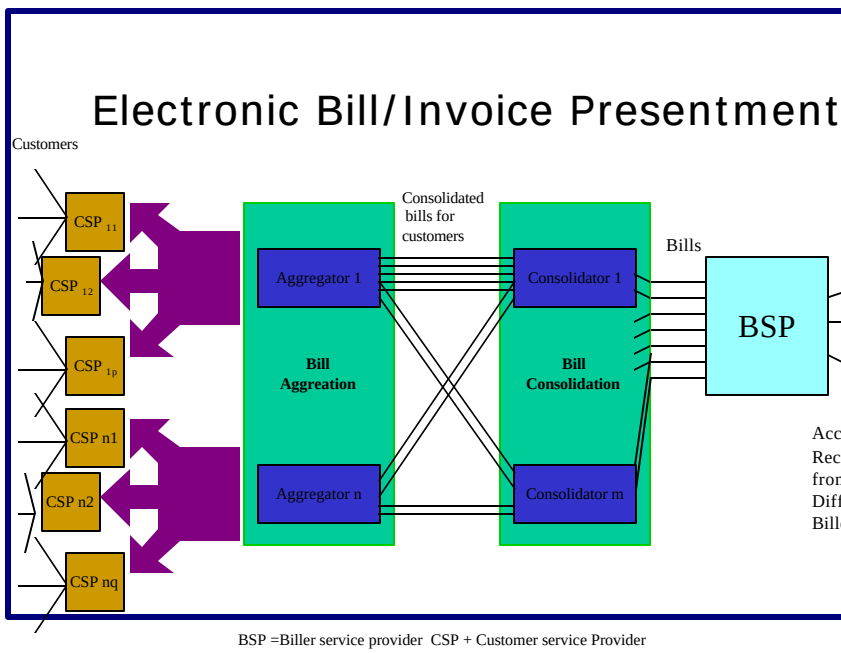
- CheckFree is the leader and being challenged by PayPal (but PayPal is losing money)
- Virtual check projects
  - OFX is on the online bill presentement specifications (Intuit, CheckFree, Microsoft, Avolent)
  - BIPS, Echeck from the Financial Services Technology Consortium (FSTC)
  - IFX (IETF)

Electronic Invoice Payment and Presentment (EIPP)

- Billing service provider (BSP) : offers billers (telephone companies, utilities) service bureau processing services
- Consolidator: BSP that aggregates bills from several bills
- Customer service Provider (CSP): presents summary from multiple bills to customers on-line
- Aggregator: CSP that combines bills or bill summaries for customers
- Customer payment provider (CPP): handles payments for customers
- Biller Payment Provider: handles payments on line for billers



BPP =Biller payment provider CPP + Customer Payment Provider

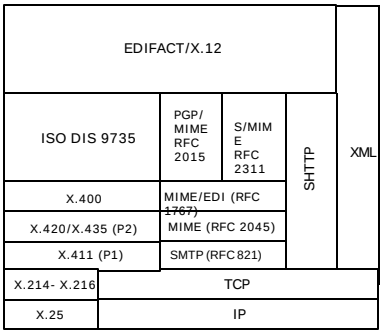


BSP =Biller service provider CSP + Customer service Provider

EDI Security

- Insert "security structures"
  - X12.58 Defined in 12/97
  - ISO 7498-2, DIS 9735-2, DIS 9735-6
- IETF Proposals
  - Based on PGP/MIME
  - S/MIME
- Interoperability of both approaches tested by CommerceNet consortium for X12

Protocol Stack for EDI Security



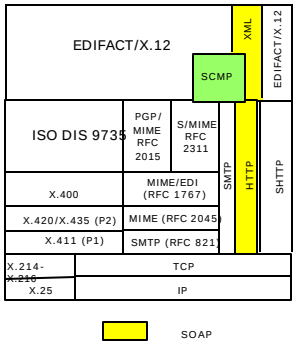
Standardization of B2B Messages

- EDI
  - EDIFACT (UN and ISO)
  - X12 (ANSI)
- EDI/XML
  - X12/XML (CommerceNet)
  - Oasis Consortium (Sun, IBM, Microsoft)
  - Electronic Business XML (ebXML): merging of alphanumeric EDIFACT and XML. Sponsored by the UN/CEFACT and OASIS (http://www.unece.org/cefact)
  - OTP (Open Trading Protocol) Consortium
  - RosettaNet

Work in Progress

- Simple Commerce Messaging Protocol (SCMP) http://www.ietf.org/internet-drafts/draft-arnold-scmp-07.txt (PKCS #7, S/MIME, v.3)- HTTP/SMTP
- IFX (Interactive Financial Exchange) protocol for on-line financial exchanges
- Simple Object Access Protocol (SOAP) http://www.ietf.org/internet-drafts/draft-box-http-soap-02.txt

Updated Protocol Stack for EDI Security



Integrated Circuit (IC) Cards

- Card with bar codes
- Card with Magnetic strips
- IC cards
  - memory cards (prepaid cards)
  - wired-logic cards (encrypted television channels) $1 US
  - microprocessor cards (smart cards) $5 to $20 U.S.
- Smart cards
  - Have large memory
  - Have computational capacities
  - Can take complex decisions

Classification of Microprocessor Cards

- Duration (disposable vs. rechargeable)
- Intelligence
- Contact vs. contactless cards
- Monoapplication vs. multiapplication cards
  - Telephone cards with contacts, monoapplication, disposable (cost 50 cents)
  - Swedish Electronic Identity Card is a multiapplication card

