Handbook of Banking Technology

Lonna Daily

First Edition, 2012

ISBN 978-81-323-2771-4

Published by:
Orange Apple
4735/22 Prakashdeep Bldg,
Ansari Road, Darya Ganj,
Delhi - 110002
Email: info@wtbooks.com

Table of Contents

Chapter- 1

Automated Clearing House

Automated Clearing House (ACH) is an electronic network for financial transactions in the United States. ACH processes large volumes of credit and debit transactions in batches. ACH credit transfers include direct deposit payroll and vendor payments. ACH direct debit transfers include consumer payments on insurance premiums, mortgage loans, and other kinds of bills. Debit transfers also include new applications such as the Point-of-Purchase (POP) check conversion pilot program sponsored by NACHA-The Electronic Payments Association. Both the government and the commercial sectors use ACH payments. Businesses are also increasingly using ACH to collect from customers online, rather than accepting credit or debit cards.

Rules and regulations governing the ACH network are established by NACHA (formerly the National Automated Clearing House Association) and the Federal Reserve. In 2002, this network processed an estimated 8.05 billion ACH transactions with a total value of $21.7 trillion. (Credit card payments are handled by separate networks.)

The Federal Reserve Banks are collectively the nation's largest automated clearinghouse operator and in 2005 processed 60% of commercial interbank ACH transactions. The Electronic Payments Network (EPN), the only private sector ACH operator in the U.S., processed the remaining 40%. FedACH is the Federal Reserve's centralized application software used to process ACH transactions. EPN and the Reserve Banks rely on each other for the processing of some transactions when either party to the transaction is not their customer. These interoperator transactions are settled by the Reserve Banks.

Uses of the ACH payment system

- Direct deposit of payroll, Social Security (United States) and other government payments, and tax refunds
- Direct debit payment of consumer bills such as mortgages, loans, utilities, insurance premiums, rents, and any other regular payment
- Business-to-business payments
- E-commerce payments
- Federal, state, and local tax payments
- Bank Treasury management departments sell this service to business and government customers

SEC Codes

Some common Standard Entry Class (SEC) Codes:

ARC
: *Accounts Receivable Entry*. A consumer check converted to a one-time ACH debit. The difference between ARC and POP is that ARC can result from a check mailed in where as POP is in-person.

BOC
: *Back Office Conversion*. A single entry debit initiated at the point of purchase or at a manned bill payment location to transfer funds through conversion to an ACH debit entry during back office processing. Unlike ARC entries, BOC conversions require the customer to be present and a notice that checks may be converted to BOC ACH entries be posted.

CBR
: *Corporate Cross-border Payment*. Used for international business transactions, replaced by SEC Code IAT.

CCD
: *Corporate Credit or Debit*. Primarily used for business-to-business transactions.

CTX
: *Corporate Trade Exchange*. Transactions that include ASC X12 or EDIFACT information.

DNE
: *Death Notification Entry*. Issued by the federal government.

IAT
: *International ACH Transaction*. This is a new SEC Code for cross-border payment traffic. The code will replace the PBR and CBR codes. The new code will be implemented September 18, 2009.

PBR
: *Consumer Cross-border Payment*. Used for international household transactions, replaced by SEC Code IAT.

POP
: *Point-of-Purchase*. A check presented in-person to a merchant for purchase is presented as an ACH entry instead of a physical check.

POS
: *Point-of-Sale*. A debit at an electronic terminal initiated by use of a plastic card. An example is using your debit card to purchase gas.

PPD
: *Prearranged Payment and Deposits*. Used to credit or debit a consumer account. Popularly used for payroll direct deposits and preauthorized bill payments.

RCK
: *Represented Check Entries*. A physical check that was presented but returned because of insufficient funds may be represented as an ACH entry.

TEL
: *Telephone Initiated-Entry*. Verbal authorization by telephone to issue an ACH entry such as checks by phone. (TEL code allowed for inbound telephone orders

only. NACHA disallows the use of this code for outbound telephone solicitations unless a prior business arrangement with the customer has been established.)

WEB

Web Initiated-Entry. Electronic authorization through the Internet to create an ACH entry.

XCK

Destroyed Check Entry. A physical check that was destroyed because of a disaster can be presented as an ACH entry.

ACH process

An ACH transaction starts with a Receiver authorizing an Originator to issue ACH debit or credit to an account. A Receiver is the account holder that grants the authorization. An Originator can be a person or a company (such as the gas company, a local cable company, or one's employer). Accounts are identified by the bank's Routing Number and the account number within that bank.

Example 1: Alice buys a tee shirt at Bob's Gift Shop with a check for $15. Alice is the Receiver; her bank account will eventually receive the order to take $15 out from her account. Bob's Gift Shop is the Originator. The check, signed by Alice, authorizes Bob's Gift Shop, Inc to originate the ACH transaction, code POP. The check has Alice's routing number and account number.

Example 2: Candice has her paycheck at Delirium Designs deposited directly to her checking account. Delirium Designs is the Originator, but cannot begin until Candice, the Receiver, fills out a form for direct deposits, including her bank routing number and account number.

In accordance with the rules and regulations of ACH, no financial institution may issue an ACH transaction (whether it be debit or credit) towards an account without prior authorization from the Receiver. Depending on the ACH transaction, the Originator must receive written (SEC Codes: ARC, POP, PPD), verbal (TEL), or electronic (WEB) authorization from the Receiver. Written authorization constitutes a signed form giving consent on the amount, date, or even frequency of the transaction. Verbal authorization needs to be either audio recorded or the Originator must send a receipt of the transaction details before or on the transaction date. An electronic authorization must include a customer being presented the terms of the agreement and typing or selecting some form of an "I agree" statement.

Once authorization is acquired, the Originator then creates an ACH entry to be given to an Originating Depository Financial Institution (ODFI), which can be any financial institution that does ACH origination. This ACH entry is then sent to an ACH Operator that passes it on to the Receiving Depository Financial Institution (RDFI), where the Receiver's account is issued either a debit or credit.

Example 1: Bob's Gift Shop, in its central office, turns the check into an ACH transaction that it submits to its bank, in this case the ODFI. This transaction reaches Alice's bank, in this case the RDFI, who debits (takes the money out of) Alice's account.

Example 2: Delirium Designs submits an ACH transaction to its bank, acting as ODFI. It traverses through the system to Candice's bank, who credits (deposits the money into) Candice's bank account.

The RDFI may, however, reject the ACH transaction and return it to the ODFI if, for example, the account had insufficient funds or the account holder indicated that the transaction was unauthorized. An RDFI has a prescribed amount of time in which to perform returns, ranging from 2 to 60 days from the receipt of the ACH transaction. However, the majority of returned transactions are completed within 24 hours from midnight of the day the RDFI receives the transaction.

Example 1: Unfortunately, Alice has been living beyond her means, and her checking account is down to $3.44, causing the ACH transaction for $15 to bounce. The original transaction is completed, so Alice's bank (the RDFI) now prepares an ACH transaction, code RCK, to grab the $15 back through the ACH system. For this transaction, however, Alice's bank is the ODFI and the Gift Shop's bank is the RDFI.

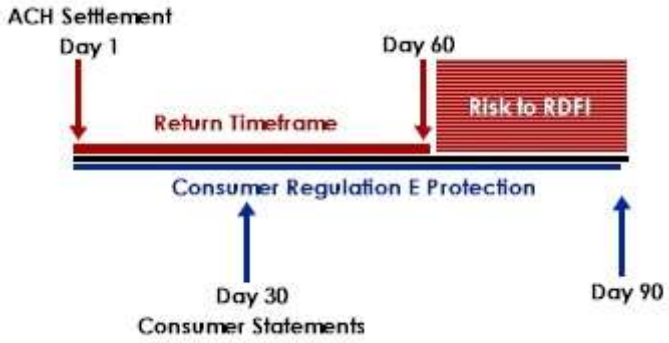
An ODFI receiving a returned ACH entry may re-present the ACH entry two more times for settlement. Again, the RDFI may reject the transaction. After which, the ODFI may no longer represent the transaction via ACH.

Example 1: Bob's Gift Shop still needs their $15. The easiest way is to just submit the original transaction again, hoping that enough money shows up in Alice's bank account so that it clears. After two tries, they have to contact Alice themselves to get their money.

Common issues

ACH payments have been around for some time now, but people are just getting used to them, especially with the ARC, POP, and RCK SEC Codes, where the original instrument was a physical check. One problem occurs when the account holder issues a stop payment on a physical check not knowing that the check was presented as an ACH entry.

Time frame differences can cause loss towards a 'Receiving Depository Financial Institution' when returned ACH entries are subject to the Regulation E. An example is for the ARC and POP SEC Codes, where an RDFI has only 60 days from the date of settlement to return an unauthorized debit, and the consumer has 60 days upon notification to dispute a transaction in his statement under Regulation E. The consumer can receive notification via a statement 30 days after settlement. With these time frames, it is possible that the 60-day period allowed for ACH return would expire even before the consumer's 60-day protection (under Regulation E) would expire, leaving the RDFI open to loss.



Another problem deals with compliance where the merchant presented with a check issues an ACH entry with SEC Codes ARC or POP. However, the merchant then fails to comply with the handling of the physical check and presents the physical check for payment as well. This causes a double-debit against a consumer account...

Chapter- 2

Automated Teller Machine

An NCR Personas 75-Series interior, multi-function ATM in the USA

Smaller indoor ATMs dispense money inside convenience stores and other busy areas, such as this off-premise Wincor Nixdorf mono-function ATM in Sweden.

An **automated teller machine** (**ATM**), also known as a **automated banking machine** (**ABM**) or **Cash Machine** and by several other names, is a computerised telecommunications device that provides the clients of a financial institution with access to financial transactions in a public space without the need for a cashier, human clerk or bank teller.

On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip, that contains a unique card number and some security information such as an expiration date or CVVC (CVV).

Authentication is provided by the customer entering a personal identification number (PIN).

Using an ATM, customers can access their bank accounts in order to make cash withdrawals, credit card cash advances, and check their account balances as well as purchase prepaid cellphone credit. If the currency being withdrawn from the ATM is different from that which the bank account is denominated in (e.g.: Withdrawing Japanese Yen from a bank account containing US Dollars), the money will be converted at a wholesale exchange rate. Thus, ATMs often provide the best possible exchange rate for foreign travelers and are heavily used for this purpose as well.

ATMs are known by various other names including **automatic banking machine** (or *automated banking machine* particularly in the United States) (**ABM**), *automated transaction machine*, *cashpoint* (particularly in the United Kingdom, where it is a trademark of Lloyds TSB), *money machine*, *bank machine*, *cash machine*, *hole-in-the-wall*, *autoteller* (after the Bank of Scotland's usage), *cashline machine* (after the Royal Bank of Scotland's usage), *MAC Machine* (in the Pittsburgh and Philadelphia areas), *Pass Machine* in Ireland, *Bankomat* (in various countries particularly in Europe and including Russia), *Multibanco* (after a registered trade mark, in Portugal), *Minibank* in Norway, *Geld Automaat* in Belgium and the Netherlands, and *All Time Money* in India.

History

An old Nixdorf ATM

The idea of self-service in retail banking developed through independent and simultaneous efforts in Japan, Sweden, the United States and the United Kingdom. In the USA, Luther George Simjian has been credited with developing and building the first cash dispenser machine. There is strong evidence to suggest that Simjian worked on this device before 1959 while his 132nd patent (US3079603) was first filed on 30 June 1960 (and granted 26 February 1963). The rollout of this machine, called Bankograph, was delayed a couple of years. This was due in part to Simjian's Reflectone Electronics Inc. being acquired by Universal Match Corporation. An experimental Bankograph was

installed in New York City in 1961 by the City Bank of New York, but removed after 6 months due to the lack of customer acceptance. The Bankograph was an automated envelope deposit machine (accepting coins, cash and cheques) and it did not have cash dispensing features. The Bankograph, however, embodied the preoccupation by US banks in finding alternative means to capture core deposits, while the concern of European and Asian banks was cash distribution.

A first cash dispensing device was used in Tokyo in 1966. Although little is known of this first device, it seems to have been activated with a credit card rather than accessing current account balances. This technology had no immediate consequence in the international market.

Plaque commemorating installation of world's first bank cash machine

In simultaneous and independent efforts, engineers in Sweden and Britain developed their own cash machines during the early 1960s. The first of these that was put into use was by Barclays Bank in Enfield Town in North London, United Kingdom, on 27 June 1967. This machine was the first in the UK and was used by English comedy actor Reg Varney, at the time so as to ensure maximum publicity for the machines that were to become mainstream in the UK. This instance of the invention has been credited to John Shepherd-Barron, while disregarding other engineers at De La Rue Instruments, since 2008 Talaris, who contributed to the design and development of that machine. Nevertheless, Shepherd-Barron was awarded an OBE in the 2005 New Year's Honours List. His design used special checks that were matched with a personal identification number, as plastic bank cards had not yet been invented.

The Barclays-De La Rue machine (called De La Rue Automatic Cash System or DACS) beat the Swedish saving banks' and a company called Metior's (a device called Bankomat) by nine days and Westminster Bank's-Smith Industries-Chubb system (called Chubb MD2) by a month. The collaboration of a small start-up called Speytec and Midland Bank developed a third machine which was marketed after 1969 in Europe and the USA by the Burroughs Corporation. The patent for this device (GB1329964) was filed on September 1969 (and granted in 1973) by John David Edwards, Leonard Perkins, John Henry Donald, Peter Lee Chappell, Sean Benjamin Newcombe & Malcom David Roe.

Both the DACS and MD2 accepted only a single-use token or voucher which was retained by the machine while the Speytec worked with a card with a magnetic stripe at the back. Hence all this these worked on various principles including Carbon-14 and low-coercivity magnetism in order to make fraud more difficult. The idea of a PIN stored on the card was developed by a British engineer working in the MD2 named James Goodfellow in 1965 (patent GB1197183 filed on 2 May 1966 with Anthony Davies). The essence of this system was that is it enabled the verification of the customer with the debited account without human intervention. This patent is also the earliest instance of a complete "currency dispenser system" in the patent record. This patent was filled on 5 March 1968 in the USA (US 3543904) and granted on 1 December 1970. It had a profound influence on the industry as a whole. Not only did future entrants into the cash dispenser market such as NCR Corporation and IBM licence Goodfellow's PIN system, but a number of later patents references this patent as "Prior Art Device".

After looking first hand at the experiences in Europe, in 1968 the networked ATM was pioneered in the US, in Dallas, Texas, by Donald Wetzel, who was a department head at an automated baggage-handling company called Docutel. On September 2, 1969, Chemical Bank installed the first ATM in the U.S. at its branch in Rockville Centre, New York. The first ATMs were designed to dispense a fixed amount of cash when a user inserted a specially coded card. A Chemical Bank advertisement boasted "On Sept. 2 our bank will open at 9:00 and never close again." Chemicals' ATM, initially known as a Docuteller was designed by Donald Wetzel and his company Docutel. Chemical executives were initially hesitant about the electronic banking transition given the high cost of the early machines. Additionally, executives were concerned that customers

would resist having machines handling their money. In 1995, the Smithsonian National Museum of American History recognised Docutel and Wetzel as the inventors of the networked ATM.

ATMs first came into use in December 1972 in the UK; the IBM 2984 was designed at the request of Lloyds Bank. The 2984 CIT (Cash Issuing Terminal) was the first true Cashpoint, similar in function to today's machines; Cashpoint is still a registered trademark of Lloyds TSB in the UK. All were online and issued a variable amount which was immediately deducted from the account. A small number of 2984s were supplied to a US bank. Notable historical models of ATMs include the IBM 3624 and 473x series, Diebold 10xx and TABS 9000 series, and NCR 50xx series.

Location

An ATM Encrypting PIN Pad (EPP) with German markings

ATMs are placed not only near or inside the premises of banks, but also in locations such as shopping centers/malls, airports, grocery stores, petrol/gas stations, restaurants, or any place large numbers of people may gather. These represent two types of ATM installations: on and off premise. On premise ATMs are typically more advanced, multi-function machines that complement an actual bank branch's capabilities and thus more expensive. Off premise machines are deployed by financial institutions and also ISOs (or Independent Sales Organizations) where there is usually just a straight need for cash, so they typically are the cheaper mono-function devices. In Canada, when an ATM is not operated by a financial institution it is known as a "White Label ATM".

In North America, banks often have drive-thru lanes providing access to ATMs.

Many ATMs have a sign above them indicating the name of the bank or organization owning the ATM, and possibly including the list of ATM networks to which that machine is connected. This type of sign is called a *topper*.

Financial networks

An ATM in the Netherlands. The logos of a number of interbank networks this ATM is connected to are shown.

Most ATMs are connected to interbank networks, enabling people to withdraw and deposit money from machines not belonging to the bank where they have their account or in the country where their accounts are held (enabling cash withdrawals in local currency). Some examples of interbank networks include PULSE, PLUS, Cirrus, Interac, Interswitch, STAR, and LINK.

ATMs rely on authorization of a financial transaction by the card issuer or other authorizing institution via the communications network. This is often performed through an ISO 8583 messaging system.

Many banks charge ATM usage fees. In some cases, these fees are charged solely to users who are not customers of the bank where the ATM is installed; in other cases, they apply to all users.

In order to allow a more diverse range of devices to attach to their networks, some interbank networks have passed rules expanding the definition of an ATM to be a

terminal that either has the vault within its footprint or utilizes the vault or cash drawer within the merchant establishment, which allows for the use of a scrip cash dispenser.

A Diebold 1063ix with a dial-up modem visible at the base

ATM in Trogir, Croatia

ATMs typically connect directly to their host or ATM Controller via either ADSL or dial-up modem over a telephone line or directly via a leased line. Leased lines are preferable to POTS lines because they require less time to establish a connection. Leased lines may be comparatively expensive to operate versus a POTS line, meaning less-trafficked machines will usually rely on a dial-up modem. That dilemma may be solved as high-speed Internet VPN connections become more ubiquitous. Common lower-level layer communication protocols used by ATMs to communicate back to the bank include SNA over SDLC, TC500 over Async, X.25, and TCP/IP over Ethernet.

In addition to methods employed for transaction security and secrecy, all communications traffic between the ATM and the Transaction Processor may also be encrypted via methods such as SSL.

Global use

There are no hard international or government-compiled numbers totaling the complete number of ATMs in use worldwide. Estimates developed by ATMIA place the number of ATMs in use currently at over 1.8 million.

For the purpose of analyzing ATM usage around the world, financial institutions generally divide the world into seven regions, due to the penetration rates, usage statistics, and features deployed. Four regions (USA, Canada, Europe, and Japan) have high numbers of ATMs per million people. and generally slowing growth rates. Despite the large number of ATMs, there is additional demand for machines in the Asia/Pacific area as well as in Latin America. ATMs have yet to reach high numbers in the Near East/Africa.

The world's most northerly installed ATM is located at Longyearbyen, Svalbard, Norway.

The world's most southerly installed ATM is located at McMurdo Station, Antarctica.

While India claims to have the world's highest installed ATM at Nathu La Pass, India installed by the Union Bank of India at 4310 meters, there are higher ATMs installed in Nagchu County, Tibet at 4500 meters by Agricultural Bank of China.

Israel has the world's lowest installed ATM at Ein Bokek at the Dead Sea, installed independently by a grocery store at 421 meters below (Mediterranean) Sea level.