Applications of Smart Cards

- Bank cards
- Pay TV
- Identification cards in mobile telephony (SIM)
- Loyalty cards
- Electronic money holders
- Access control through biometric identification

Reasons for Interest

- Visa: 0.11% of transactions on the Internet are fraudulent (compared to 0.05% overall)
- In 2000, bank losses in the European Union increased by 48% to reach .07% of the trunover
- Half of the contested transactions in the US are on on-line transactions, even though they are only 1-2% of the turnover

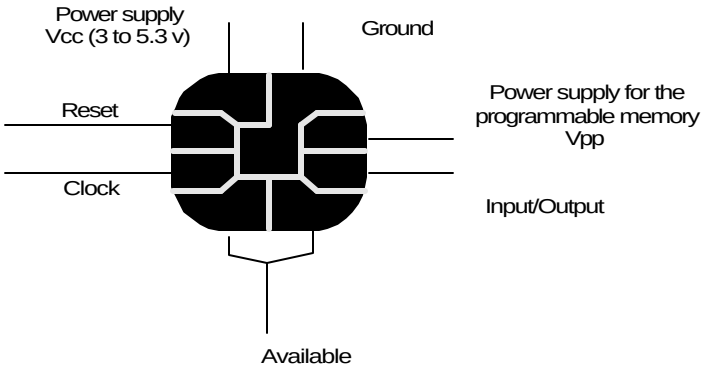
Criteria for Classification of Smart Cards

- Open or closed system
- Rechargeable or one-time usage
- Intelligence (storage only, wired logic or microprocessor)
- contact or contact-less
- single application or multiapplications

Examples

- Pre-paid telephone cards
- Health cards (Germany, France, Belgium)
- University cards
- SIM card in GSM
- Access control cards: need a display and keyboard

Contact Cards



Characteristics

- 8-bit processor
- Clock between 3.5 MHz and 5 MHz
- Power supply 3 - 5 volts
- Standardized contacts (8)
- Data bit rate of 9.6 kbit/s
- Wear and tear of readers

Contactless Cards

- Frequency: industrial band (< 150 KHz) or unlicensed (about 6.78 MHz)
- No mechanical contact
- 8-bit processor - Power supply: batteries (Li, carbone, manganese, photovoltaic) or inductive/capacitive coupling
- Exchange of data at 8-20 cm from the reader
- Bit rate can reach 106 kbit/s
- Public Transport systems in Paris and London

Modeus/Moneo Contactless Card

- Parisian system based on the German GeldKarte to be introduced between 2001 and 2004
- Antenna incorporated in the card
- EEPROM: 2 Kbytes
- Frequency: 13.56 MHz
- Maximum distance: 8-10 cm
- Reader at each entrance for the metro or commuter train
- Control server at each station or on each bus
- Proprietary OS (CD7 from ASK)

Memory Security

- Type of memory
  - ROM: 16 -32 kbytes- contains the proprietary OS of the card
  - RAM: 256 - 1024 bytes
  - EEPROM/Flash Card: 3 -64 Kbytes
- Fabrication zone: accessed only during fabrication
- Secret zone: cryptographic parameters of the user and the card
- Temporary work area
- Access control area where access attempts are recorded
- Open area accessible to all applications

Operating System

- Most OSs are currently proprietary (the most used one is the M4 for single application cards)
- ZeitControl (proprietary OS with elliptic curve cryptography)
- Attempts to establish de-facto standards:
  - MULTOS (Mondex, Mastercard)
  - JavaCard (VISA, SUN)
  - Windows for Smart Card

Security of Smart Card

- Protect the data stored in the card and access rights to service
- Security measures during the production
- Security measures during use

Production of Smart Cards

- Design and development of the integrated circuits
- Design and development of the card firmware
- Fabrication of silicon wafers
- Burning of firmware, packaging of integrated circuit, and final testing
- Pre-personalization (addition of programs needed for the application)
- Personalization (adding the names of the issuer and application software)
- Issuance of smart card on the plastic support with embossing, imprinting of logos, and distribution of cards

Memory Access Conditions

Phase in the life cycle	Fabrication	Prepersonalization	Personalization	Utilization	Invalidation
Access mode	Physical addressing		Logical addressing		
Operating System	Not accessible				
Fabrication data	Read. write. update	Read, but can be blocked			
Directories	Read, write, update			Not accessible in most cards	
Data	Read, write, update				
PIN	Read, write, update				

Information to be protected

- Design document
- Software
- Silicon wafers during transport from the foundry to the card supplier (using a key of 8 to 16 bits)
- Once the OS is added, all physical access to the memory is blocked

Card Invalidation

- Expiration date
- All memory space for recording new transactions has been exhausted
- Fraudulent use
- Card can be blocked when maximum number of attempts reached (3 to 7)

Physical Security of the Card during Usage

- Standard contacts to the reader
- Logo of the card issuer, financial institution, etc.
- Embossing of the card serial number
- A hologram
- Passive protection from impurities, dust, radiation, etc.

Tamper-Resistance

- Deactivation of test circuits before distribution of the card
- Inhibit output operation when there is a physical attack
- Physical protection of the memory cells to prevent selective erasures
- Storage of sequential words in noncontiguous memory locations

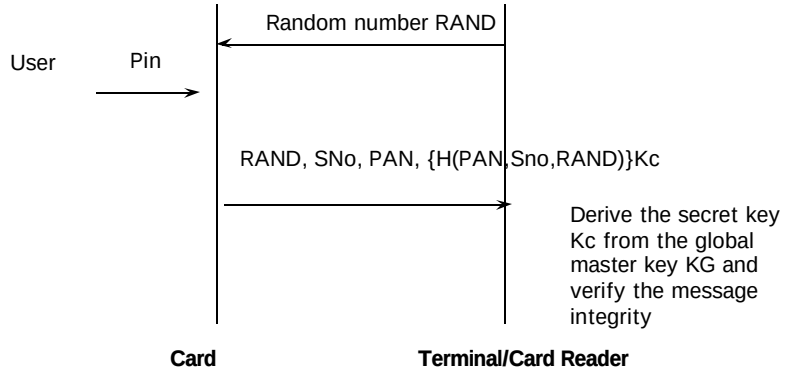
Logical Security

- Authentication of the legitimate user using the PIN
- Authentication of the card
- Establishment of a secure logical communication channel between the card and the host through the terminal reader
- Time-stamping for non-repudiation
- Limit the time validity of the card

Authentication

- Can use symmetric or asymmetric cryptographic
- Symmetric cryptography reduces the cost of the card
- On-line and off-line authentication
- Most systems are proprietary with notable exceptions
  - EMV (EuroPay, MasterCard, Visa) for payments
  - GSM for mobile telephony

Off-line Card Authentication with Symmetric Encryption



Off-line Card Authentication with Public Key Cryptography

- Static authentication
  - data used for authentication set once and for all
  - danger of cloning
- Dynamic authentication
  - It is not possible to guess the card's secrets by observing the exchange.

Static Authentication (Example)

- Used by French Banks - Public key of 320 bits
- Authentic card has a secret A and sends it to the terminal together with ID
- A is related to its ID as follows:

$$A^3 \mod n = J$$

$$J = (1 + 2^{160}) \, ID$$

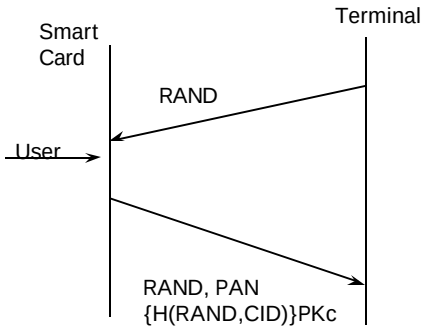
- The difficulty is in finding the cubic root of J (mod n)

Breaking Static Authentication of French Banks

- Observe the exchanges
  - deduce n and the mapping between the card parameters and the card ID or PAN (Primary Account Number)
  - decompose n into its primes
- Make up a PAN, calculate J and then A as cubic root of J (mod n)
- Fool the terminal by sending ID and A as long as the central server does not intervene for verification
- Serge Humpich (1998)

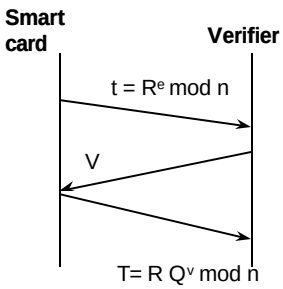
Deterministic Dynamic Authentication

- Use Public Key Encryption
- Computationally intensive
- Needs a cryptographic co-processor



Probabilistic Dynamic authentication (Guillou & Quisquater)

- $G \times Q^e \equiv 1 \bmod(n)$
- (e,n) public key of the verifier d private key
- G is derived from the identity of the card , and Q is the signature of the certification authority on the card identity (used for card authentication)
- $1 < R < (n-1)$ a random number
  - $1 < V < (e-1)$ random number
- GV $T^e \bmod n = R^e \bmod n$
- Q is kept secret.
- Legitimate owner can succeed at each step
- One chance out of (e-1) that an imposter can guess the value of Q
- For $e = 2^{16} + 1$, V is 16 bits, and the chance of an imposter is 1 out 65,536



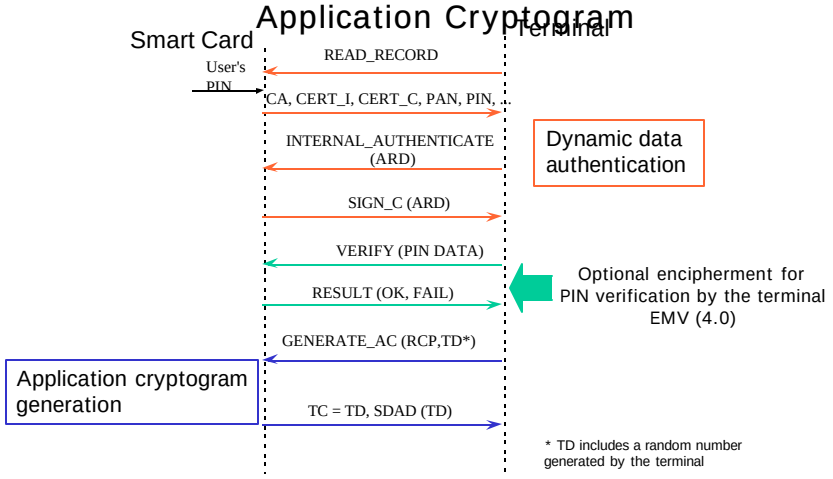
EMV

- Specifications due to EuroPay, MasterCard, Visa
- Version 4.0 issued in December 2000
- Has three authentication modes for off-line authentication
  - static data authentication
  - dynamic data authentication
  - dynamic data authentication with generation of application cryptogram