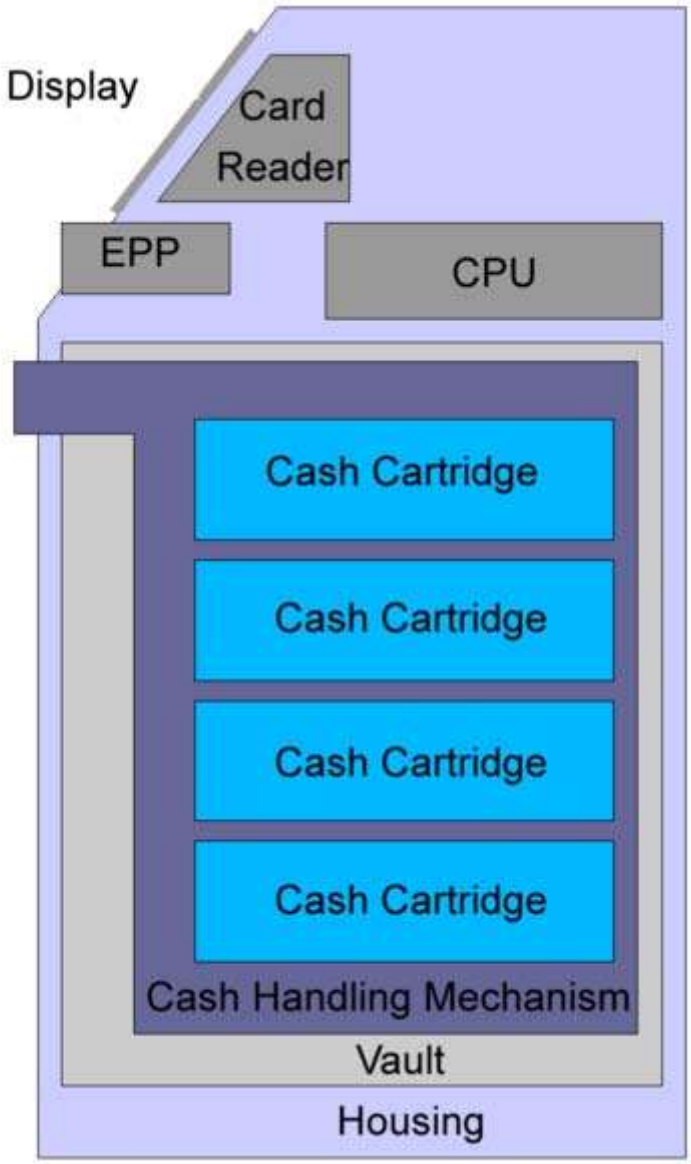
While ATMs are ubiquitous on modern cruise ships, ATMs can also be found on some US Navy ships.

In the United Kingdom, an ATM may be colloquially referred to as a "Cashpoint", named after the Lloyds Bank ATM brand, or "hole-in-the-wall", after which the equivalent Barclays brand was later named. In Scotland the term Cashline has become a generic term for an ATM, based on the branding from the Royal Bank of Scotland.

In the Republic of Ireland, ATMs are also commonly referred to as a "Banklink", named after the Allied Irish Bank brand of machines.

In Israel, ATMs are commonly referred to as "Kaspomat" (Hebrew: כספומט), which is a compound word meaning "automatic money" in Hebrew, named after the Bank Leumi & Israel Discount Bank brand of machines.

Hardware



A block diagram of an ATM

An ATM is typically made up of the following devices:

- CPU (to control the user interface and transaction devices)
- Magnetic and/or Chip card reader (to identify the customer)
- PIN Pad (similar in layout to a Touch tone or Calculator keypad), often manufactured as part of a secure enclosure.
- Secure cryptoprocessor, generally within a secure enclosure.
- Display (used by the customer for performing the transaction)

- Function key buttons (usually close to the display) or a Touchscreen (used to select the various aspects of the transaction)

- Record Printer (to provide the customer with a record of their transaction)
- Vault (to store the parts of the machinery requiring restricted access)
- Housing (for aesthetics and to attach signage to)

Recently, due to heavier computing demands and the falling price of computer-like architectures, ATMs have moved away from custom hardware architectures using microcontrollers and/or application-specific integrated circuits to adopting the hardware architecture of a personal computer, such as, USB connections for peripherals, ethernet and IP communications, and use personal computer operating systems. Although it is undoubtedly cheaper to use commercial off-the-shelf hardware, it does make ATMs potentially vulnerable to the same sort of problems exhibited by conventional computers.

Business owners often lease ATM terminals from ATM service providers.

Two Loomis employees refilling an ATM at the Downtown Seattle REI.

The vault of an ATM is within the footprint of the device itself and is where items of value are kept. Scrip cash dispensers do not incorporate a vault.

Mechanisms found inside the vault may include:

- Dispensing mechanism (to provide cash or other items of value)
- Deposit mechanism including a Check Processing Module and Bulk Note Acceptor (to allow the customer to make deposits)
- Security sensors (Magnetic, Thermal, Seismic, gas)
- Locks: (to ensure controlled access to the contents of the vault)

- Journaling systems; many are electronic (a sealed flash memory device based on proprietary standards) or a solid-state device (an actual printer) which accrues all records of activity including access timestamps, number of bills dispensed, etc. - This is considered sensitive data and is secured in similar fashion to the cash as it is a similar liability.

ATM vaults are supplied by manufacturers in several grades. Factors influencing vault grade selection include cost, weight, regulatory requirements, ATM type, operator risk avoidance practices, and internal volume requirements. Industry standard vault configurations include Underwriters Laboratories UL-291 "Business Hours" and Level 1 Safes, RAL TL-30 derivatives, and CEN EN 1143-1:2005 - CEN III/VdS and CEN IV/LGAI/VdS.

ATM manufacturers recommend that vaults be attached to the floor to prevent theft.

Software

A Suncorp Metway ATM running OS/2

With the migration to commodity PC hardware, standard commercial "off-the-shelf" operating systems and programming environments can be used inside of ATMs. Typical platforms previously used in ATM development include RMX or OS/2. Today the vast

majority of ATMs worldwide use a Microsoft OS, primarily Windows XP Professional or Windows XP Embedded.

A small number of deployments may still be running older versions such as Windows NT, Windows CE or Windows 2000. Notably, Vista was not widely adopted in ATMs. There is a computer industry security view or consensus that desktop operating systems have greater risks as operating systems for cash dispensing machines than other types of operating systems like (Secure) Real Time Operating Systems (RTOSs). RISKS Digest has many articles about cash machine operating system vulnerabilities .

A Wincor Nixdorf ATM running Windows 2000

Linux is also finding some reception in the ATM marketplace. An example of this is Banrisul, the largest bank in the south of Brazil, which has replaced the MS-DOS operating systems in its ATMs with Linux. Banco do Brasil is also migrating ATMs to Linux.

Common application layer transaction protocols, such as Diebold 91x (911 or 912) and NCR NDC or NDC+ provide emulation of older generations of hardware on newer platforms with incremental extensions made over time to address new capabilities, although companies like NCR continuously improve these protocols issuing newer versions (e.g. NCR's AANDC v3.x.y, where x.y are subversions). Most major ATM

manufacturers provide software packages that implement these protocols. Newer protocols such as IFX have yet to find wide acceptance by transaction processors.

With the move to a more standardized software base, financial institutions have been increasingly interested in the ability to pick and choose the application programs that drive their equipment. WOSA/XFS, now known as CEN XFS (or simply XFS), provides a common API for accessing and manipulating the various devices of an ATM. J/XFS is a Java implementation of the CEN XFS API.

While the perceived benefit of XFS is similar to the Java's "Write once, run anywhere" mantra, often different ATM hardware vendors have different interpretations of the XFS standard. The result of these differences in interpretation means that ATM applications typically use a middleware to even out the differences between various platforms.

With the onset of Windows operating systems and XFS on ATM's, the software applications have the ability to become more intelligent. This has created a new breed of ATM applications commonly referred to as programmable applications. These types of applications allows for an entirely new host of applications in which the ATM terminal can do more than only communicate with the ATM switch. It is now empowered to connected to other content servers and video banking systems.

Notable ATM software that operates on XFS platforms include Triton PRISM, Diebold Agilis EmPower, NCR APTRA Edge, CR2 BankWorld, KAL Kalignite, Phoenix Interactive VISTAatm, and Wincor Nixdorf ProTopas.

With the move of ATMs to industry-standard computing environments, concern has risen about the integrity of the ATM's software stack.

Security

A Triton brand ATM with a dip style card reader and a triple DES keypad

Security, as it relates to ATMs, has several dimensions. ATMs also provide a practical demonstration of a number of security systems and concepts operating together and how various security concerns are dealt with.

Physical

A Wincor Nixdorf Procash 2100xe Frontload that was opened with an angle grinder

Early ATM security focused on making the ATMs invulnerable to physical attack; they were effectively safes with dispenser mechanisms. A number of attacks on ATMs resulted, with thieves attempting to steal entire ATMs by ram-raiding. Since late 1990s, criminal groups operating in Japan improved ram-raiding by stealing and using a truck loaded with a heavy construction machinery to effectively demolish or uproot an entire ATM and any housing to steal its cash.

Another attack method, plofkraak, is to seal all openings of the ATM with silicone and fill the vault with a combustible gas or to place an explosive inside, attached, or near the

ATM. This gas or explosive is ignited and the vault is opened or distorted by the force of the resulting explosion and the criminals can break in.

Modern ATM physical security, per other modern money-handling security, concentrates on denying the use of the money inside the machine to a thief, by means of techniques such as dye markers and smoke canisters.

A common method is to simply rob the staff filling the machine with money. To avoid this, the schedule for filling them is kept secret, varying and random. The money is often kept in cassettes, which will dye the money if incorrectly opened.

Transactional secrecy and integrity

The security of ATM transactions relies mostly on the integrity of the secure cryptoprocessor: the ATM often uses commodity components that are not considered to be "trusted systems".

Encryption of personal information, required by law in many jurisdictions, is used to prevent fraud. Sensitive data in ATM transactions are usually encrypted with DES, but transaction processors now usually require the use of Triple DES. Remote Key Loading techniques may be used to ensure the secrecy of the initialization of the encryption keys in the ATM. Message Authentication Code (MAC) or Partial MAC may also be used to ensure messages have not been tampered with while in transit between the ATM and the financial network.

Customer identity integrity

A BTMU ATM with a palm scanner (to the right of the screen)

There have also been a number of incidents of fraud by Man-in-the-middle attacks, where criminals have attached fake keypads or card readers to existing machines. These have then been used to record customers' PINs and bank card information in order to gain unauthorized access to their accounts. Various ATM manufacturers have put in place countermeasures to protect the equipment they manufacture from these threats.

Alternate methods to verify cardholder identities have been tested and deployed in some countries, such as finger and palm vein patterns, iris, and facial recognition technologies. However, recently, cheaper mass production equipment has been developed and is being installed in machines globally that detect the presence of foreign objects on the front of ATMs, current tests have shown 99% detection success for all types of skimming devices.

Device operation integrity

ATMs that are exposed to the outside must be vandal and weather resistant.

Openings on the customer-side of ATMs are often covered by mechanical shutters to prevent tampering with the mechanisms when they are not in use. Alarm sensors are placed inside the ATM and in ATM servicing areas to alert their operators when doors have been opened by unauthorized personnel.

Rules are usually set by the government or ATM operating body that dictate what happens when integrity systems fail. Depending on the jurisdiction, a bank may or may not be liable when an attempt is made to dispense a customer's money from an ATM and the money either gets outside of the ATM's vault, or was exposed in a non-secure

fashion, or they are unable to determine the state of the money after a failed transaction. Bank customers often complain that banks have made it difficult to recover money lost in this way, but this is often complicated by the bank's own internal policies regarding suspicious activities typical of the criminal element.

Customer security

Dunbar Armored ATM Techs watching over ATMs that have been installed in a van.

In some countries, multiple security cameras and security guards are a common feature. In the United States, The New York State Comptroller's Office has criticized the New York State Department of Banking for not following through on safety inspections of ATMs in high crime areas.

Critics of ATM operators assert that the issue of customer security appears to have been abandoned by the banking industry; it has been suggested that efforts are now more concentrated on deterrent legislation than on solving the problem of forced withdrawals.

At least as far back as July 30, 1986, critics of the industry have called for the adoption of an emergency PIN system for ATMs, where the user is able to send a silent alarm in response to a threat. Legislative efforts to require an emergency PIN system have appeared in Illinois, Kansas and Georgia, but none have succeeded as of yet. In January

2009, Senate Bill 1355 was proposed in the Illinois Senate that revisits the issue of the reverse emergency PIN system. The bill is again resisted by the banking lobby and supported by the police. In 1998 three towns outside of Cleveland Ohio, in response to an ATM crime wave, adopted ATM Consumer Security Legislation requiring that a 9-1-1 switch be installed at all outside ATMs within their jurisdiction. Since the passing of these laws 11 years ago, there have been no repeat crimes. In the wake of an ATM Murder in Sharon Hill, Pennsylvania, The City Council of Sharon Hill passed an ATM Consumer Security Bill as well, with the same result. As of July 2009, ATM Consumer Security Legislation is currently pending in New York, New Jersey, and Washington D.C. In China, many efforts to promote security have been made. On-premises ATMs are often located inside the bank's lobby which may be accessible 24 hours a day. These lobbies have extensive CCTV coverage, an emergency telephone and a security guard on the premises. Bank lobbies that aren't guarded 24 hours a day may also have secure doors that can only be opened from outside by swiping your bank card against a wall-mounted scanner, allowing the bank to identify who enters the building. Most ATMs will also display on-screen safety warnings and may also be fitted with convex mirrors above the display allowing the user to see what is happening behind them.

Alternative uses

Two NCR Personas 84 ATMs at a bank in Jersey dispensing two types of pound sterling banknotes: Bank of England notes on the left, and States of Jersey notes on the right

Although ATMs were originally developed as just cash dispensers, they have evolved to include many other bank-related functions. In some countries, especially those which benefit from a fully integrated cross-bank ATM network (e.g.: Multibanco in Portugal), ATMs include many functions which are not directly related to the management of one's own bank account, such as:

- Deposit currency recognition, acceptance, and recycling

- Paying routine bills, fees, and taxes (utilities, phone bills, social security, legal fees, taxes, etc.)
- Printing bank statements
- Updating passbooks
- Loading monetary value into stored value cards
- Purchasing
    - Postage stamps.
    - Lottery tickets
    - Train tickets
    - Concert tickets
    - Movie tickets
    - Shopping mall gift certificates.
- Games and promotional features
- Donating to charities
- Cheque Processing Module
- Adding pre-paid cell phone / mobile phone credit.
- Paying (in full or partially) the credit balance on a card linked to a specific current account.

Increasingly banks are seeking to use the ATM as a sales device to deliver pre approved loans and targeted advertising using products such as ITM (the Intelligent Teller Machine) from CR2 or Aptra Relate from NCR. ATMs can also act as an advertising channel for companies to advertise their own products or third-party products and services.

In Canada, ATMs are called *guichets automatiques* in French and sometimes "Bank Machines" in English. The Interac shared cash network does not allow for the selling of goods from ATMs due to specific security requirements for PIN entry when buying goods. CIBC machines in Canada, are able to top-up the minutes on certain pay as you go phones.

A South Korean ATM with mobile bank port and bar code reader

Manufacturers have demonstrated and have deployed several different technologies on ATMs that have not yet reached worldwide acceptance, such as:

- Biometrics, where authorization of transactions is based on the scanning of a customer's fingerprint, iris, face, etc. Biometrics on ATMs can be found in Asia.
- Cheque/Cash Acceptance, where the ATM accepts and recognise cheques and/or currency without using envelopes Expected to grow in importance in the US through Check 21 legislation.
- Bar code scanning
- On-demand printing of "items of value" (such as movie tickets, traveler's cheques, etc.)

- Dispensing additional media (such as phone cards)
- Co-ordination of ATMs with mobile phones
- Customer-specific advertising
- Integration with non-banking equipment

Reliability

An ATM running Microsoft Windows that has crashed

Before an ATM is placed in a public place, it typically has undergone extensive testing with both test money and the backend computer systems that allow it to perform transactions. Banking customers also have come to expect high reliability in their ATMs, which provides incentives to ATM providers to minimize machine and network failures.

Financial consequences of incorrect machine operation also provide high degrees of incentive to minimize malfunctions.

ATMs and the supporting electronic financial networks are generally very reliable, with industry benchmarks typically producing 98.25% customer availability for ATMs and up to 99.999% availability for host systems. If ATMs do go out of service, customers could be left without the ability to make transactions until the beginning of their bank's next time of opening hours.

This said, not all errors are to the detriment of customers; there have been cases of machines giving out money without debiting the account, or giving out higher value notes as a result of incorrect denomination of banknote being loaded in the money cassettes. Errors that can occur may be mechanical (such as card transport mechanisms; keypads; hard disk failures); software (such as operating system; device driver; application); communications; or purely down to operator error.

An ATM running OS/2 that has crashed

To aid in reliability, some ATMs print each transaction to a roll paper journal that is stored inside the ATM, which allows both the users of the ATMs and the related financial institutions to settle things based on the records in the journal in case there is a dispute. In some cases, transactions are posted to an electronic journal to remove the cost of supplying journal paper to the ATM and for more convenient searching of data.

Improper money checking can cause the possibility of a customer receiving counterfeit banknotes from an ATM. While bank personnel are generally trained better at spotting

and removing counterfeit cash, the resulting ATM money supplies used by banks provide no absolute guarantee for proper banknotes, as the Federal Criminal Police Office of Germany has confirmed that there are regularly incidents of false banknotes having been dispensed through bank ATMs. Some ATMs may be stocked and wholly owned by outside companies, which can further complicate this problem. Bill validation technology can be used by ATM providers to help ensure the authenticity of the cash before it is stocked in an ATM; ATMs that have cash recycling capabilities include this capability.

Fraud

As with any device containing objects of value, ATMs and the systems they depend on to function are the targets of fraud. Fraud against ATMs and people's attempts to use them takes several forms.

The first known instance of a fake ATM was installed at a shopping mall in Manchester, Connecticut in 1993. By modifying the inner workings of a Fujitsu model 7020 ATM, a criminal gang known as The Bucklands Boys were able to steal information from cards inserted into the machine by customers.

In some cases, bank fraud could occur at ATMs whereby the bank accidentally stocks the ATM with bills in the wrong denomination, therefore giving the customer more money than should be dispensed. The result of receiving too much money may be influenced on the card holder agreement in place between the customer and the bank.

In a variation of this, WAVY-TV reported an incident in Virginia Beach of September 2006 where a hacker who had probably obtained a factory-default admin password for a gas station's white label ATM caused the unit to assume it was loaded with $5 USD bills instead of $20s, enabling himself—and many subsequent customers—to walk away with four times the money they said they wanted to withdraw. This type of scam was featured on the TV series The Real Hustle.

ATM behavior can change during what is called "stand-in" time, where the bank's cash dispensing network is unable to access databases that contain account information (possibly for database maintenance). In order to give customers access to cash, customers may be allowed to withdraw cash up to a certain amount that may be less than their usual daily withdrawal limit, but may still exceed the amount of available money in their account, which could result in fraud.

Card fraud

ATM lineup

A big queue at an ATM in Masalli, Azerbaijan.

In an attempt to prevent criminals from shoulder surfing the customer's PINs, some banks draw privacy areas on the floor.

For a low-tech form of fraud, the easiest is to simply steal a customer's card. A later variant of this approach is to trap the card inside of the ATM's card reader with a device often referred to as a Lebanese loop. When the customer gets frustrated by not getting the card back and walks away from the machine, the criminal is able to remove the card and withdraw cash from the customer's account.

Another simple form of fraud involves attempting to get the customer's bank to issue a new card and stealing it from their mail.

Some ATMs may put up warning messages to customers to not use them when it detects possible tampering

The concept and various methods of copying the contents of an ATM card's magnetic stripe on to a duplicate card to access other people's financial information was well known in the hacking communities by late 1990.

In 1996 Andrew Stone, a computer security consultant from Hampshire in the UK, was convicted of stealing more than £1 million (at the time equivalent to US$1.6 million) by pointing high definition video cameras at ATMs from a considerable distance, and by recording the card numbers, expiry dates, etc. from the embossed detail on the ATM cards along with video footage of the PINs being entered. After getting all the information from the videotapes, he was able to produce clone cards which not only

allowed him to withdraw the full daily limit for each account, but also allowed him to sidestep withdrawal limits by using multiple copied cards. In court, it was shown that he could withdraw as much as £10,000 per hour by using this method. Stone was sentenced to five years and six months in prison.

By contrast, a newer high-tech method of operating sometimes called **card skimming** or **card cloning** involves the installation of a magnetic card reader over the real ATM's card slot and the use of a wireless surveillance camera or a modified digital camera to observe the user's PIN. Card data is then cloned onto a second card and the criminal attempts a standard cash withdrawal. The availability of low-cost commodity wireless cameras and card readers has made it a relatively simple form of fraud, with comparatively low risk to the fraudsters.