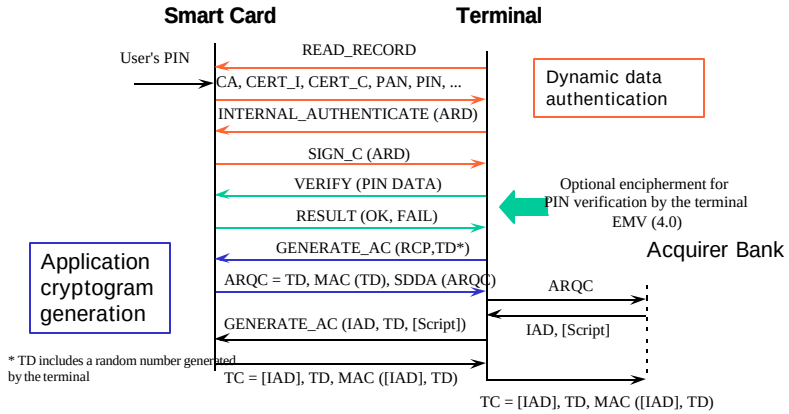
EMV - Static Authentication

- Each card contains a signature of its identity by the issuer and the certificate of the certification authority for the application
- Can recognize up to 6 public certification authorities per recognized application
- Does not protect against cloning

EMV -Dynamic Off-line Authentication with Application Cryptogram



EMV -Dynamic On-line Authentication with Application Cryptogram



Multi-application Smart Cards

- ISO 7816-4 is the starting point
- File system of ISO 7816-4:
  - dedicated (application) files (max. 62)
  - elementary files (maximum 3969 files)
  - DIR elementary file is a "directory" of applications
  - ATR elementary file points to the application or object
  - master file is the root

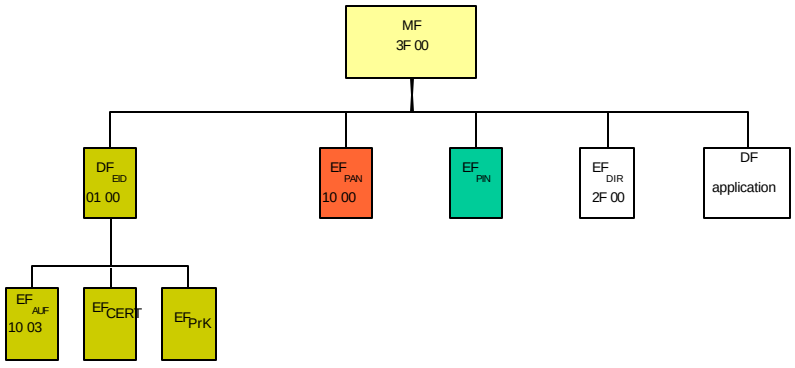
Limitations of ISO 7816-4

- Two types of elementary files:
  - internal EFs: storage of keys, certificates, storage of PINs, purse files: maximum balance, current balance, etc.
  - working EFs (for external entities)
- Cannot create new files
- Smart cards have proprietary file management commands

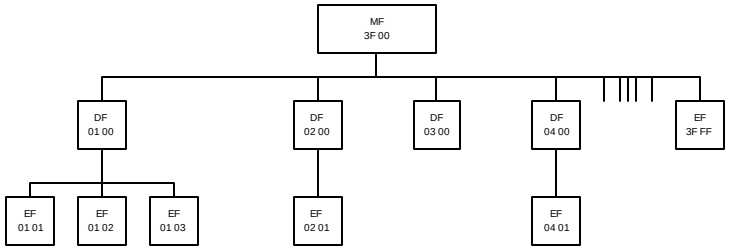
Management of Multi-application Cards

- All applications are under the control of one application. Perfect coordination among the providers of applications
- Several applications under the control of a central authority, e.g., card supplier
- Independent applications

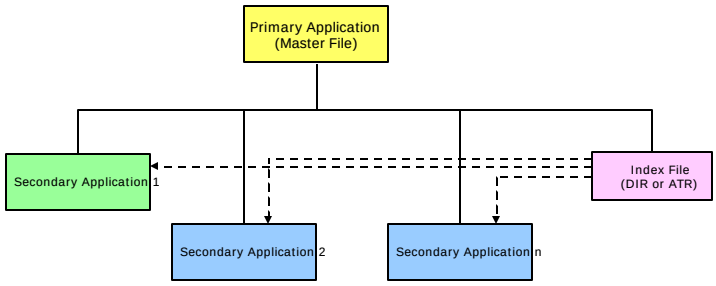
Swedish Electronic Identity Card (SEID)



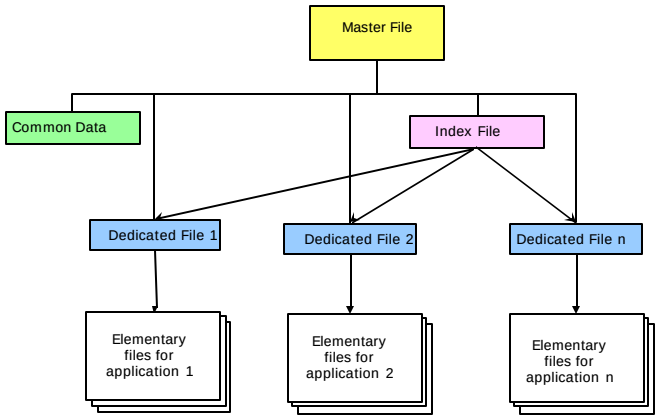
Multiapplication Smart Cards
File system ISO 7816-4