In an attempt to stop these practices, countermeasures against card cloning have been developed by the banking industry, in particular by the use of smart cards which cannot easily be copied or spoofed by unauthenticated devices, and by attempting to make the outside of their ATMs tamper evident. Older chip-card security systems include the French Carte Bleue, Visa Cash, Mondex, Blue from American Express and EMV '96 or EMV 3.11. The most actively developed form of smart card security in the industry today is known as EMV 2000 or EMV 4.x.

EMV is widely used in the UK (Chip and PIN) and other parts of Europe, but when it is not available in a specific area, ATMs must fallback to using the easy–to–copy magnetic stripe to perform transactions. This fallback behaviour can be exploited. However the fallback option has been removed by several UK banks, meaning if the chip is not read, the transaction will be declined.

In February 2009, a group of criminals used counterfeit ATM cards to steal $9 million from 130 ATMs in 49 cities around the world all within a time period of 30 minutes.

Card cloning and skimming can be detected by the implementation of magnetic card reader heads and firmware that can read a signature embedded in all magnetic stripes during the card production process. This signature known as a "MagnePrint" or "BluPrint" can be used in conjunction with common two factor authentication schemes utilized in ATM, debit/retail point-of-sale and prepaid card applications.

Another ATM fraud issue is ATM card theft which includes credit card trapping and debit card trapping at ATMs. Originating in South America this type of ATM fraud has spread globally. Although somewhat replaced in terms of volume by ATM skimming incidents, a re-emergence of card trapping has been noticed in regions such as Europe where EMV Chip and PIN cards have increased in circulation.

Related devices

A Talking ATM is a type of ATM that provides audible instructions so that persons who cannot read an ATM screen can independently use the machine. All audible information

is delivered privately through a standard headphone jack on the face of the machine. Alternatively, some banks such as the Nordea and Swedbank use a built-in external speaker which may be invoked by pressing the talk button on the keypad. Information is delivered to the customer either through pre-recorded sound files or via text-to-speech speech synthesis.

A postal interactive kiosk may also share many of the same components as an ATM (including a vault), but only dispenses items relating to postage.

A scrip cash dispenser may share many of the same components as an ATM, but lacks the ability to dispense physical cash and consequently requires no vault. Instead, the customer requests a withdrawal transaction from the machine, which prints a receipt. The customer then takes this receipt to a nearby sales clerk, who then exchanges it for cash from the till.

A Teller Assist Unit may also share many of the same components as an ATM (including a vault), but they are distinct in that they are designed to be operated solely by trained personnel and not the general public, they do not integrate directly into interbank networks, and are usually controlled by a computer that is not directly integrated into the overall construction of the unit.

Health

January 2011, scientists in England has proved that Automated Teller Machines 'as dirty as a public toilets'. And according to Britons, the top 10 dirties places in the UK were number 1.Public toilets, 2.Public telephones, 3.Bus stops, etc.

Chapter- 3

Contactless Smart Card

Size comparison of chip
(compared to a Canadian one cent piece)

A **contactless smart card** is any pocket-sized card with embedded integrated circuits that can process and store data, and communicate with a terminal via radio waves. There are two broad categories of contactless smart cards. Memory cards contain non-volatile memory storage components, and perhaps some specific security logic. Contactless smart cards do not contain an ordinary read-only RFID, but they do contain a re-writable smart card microchip that can be transcribed via radio waves.

The first contactless smart card was the Octopus card, introduced in Hong Kong in 1997 for the territory's mass transit system.

Overview

A "contactless smart card" is also characterized as follows:

- Dimensions are normally credit card size. The ID-1 of ISO/IEC 7810 standard defines them as 85.60 × 53.98 mm. Another popular size is ID-000 which is 25 × 15 mm. Both are 0.76 mm thick.
- Contains a security system with tamper-resistant properties (e.g. a secure cryptoprocessor, secure file system, human-readable features) and is capable of providing security services (e.g. confidentiality of information in the memory).
- Asset managed by way of a central administration system which interchanges information and configuration settings with the card through the security system. The latter includes card hotlisting, updates for application data.
- Card data is transferred via radio waves to the central administration system through card reading devices, such as ticket readers, ATMs etc.

Benefits

Contactless smart cards can be used for identification, authentication, and data storage.

Contactless smart cards provide a means of effecting business transactions in a flexible, secure, standard way with minimal human intervention.

History

Universal contactless smart card reader symbol

Smart cards with contactless interfaces are becoming increasingly popular for payment and ticketing applications such as mass transit. Visa and MasterCard have agreed to an easy-to-implement version currently being deployed (2004–2006) in the USA. Globally, contactless fare collection is being employed for efficiencies in public transit. The

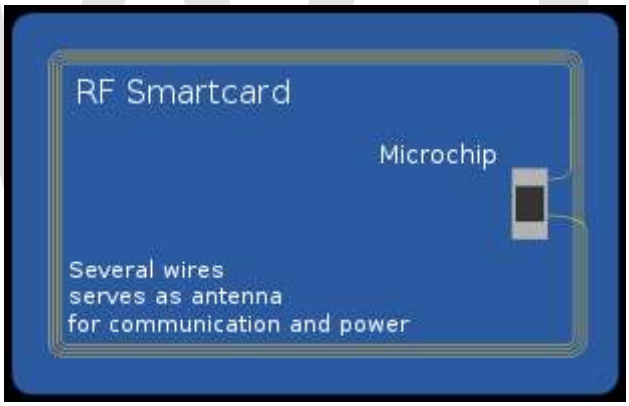
various standards emerging are local in focus and are not compatible, though the MIFARE Standard card from Philips has a large market share in the US and Europe.

Smart cards are being introduced in personal identification and entitlement schemes at regional, national, and international levels. Citizen cards, drivers' licenses, and patient card schemes are becoming more prevalent. In Malaysia, the compulsory national ID scheme MyKad includes 8 different applications and is rolled out for 18 million users. Contactless smart cards are being integrated into ICAO biometric passports to enhance security for international travel.

Readers

Contactless smart card readers use radio waves to communicate with, and both read and write data on a smart card. When used for electronic payment, they are commonly located near PIN pads, cash registers and other places of payment. When the readers are used for public transit they are commonly located on fare boxes, ticket machines, turnstiles, and station platforms as a standalone unit. When used for security, readers are usually located to the side of an entry door.

Technology



RF smart card schematic

A *contactless smart card* is a card in which the chip communicates with the card reader through an induction technology similar to that of an RFID (at data rates of 106 to 848 kbit/s). These cards require only close proximity to an antenna to complete a transaction. They are often used when transactions must be processed quickly or hands-free, such as on mass transit systems, where a smart card can be used without even removing it from a wallet.

The standard for contactless smart card communications is ISO/IEC 14443. It defines two types of contactless cards ("A" and "B") and allows for communications at distances up to 10 cm. There had been proposals for ISO/IEC 14443 types C, D, E, F and G that have been rejected by the International Organization for Standardization. An alternative

standard for contactless smart cards is ISO/IEC 15693, which allows communications at distances up to 50 cm.

Example of widely used contactless smart cards are Taiwan's Easy Card, Hong Kong's Octopus card, Shanghai's Public Transportation Card, South Korea's T-money (bus, subway, taxi), London's Oyster card, Beijing's Municipal Administration and Communications Card, Japan Rail's Suica Card, which predate the ISO/IEC 14443 standard. The following tables list smart cards used for public transportation and other electronic purse applications. First Data delivers Contactless Credit and Debit cards for its customers.

A related contactless technology is RFID (radio frequency identification). In certain cases, it can be used for applications similar to those of contactless smart cards, such as for electronic toll collection. RFID devices usually do not include writeable memory or microcontroller processing capability as contactless smart cards often do.

There are dual-interface cards that implement contactless and contact interfaces on a single card with some shared storage and processing. An example is Porto's multi-application transport card, called Andante, that uses a chip in contact and contactless (ISO/IEC 14443 type B) mode.

Like smart cards with contacts, contactless cards do not have a battery. Instead, they use a built-in inductor, using the principle of resonant inductive coupling, to capture some of the incident electromagnetic signal, rectify it, and use it to power the card's electronics.

Communication protocols

Communication protocols

Name	Description
ISO/IEC 14443	APDU transmission via the protocol defined in ISO/IEC 14443-4

Applications

Credit card contactless technology

These are the best known payment cards (classical plastic card):

- Visa: Visa Contactless, Quick VSDC - "qVSDC", Visa Wave, MSD, payWave
- MasterCard: PayPass MChip
- American Express: ExpressPay
- Discover: Zip

Roll-outs started in 2005 in USA, and in 2006 in some parts of Europe (England) and Asia (Singapore). In USA, contactless (non PIN) transactions cover a payment range of

~$5–50. There is an ISO/IEC 14443 PayPass implementation. All PayPass implementations may be separated on EMV and non EMV.

Non-EMV cards work like magnetic stripe cards. This is a typical card technology in the USA (PayPass Magstripe and VISA MSD). The cards do not control amount remaining. All payment passes without a PIN and usually in off-line mode. The security level of such a transaction is no greater than with classical magnetic stripe card transaction.

EMV cards have two interfaces (contact and contactless) and they work as a normal EMV card via contact interface. Via contactless interface they work almost like an EMV (card command sequence adopted on contactless features as low power and short transaction time).

Other financial application

The applications of Contactless smart cards include their use as credit or ATM cards, in a fuel card, authorization cards for pay television, pre-pay utilities in household, high-security identification and access-control cards, and public transport payment cards.

Smart cards may also be used as electronic wallets. The smart card chip can be loaded with funds which can be spent in vending machines or at various merchants. Cryptographic protocols protect the exchange of money between the Contactless smart card and the accepting machine.

Identification

A quickly growing application is in digital identification cards. In this application, the cards are used for authentication of identity. The most common example is in conjunction with a PKI. The smart card will store an encrypted digital certificate issued from the PKI along with any other relevant or needed information about the card holder. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC), and the use of various smart cards by many governments as identification cards for their citizens. When combined with biometrics, smart cards can provide two- or three-factor authentication. Smart cards are not always a privacy-enhancing technology, for the subject carries possibly incriminating information about him all the time. By employing contactless smart cards, that can be read without having to remove the card from the wallet or even the garment it is in, one can add even more authentication value to the human carrier of the cards.

Transportation

Examples of contactless smart cards used for transportation are:

- Oyster card in London
- Navigo pass in Paris
- Suica in Tokyo

- SL Access card in Stockholm
- Clipper card in San Francisco
- Delhi Metro rail in India
- Octopus card in Hong Kong
- Gautrain Goldcard in Johannesburg
- go card in Brisbane
- SmarTrip card in the Washington, DC Metropolitan Area
- Myki card in Melbourne
- Snapper in Wellington, New Zealand

These cards usually contain electronic purses, and may also store access rights.

Other

The Malaysian government uses smart card technology in identity cards carried by all Malaysian citizens and resident non-citizens. The personal information inside the smart card (called MYKAD) can be read using special APDU commands.MYKAD SDK

Security

Smart cards have been advertised as suitable for personal identification tasks, because they are engineered to be tamper resistant. The embedded chip of a smart card usually implements some cryptographic algorithm. There are, however, several methods of recovering some of the algorithm's internal state.

Differential power analysis

Differential power analysis involves measuring the precise time and electrical current required for certain encryption or decryption operations. This is most often used against public key algorithms such as RSA in order to deduce the on-chip private key, although some implementations of symmetric ciphers can be vulnerable to timing or power attacks as well.

Physical disassembly

Smart cards can be physically disassembled by using acid, abrasives, or some other technique to obtain direct, unrestricted access to the on-board microprocessor. Although such techniques obviously involve a fairly high risk of permanent damage to the chip, they permit much more detailed information (e.g. photomicrographs of encryption hardware) to be extracted.

Problems

Another problem of smart cards may be the failure rate. The plastic card in which the chip is embedded is fairly flexible, and the larger the chip, the higher the probability of

breaking. Smart cards are often carried in wallets or pockets — a fairly harsh environment for a chip. However, for large banking systems, the failure-management cost can be more than offset by the fraud reduction. A card enclosure may be used as an alternative to help prevent the smart card from failing.

Using a smart card for mass transit presents a risk for privacy, because such a system enables the mass transit operator (and the authorities) to track the movement of individuals. In Finland, the Data Protection Ombudsman prohibited the transport operator YTV from collecting such information, in spite of YTV's argument that the owner of the card has the right to get a list of journeys paid with the card. Prior to this, such information was used in the investigation of the Myyrmanni bombing.

Proper disposal

While many contactless smart card users are unaware they are carrying a computer chip in their card and dispose of it by simply throwing it away, it is recommended by most manufacturers and RFID technology experts that these cards be disposed of by shredding them in a paper shredder, or cutting into pieces smaller than 1 cm, to avoid identity theft and/or fraudulent use.

Chapter- 4

EBPP

Electronic bill presentment & payment (EBPP) is a form of electronic billing in which a company presents (sends) its bills and customers pay these electronically over the Internet.

History

The EBPP model was created by the Council for Electronic Billing and Payment of the National Automated Clearing House Association. Certain electronic billing applications also provide the ability to electronically settle payment for goods or services. Customers of banks and billing companies can use the internet or the phone to conveniently remit payments as well as access their billing information. The service is also supported by customer service representatives (CSRs) contacted directly by the consumer to facilitate payments or receive general assistance and answer questions. EBPP can produce substantial savings to traditional print & mail billing and payment remittance, and as an added benefit is a significant reduction in the use of paper.

Types of EBPP

- **Biller-direct -** This refers to an approach in which consumers make payments directly to one biller that issues bills that they receive at the website of the firm that issued the bill. An example would be of a public utility company offering this payment service to its consumers. A market has emerged for outsourced billing providers who specialize in electronic billing processes and technology for companies that need to send bills directly to their customers. Examples of billing outsourcing specialists are InfoSend, Inc and Billtrust.
- **Bank-aggregator -** The approach under this model is to make payment at an aggregator or consolidator site, usually from a consumer's bank's website. This model allows the consumer to make payments to multiple billers that are pre-registered to receive payments. An example in the UK is OneVu and Getitkeepit in Ireland.

Parties involved

Billers, bankers, aggregators and consolidators implementing EBPP can play various roles in the overall EBPP process. Once roles are defined, it is easier to identify which model is most appropriate for the client's EBPP strategy. Billers may also implement more than one model in order to best serve their clients. Because the industry is continuously changing and redefining, the options and opportunities for EBPP will continue to expand.

- Biller payment provider (BPP) - An agent of the biller that accepts remittance information on behalf of the Biller.
- Biller service provider (BSP) - An agent of the biller that provides an EBPP service for the Biller.
- Consolidator - A biller service provider that consolidates bills from multiple Billers or other bill service providers (BSPs) and delivers them for presentment to the customer service provider (CSP).

- Customer service provider (CSP) – An agent of the customer that provides an interface directly to customers, businesses or others for bill presentment. CSP enrolls customers, enables presentment and provides customer care, among other functions.

NACHA

NACHA-The Electronic Payments Association is a not-for-profit trade association that develops operating rules and business practices for the Automated Clearing House (ACH) Network and for other areas of electronic payments. NACHA activities and initiatives facilitate the adoption of electronic payments in the areas of Internet commerce, electronic bill payment and presentment (EBPP), financial electronic data interchange (EDI), international payments, electronic checks, electronic benefits transfer (EBT) and student lending.

To define some guidelines for best practices, NACHA has created the Council for Electronic Billing and Payment of the NACHA InteroperaBILL Initiative of the Banking Industry Technology Secretariat (BITS).

Online banking

Electronic bill payment is a now-common feature of online banking, similar in effect to a giro, allowing a depositor to send money from his demand account to a creditor or vendor such as a public utility or a department store to be credited against a specific account. The payment is optimally executed electronically in real time, though some financial institutions or payment services will wait until the next business day to send out the payment. The bank can usually also generate and mail a paper cheque or banker's draft to a creditor who is not set up to receive electronic payments.

Most large banks also offer various convenience features with their electronic bill payment systems, such as the ability to schedule payments in advance to be made on a specified date, the ability to manage payments from any computer with a web browser over internet, and various options for searching one's recent payment history: when did I last pay Company X? To whom did I make my most recent payment? In many cases one can also integrate the electronic payment data with accounting or personal finance software.

Limitations (United States)

Typically, US financial institutions formally prohibit the use of their consumer electronic bill payment systems for payments to any tax authorities, collection agencies, or recipients of court-ordered payments like child support or alimony. Any organizations or individuals outside of the United States are also usually excluded. Payments to government agencies for utilities such as water are usually permitted.

Electronic bill pay systems fall into two categories, "pay-anyone" services and restricted biller list services. In a pay-anyone service, the provider will facilitate a payment to the payee regardless of whether they have an electronic connection with that payee or not. If they cannot deliver the payment to the payee electronically, they will print and mail a paper check on the payer's behalf. The largest providers of electronic bill pay services can deliver about 80% of their payments electronically, so 20% of payments facilitated by the large pay-anyone services are still made by mailing a paper check to the biller. This is the primary reason why some billers in a pay-anyone service require as much as a 5 day lead time for the payment to reach the payee.

Restricted biller list payment services allow you to pay any biller that is in the provider's network, and in these services where the provider has an electronic relationship with the biller, the payments will be delivered electronically.

SADAD Payment System (Saudi Arabia)

SADAD Payment System SADAD was established by the Saudi Arabian Monetary Agency (SAMA) to be the national Electronic Bill Presentment and Payment (EBPP) service provider for the Kingdom of Saudi Arabia (KSA). The core mandate for SADAD is to facilitate and streamline bill payment transactions of end consumers through all channels of the Kingdom’s Banks. SADAD was launched on October 3, 2004.

SADAD links the commercial sector and local banks, offering the ability to collect customer payments electronically through all the banking channels in the kingdom 24 hours a day.

Chapter- 5

Electronic Money

Electronic money (also known as **e-currency**, **e-money**, **electronic cash**, **electronic currency**, **digital money**, **digital cash**, **digital currency**, **cyber currency**) refers to money or scrip which is only exchanged electronically. Typically, this involves the use of computer networks, the internet and digital stored value systems. Electronic Funds Transfer (EFT), direct deposit, digital gold currency and virtual currency are all examples of electronic money. Also, it is a collective term for financial cryptography and technologies enabling it.

While electronic money has been an interesting problem for cryptography, to date, the use of e-money has been relatively low-scale. One rare success has been Hong Kong's Octopus card system, which started as a transit payment system and has grown into a widely used electronic money system. London Transport's Oyster card system remains essentially a contactless pre-paid travelcard. Two other cities have implemented functioning electronic money systems. Very similar to Hong Kong's Octopus card, Singapore has an electronic money program for its public transportation system (commuter trains, bus, etc.), based on the same type of (FeliCa) system. The Netherlands has also implemented a nation wide electronic money system known as Chipknip for general purpose, as well as OV-Chipkaart for transit fare collection. In Belgium, a payment service company, Proton, owned by 60 Belgian banks issuing stored value cards was developed in 1995.

A number of electronic money systems use Contactless payment transfer in order to facilitate easy payment and give the payee more confidence in not letting go of their electronic wallet during the transaction.

Electronic money systems

In technical terms, electronic money is an online representation, or a system of debits and credits, used to exchange value within another system, or within itself as a stand alone system. In principle this process could also be done offline.

Occasionally, the term electronic money is also used to refer to the provider itself. A private currency may use gold to provide extra security, such as digital gold currency. Some private organizations, such as the United States armed forces use independent currencies such as Eagle Cash.

Centralised systems

Many systems—such as PayPal, WebMoney, cashU, and Hub Culture's Ven—will sell their electronic currency directly to the end user, but other systems such as Liberty Reserve only sell through third party digital currency exchangers.

In the case of Octopus card in Hong Kong, electronic money deposits work similarly to regular bank deposits. After Octopus Card Limited receives money for deposit from users, the money is deposited into a bank. This is similar to debit-card-issuing banks redepositing money at central banks.

Africa & Afghanistan is seeing prepaid cell phone minutes being used as electronic eoney using the M-Pesa system.

Some community currencies, like some Local Exchange Trading Systems (LETS) and the Community Exchange System, work with electronic transactions.