Secondary Applications Management
by the Primary Application

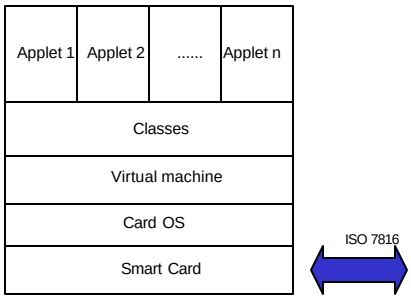


Several Applications Controlled by a Central Authority



Totally Independent Applications

- MULTOS (Mondex, MasterCard)
- JavaCard (VISA, SUN)
- Windows for Smart Card



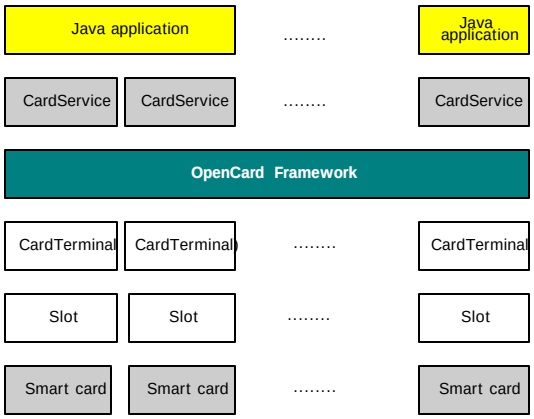
Integration of Smart Cards with PC

- OpenCard Framework for Java
- PC/SC for Windows
- MUSCLE (Movement for the use of smart cards in a Linux environment)

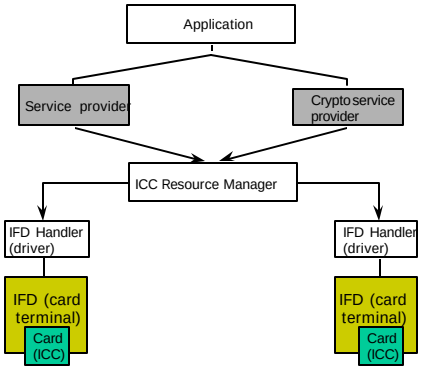
Integrated Cards and Computers

- OpenCard Framework (OpenCard Consortium)
  - Java technology
  - Mutiple-slot readers
- PC/SC Specifications
  - Windows
  - Microsoft cryptographic library CryptoAOI
- Java Card
- For multiapplication cards there are two competing operating systems (Multos and Java-based)

OpenCard Framework



PC/SC



IFD = Interface device

Limits to Cryptographic Security

- Logical (non-invasive attacks)
  - exploit faulty implementations
  - perturb the function through change of voltage, temperature or in clock frequency
  - eavesdropping (leakages, radiation, differential power analysis of power consumption)
- Physical destructive attacks
  - chemical attacks
  - laser probes, focused ion beams etc.

Security of Microprocessor Cards

- Physical security covers all phases: fabrication, personalization, distribution and usage
- Logical security:
  - authentication of the user with PIN
  - authentication of the card
  - secure communication channel between the card and the host system
- For online authorization:
  - reciprocal authentication of the cardholder and the card
  - reciprocal authentication of the card and the network terminal

Micropayments

- Micropayments < $10 U.S.
- Replace petty cash payments
  - Electronic purses in face to face commerce
  - Virtual purses for remote commerce
- To reduce operating costs through:
  - prepayment
  - reduce the computational intensity or complexity through less reliance on public key algorithms
  - offline authorization and local verification
  - grouped billing and financial clearance of transactions

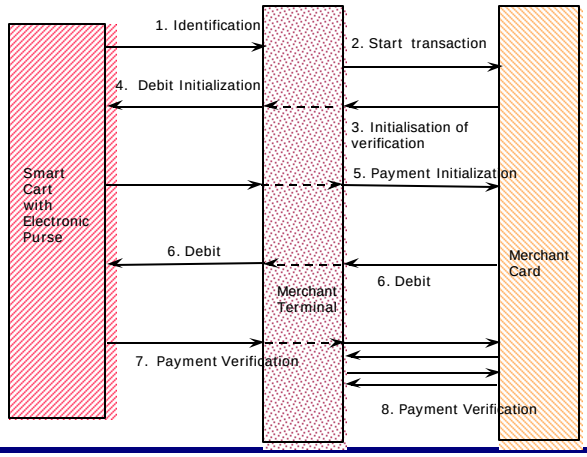
On-line Charging of the Purse

- Identification and authentication of the card
- Identification and authentication of the card holder (PIN)
- Verification with authorization server
- Update and synchronization

Off-Line Payment Authorization

- Reciprocal authentication of the client's purse and the Security Application Module (SAM) of the merchant
- Transfer of the debit amount from the client's purse to the terminal then to the merchant's card
- Production of encrypted electronic receipts
- Exchange of verification data among both parties

Message Exchange for a Payment with an Electronic Purse



Security of Purses

- Authentication of merchants, cardholders and cards
- Message Integrity through MAC computation
- Implementation quality:
  - Card Manufacturer
  - Chip Manufacturer

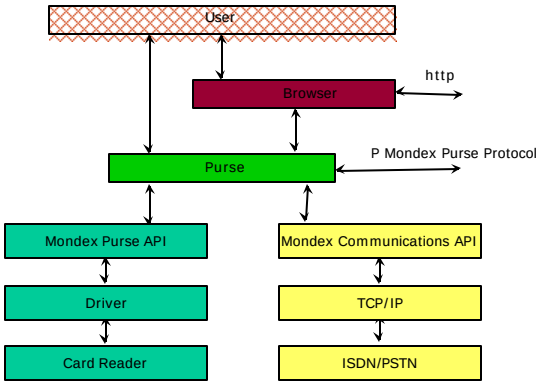
Some Purse Systems

- CHIPPER (KPN and Postbank - Netherlands)
- GeldKarte (Germany, Austria, Netherlands, Switzerland, France)
- Minipay (Italy)
- Mondex
- P-CARD (Germany)
- PAYCHIP (Austria)
- PROTON (Belgium and many other countries)