Decentralised systems

Decentralised electronic money systems include:

- Ripple monetary system, a project to develop a distributed system of electronic money independent of local currency.
- Bitcoin, an existing peer-to-peer electronic money system with a maximum inflation limit

Offline 'anonymous' systems

In the use of offline electronic money, the merchant does not need to interact with the bank before accepting money from the user. Instead merchants can collect monies *spent* by users and *deposit* them later with the bank. In principle this could be done offline, i.e. the merchant could go to the bank with his storage media to exchange e-money for cash. Nevertheless the merchant is guaranteed that the user's e-money will either be accepted by the bank, or the bank will be able to identify and punish the cheating user. In this way a user is prevented from spending the same funds twice (double-spending). Offline e-money schemes also need to protect against cheating merchants, i.e. merchants that want to deposit money twice (and then blame the user).

Using cryptography, anonymous ecash was introduced by David Chaum. He used blind signatures to achieve unlinkability between withdrawal and spend transactions. In cryptography, e-cash usually refers to anonymous e-cash. Depending on the properties of the payment transactions, one distinguishes between online and offline e-cash. The first offline e-cash system was proposed by Chaum and Naor. Like the first on-line scheme, it is based on RSA blind signatures.

Hard vs soft electronic currencies

A **hard electronic currency** is one that does not have services to dispute or reverse charges. In other words, it only supports non-reversible transactions. Reversing transactions, even in case of a legitimate error, unauthorized use, or failure of a vendor to supply goods is difficult, if not impossible. The advantage of this arrangement is that the operating costs of the electronic currency system are greatly reduced by not having to resolve payment disputes. Additionally, it allows the electronic currency transactions to clear instantly, making the funds available immediately to the recipient. This means that using hard electronic currency is more akin to a cash transaction. Examples are Pecunix, Liberty Reserve, Wester Union and Bitcoin.

A **soft electronic currency** is one that allows for reversal of payments, for example in case of fraud or disputes. Reversible payment methods generally have a "clearing time" of 72 hours or more. Examples are PayPal and credit card.

Future progression

The main focuses of electronic money development are:

1. being able to use it through a wider range of hardware such as secured credit cards
2. linked bank accounts that would generally be used over an internet means, for exchange with a secure micropayment system such as in large corporations (PayPal).

Issues

Although electronic money can provide many benefits—such as convenience and privacy, increased efficiency of transactions, lower transaction fees, and new business opportunities with the expansion of economic activities on the Internet—there are many potential issues with the use of e-money. The transfer of digital currencies raises local issues such as how to levy taxes or the possible ease of money laundering. There are also potential macro-economic effects such as exchange rate instabilities and shortage of money supplies (total amount of electronic money versus the total amount of real money available, basically the possibility that digital cash could exceed the real cash available).

Another issue is related to computer crime, in which computer criminals may actually alter computer databases to steal electronic money or by reducing an account's amount of electronic money. One way to resolve these issues is by implementing cyberspace regulations or laws that regulate the transactions and watch for signs of fraud or deceit.

Chapter- 6

Digital Gold Currency

Digital gold currency (or **DGC**) is a form of electronic money based on ounces of gold. It is a kind of representative money, like a US paper gold certificate at the time (from 1873 to 1933) that these were exchangeable for gold on demand. The typical unit of account for such currency is the gold gram or the troy ounce, although other units such as the gold dinar are sometimes used. DGCs are backed by gold through unallocated or allocated gold storage.

Digital gold currencies are issued by a number of companies, each of which provides a system that enables users to pay each other in units that hold the same value as gold bullion. These competing providers issue independent currency.

Features

Universal currency

Proponents claim that DGC offers a truly global and borderless world currency system which is independent of exchange rate variations and political manipulation. Gold, silver, platinum and palladium each have recognized international currency codes under ISO 4217. In addition to digital gold currency, GoldMoney also provide digital currency backed by silver.

Asset protection

Unlike fractional-reserve banking, DGCs hold 100% of clients' funds in reserve as gold, silver, and/or platinum, which can be exchanged via digital certificates. Proponents of DGC systems say that deposits are protected against inflation, devaluation and other economic risks inherent in fiat currencies. These risks include the monetary policy of countries or territories, which are said by proponents to be harmful to the value of paper currency.

Bullion investing

For example, GoldMoney is accessible and approved for U.S. self-directed Individual Retirement Accounts through The Entrust Group.

All of the other digital gold currency systems can be used to buy, hold, and sell precious metals, but do not promote themselves as an "investment", as this implies an anticipated return.

Exchanging national currency

Some providers, like e-gold, Pecunix, Liberty Reserve do not sell DGC directly to clients. For those DGCs, e-currency must be bought and sold via a digital currency exchanger.

Currency exchangers accept payment in national currencies by a variety of methods, including Bank Wire, Direct Deposit, Cheque, Money Order. Some exchangers also sell and fund pre-paid debit cards to make it easier for their clientele to convert DGC into an easily spendable form of national currency.

DGCs are known as private currency as they are not issued by governments.

Non-reversible transactions

Unlike the credit card industry, digital gold currency issuers generally do not have services to dispute or reverse charges. So, reversing transactions, even in case of a legitimate error, unauthorized use, or failure of a vendor to supply goods is difficult, if not impossible. This means that using digital gold currency is more akin to a cash transaction, while PayPal transfers, for example, could be considered more similar to credit card transactions.

The advantage of this arrangement is that the operating costs of the digital currency system are greatly reduced by not having to resolve payment disputes. Additionally, it allows digital gold currency transactions to clear instantly, making the funds available immediately to the recipient. By contrast, credit cards, checks, ACH and other reversible payment methods generally have a "clearing time" of 72 hours or more.

Risks

As with all financial media, there are several types of risk inherent to the use of DGCs: management risk, political risk, data security and exchange risk.

Management and political risks

DGCs, like all financial institutions and public securities, have a layer of risk in the form of the management of the issuing institution. Controls aimed to limit management risk are called "governance".

GoldMoney is the only DGC that is a government registered and financially regulated money service business. All other DGC providers operate under self-regulation. DGC providers are not banks and therefore not subject to many bank regulations that pertain to

fractional reserve lending as they do not engage in lending. However, DGCs do provide a method for transferring currency from one person to another, and therefore may fall under regulations pertaining to money transmitting in various jurisdictions.

The Global Digital Currency Association (GDCA), which was founded in 2002, is a non-profit association of online currency operators, exchangers, merchants and users. The GDCA is an example of the DGC industry's attempt at self-regulation. On their website they claim their goal is to "further the interests of the industry as a whole and help with fighting fraud and other illegal activities, arbitrate disputes and act as escrow agent when and where required." Of the current DGC providers, Pecunix, Liberty Reserve and eight others have become members of the association. It costs one gram of gold to file a complaint if you are not a member, and the list of filable complaints is not exhaustive.

OS-Gold, Standard Reserve and INTGold

Several companies claiming to be Digital Gold Currencies sprang up and failed between 1999 and 2004, such as OS-Gold, Standard Reserve and INTGold. All these companies failed because the principals diverted deposits for other purposes instead of holding them in the form of gold. In each of these cases, account holders lost several million dollars worth of gold when the "institution" failed.

e-gold and 1mdc

Following April 27, 2007, the United States Department of Justice forced e-gold to liquidate some 10 to 20 million dollars worth of e-gold, and is attempting to bring a case against e-gold. e-gold has committed to counter what its founders have declared to be groundless allegations.

1mdc was backed by e-gold, so events that affected e-gold also affected 1mdc. Once e-gold Ltd. was instructed by the US government to freeze and liquidate all 1mdc accounts, 1mdc became insolvent by default along with all other e-gold accounts seized in the April 27 action.

e-Bullion

As of August 2008 Jim Fayed of e-Bullion is in United States Federal custody where he faces felony charges of conducting unlicensed money transactions and the murder of his business partner.

As of January 2010 e-Bullion is closed for business and the website unavailable.

Data security

Digital Gold Systems are completely dependent on electronic storage and transmission of account ownership information. Therefore the security of a given digital currency account

is dependent upon the security of the Issuer as well as the security of the Account Holder's computer.

While the Digital Gold Issuers employ data security experts to protect their systems, the average account holder's computer is poorly protected against malware (trojans, worms, and viruses) that can be used to intercept information that could be used to access the user's DGC account. Therefore the most common attacks on digital currency systems are directed against account holder's computer through the use of malicious spam, phishing and other methods.

Issuers have taken quite different approaches to this problem. E-gold basically places the entire responsibility on the shoulders of the user, and uses a user-name and password authentication system that is weak and highly vulnerable to interception by malware. (Though it is the most common authentication method used by online banks.) The "not our problem" approach to user security has negatively contributed to e-gold's public image, as not a few e-gold accounts have been hacked and swept clean by attackers..

e-Bullion offers account holders a "Cryptocard" security token that changes the passphrase with each logon, but charges the account holder USD $99.50 for the token. E-bullion does not require customers to use the Cryptocard, so account holders who choose not to get one may suffer from the same security issues as e-gold customers.

GoldMoney allows the user to login with user-name and passphrase, but sends an email with a unique personal identification number (PIN) that the user must enter in the form to complete the transaction. This reduces the likelihood of a successful attack because the attacker must gain control of the user's email account in addition to his login information, and must further prevent the user from receiving the email with the PIN, which would alert the user that someone is attempting to transfer gold out of his holding.

Pecunix devised a unique rotating key system that provides many of the benefits of a security token without requiring the user to buy one. Pecunix also supports the use of PGP signatures to access an account, which is probably the strongest of all authentication methods.

Exchange risk

Digital gold currency is a form of representative money as it directly represents gold metal on deposit or in custody, and denominated in units of mass (grams or troy ounces). Just as the exchange rates of national currencies fluctuate against each other, the exchange rates of DGCs fluctuate against national currencies, which is reflected by the price of gold in a particular currency. This creates exchange risk for any account holder, in the same way one would experience exchange risk by holding a bank account in a foreign currency.

Some DGC holders make use of the digital currency for daily monetary transactions, even though most of their normal income and expenses are denominated in the national

currency of their home country. Fluctuations in the value of gold against their national currency can create some confusion and difficulty for new users as they see the "value" of their DGC account fluctuate in terms of their native currency.

In contrast to exchange risk, caused by gold's fluctuation against national currency, the purchasing power of gold (and therefore DGCs) is measured by its fluctuation against other commodities, goods and services. Since gold has historically been the refuge of choice in times of inflation or economic hardship, the purchasing power of gold becomes stronger during times of negative sentiment in the markets. Due to this speculative interference, there are times when purchasing power has also declined. For example, in 2007–2008, gold volatility closely tracked the run-up in oil prices.

Providers

Comparison of operating DGCs (as of July 2010):

Digital gold currency	Date founded	Financially regulated	GDCA member	Bullion stored	Bullion audit trail	Number of user accounts	DCE transfers accepted	Wire transfers accepted	Annual storage fee	Processing fee (when receiving from another user)
e-dinar	2000	✗	✗	Undisclosed	✗	Undisclosed	✗	✓	1%	1% (with max. 0.015 gold dinar)
GoldMoney	2001	✓	✗	498,567 oz gold, 19,628,087 oz silver	✓	13,316	✗	✓	0.15 - 0.18%	1% (with min. 0.01 - max. 0.1 gold grams)
Pecunix	2002	✗	✓	2,777 oz gold	✓	Undisclosed	✓	✗	0%	0.15 - 0.50% (with min. 0.0001 - max. 3.0 gold grams)

Criticisms

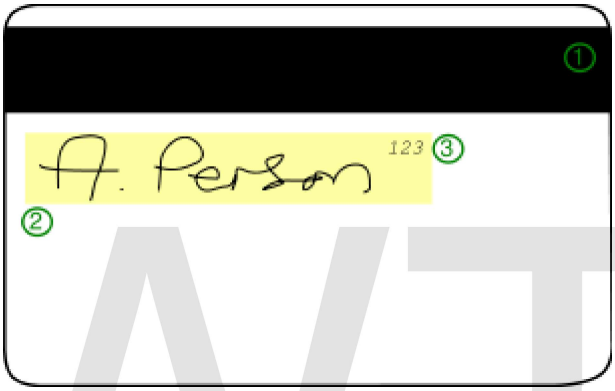
DGC providers and exchangers have been accused of being a medium for fraudulent high-yield investment program (HYIP) schemes. In January 2006, *BusinessWeek* reported that ShadowCrew, an online gang, used the e-gold system in a massive identity theft and fraud scheme. Traditional banks are also used frequently for such fraud. Allegations that e-gold is a safe medium for crime and fraud are strongly denied by its Chairman and founder, Dr. Douglas Jackson.

Many DGC providers do not disclose the amount of bullion stored, or do not allow independent external bullion audits, raising concerns that such companies do not maintain

a 100% reserve ratio, or that their currency is entirely virtual and not backed by physical gold at all.

Chapter- 7

Magnetic Stripe Card



An example of the reverse side of a typical credit card: Green circle #1 labels the Magnetic stripe

A **magnetic stripe card** is a type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card. The magnetic stripe, sometimes called **swipe card** or **magstripe**, is read by physical contact and swiping past a magnetic reading head.

A number of International Organization for Standardization standards, ISO/IEC 7810, ISO/IEC 7811, ISO/IEC 7812, ISO/IEC 7813, ISO 8583, and ISO/IEC 4909, define the physical properties of the card, including size, flexibility, location of the magstripe, magnetic characteristics, and data formats. They also provide the standards for financial cards, including the allocation of card number ranges to different card issuing institutions.

The magnetic stripe

The process of attaching a magnetic stripe to a plastic card was invented by IBM in 1960 under a contract with the US government for a security system. Forrest Parry, an IBM Engineer, had the idea of securing a piece of magnetic tape, the predominant storage medium at the time, to a plastic card base. He became frustrated because every adhesive he tried produced unacceptable results. The tape strip either warped or its characteristics were affected by the adhesive, rendering the tape strip unusable. After a frustrating day in the laboratory, trying to get the right adhesive, he came home with several pieces of

magnetic tape and several plastic cards. As he walked in the door at home, his wife Dorothea was ironing and watching TV. She immediately saw the frustration on his face and asked what was wrong. He explained the source of his frustration: inability to get the tape to "stick" to the plastic in a way that would work. She said, "Here, let me try the iron." She did and the problem was solved. The heat of the iron was just high enough to bond the tape to the card.

There were a number of steps required to convert the magnetic striped media into an industry acceptable device. These steps included: 1) Creating the international standards for stripe record content, including which information, in what format, and using which defining codes. 2) Field testing the proposed device and standards for market acceptance. 3) Developing the manufacturing steps needed to mass produce the large number of cards required. 4) Adding stripe issue and acceptance capabilities to available equipment. These steps were initially managed by Jerome Svigals of the Advanced Systems Division of IBM, Los Gatos, California from 1966 to 1975.

In most magnetic stripe cards, the magnetic stripe is contained in a plastic-like film. The magnetic stripe is located 0.223 inches (5.56 mm) from the edge of the card, and is 0.375 inches (9.52 mm) wide. The magnetic stripe contains three tracks, each 0.110 inches (2.79 mm) wide. Tracks one and three are typically recorded at 210 bits per inch (8.27 bits per mm), while track two typically has a recording density of 75 bits per inch (2.95 bits per mm). Each track can either contain 7-bit alphanumeric characters, or 5-bit numeric characters. Track 1 standards were created by the airlines industry (IATA). Track 2 standards were created by the banking industry (ABA). Track 3 standards were created by the Thrift-Savings industry.

Magstripes following these specifications can typically be read by most point-of-sale hardware, which are simply general-purpose computers that can be programmed to perform specific tasks. Examples of cards adhering to these standards include ATM cards, bank cards (credit and debit cards including VISA and MasterCard), gift cards, loyalty cards, driver's licenses, telephone cards, membership cards, electronic benefit transfer cards (e.g. food stamps), and nearly any application in which value or secure information is *not* stored on the card itself. Many video game and amusement centers now use debit card systems based on magnetic stripe cards.

Magnetic stripe cloning can be detected by the implementation of magnetic card reader heads and firmware that can read a signature of magnetic noise permanently embedded in all magnetic stripes during the card production process. This signature can be used in conjunction with common two factor authentication schemes utilized in ATM, debit/retail point-of-sale and prepaid card applications.

Counterexamples of cards which intentionally ignore ISO standards include hotel key cards, most subway and bus cards, and some national prepaid calling cards (such as for the country of Cyprus) in which the balance is stored and maintained directly on the stripe and not retrieved from a remote database.

Magnetic stripe coercivity

Magstripes come in two main varieties: high-coercivity (HiCo) at 4000 Oe and low-coercivity (LoCo) at 300 Oe but it is not infrequent to have intermediate values at 2750 Oe. High-coercivity magstripes are harder to erase, and therefore are appropriate for cards that are frequently used or that need to have a long life. Low-coercivity magstripes require a lower amount of magnetic energy to record, and hence the card writers are much cheaper than machines which are capable of recording high-coercivity magstripes. A card reader can read either type of magstripe, and a high-coercivity card writer may write both high and low-coercivity cards (most have two settings, but writing a LoCo card in HiCo may sometimes work), while a low-coercivity card writer may write only low-coercivity cards.

In practical terms, usually low coercivity magnetic stripes are a light brown color, and high coercivity stripes are nearly black; exceptions include a proprietary silver-colored formulation on transparent American Express cards. High coercivity stripes are resistant to damage from most magnets likely to be owned by consumers. Low coercivity stripes are easily damaged by even a brief contact with a magnetic purse strap or fastener. Because of this, virtually all bank cards today are encoded on high coercivity stripes despite a slightly higher per-unit cost.

Magnetic stripe cards are used in very high volumes in the mass transit sector, replacing paper based tickets with either a directly applied magnetic slurry or hot foil stripe. Slurry applied stripes are generally less expensive to produce and are less resilient but are suitable for cards meant to be disposed after a few uses.

Financial cards

There are up to three tracks on magnetic cards used for financial transactions, known as tracks 1, 2, and 3. Track 3 is virtually unused by the major worldwide networks such as VISA, and often isn't even physically present on the card by virtue of a narrower magnetic stripe. Point-of-sale card readers almost always read track 1, or track 2, and sometimes both, in case one track is unreadable. The minimum cardholder account information needed to complete a transaction is present on both tracks. Track 1 has a higher bit density (210 bits per inch vs. 75), is the only track that may contain alphabetic text, and hence is the only track that contains the cardholder's name.

Track 1 is written with code known as DEC SIXBIT plus odd parity. The information on track 1 on financial cards is contained in several formats: **A**, which is reserved for proprietary use of the card issuer, **B**, which is described below, **C-M**, which are reserved for use by ANSI Subcommittee X3B10 and **N-Z**, which are available for use by individual card issuers:

Track 1, Format B:

- **Start sentinel** — one character (generally '%')
- **Format code="B"** — one character (alpha only)
- **Primary account number** (PAN) — up to 19 characters. Usually, but not always, matches the credit card number printed on the front of the card.
- **Field Separator** — one character (generally '^')
- **Name** — two to 26 characters
- **Field Separator** — one character (generally '^')
- **Expiration date** — four characters in the form YYMM.
- **Service code** — three characters
- **Discretionary data** — may include Pin Verification Key Indicator (PVKI, 1 character), PIN Verification Value (PVV, 4 characters), Card Verification Value or Card Verification Code (CVV or CVK, 3 characters)
- **End sentinel** — one character (generally '?')
- **Longitudinal redundancy check** (LRC) — it is one character and a validity character calculated from other data on the track. Most reader devices do not return this value when the card is swiped to the presentation layer, and use it only to verify the input internally to the reader.

Track 2: This format was developed by the banking industry (ABA). This track is written with a 5-bit scheme (4 data bits + 1 parity), which allows for sixteen possible characters, which are the numbers 0-9, plus the six characters `: ; < = > ?` . The selection of six punctuation symbols may seem odd, but in fact the sixteen codes simply map to the ASCII range 0x30 through 0x3f, which defines ten digit characters plus those six symbols. The data format is as follows:

- **Start sentinel** — one character (generally ';')
- **Primary account number** (PAN) — up to 19 characters. Usually, but not always, matches the credit card number printed on the front of the card.
- **Separator** — one char (generally '=')
- **Expiration date** — four characters in the form YYMM.
- **Service code** — three digits. The first digit specifies the interchange rules, the second specifies authorisation processing and the third specifies the range of services
- **Discretionary data** — as in track one
- **End sentinel** — one character (generally '?')
- **Longitudinal redundancy check** (LRC) — it is one character and a validity character calculated from other data on the track. Most reader devices do not return this value when the card is swiped to the presentation layer, and use it only to verify the input internally to the reader.