Characteristics

- Currency
- Maximum value
- Size of RAM, ROM, EEPROM
- Security algorithms
- New standard for purses (wallets) is ECML (Electronic Commerce Markup Language) to standardize the format of the messages exchanged

Configuration of a Mondex Client



Mondex Pilot Experiments

- Swindon (UK)
- Guelph (Canada)
- San Francisco and Manhattan (USA)
- Hong Kong
- No success yet

Remote Payment

- Commercial offers
  - Milicent
  - KLELine/Odysseo
- Research experiments
  - NetBill
  - PayWord and MicroMint

Characteristics

- Services offered (authentication, integrity, confidentiality)
- Authorization (Online or offline)
- Security protocols
- Type of customer's secrets and their storage location
- Nature of money
- Minimum payment and payment revocability
- How value is stored
- Billing (per transaction or grouped)

KLELine

- Platform for secure payments
- Under the control of a bank
- Multiple currencies
- Discontinued in January 2000 and phased-out for the benefit of CyberCom
- Re-emerged with some differences on the client side as Odysseo

Millicent

- A Jeton called scrip (value from 0.1 cent to $50 U.S.) that is a promise of service
  - Vendor ID
  - Value
  - Customer ID
  - Expiration date
  - Proof of Integrity
  - Comments
- Vendor scrip = timed account
- Broker scrip can be accepted by several vendors

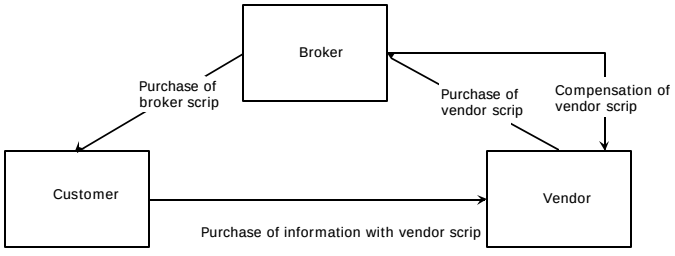
Levels of Security

- No protection
- Using an encrypted channel between the customer and the vendor (using a shared secret) for confidentiality
- Protection against scrip tampering or falsification for integrity

Reduction of Cost per Transaction

- Prepayment:
  - subscription to open an account
  - prepayment of service with vendor scrip before receiving the service
- Reduction of cryptographic load: authentication is with symmetric algorithms
- Offline authorization
- Local verification and timed scrips
- Grouping of transactions
- No revocation or contest of transactions

Cycle of Various Scrips in Millicent



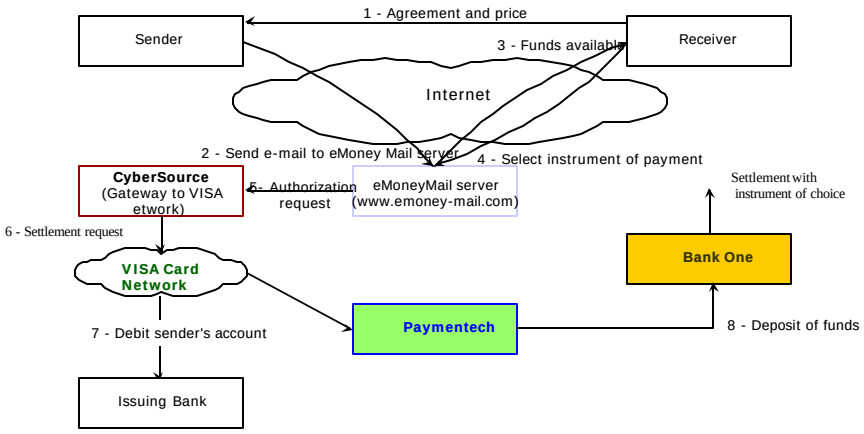
New Remote Payment Intermediaries

- Facilitators (PayPal.com)
- Minitel model: Network of ISP's and merchants: software that represents the client installed on ISP's server
  - Intermediary records the transactions and collects the payment and payback the ISP and merchants (1ClickCharge)
  - Intermediary relies on the ISP for collecting payments and getting its fees (Minitel model)
- Virtual jeton-holder (Qpass and eCoin)

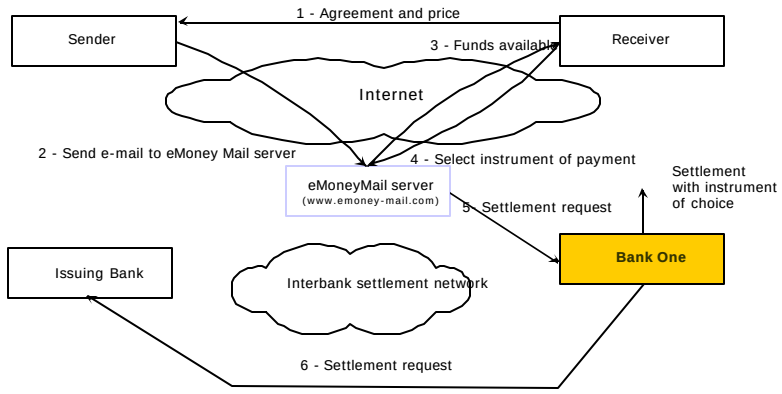
eMoney Mail

- BankOne, GTE Internetworking, Cybersource, Visa, Paymentech
- Sender can chose payment type (debit, credit, check)
- Certificate issued by Verisign for authentication
- Encryption with a symmetric session key of 128 bits
- Link between the server and BankOne encrypted with symmetric encryption with 1024-bit key