Service code values common in financial cards:

First digit

1: International interchange OK
2: International interchange, use IC (chip) where feasible

5: National interchange only except under bilateral agreement
6: National interchange only except under bilateral agreement, use IC (chip) where feasible
7: No interchange except under bilateral agreement (closed loop)
9: Test

Second digit

0: Normal
2: Contact issuer via online means
4: Contact issuer via online means except under bilateral agreement

Third digit

0: No restrictions, PIN required
1: No restrictions
2: Goods and services only (no cash)
3: ATM only, PIN required
4: Cash only
5: Goods and services only (no cash), PIN required
6: No restrictions, use PIN where feasible
7: Goods and services only (no cash), use PIN where feasible

All values not explicitly mentioned above are reserved for future use

Notes:

- It is possible for these strips to be completely erased if brought close to high strength Neodymium magnets
- Commercial encoders might use '~' for Start sentinel, ';' for separator.
- Example Code: '~#;data?'

United States driver's licenses

The data stored on magnetic stripes on American driver's licenses is specified by the American Association of Motor Vehicle Administrators (AAMVA). Not all states use a magnetic stripe on their driver's licenses. The AAMVA site also contains a list of the Canadian jurisdictions that use magnetic stripes on their driver's licenses.

The following data is stored on track 1 :

- **Start Sentinel -** one character (generally '%')
- **State or Province -** two characters
- **City -** variable length (seems to max out at 13 characters)
- **Field Separator -** one character (generally '^') (absent if city reaches max length)
- **Last Name -** variable length

- **Field Separator -** one character (generally '$')
- **First Name -** variable length
- **Field Separator -** one character (generally '$')
- **Middle Name -** variable length
- **Field Separator -** one character (generally '^')
- **Home Address (house number and street) -** variable length
- **Field Separator** - one character (generally '^')
- **Unknown -** variable length
- **End Sentinel -** one character (generally '?')

The following data is stored on track 2:

- **ISO Issuer Identifier Number (IIN) -** 6 digits
- **Drivers License / Identification Number -** 13 digits
- **Field Separator —** generally '='
- **Expiration Date (YYMM) -** 4 digits
- **Birth date (YYYYMMDD) -** 8 digits
- **DL/ID# overflow-** 5 digits (If no information is used then a field separator is used in this field.)
- **End Sentinel -** one character ('?')

The following data is stored on track 3:

- **Template V#**
- **Security V#**
- **Postal Code**
- **Class**
- **Restrictions**
- **Endorsements**
- **Sex**
- **Height**
- **Weight**
- **Hair Color**
- **Eye Color**
- **ID#**
- **Reserved Space**
- **Error Correction**
- **Security**

Note: Each state has a different selection of information they encode, not all states are the same. Note: Some states, such as Texas, have laws restricting drivers licenses being swiped under certain circumstances.

Other card types

Smart cards are a newer generation of card containing an integrated circuit chip. The card may have metal contacts connecting the card physically to the reader, while contactless cards use a magnetic field or radio frequency (RFID) for proximity reading.

Hybrid smart cards include a magnetic stripe in addition to the chip — this is most commonly found in a payment card, so that the cards are also compatible with payment terminals that do not include a smart card reader.

Cards with all three features: magnetic stripe, smart card chip, and RFID chip are also becoming common as more activities require the use of such cards.

Chapter- 8

Mobile Banking

Mobile banking (also known as M-Banking, mbanking, SMS Banking etc.) is a term used for performing balance checks, account transactions, payments, credit applications etc. via a mobile device such as a mobile phone or Personal Digital Assistant (PDA). The earliest mobile banking services were offered via SMS. With the introduction of the first primitive smart phones with WAP support enabling the use of the mobile web in 1999, the first European banks started to offer mobile banking on this platform to their customers .

Mobile banking has until recently (2010) most often been performed via SMS or the Mobile Web. Apple's initial success with iPhone and the rapid growth of phones based on Google's Android (operating system) has led to increasing use of special client programs, called apps, downloaded to the mobile device.

A mobile banking conceptual model

In one academic model, mobile banking is defined as:

Mobile Banking refers to provision and availment of banking- and financial services with the help of mobile telecommunication devices.The scope of offered services may include facilities to conduct bank and stock market transactions, to administer accounts and to access customised information."

According to this model Mobile Banking can be said to consist of three inter-related concepts:

- Mobile Accounting
- Mobile Brokerage
- Mobile Financial Information Services

Most services in the categories designated *Accounting* and *Brokerage* are transaction-based. The non-transaction-based services of an informational nature are however essential for conducting transactions - for instance, balance inquiries might be needed before committing a money remittance. The accounting and brokerage services are

therefore offered invariably in combination with information services. Information services, on the other hand, may be offered as an independent module.

Mobile phone banking may also be used to help in business situations

Trends in mobile banking

The advent of the Internet has enabled new ways to conduct banking business, resulting in the creation of new institutions, such as online banks, online brokers and wealth managers. Such institutions still account for a tiny percentage of the industry.

Over the last few years, the mobile and wireless market has been one of the fastest growing markets in the world and it is still growing at a rapid pace. According to the GSM Association and Ovum, the number of mobile subscribers exceeded 2 billion in September 2005, and now exceeds 2.5 billion (of which more than 2 billion are GSM).

With mobile technology, banks can offer services to their customers such as doing funds transfer while travelling, receiving online updates of stock price or even performing stock trading while being stuck in traffic. Smartphones and 3G connectivity provide some capabilities that older text message-only phones do not.

According to a study by financial consultancy Celent, 35% of online banking households will be using mobile banking by 2010, up from less than 1% today. Upwards of 70% of bank center call volume is projected to come from mobile phones. Mobile banking will eventually allow users to make payments at the physical point of sale. "Mobile contactless payments" will make up 10% of the contactless market by 2010. Another study from 2010 by Berg Insight forecasts that the number of mobile banking users in the US will grow from 12 million in 2009 to 86 million in 2015. The same study also predicts that the European market will grow from 7 million mobile banking users in 2009 to 115 million users in 2015.

Many believe that mobile users have just started to fully utilize the data capabilities in their mobile phones. In Asian countries like India, China, Bangladesh, Indonesia and Philippines, where mobile infrastructure is comparatively better than the fixed-line infrastructure, and in European countries, where mobile phone penetration is very high (at least 80% of consumers use a mobile phone), mobile banking is likely to appeal even more.

Mobile banking business models

A wide spectrum of Mobile/branchless banking models is evolving. However, no matter what business model, if mobile banking is being used to attract low-income populations in often rural locations, the business model will depend on banking agents, i.e., retail or postal outlets that process financial transactions on behalf telcos or banks. The banking agent is an important part of the mobile banking business model since customer care,

service quality, and cash management will depend on them. Many telcos will work through their local airtime resellers. However, banks in Colombia, Brazil, Peru, and other markets use pharmacies, bakeries, etc.

These models differ primarily on the question that who will establish the relationship (account opening, deposit taking, lending etc.) to the end customer, the Bank or the Non-Bank/Telecommunication Company (Telco). Another difference lies in the nature of agency agreement between bank and the Non-Bank. Models of branchless banking can be classified into three broad categories - Bank Focused, Bank-Led and Nonbank-Led.

Bank-focused model

The bank-focused model emerges when a traditional bank uses non-traditional low-cost delivery channels to provide banking services to its existing customers. Examples range from use of automatic teller machines (ATMs) to internet banking or mobile phone banking to provide certain limited banking services to banks' customers. This model is additive in nature and may be seen as a modest extension of conventional branch-based banking.

Bank-led model

The bank-led model offers a distinct alternative to conventional branch-based banking in that customer conducts financial transactions at a whole range of retail agents (or through mobile phone) instead of at bank branches or through bank employees. This model promises the potential to substantially increase the financial services outreach by using a different delivery channel (retailers/ mobile phones), a different trade partner (telco / chain store) having experience and target market distinct from traditional banks, and may be significantly cheaper than the bank-based alternatives. The bank-led model may be implemented by either using correspondent arrangements or by creating a JV between Bank and Telco/non-bank. In this model customer account relationship rests with the bank

Non-bank-led model

The non-bank-led model is where a bank has a limited role in the day-to-day account management. Typically its role in this model is limited to safe-keeping of funds. Account management functions are conducted by a non-bank (e.g. telco) who has direct contact with individual customers.

Mobile Banking Services

Mobile banking can offer services such as the following:

Account Information

1. Mini-statements and checking of account history
2. Alerts on account activity or passing of set thresholds
3. Monitoring of term deposits
4. Access to loan statements
5. Access to card statements
6. Mutual funds / equity statements
7. Insurance policy management
8. Pension plan management
9. Status on cheque, stop payment on cheque
10. Ordering cheque books
11. Balance checking in the account
12. Recent transactions
13. Due date of payment (functionality for stop, change and deleting of payments)
14. PIN provision, Change of PIN and reminder over the Internet
15. Blocking of (lost, stolen) cards

Payments, Deposits, Withdrawals, and Transfers

1. Domestic and international fund transfers
2. Micro-payment handling
3. Mobile recharging
4. Commercial payment processing
5. Bill payment processing
6. Peer to Peer payments
7. Withdrawal at banking agent
8. Deposit at banking agent

A specific sequence of SMS messages will enable the system to verify if the client has sufficient funds in his or her wallet and authorize a deposit or withdrawal transaction at the agent. When depositing money, the merchant receives cash and the system credits the client's bank account or mobile wallet. In the same way the client can also withdraw money at the merchant: through exchanging sms to provide authorization, the merchant hands the client cash and debits the merchant's account.

Investments

1. Portfolio management services
2. Real-time stock quotes
3. Personalized alerts and notifications on security prices
4. mobile banking

Support

1. Status of requests for credit, including mortgage approval, and insurance coverage

2. Check (cheque) book and card requests
3. Exchange of data messages and email, including complaint submission and tracking
4. ATM Location

Content Services

1. General information such as weather updates, news
2. Loyalty-related offers
3. Location-based services

Based on a survey conducted by Forrester, mobile banking will be attractive mainly to the younger, more "tech-savvy" customer segment. A third of mobile phone users say that they may consider performing some kind of financial transaction through their mobile phone. But most of the users are interested in performing basic transactions such as querying for account balance and making bill payment.

Challenges for a Mobile Banking Solution

Key challenges in developing a sophisticated mobile banking application are :

Handset operability

There are a large number of different mobile phone devices and it is a big challenge for banks to offer mobile banking solution on any type of device. Some of these devices support Java ME and others support SIM Application Toolkit, a WAP browser, or only SMS.

Initial interoperability issues however have been localized, with countries like India using portals like R-World to enable the limitations of low end java based phones, while focus on areas such as South Africa have defaulted to the USSD as a basis of communication achievable with any phone.

The desire for interoperability is largely dependent on the banks themselves, where installed applications(Java based or native) provide better security, are easier to use and allow development of more complex capabilities similar to those of internet banking while SMS can provide the basics but becomes difficult to operate with more complex transactions.

There is a myth that there is a challenge of interoperability between mobile banking applications due to perceived lack of common technology standards for mobile banking. In practice it is too early in the service lifecycle for interoperability to be addressed within an individual country, as very few countries have more than one mobile banking service provider. In practice, banking interfaces are well defined and money movements between banks follow the IS0-8583 standard. As mobile banking matures, money

movements between service providers will naturally adopt the same standards as in the banking world.

On January 2009, Mobile Marketing Association (MMA) Banking Sub-Committee, chaired by CellTrust and VeriSign Inc., published the Mobile Banking Overview for financial institutions in which it discussed the advantages and disadvantages of Mobile Channel Platforms such as Short Message Services (SMS), Mobile Web, Mobile Client Applications, SMS with Mobile Web and Secure SMS.

Security

Security of financial transactions, being executed from some remote location and transmission of financial information over the air, are the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the banks' IT departments.

The following aspects need to be addressed to offer a secure infrastructure for financial transaction over wireless network :

1. Physical part of the hand-held device. If the bank is offering smart-card based security, the physical security of the device is more important.
2. Security of any thick-client application running on the device. In case the device is stolen, the hacker should require at least an ID/Password to access the application.
3. Authentication of the device with service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions.
4. User ID / Password authentication of bank's customer.
5. Encryption of the data being transmitted over the air.
6. Encryption of the data that will be stored in device for later / off-line analysis by the customer.

One-time password (OTPs) are the latest tool used by financial and banking service providers in the fight against cyber fraud . Instead of relying on traditional memorized passwords, OTPs are requested by consumers each time they want to perform transactions using the online or mobile banking interface. When the request is received the password is sent to the consumer's phone via SMS. The password is expired once it has been used or once its scheduled life-cycle has expired.

Because of the concerns made explicit above, it is extremely important that SMS gateway providers can provide a decent quality of service for banks and financial institutions in regards to SMS services. Therefore, the provision of service level agreements (SLAs) is a requirement for this industry; it is necessary to give the bank customer delivery guarantees of all messages, as well as measurements on the speed of delivery, throughput, etc. SLAs give the service parameters in which a messaging solution is guaranteed to perform.

Scalability & Reliability

Another challenge for the CIOs and CTOs of the banks is to scale-up the mobile banking infrastructure to handle exponential growth of the customer base. With mobile banking, the customer may be sitting in any part of the world (true anytime, anywhere banking) and hence banks need to ensure that the systems are up and running in a true 24 x 7 fashion. As customers will find mobile banking more and more useful, their expectations from the solution will increase. Banks unable to meet the performance and reliability expectations may lose customer confidence. There are systems such as Mobile Transaction Platform which allow quick and secure mobile enabling of various banking services. Recently in India there has been a phenomenal growth in the use of Mobile Banking applications, with leading banks adopting Mobile Transaction Platform and the Central Bank publishing guidelines for mobile banking operations.

Application distribution

Due to the nature of the connectivity between bank and its customers, it would be impractical to expect customers to regularly visit banks or connect to a web site for regular upgrade of their mobile banking application. It will be expected that the mobile application itself check the upgrades and updates and download necessary patches (so called "Over The Air" updates). However, there could be many issues to implement this approach such as upgrade / synchronization of other dependent components.

Personalization

It would be expected from the mobile application to support personalization such as :

1. Preferred Language
2. Date / Time format
3. Amount format
4. Default transactions
5. Standard Beneficiary list
6. Alerts

Mobile banking in the world

Mobile banking has come in handy in many parts of the world with little or no Infrastructure development, especially in remote and rural areas. This part of the mobile commerce is also very popular in countries where most of their population is unbanked. In most of these places banks can only be found in big cities and customers have to travel hundreds of miles to the nearest bank.
Countries like Sudan, Ghana and South Africa received this new commerce very well.
In Latin America countries like Uruguay, Paraguay, Argentina, Brazil, Venezuela, Colombia, Guatemala and recently Mexico started with a huge success.
In Colombia was released with Redesign.

In Iran banks like Parsian, Tejarat, Mellat, Saderat, Sepah, edbi and bankmelli offer this service. Guatemala have the support of Banco industrial.
Mexico released the mobile commerce with Omnilife, Bancomer and a private company(MPower Ventures). Kenya's Safaricom (Part of the Vodafone Group) has had the very popular M-Pesa Service - mainly used to transfer limited amounts of money, but has been increasingly used to pay utility bills. Zain in 2009 launched their own mobile money transfer business known as ZAP in Kenya and other African countries.

Telenor Pakistan has also launched Mobile banking solution, in coordination with Taameer Bank, under the label "Easy Paisa". Telenor rolled out its Mobile banking solution in Q4, 2009. It was a huge success and customers embraced the wide set of services offered. Eko India Financial Services the is business correspondent of State Bank of India (SBI) and ICICI Bank, India's top two largest banks, and provides no-frills bank accounts and deposit, withdrawal and remittance services to customers (nearly 80% of whom are migrants or the unbanked section of the population) through mobile banking. , and also offer micro-insurance and micro-finance facilities to its customers.

Chapter- 9

Online Banking

Online banking (or **Internet banking**) allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society.

Features

Online banking solutions have many features and capabilities in common, but traditionally also have some that are application specific.

The common features fall broadly into several categories

- Transactional (e.g., performing a financial transaction such as an account to account transfer, paying a bill, wire transfer... and applications... apply for a loan, new account, etc.)
    - Electronic bill presentment and payment - EBPP
    - Funds transfer between a customer's own checking and savings accounts, or to another customer's account
    - Investment purchase or sale
    - Loan applications and transactions, such as repayments of enrollments

- Non-transactional (e.g., online statements, check links, cobrowsing, chat)
    - Bank statements
- Financial Institution Administration -
- Support of multiple users having varying levels of authority
- Transaction approval process
- Wire transfer

Features commonly unique to Internet banking include

- Personal financial management support, such as importing data into personal accounting software. Some online banking platforms support account aggregation to allow the customers to monitor all of their accounts in one place whether they are with their main bank or with other institutions.

History

The precursor for the modern home online banking services were the distance banking services over electronic media from the early 1980s. The term online became popular in the late '80s and referred to the use of a terminal, keyboard and TV (or monitor) to access the banking system using a phone line. ‘Home banking’ can also refer to the use of a numeric keypad to send tones down a phone line with instructions to the bank. Online services started in New York in 1981 when four of the city’s major banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) offered home banking services using the videotex system. Because of the commercial failure of videotex these banking services never became popular except in France where the use of videotex (Minitel) was subsidised by the telecom provider and the UK, where the Prestel system was used.

The UK's first home online banking services was set up by Bank of Scotland for customers of the Nottingham Building Society (NBS) in 1983. The system used was based on the UK's Prestel system and used a computer, such as the BBC Micro, or keyboard (Tandata Td1400) connected to the telephone system and television set. The system (known as 'Homelink') allowed on-line viewing of statements, bank transfers and bill payments. In order to make bank transfers and bill payments, a written instruction giving details of the intended recipient had to be sent to the NBS who set the details up on the Homelink system. Typical recipients were gas, electricity and telephone companies and accounts with other banks. Details of payments to be made were input into the NBS system by the account holder via Prestel. A cheque was then sent by NBS to the payee and an advice giving details of the payment was sent to the account holder. BACS was later used to transfer the payment directly.

Stanford Federal Credit Union was the first financial institution to offer online internet banking services to all of its members in October 1994.

Today, many banks are internet only banks. Unlike their predecessors, these internet only banks do not maintain brick and mortar bank branches. Instead, they typically differentiate themselves by offering better interest rates and online banking features.

Security

Security token devices

Protection through single password authentication, as is the case in most secure Internet shopping sites, is not considered secure enough for personal online banking applications in some countries. Basically there exist two different security methods for online banking.

- The PIN/TAN system where the PIN represents a password, used for the login and TANs representing one-time passwords to authenticate transactions. TANs can be distributed in different ways, the most popular one is to send a list of TANs to the online banking user by postal letter. The most secure way of using TANs is to generate them by need using a security token. These token generated TANs depend on the time and a unique secret, stored in the security token (this is called two-factor authentication or 2FA). Usually online banking with PIN/TAN is done via a web browser using SSL secured connections, so that there is no additional encryption needed.

Another way to provide TANs to an online banking user, is to send the TAN of the current bank transaction to the user's (GSM) mobile phone via SMS. The SMS text usually quotes the transaction amount and details, the TAN is only valid for a short period of time. Especially in Germany and Austria, many banks have adapted this "SMS TAN" service as it is considered as very secure.

- Signature based online banking where all transactions are signed and encrypted digitally. The Keys for the signature generation and encryption can be stored on smartcards or any memory medium, depending on the concrete implementation.

Attacks

Most of the attacks on online banking used today are based on deceiving the user to steal login data and valid TANs. Two well known examples for those attacks are phishing and pharming. Cross-site scripting and keylogger/Trojan horses can also be used to steal login information.

A method to attack signature based online banking methods is to manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background.

A recent FDIC Technology Incident Report, compiled from suspicious activity reports banks file quarterly, lists 536 cases of computer intrusion, with an average loss per incident of $30,000. That adds up to a nearly $16-million loss in the second quarter of 2007. Computer intrusions increased by 150 percent between the first quarter of 2007 and the second. In 80 percent of the cases, the source of the intrusion is unknown but it occurred during online banking, the report states.

The most recent kind of attack is the so-called Man in the Browser attack, where a Trojan horses permits a remote attacker to modify the destination account number and also the amount.

Countermeasures

There exist several countermeasures which try to avoid attacks. Digital certificates are used against phishing and pharming, the use of class-3 card readers is a measure to avoid manipulation of transactions by the software in signature based online banking variants. To protect their systems against Trojan horses, users should use virus scanners and be careful with downloaded software or e-mail attachments.

In 2001 the FFIEC issued guidance for multifactor authentication (MFA) and then required to be in place by the end of 2006.

Online Banking ePayments

Online Banking ePayments (OBeP) is a type of payments network, developed by the banking industry in conjunction with technology providers, specifically designed to address the unique requirements of payments made via the Internet.

Key aspects of OBeP which distinguish it from other online payments systems are:

1. The consumer is authenticated in real-time by the consumer financial institution's online banking infrastructure.
2. The availability of funds is validated in real-time by the consumer's financial institution.
3. The consumer's financial institution provides guarantee of payment to the merchant.
4. Payment is made as a credit transfer (push payment) from the consumer's financial institution to the merchant, as opposed to a debit transfer (pull payment).
5. Payment is made directly from the consumer's account rather than through a third-party account.

Privacy & Security Features

OBeP systems protect consumer personal information by not requiring the disclosure of account numbers or other sensitive personal data to online merchants or other third parties. During the checkout process, the merchant redirects the consumer to their financial institution's online banking site where they login and authorize charges. After charges are authorized, the financial institution redirects the consumer back to the merchant site. All network communications are protected using industry standard encryption. Additionally, communications with the OBeP network take place on a virtual private network, not over the public Internet.

Costs

Costs associated with fraud, estimated at 1.2% of sales by online retailers in 2009, are reported to be dramatically reduced with OBeP, because the issuer bank is responsible for the authentication of the credit transaction and provides guaranteed funds to the merchant.

Because the merchant is not responsible for storing and protecting confidential consumer information, OBeP systems also reduce costs associated with mitigating fraud , fraud screening, and PCI audits.

Transaction fees on Online Banking ePayments vary by network, but are often fixed, and lower than the average 1.9% merchant fees associated with credit card transactions – especially for larger purchases.

Other Benefits

For Consumers

- use of cash-like payment encourages responsible consumerism
- does not require set-up or registration with a third-party payments entity
- presents familiar interface to facilitate online payment
- awareness of funds availability

For Merchants

- improved sales conversion / reduced abandoned carts
- real time authorization of guaranteed ACH payment (good funds)
- offering preferred payment methods may drive repeat transactions

For Financial Institutions

- recapture revenue being lost to alternative payment providers
- encourages consumers to move to online banking, replacing more costly branch and telephone alternatives

Types & Implementations

OBeP networks may be divided into two categories, based on the network architecture:

1. Multi-Bank – requires that a merchant have a single connection to the OBeP network in order to accept payment from any participating financial institution.

> *Examples include:* EPS, IDEAL, Interac Online, Giropay, and Secure Vault Payments

2. Mono-Bank – requires that a merchant have a separate connection to each participating financial institution.

A third category, also known as "overlay payment solutions" provide a similar consumer experience to Online Banking ePayments, but violate a key tenet of the OBeP definition by requiring the consumer to share their online banking credentials with a third party. Examples include: DIRECTebanking.com, sofortüberweisung.de, SafetyPay, UseMyServicesand POLi

A fourth category requires that a merchant have a single connection to an alternative payment provider. This alternative payment provider then have connections to multiple online banks. This does not require the consumer to share their online banking credentials, but still offer the same advantages to the merchants as "overlay payment solutions". Examples include: inpay.com and gluepay.

Chapter- 10

SMS Banking

Screenshot of a typical SMS Banking message on a mobile screen

SMS banking is a technology-enabled service offering from banks to its customers, permitting them to operate selected banking services over their mobile phones using SMS messaging.

Push and pull messages

SMS banking services are operated using both push and pull messages. Push messages are those that the bank chooses to send out to a customer's mobile phone, without the customer initiating a request for the information. Typically push messages could be either Mobile marketing messages or messages alerting an event which happens in the customer's bank account, such as a large withdrawal of funds from the ATM or a large payment using the customer's credit card, etc.

Another type of push message is One-time password (OTPs). OTPs are the latest tool used by financial and banking service providers in the fight against cyber fraud. Instead of relying on traditional memorized passwords, OTPs are requested by consumers each time they want to perform transactions using the online or mobile banking interface.

When the request is received the password is sent to the consumer's phone via SMS. The password is expired once it has been used or once its scheduled life-cycle has expired.

Pull messages are those that are initiated by the customer, using a mobile phone, for obtaining information or performing a transaction in the bank account. Examples of pull messages for information include an account balance enquiry, or requests for current information like currency exchange rates and deposit interest rates, as published and updated by the bank.

The bank's customer is empowered with the capability to select the list of activities (or alerts) that he/she needs to be informed. This functionality to choose activities can be done either by integrating to the internet banking channel or through the bank's customer service call centre.

Typical push and pull services offered under SMS banking

Depending on the selected extent of SMS banking transactions offered by the bank, a customer can be authorized to carry out either non-financial transactions, or both and financial and non-financial transactions. SMS banking solutions offer customers a range of functionality, classified by push and pull services as outlined below.

Typical push services would include:

- Periodic account balance reporting (say at the end of month);
- Reporting of salary and other credits to the bank account;
- Successful or un-successful execution of a standing order;
- Successful payment of a cheque issued on the account;
- Insufficient funds;
- Large value withdrawals on an account;
- Large value withdrawals on the ATM or EFTPOS on a debit card;
- Large value payment on a credit card or out of country activity on a credit card.
- One-time password and authentication

Typical pull services would include:

- Account balance enquiry;
- Mini statement request;
- Electronic bill payment;
- Transfers between customer's own accounts, like moving money from a savings account to a current account to fund a cheque;
- Stop payment instruction on a cheque;
- Requesting for an ATM card or credit card to be suspended;
- De-activating a credit or debit card when it is lost or the PIN is known to be compromised;

- Foreign currency exchange rates enquiry;
- Fixed deposit interest rates enquiry.

Concerns and skepticism about SMS banking

There is a very real possibility for fraud when SMS banking is involved, as SMS uses insecure encryption and is easily spoofable. Supporters of SMS banking claim that while SMS banking is not as secure as other conventional banking channels, like the ATM and internet banking, the SMS banking channel is not intended to be used for very high-risk transactions.

Quality of service in SMS banking

Because of the concerns made explicit above, it is extremely important that SMS gateway providers can provide a decent quality of service for banks and financial institutions in regards to SMS services. Therefore, the provision of Service Level Agreement(SLA) is a requirement for this industry; it is necessary to give the bank customer delivery guarantees of all messages, as well as measurements on the speed of delivery, throughput, etc. SLAs give the service parameters in which a messaging solution is guaranteed to perform.

The convenience factor

The convenience of executing simple transactions and sending out information or alerting a customer on the mobile phone is often the overriding factor that dominates over the skeptics who tend to be overly bitten by security concerns.

As a personalized end-user communication instrument, today mobile phones are perhaps the easiest channel on which customers can be reached on the spot, as they carry the mobile phone all the time no matter where they are. Besides, the operation of SMS banking functionality over phone key instructions makes its use very simple. This is quite different from internet banking which can offer broader functionality, but has the limitation of use only when the customer has access to a computer and the Internet. Also, urgent warning messages, such as SMS alerts, are received by the customer instantaneously; unlike other channels such as the post, email, Internet, telephone banking, etc. on which a bank's notifications to the customer involves the risk of delayed delivery and response.

The SMS banking channel also acts as the bank’s means of alerting its customers, especially in an emergency situation; e.g. when there is an ATM fraud happening in the region, the bank can push a mass alert (although not subscribed by all customers) or automatically alert on an individual basis when a predefined ‘abnormal’ transaction happens on a customer’s account using the ATM or credit card. This capability mitigates the risk of fraud going unnoticed for a long time and increases customer confidence in the bank’s information systems.

Compensating controls for lack of encryption

The lack of encryption on SMS messages is an area of concern that is often discussed. This concern sometimes arises within the group of the bank's technology personnel, due to their familiarity and past experience with encryption on the ATM and other payment channels. The lack of encryption is inherent to the SMS banking channel and several banks that use it have overcome their fears by introducing compensating controls and limiting the scope of the SMS banking application to where it offers an advantage over other channels.

Suppliers of SMS banking software solutions have found reliable means by which the security concerns can be addressed. Typically the methods employed are by pre-registration and using security tokens where the transaction risk is perceived to be high. Sometimes ATM type PINs are also employed, but the usage of PINs in SMS banking makes the customer's task more cumbersome.

Technologies employed for SMS banking

Most SMS banking solutions are add-on products and work with the bank's existing host systems deployed in its computer and communications environment. As most banks have multiple backend hosts, the more advanced SMS banking systems are built to be able to work in a multi-host banking environment; and to have open interfaces which allow for messaging between existing banking host systems using industry or de-facto standards.

Well developed and mature SMS banking software solutions normally provide a robust control environment and a flexible and scalable operating environment. These solutions are able to connect seamlessly to multiple SMSC operators in the country of operation. Depending on the volume of messages that are require to be pushed, means to connect to the SMSC could be different, such as using simple modems or connecting over leased line using low level communication protocols (like SMPP, UCP etc.). Advanced SMS banking solutions also cater to providing failover mechanisms and least-cost routing options.

Chapter- 11

Smart Card

Many different pad layouts can be found on a contact Smart card

A **smart card**, **chip card**, or **integrated circuit card** (**ICC**), is any pocket-sized card with embedded integrated circuits. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps dedicated security logic. Microprocessor cards contain volatile memory and microprocessor components. The card is made of plastic, generally polyvinyl chloride, but sometimes acrylonitrile butadiene styrene or polycarbonate . Smart cards may also provide strong security authentication for single sign-on within large organizations.

Overview

Smart card used for health insurance in France

A smart card may have the following generic characteristics:

- Dimensions similar to those of a credit card. ID-1 of the ISO/IEC 7810 standard defines cards as nominally 85.60 by 53.98 millimetres (3.370 × 2.125 in). Another popular size is ID-000 which is nominally 25 by 15 millimetres (0.984 × 0.591 in) (commonly used in SIM cards). Both are 0.76 millimetres (0.030 in) thick.
- Contains a tamper-resistant security system (for example a secure cryptoprocessor and a secure file system) and provides security services (e.g., protects in-memory information).
- Managed by an administration system which securely interchanges information and configuration settings with the card, controlling card blacklisting and application-data updates.
- Communicates with external services via card-reading devices, such as ticket readers, ATMs, etc.

Benefits

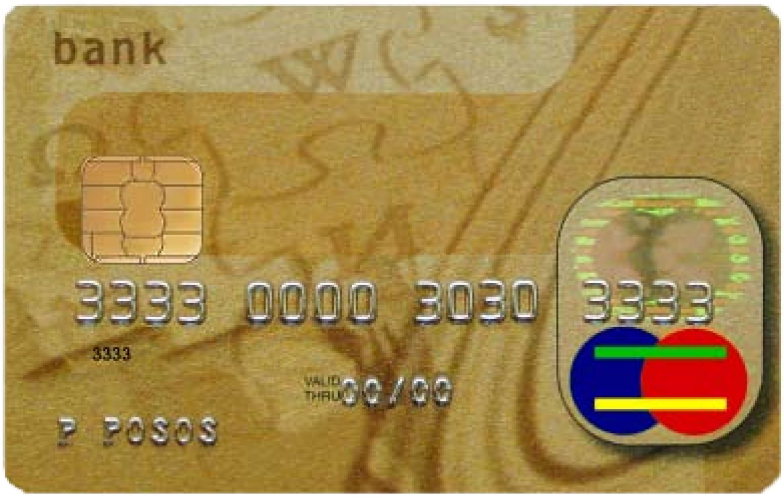
Smart cards can provide identification, authentication, data storage and application processing.

The benefits of smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contactless smart card can be programed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card. For example, a smart card can be programed to only allow a contactless transaction if it is also within range of another device like a uniquely paired mobile phone. This can significantly increase the security of the smart card.

Governments gain a significant enhancement to the provision of publicly funded services through the increased security offered by smart cards. These savings are passed onto society through a reduction in the necessary funding or enhanced public services.

Individuals gain increased security and convenience when using smart cards designed for interoperability between services. For example, consumers only need to replace one card if their wallet is lost or stolen. Additionally, the data storage available on a card could contain medical information that is critical in an emergency should the card holder allow access to this.

History



A smart card, combining credit card and debit card properties. The 3 by 5 mm security chip embedded in the card is shown enlarged in the inset. The contact pads on the card enables electronic access to the chip.

In 1968 German rocket scientist Helmut Gröttrup and his colleague Jürgen Dethloff invented the automated chip card, receiving a patent only in 1982, while working for German company Giesecke & Devrient. The first mass use of the cards was as a *Télécarte* for payment in French pay phones, starting in 1983.

French inventor Roland Moreno patented the memory card concept in 1974. In 1977, Michel Ugon from Honeywell Bull invented the first microprocessor smart card. In 1978, Bull patented the SPOM (Self Programmable One-chip Microcomputer) that defines the necessary architecture to program the chip. Three years later, Motorola used this patent in its "CP8". At that time, Bull had 1,200 patents related to smart cards. In 2001, Bull sold its CP8 division together with its patents to Schlumberger, who subsequently combined its own internal smart card department and CP8 to create Axalto. In 2006, Axalto and Gemplus, at the time the world's no. 2 and no. 1 smart card manufacturers, merged and became Gemalto.

The second use integrated microchips into all French *Carte Bleue* debit cards in 1992. Customers inserted the card into the merchant's POS terminal, then typed the PIN, before the transaction was accepted. Only very limited transactions (such as paying small highway tolls) are processed without a PIN.

Smart-card-based "electronic purse" systems store funds on the card so that readers do not need network connectivity and entered service throughout Europe in the mid-1990s, most notably in Germany (Geldkarte), Austria (Quick), Belgium (Proton), France (Mon€o), the Netherlands (Chipknip and Chipper), Switzerland ("Cash"), Norway ("Mondex"), Sweden ("Cash", decommissioned in 2004), Finland ("Avant"), UK ("Mondex"), Denmark ("Danmønt") and Portugal ("Porta-moedas Multibanco").

The major boom in smart card use came in the 1990s, with the introduction of smart-card-based SIMs used in GSM mobile phone equipment in Europe. With the ubiquity of mobile phones in Europe, smart cards have become very common.

The international payment brands MasterCard, Visa, and Europay agreed in 1993 to work together to develop the specifications for smart cards as either a debit or a credit card. The first version of the EMV system was released in 1994. In 1998 a stable release of the specifications became available. EMVco, the company responsible for the long-term maintenance of the system, upgraded the specification in 2000 and in 2004. EMVco's purpose is to assure the various financial institutions and retailers that the specifications retain backward compatibility with the 1998 version.

With the exception of countries such as the United States EMV-compliant cards and equipment are widespread. Typically, a country's national payment association, in

coordination with MasterCard International, Visa International, American Express and JCB, jointly plan and implement EMV systems.

Contactless smart cards that do not require physical contact between card and reader are becoming increasingly popular for payment and ticketing applications such as mass transit and highway tolls. Visa and MasterCard have agreed to an easy-to-implement version that was deployed in 2004–2006 in the USA. Most contactless fare collection implementations are custom and incompatible, though the MIFARE Standard card from Philips has a considerable market share in the US and Europe.

Smart cards are also being introduced in personal identification and entitlement schemes at regional, national, and international levels. Citizen cards, drivers' licenses, and patient card schemes are appearing. In Malaysia, the compulsory national ID scheme MyKad includes eight different applications and has 18 million users. Contactless smart cards are part of ICAO biometric passports to enhance security for international travel.

Contact smart card

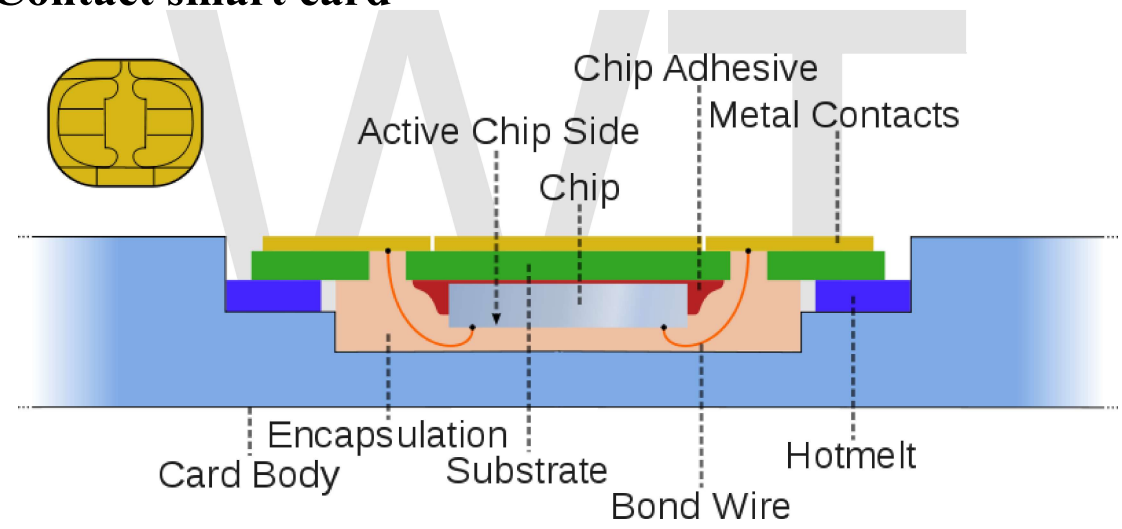


Illustration of smart card structure and packaging

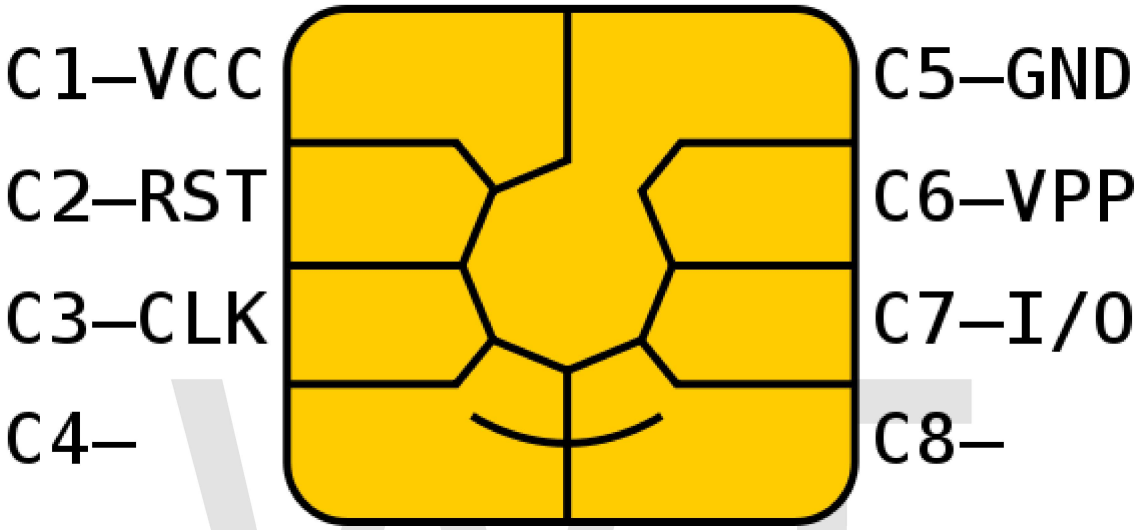
Contact smart cards have a contact area of approximately 1 square centimetre (0.16 sq in), comprising several gold-plated contact pads. These pads provide electrical connectivity when inserted into a reader.

The ISO/IEC 7810 and ISO/IEC 7816 series of standards define:

- physical shape and characteristics
- electrical connector positions and shapes
- electrical characteristics
- communications protocols, including commands sent to and responses from the card
- basic functionality

Cards do not contain batteries; power is supplied by the card reader.