Payment with a Visa Card



Payment with a Check

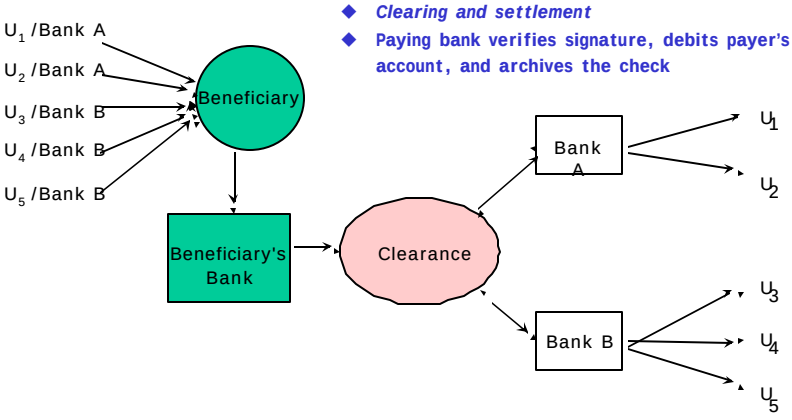


Dematerialized Processing of Paper-Based Checks

- Electronic Check Presentment (ECP)
- Check Imaging
- POS Check Approval

Processing Paper Checks

- **Payer writes a check, signs it, and sends it to the beneficiary**
- ***Clearing and settlement***
- **Paying bank verifies signature, debits payer's account, and archives the check**



Dematerialized Checks

- Of interest in the US and France
- Dematerialized processing of paper checks
  - electronic check presentment
  - check imaging
- Replacement of paper checks
  - Virtual checks

Electronic Check Presentment (ECP)

- Present the data on the check electronically to the paying bank then send the paper checks
- Reduce cost and increase speed of payment to the payees
- Digital information from checks covered under the Electronic Signatures in Global and National Commerce Act of 2000
- ANSI X9.37US since 1998

CREIC

- France (since1990)
- Driver: cost reduction
- Information in magnetic ink according to CMC7 specifications
- In 1996 covered 10% of checks

Check Imaging

- Avoid the physical transport of checks from the payment cycle at the bank of first deposit
  - ANSI X9.46 for image format
  - Output TIFF or COFF
  - CIIP (Check Image Interchange Protocol) to transmit the image file on command
- Tested in US by FSTC (Financial Services Technology Consortium)- Transferred to SVPCo(SafeCheck Payment Service Co) a commercial venture
- Implementation expected within a year

Point of Sale (POS) Check Approval

- Pilot service called SafeCheck developed by SVPCo (SafeCheck Payment Service Co.)
- Combination of ECP and debit card technologies
  - Capture MICR data at the POS
  - Verify with issuer bank (customer's bank)
  - Cancel approved check
  - Return to customer
- Difficulties
  - Variability of MICR formats
  - Many banks have to improve their systems

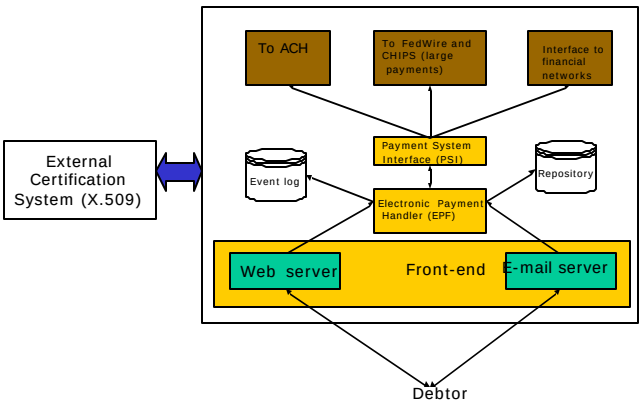
Virtual Checks Projects

- BIPS (Bank Internet Payment System)
- Echeck (co-sponsored wit the U.S. Treasury)
- Both are from FSTC (Financial Services Technology Consortium)
- Must take into considerations banks that cannot process virtual checks
- Reconciliation of customer's data and bank data

Virtual Checks Protocols

- Financial Services Technology Consortium (FSTC)
  - BIPS uses NPP (Network Payment Protocol)
- Open Finance Exchange (OFX) :Microsoft, Intuit and Checkfree not compatible with XML or SWIFT
- Gold Integrion

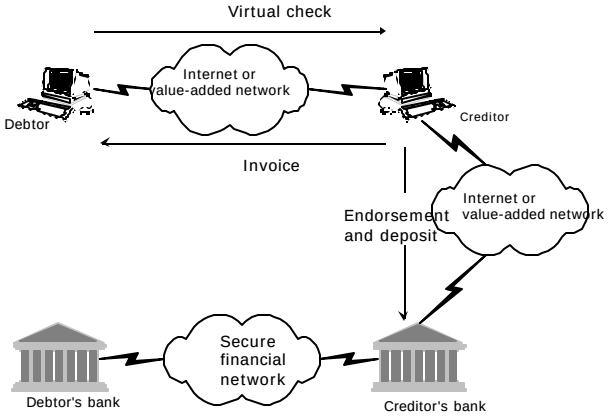
BIPS Banking Server



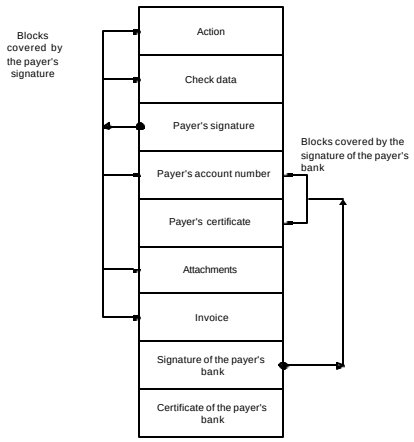
Echeck Characteristics

- Financial Services Markup Language (FSML)
  - SGML -> SDML (Signed Document Markup Language) -> FSML
  - Designed for financial applications of microprocessor cards
  - Not compatible with XML
- Signature
  - MD5/RSA
  - SHA1/DSA

Exchanges with Echeck



Representation of a Virtual Check in Echeck



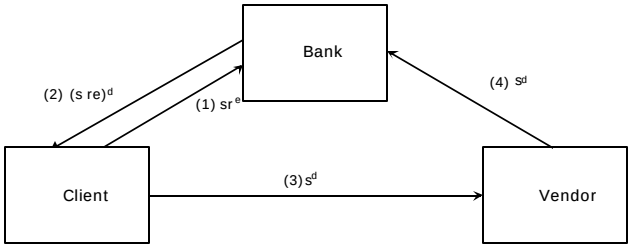
Digital Money

- Similar to cash: anonymous and untraceable
- Confidentiality and authentication may be added
- Support is "virtual" (hard disk of the user or microprocessor memory)
- Value stored in the form of an algorithm
- Raises many legal and financial issues

Untraceability

- Work of David Chaum
- Operations based on blind signature
  - The payer mints the digital coin
  - The bank seals it without having access to the coin's serial number
- Debtor untraceability
- Creditor untraceability
- Mutual untraceability

Debtor Untraceability

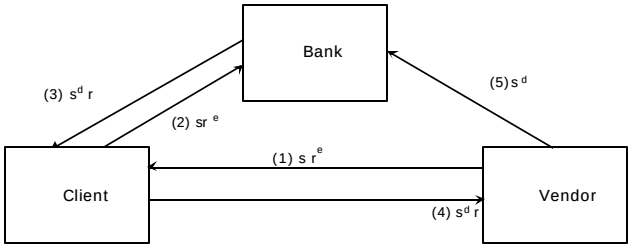


N = pq, p and q are prime odd numbers

$1 \leq r \leq (N-1)$ is a random number called *blinding factor*

e public key, d private key, $e \times d = 1 \bmod (p-1)(q-1)$

Creditor Untraceability

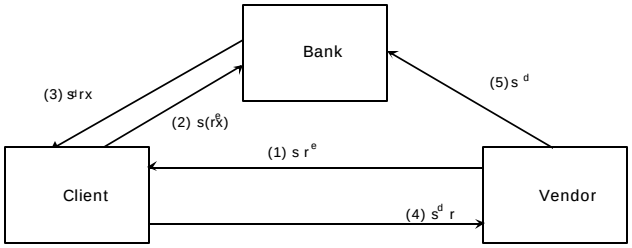


N = pq, p and q are prime odd numbers

$1 \le r \le (N-1)$ is a random number called *blinding factor*

e public key, d private key, $e \times d = 1 \bmod (p-1)(q-1)$

Mutual Untraceability



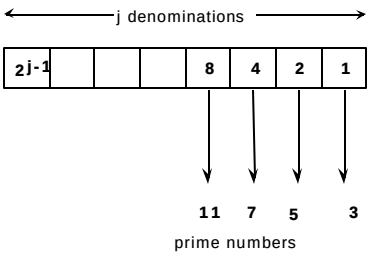
N = pq, p and q are prime odd numbers

$1 \le r, x \le (N-1)$ are random numbers called *blinding factors*

e public key, d private key, $e \times d = 1 \bmod (p-1)(q-1)$

Representations of Denominations

- Solves the problems of change
- Detection of counterfeit (multiple spending)



DigiCash

- Formed by David Chaum in 1990 in the Netherlands and the US
- Initially supported by Mark Twain Bank of St. Louis, MO until 1999
- European trials in the CAFE program
- Filed for bankruptcy in 1999
- Technology and patents now under control of Ecash Technologies which

NETCASH

- Online payment system with digital coins
- USC-ISI and MIT
- Uses ARDP (Asynchronous Reliable Delivery Protocol) on top of UDP
- Research prototype

Limits to Security

- Non-invasive attacks
- Destructive attack
- Negligence in the implementation of security

General Remarks

- Incompatible payment systems
- Attempts at solutions:
  - SEMPER
  - CommerceNet
  - ECML as a common language to wallets

Need for Standardization

- Operating systems of smart cards
- Protocols for charging electronic or virtual purses or jeton holders with value
- Interface between the user and the various applications (Electronic Bill Presentment and Payment, data from various stock exchanges)
- Interoperability of payment systems (particularly micropayment systems)
- Certification and revocation of certificates

Evolution

- Business-to-Business
  - Integration with legacy procedures and systems
- Business-to-consumer
  - incentives
  - currency conversion
- Face-to-face transactions

Perspectives