Signals



A smart card pinout

VCC
: Power supply.

RST
: Reset signal, used to reset the card's communications.

CLK
: Provides the card with a clock signal, from which data communications timing is derived.

GND
: Ground (reference voltage).

VPP
: Programming voltage input - originally an input for a higher voltage to program persistent memory (e.g., EEPROM), but now deprecated.

I/O
: Serial input and output (half-duplex).

C4, C8
: The two remaining contacts are AUX1 and AUX2 respectively, and used for USB interfaces and other uses.

Reader

Contact smart card readers are used as a communications medium between the smart card and a host (e.g., a computer, a point of sale terminal) or a mobile telephone.

Because the chips in financial cards are the same as those used in Subscriber Identity Modules (SIMs) in mobile phones, programmed differently and embedded in a different piece of PVC, chip manufacturers are building to the more demanding GSM/3G standards. So, for example, although the EMV standard allows a chip card to draw 50 mA from its terminal, cards are normally well below the telephone industry's 6 mA limit. This allows smaller and cheaper financial card terminals.

Contactless

A second card type is the *contactless smart card*, in which the card communicates with and is powered by the reader through RF induction technology (at data rates of 106–848 kbit/s). These cards require only proximity to an antenna to communicate. They are often used for quick or hands-free transactions such as paying for public transportation without removing the card from a wallet.

ISO/IEC 14443 is the standard for contactless smart card communications. It defines two types of contactless cards (*A* and *B*). Proposals for ISO/IEC 14443 types C, D, E, F and G have been rejected by the International Organization for Standardization. An alternative standard is ISO/IEC 15693, which allows communications at distances up to 50 cm (20 in).

Examples of widely used contactless smart cards are Montreal's Opus card, Hong Kong's Octopus card, Shanghai's Public Transportation Card, Moscow's Transport/Social Card, Bucharest's Cardul Activ used as a cash card for public transport within Bucharest, South Korea's T-money (bus, subway, taxi), Melbourne's myki, the Netherlands' OV-chipkaart, Milan's Itinero, London's Oyster card, London's sQuidcard which is used for small payments in Thames Ditton, Bolton and Dundee, Japan Rail's Suica card, Iran's Metropolitans Subway Corp., Israel's Rav-Kav, Mumbai's Brihanmumbai Electric Supply and Transport and Beijing's Municipal Administration and Communications Card. All of them are primarily designed for public transportation payment and other electronic purse applications.

Novosibirsk (Russia). Transport fare collection terminal CFT

Smart card being used to pay for public transportation in the Helsinki area.

Like smart cards with contacts, contactless cards do not have a battery. Instead, they use a built-in inductor to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics.

Credit cards

These are the best known payment cards (classic plastic card):

- Visa: Visa Contactless, Quick VSDC—"qVSDC", Visa Wave, MSD, payWave
- MasterCard: PayPass Magstripe, PayPass MChip
- American Express: ExpressPay
- Discover: Zip

Roll-outs started in 2005 in USA. Asia and Europe followed in 2006. Contactless (non PIN) transactions cover a payment range of ~$5–50. There is an ISO/IEC 14443 PayPass implementation. Some, but not all PayPass implementations conform to EMV.

Non-EMV cards work like magnetic stripe cards. This is a typical USA card technology (PayPass Magstripe and VISA MSD). The cards do not hold/maintain the account

balance. All payment passes without a PIN, usually in off-line mode. The security of such a transaction is no greater than with a magnetic stripe card transaction.

EMV cards have contact and contactless interfaces. They work as a normal EMV card via contact interface. Via contactless interface they work somewhat differently in that the card command sequence adopts contactless features such as low power and short transaction time.

Hybrids

Dual-interface cards implement contactless and contact interfaces on a single card with some shared storage and processing. An example is Porto's multi-application transport card, called Andante, that uses a chip with both contact and contactless (ISO/IEC 14443 Type B) interfaces.

Communication protocols

Communication protocols

Name	Description
T=0	Character-level transmission protocol, defined in ISO/IEC 7816-3
T=1	Block-level transmission protocol, defined in ISO/IEC 7816-3
ISO/IEC 14443	APDU transmission via contactless interface, defined in ISO/IEC 14443-4

Cryptographic smart cards

Cryptographic smart cards are often used for single sign-on. Most advanced smart cards include specialized cryptographic hardware that uses algorithms such as RSA and DSA. Today's cryptographic smart cards generate key pairs on board, to avoid the risk from having more than one copy of the key (since by design there usually isn't a way to extract private keys from a smart card). Such smart cards are mainly used for digital signature and secure identification.

The most common way to access cryptographic smart card functions on a computer is to use a vendor-provided PKCS#11 library. On Microsoft Windows the CSP API is also supported.

The most widely used cryptographic algorithms in smart cards (excluding the GSM so-called "crypto algorithm") are Triple DES and RSA. The key set is usually loaded (DES) or generated (RSA) on the card at the personalization stage.

Some of these smart card are also made to support the NIST standard for Personal Identity Verification (PIV).

Applications

Computer security

The Mozilla Firefox web browser can use smart cards to store certificates for use in secure web browsing.

Some disk encryption systems, such as FreeOTFE, TrueCrypt and Microsoft Windows 7 BitLocker, can use smart cards to securely hold encryption keys, and also to add another layer of encryption to critical parts of the secured disk.

Smart cards are also used for single sign-on to log on to computers.

Smart cards support functionality has been added to Windows Live Passports.

Financial

Smart cards serve as credit or ATM cards, fuel cards, mobile phone SIMs, authorization cards for pay television, household utility pre-payment cards, high-security identification and access-control cards, and public transport and public phone payment cards.

Smart cards may also be used as electronic wallets. The smart card chip can be "loaded" with funds to pay parking meters and vending machines or at various merchants. Cryptographic protocols protect the exchange of money between the smart card and the accepting machine. No connection to the issuing bank is necessary, so the holder of the card can use it even if not the owner. Examples are Proton, Geldkarte, Chipknip and Mon€o. The German Geldkarte is also used to validate customer age at vending machines for cigarettes.

Health care (medical)

Smart health cards can improve the security and privacy of patient information, provide a secure carrier for portable medical records, reduce health care fraud, support new processes for portable medical records, provide secure access to emergency medical information, enable compliance with government initiatives and mandates, and provide the platform to implement other applications as needed by the health care organization.

Identification

A quickly growing application is in digital identification. In this application, the cards authenticate identity. The most common example employs PKI. The card stores an encrypted digital certificate issued from the PKI provider along with other relevant information. Examples include the U.S. Department of Defense (DoD) Common Access Card (CAC), and various identification cards used by many governments for their citizens. Combined with biometrics, cards can provide two- or three-factor

authentication. Smart cards are not always privacy-enhancing, because the subject carries possibly incriminating information on the card. Contactless smart cards that can be read from within a wallet or even a garment simplify authentication.

The first smart card driver's license system in the world was implemented in 1987 in Turkey. Turkey had a high level of road accidents and decided to develop and use digital tachograph devices on heavy vehicles, instead of the existing mechanical ones, to reduce speed violations. Since 1987, the professional driver's licenses in Turkey are issued as smart cards and the driver is required to insert his driver's license into the digital tachograph before starting to drive. The tachograph unit records speed violations for each driver and gives a printed report. The driving hours for each driver is also being monitored and reported. In 1990 the European Union conducted a feasibility study through BEVAC Consulting Engineers, titled "Feasibility study with respect to a European electronic drivers licence (based on a smart-card)on behalf of Directorate General VII". In this study, chapter seven is dedicated to the experience in Turkey, stating that the electronic driver's license application, in the form of smart cards, was first implemented in Turkey in 1987.

A smart card driver's license system was later issued in 1995 in Mendoza province of Argentina. Mendoza had a high level of road accidents, driving offenses, and a poor record of recovering outstanding fines. Smart licenses hold up-to-date records of driving offenses and unpaid fines. They also store personal information, license type and number, and a photograph. Emergency medical information such as blood type, allergies, and biometrics (fingerprints) can be stored on the chip if the card holder wishes. The Argentina government anticipates that this system will help to collect more than $10 million per year in fines.

In 1999 Gujarat was the first Indian state to introduce a smart card license system. To date it has issued 5 million smart card driving licenses to its people.

> “a national ID card, protected by a 1,024-bit key code, is impossible to break without a supercomputer working away for a hundred years”

In 2002, the Estonian government started to issue smart cards named ID Kaart as primary identification for citizens to replace the usual passport in domestic and EU use. As of 2010 about 1 million smart cards have been issued (total population is about 1.3 million) and they are widely used in internet banking, buying public transport tickets, authorization on various websites etc.

By the start of 2009 the entire population of Spain and Belgium will have an eID card that is used for identification. These cards contain two certificates: one for authentication and one for signature. This signature is legally enforceable. More and more services in these countries use eID for authorization.

Smart cards are also beginning to be used in emergency situations. In 2004, The Smart Card Alliance issued a statement expressing the need to "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification". In light of this, emergency response personnel have now begun to carry these cards so that they can be positively identified in emergency situations. WidePoint Corporation, a smart card provider to FEMA, produces cards that contain additional personal information, such as medical records and skill sets. Cards like these provide immediate access to information, which allows first responders to bypass organizational paperwork and focus more time on the emergency resolution.

Other

Smart cards are widely used to protect digital television streams. VideoGuard is a specific example of how smart card security worked (and was cracked).

The Malaysian government uses smart identity cards carried by all citizens and resident non-citizens. The personal information inside the MYKAD card can be read using special APDU commands.

Since April 2009, *Toppan Printing Company* (凸版印刷 *Toppan insatsu*?) has manufactured reusable smart cards for money transfer and made from paper instead of plastic.

Security

Smart cards have been advertised as suitable for personal identification tasks, because they are engineered to be tamper resistant. The chip usually implements some cryptographic algorithm. There are, however, several methods for recovering some of the algorithm's internal state.

Differential power analysis

Differential power analysis involves measuring the precise time and electrical current required for certain encryption or decryption operations. This can deduce the on-chip private key used by public key algorithms such as RSA. Some implementations of symmetric ciphers can be vulnerable to timing or power attacks as well.

Physical disassembly

Smart cards can be physically disassembled by using acid, abrasives, or some other technique to obtain unrestricted access to the on-board microprocessor. Although such techniques obviously involve a fairly high risk of permanent damage to the chip, they permit much more detailed information (e.g. photomicrographs of encryption hardware) to be extracted.

Problems

The plastic card in which the chip is embedded is fairly flexible, and the larger the chip, the higher the probability that normal use could damage it. Cards are often carried in wallets or pockets—a harsh environment for a chip. However, for large banking systems, failure-management costs can be more than offset by fraud reduction. Using a smart card for mass transit presents a privacy risk, because it allows the mass transit operator (and the government) to track an individual's movement. In Finland, the Data Protection Ombudsman prohibited the transport operator YTV from collecting such information, despite YTV's argument that the card owner has the right to a list of trips paid with the card. Prior to this, such information was used in the investigation of the Myyrmanni bombing. Client-side identification and authentication cards are the most secure way for e.g., internet banking applications, but security is never 100% sure. If the account holder's computer hosts malware, the security model may be broken. Malware can override the communication (both input via keyboard and output via application screen) between the user and the application. The malware (e.g. the trojan Silentbanker) could modify a transaction, unnoticed by the user. Banks like Fortis and Dexia in Belgium combine a smart card with an unconnected card reader to avoid this problem. The customer enters a challenge received from the bank's website, a PIN and the transaction amount into the reader, The reader returns an 8-digit signature. This signature is manually entered into the personal computer and verified by the bank, preventing malware from changing the transaction amount.

Another problem is the lack of standards for functionality and security. To address this problem, The Berlin Group launched the ERIDANE Project to propose "a new functional and security framework for smart-card based Point of Interaction (POI) equipment".

Terminology

- ATR: Answer to reset
- BCD: Binary-coded decimal
- CHV: Card Holder Verification
- COS: Card operating system
- DF: Dedicated File
- IC: Integrated circuit
- PC/SC: Personal computer / smart card
- MF: Master File

- PPS: Protocol and Parameter Select
- RFU: Reserved for Future Use

Chapter- 12

Other Banking Technologies

Telephone banking

Telephone banking is a service provided by a financial institution, which allows its customers to perform transactions over the telephone.

Most telephone banking services use an automated phone answering system with phone keypad response or voice recognition capability. To guarantee security, the customer must first authenticate through a numeric or verbal password or through security questions asked by a live representative. With the obvious exception of cash withdrawals and deposits, it offers virtually all the features of an automated teller machine: account balance information and list of latest transactions, electronic bill payments, funds transfers between a customer's accounts, etc.

Usually, customers can also speak to a live representative located in a call centre or a branch, although this feature is not always guaranteed to be offered 24/7. In addition to the self-service transactions listed earlier, telephone banking representatives are usually trained to do what was traditionally available only at the branch: loan applications, investment purchases and redemptions, chequebook orders, debit card replacements, change of address, etc.

Banks which operate mostly or exclusively by telephone are known as phone banks. They also help modernise the user by using special technology.

Standardization

This makes it possible for a customer of the bank to know account related information over a telephone.

TeleBanker is a state-of-the-art interactive voice response system (IVRS) that facilitates 24-hours-a-day, 365-days-a-year banking from a plain Telephone instrument! Unique Features of Tele Banking : Data input by voice/keypad Encryption of input/output data Data output by voice/fax/e-mail Customer authentication by password/PIN Services Available Balance enquiry Issue cheque book/DD Enquiry on last few transactions Fund transfer Inward/outward cheque status Telephone/electricity/credit card bill payment

Video banking

Video banking is a term used for performing banking transactions or professional banking consultations via a remote video connection. Video banking can be performed via purpose built banking transaction machines (similar to an Automated teller machine), or via a videoconference enabled bank branch.

Types of Video Banking

Today, video banking has many forms, each with its own benefits and limitations.

In-branch

Video banking can be conducted in a traditional banking branch. This form of video banking replaces or partially displaces the traditional banking tellers to a location outside of the main banking branch area. Via the video and audio link, the tellers are able to service the banking customer. The customer in the branch uses a purpose built machine to process viable medias such as cheques, cash, or coins.

Time Convenience

Video banking can provide professional banking services to bank customers during nontraditional banking hours at convenient times such as in after hours banking branch vestibules that could be open up to 24 hours a day. This gives bank customers the benefit of personal teller service during hours when bank branches are not typically open.

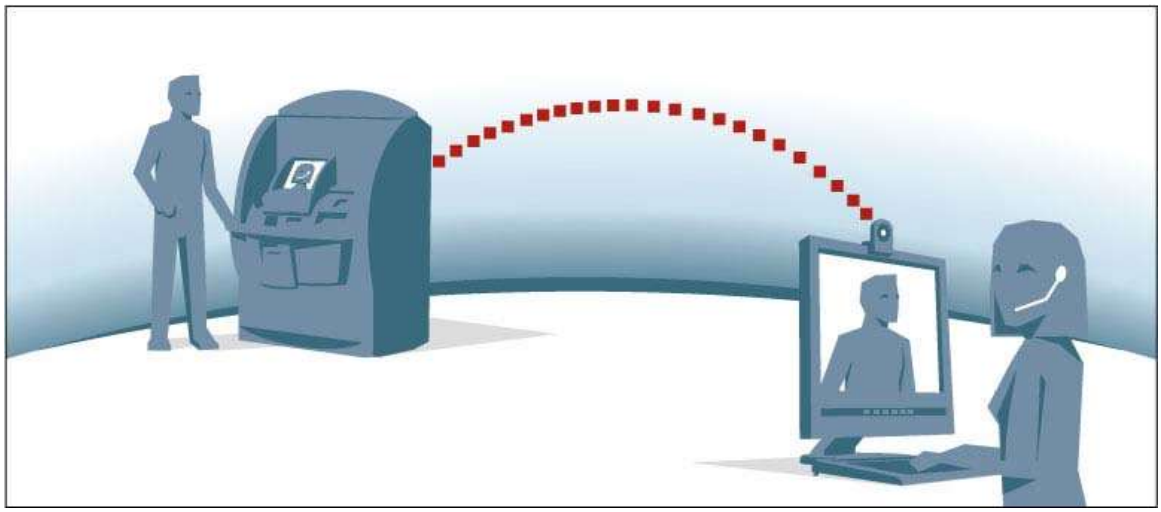
Location Convenience

Video banking can provide professional banking services in nontraditional banking locations such as after hours banking branch vestibules, grocery stores, office buildings, factories, or educational campuses.

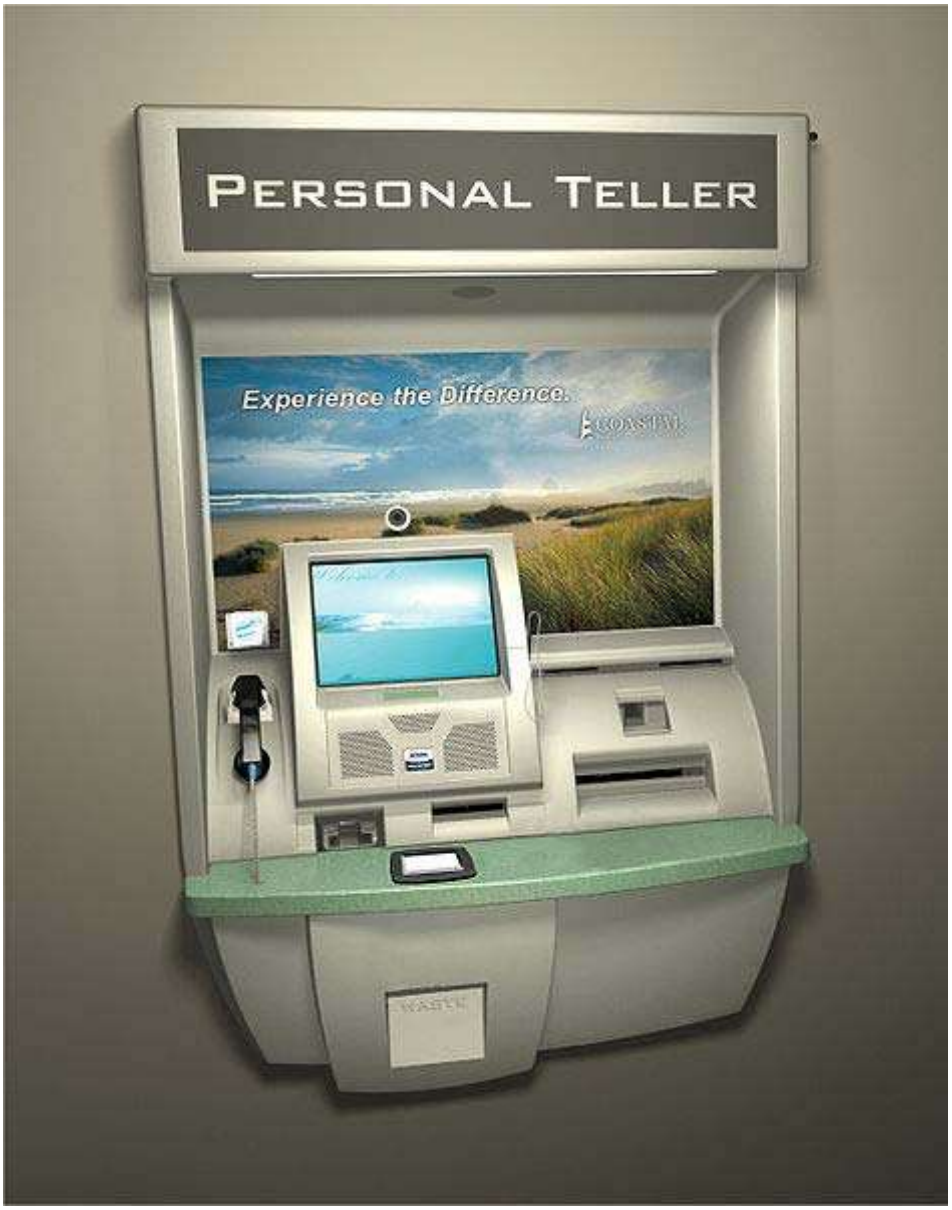
Technology Branches

Video banking can enable banks to expand real-time availability of high-value banking consultative services in branches that might not otherwise have access to the banking expertise.

Technology of Video Banking



Graphical Depiction of a Video Banking Transaction System



Example of a uGenius Technology video banking system that has been customized for a production deployment.

Although video banking has many different forms, they all have similar basic components.

Video Connection

Although termed video banking, the video connection is always accompanied by an audio link which ensures the customer and bank representative can communicate clearly with one another. The communication link for that video and audio tyically requires a high-speed data connection for applications where the tellers are not in the same physical location. Various technologies are employed by the vendors of video banking, but recent

advances in audio and video compression make the use of these technologies much more affordable.

Transaction Equipment

Other than the deployment location, one of the major differences between video banking and videoconferencing is the ability to conduct banking transactions and exchange viable medias such as checks, cash, and coins. Purpose built machines, such as a Personal Teller Machine (PTM), enable both the video / audio link to the customer plus the ability to accept and dispense viable medias. The system typically allows the bank teller to manipulate the PTM machine to accept or dispense the cash and checks.

Purpose-built transaction equipment is currently available, but in the future these video banking systems will likely leverage existing automated teller machines which will be modified to enable the audio and video communication.

Video Banking Services

Depending on the type of video banking solution deployed there are numerous types of services that can be offered. In conjunction with transaction hardware video banking can include all of the following types of services.

- Customer authentication
- Cash Deposits
- Check Deposits
- Cash Withdrawal
- Coin Withdrawals
- Check Print
- Account Transfers
- Bill Payments
- Account inquiries
- Process New Accounts

With all types of video banking the following services are enabled:

- Process New Loans
- Consult with banking professionals
- Process New Accounts
- Inquire about banking services

Magnetic ink character recognition

Magnetic Ink Character Recognition, or **MICR**, is a character recognition technology used primarily by the banking industry to facilitate the processing of cheques. The technology allows computers to read information (such as account numbers) off of printed documents. Unlike barcodes or similar technologies, however, MICR codes can be easily read by humans.

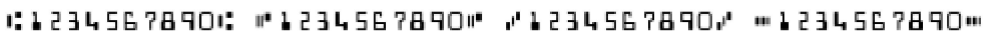
MICR characters are printed in special typefaces with a magnetic ink or toner, usually containing iron oxide. As a machine decodes the MICR text, it first magnetizes the characters in the plane of the paper. Then the characters are passed over a MICR read head, a device similar to the playback head of a tape recorder. As each character passes over the head it produces a unique waveform that can be easily identified by the system.

The use of magnetic printing allows the characters to be read reliably even if they have been overprinted or obscured by other marks, such as cancellation stamps and signature. The error rate for the magnetic scanning of a typical check is smaller than with optical character recognition systems. For well printed MICR documents, the "can't read" rate is usually less than 1% while the substitution rate (misread rate) is in the order of 1 per 100,000 characters.

MICR is standardized by **ISO 1004:1995**.

Fonts

The major MICR fonts used around the world are **E-13B** and **CMC-7**. In the 1960s, the MICR fonts became a symbol of modernity or futurism, leading to the creation of lookalike "computer" typefaces that imitated the appearance of the MICR fonts, which unlike real MICR fonts, had a full character repertoire.



The 14 characters of the **E-13B** font. The control characters bracketing each numeral block are (from left to right) *transit*, *on-us*, *amount*, and *dash*.

Almost all Indian, US, Canadian and UK cheques use the E-13B font. (The "13" in the font's name refers to the 0.013 inch grid used to design it.) Besides decimal digits it also contains the following symbols: ⑆ (transit: used to delimit a bank branch routing transit

number), ⑈ (amount: used to delimit a transaction amount), ⑉ (on-us: used to delimit a customer account number), and ⑊ (dash: used to delimit parts of numbers, e.g., routing numbers or account numbers).

An example of the CMC-7 MICR font. Shown are the 15 characters of the **CMC-7** font. The control characters after the numerals are (from left to right) *internal*, *terminator*, *amount*, *routing*, and an unused character.

Some countries, including France, use the CMC-7 font developed by Bull.

Electronic funds transfer

Electronic funds transfer or **EFT** is the electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions, through computer-based systems.

The term is used for a number of different concepts:

- Cardholder-initiated transactions, where a cardholder makes use of a payment card
- Direct deposit payroll payments for a business to its employees, possibly via a payroll service bureau
- Direct debit payments, sometimes called ***electronic checks***, for which a business debits the consumer's bank accounts for payment for goods or services
- Electronic bill payment in online banking, which may be delivered by EFT or paper check
- Transactions involving stored value of electronic money, possibly in a private currency
- Wire transfer via an international banking network (generally carries a higher fee)
- Electronic Benefit Transfer

In 1978 U.S. Congress passed the Electronic Funds Transfer Act to establish the rights and liabilities of consumers as well as the responsibilities of all participants in EFT activities in the United States.

Anonymous internet banking

Anonymous Internet Banking is the name given to the proposed use of strong financial cryptography to make electronic bank secrecy (or more precisely pseudonymous banking) possible. The bank issues currency in the form of electronic tokens that can be converted on presentation to the bank to some other currency. This concept has a long history in which free banking institutions have issued their own paper currency often backed by a physical commodity.

History

Whilst the academic study of trust relationships and systems has long been the forte of intelligence services such as the American NSA, the growth of the internet in the 1990s and the contemporary declassification of related knowledge allowed for greater public discussion of the potential for anonymous banking services by groups such as the cryptoanarchists and cypherpunks.

Implemented systems

Examples of anonymous internet banking services and software that have already been implemented include:

- eCache: an anonymous bank operating over the Tor network.
- Bitcoin: distributed P2P cryptocurrency.
- Pecunix: an (optionally?) anonymous digital gold currency.
- Yodelbank: an anonymous bank built on top of various digital gold currencies which ended operations during November 2005.
- Open Transactions: Open-source software, including a library, server, and test client, implementing untraceable digital cash and anonymous numbered accounts.

The underlying mathematics

Anonymous internet banking depends on the mathematics of public key cryptography and blind signature algorithms. In this simple example we have Alice and Bob and a banker. The banker generates an RSA public key with modulus $n = PQ$, where P and Q are large primes, making n a semiprime. As described in RSA operation, the bank also generates public key exponent e and private key exponent d.

Bob asks the banker for a $100 deposit slip in anticipation of Alice wanting to transfer money to him. To generate a deposit slip the bank selects a large, globally unique random

number R and encrypts it using the bank's public key; this means that it can only be decrypted with the bank's secret key:

$R' = R^e \pmod{n}$

This encrypted value R' is sent to Bob with the promise to deposit $100 into his account when Bob sends the value R back to the bank. The bank is confident that Bob won't be able to break RSA to generate R from R' within the heat death of the universe without knowledge of d, so it does not worry about handing out the deposit slips without receiving anything from Bob.

When Alice wants to pay Bob $100 she asks for the deposit slip and Bob sends her R'. Alice selects a large random value w coprime with n (so as to have an inverse modulo n) and uses it to blind $R'' = w^e * R'$ and sends it to the bank to be blind signed. The Bank charges Alice $100 for this operation and returns the blind signed value R'''. Due to the symmetric properties of RSA, this provides her with R:

$$\begin{aligned} R''' &= (w^e * R')^d \pmod{n} \\ &= (w^e * R^e)^d \pmod{n} \\ &= (w * R)^{ed} \pmod{n} \\ &= w * R \pmod{n} \end{aligned}$$

Because of the blinding process, the Bank is not able to associate R'' with R' or R, so it is unable to determine that Bob and Alice are doing business together, preserving the anonymity of the transaction. Alice unblinds R''' (by dividing it by w) to generate the original value R, which she sends to Bob. Bob verifies that R can be encrypted with the bank's public key by computing $R' = R^e \pmod{n}$, which means that Alice has deposited $100 into the bank. Bob then sends this value to the bank and the bank checks its records to be sure that R has not been already used. If it has not, it deposits $100 into his account and updates its database that the unique value R has been redeemed.

Different public keys can be used for different denominations of currency so this system doesn't take appreciably longer for large transactions.

Note that if neither Alice nor Bob wishes the bank to know that they performed a transaction with each other, then it is hard for the bank to find out. However, in order to ensure this is the case many people need to be making transactions at the same time. Otherwise the bank can figure it out by the timing of the transactions, using traffic analysis.

ecash

Using cryptography, **ecash** was introduced by David Chaum as an anonymous electronic cash system. He used blind signatures to achieve unlinkability between withdrawal and spend transactions. Depending on the properties of the payment transactions, one distinguishes between on-line and off-line electronic cash. The first off-line e-cash system was proposed by Chaum and Naor. Like the first on-line method, it is based on RSA blind signatures.

In the United States, only one bank implemented ecash, the Mark Twain bank, and the system was dissolved in 1997 after the bank was purchased by Mercantile Bank, a large issuer of credit cards. Similar to credit cards, the system was free to purchasers, while merchants paid a transaction fee.

In Australia ecash was implemented by The St. Georges Bank, but the transactions were not free to purchasers. In June 1998, ecash became available through Credit Suisse in Switzerland. It was also available from Deutsche Bank in Germany, Bank Austria, Finland's Merita Bank/Eunet, Sweden's Posten, and Den norske Bank of Norway.

"ecash" was a trademark of DigiCash, which went bankrupt in 1998, and was sold to eCash Technologies, which was acquired by InfoSpace in 2002.

Direct corporate access

Direct Corporate Access (DCA) is part of the Faster Payments Service which provides a same day clearing payment service to UK member banks. **Direct Corporate Access** (DCA) will provide Banks' business customers with direct access to the Faster Payments Service (FPS) clearing service in a very similar way that Bacstel-IP provides access to BACS.

Direct Corporate Access only enables submission of files of payments, however as the central FPS processes payments individually, VocaLink the operators of DCA will split the files into individual instructions for processing through FPS.

It was developed by APACS on behalf of the FPS member banks and the infrastructure went live in March 2009. Barclays is expected to be the first Bank live for customer sponsorship in August 2009.

Albany Software was the first solution supplier to successfully process a payment through the Faster Payments Service via DCA, using Albany ePAY on Wednesday 22 July 2009.

Key Features

- DCA is available for file submission Monday to Friday 03.00 to 23.00.
- Sterling payments only
- Maximum individual payment value is £100,000
- Payments submitted in files via the Secure-IP channel
- Beneficiaries must use FPS addressable sort code
- DCA users must be sponsored by their bankers (however only Barclays offering sponsorship in the first instance).

Secure-IP

Secure-IP is a clone of the existing Bacstel-IP channel used for BACS. Files of payments are secured using a smart card or Hardware Security Module (HSM).

Files of payments submitted by Secure-IP will be disaggregated by VocaLink, the operators of DCA, and submitted into the Faster Payments Service. Disaggregation and acceptance may take up to 30 minutes and beneficiaries will receive access to the funds within 2 hours of acceptance.

The software used to access Secure-IP must be approved. This is an extension to the existing Bacs Approved Software Service (BASS). In March 2009 Albany Software and Bottomline Technologies Europe Ltd received approved status for their first DCA capable products. They were joined in May 2009 by Barron McCann. In 2010 they were joined by Experian , Direct Debit Ltd.

Bureaux

Bureau organisations can submit files of payments on behalf of other registered Service Users of Direct Corporate Access.

The Bureau needs to be sponsored by a DCA enabled Bank (initially only Barclays) and to use a Bureau/DCA version of the approved Bacs Approved Software Service (BASS) software.

The Bureau's sponsor bank issues PKI certificates for authorising files in the form of a smart card or Hardware Security Module (HSM). The same PKI certificates can be used to authorise Bacs file submissions via Bacstel-IP.

File submissions can only be made on behalf Service Users of a DCA enabled Bank (initially only Barclays).

Weaknesses

- Direct Corporate Access operates a limited window for payment submission whereas the underlying Faster Payments service operates 24 x 7.
- Bureau can only submit for their clients who are sponsored by Barclays.

Alternative Products

- Royal Bank of Scotland (including National Westminster and Coutts Banks) and HSBC offer Faster Payments via their electronic banking channels (Bankline and HSBC.Net).

Currency-counting machine

A **currency-counting machine** is a machine that counts money—either stacks of banknotes or loose collections of coins. Counters may be purely mechanical or use electronic components. The machines typically provide a total count of all money, or count off specific batch sizes for wrapping and storage.

Currency counters are commonly used in vending machines to determine what amount of money has been deposited by customers.

In some modern automated teller machines, currency counters allow for cash deposits without envelopes, since they can identify which bills have been inserted instead of just how many. The user is given the chance to review the automatic counter's idea of the quantity and kinds of the inserted banknotes before the deposit is complete.

A U.S. Navy Disbursing Clerk using a Cummins JetScan to count United States twenty-dollar bills.

Banknote counters

Basic banknote counters only provide a total number of notes in the supply hopper. More advanced counters can identify different bill denominations to provide a total currency value of mixed banknotes. Some banknote counters can also detect counterfeit bills either magnetically and/or using blacklight. Blacklight (UV) based detectors exploit the fact that in many countries, real banknotes have fluorescent symbols on them that only show under a black light. Also, the paper used for printing money does not contain any of the brightening agents which make commercially available papers fluoresce under black light. Both features make counterfeit notes both easier to detect and more difficult to successfully produce.

A stack of bills are placed in a compartment of the machine, and then one bill at the time is mechanically pulled through the machine. By counting the number of times a beam of light is interrupted, the machine can count the bills. By comparing an image of each bill to pattern recognition criteria, the machine can figure out how much genuine money was placed in the compartment.

Coin sorter

A coin sorter is a device which sorts a random collection of coins into separate bins for various denominations. Coin sorters are typically specific to the currency of certain countries due to different currencies often issuing similarly sized coins of different value. A sorter usually makes no attempt at counting, providing only collections of uncounted coins to be separately passed through a counter.

Coin counter

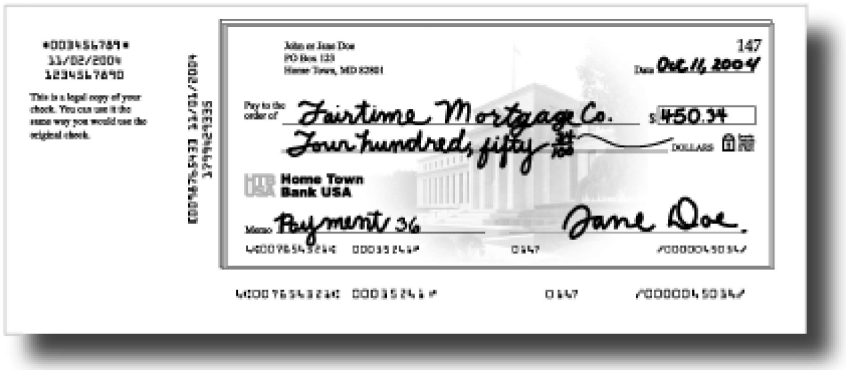
The phrase *coin counter* may refer to a device which both sorts and counts coins at the same time, or only counts presorted coins that are all the same size.

A typical counter of presorted coins uses a bowl with flat spinning disc at the bottom to distribute coins around the bowl perimeter. An opening in the edge of the bowl is only wide enough to accept one coin at a time. Coins either pass through a light-beam counter, or are pushed through a spring loaded cam that only accepts one coin at a time.

Cheque truncation

Cheque truncation is the conversion of physical cheque into electronic form for transmission to the paying bank. Cheque truncation eliminates cumbersome physical presentation of the cheque and saves time and processing costs.

Example of a US truncated cheque
(Substitute check)



Front view

Rear view

History

To settle a cheque it has to be presented to the drawee bank for payment. Originally this was done by taking the cheque in person to the drawee bank, however as cheque usage increased this became cumbersome and banks arranged between each other to meet each day at a central location to exchange cheques and settle the money. This became known as central clearing. Bank customers who received cheques could now deposit cheques at their own bank and their bank would arrange for the cheque to be returned to the drawee bank and any funds credited and debited from the appropriate accounts. If a cheque was dishonoured or bounced it would be physically returned to the original bank marked as such.

This process would take several days as physical cheques had to be transported to the central clearing location, from where they had to be transported to the payee bank. If the cheque bounced it would be transported back to the bank where the cheque was deposited. This is known as the clearing cycle.

Cheques had to be examined by hand at each stage and required a large amount of man power and handling.

In 1960 machine readable codes were added to the bottom of cheques in MICR format which allowed the clearing and sorting process to be automated. This helped to speedup the clearing process, however the law in most countries still required the physical cheques to be delivered back to the payee bank and so physical movement of the paper continued.

Starting in the mid 1990s some countries started to change their laws in relation to cheques to allow for truncation. Cheques would be imaged and digital representation of the cheque would be transmitted to the drawee bank at which point the original cheques could be destroyed. The MICR codes and cheque details are normally encoded as text in addition to the image. The bank where the cheque was deposited would typically do the truncation and this dramatically decreased the time it took to clear a cheque. In some cases large retailers that received large volumes of cheques were also able to carry out this truncation process.

Once the cheque has been turned into a digital document it can be processed through the banking system just like any other electronic payment.

Laws

Although technology needed to exist to be able to truncate a cheque, it was the laws related to cheques that were the main impediment to their introduction. New Zealand was one of the first countries to introduce truncation and imaging of cheques, when in 1995 they amended the cheque act 1960 to provide for the electronic presentment of cheques. A number of other countries followed over the next few years, but progress was mixed due to the decline in the use of cheques in favour of electronic payment systems. Some countries decided that the effort to implement truncation could not be justified for a declining payment method and instead phased out the use of cheques altogether.

In 2004, the Check 21 Act was implemented in the United States to authorize the recognition and acceptance of a "substitute check" after truncating the original paper check from the clearing process.

New laws needed to address ways to make sure that the digital image was a true and accurate copy of the original cheque as well as mechanism to make sure that the process could be audited to protect consumers.

It also needed to address the mechanism for dishonoured cheques as cheques could no longer be returned. A typical solution, as defined by Monetary Authority of Singapore for the Singapore cheque truncation system, was that a special 'Image Return Document' was created and sent back to bank that had truncated the cheque.

Operations and clearing

The security related to imaging and creating the electronic cheque needed to be defined and the clearing process adjusted to accommodate electronic cheques.

ATMC

An ATMC (ATM Controller) is a system used in financial institutions to route financial transactions between ATMs, core banking systems and other banks. An ATMC is sometimes referred to as an "EFTPOS Switch."

A message may enter an ATMC from an ATM, another ATMC or a third party. When receiving a message, the ATMC will examine the message, validate the PIN block if present, and then route the message according to the leading digits of the account number referenced.

This routing may be to a core banking system to check the available balances and to authorise the transaction, or to another bank's ATMC. For example, if a customer of Bank A used their card at an ATM belonging to Bank B, the message would be forwarded to Bank B's ATMC. The ATMC would examine the message, and based upon the account number determine that the appropriate ATMC to contact would be Bank A. It would then forward the message to Bank A's ATMC for authorisation.

An important aspect of an ATMC system is its ability to perform stand-in processing when core banking systems are unavailable. This allows a bank's ATMs to operate (usually with reduced limits) during periods of outage or maintenance on core banking systems. ATMCs make use of a SAF (Store And Forward) queue to ensure transactions are not lost.

An ATMC will usually have at least one attached Hardware Security Module to manage the keys relating to PIN validation and encryption of connections.

ATM SafetyPIN software

ATM SafetyPIN software is a software application that would allow users of automated teller machines (ATMs) to alert the police of a forced cash withdrawal by entering their personal identification number (PIN) in reverse order. The system was invented and patented by Illinois lawyer Joseph Zingher (U.S. Patent 5,731,575).

History

The concept of an alternative emergency PIN system, or duress code, for ATM systems has been around since at least July 30, 1986, when Representative Mario Biaggi, a former police officer, proposed it in the U.S. Congressional Record, pp. 18232 et seq. Biaggi then proposed House Resolution 785 in 1987 which would have had the FBI track the problem of express kidnappings and evaluate the idea of an emergency PIN system. HR785 died in committee without debate.

Zingher has not been successful in marketing his invention. Police in New York, New Jersey, Ohio, Illinois, and Kansas have supported the concept. Police support prompted the Illinois legislature to pass a law making it mandatory on all ATMs in Illinois. The law was changed shortly after it was passed by a "follow-on" bill that changed the meaning to the exact opposite of what they were seeking.

In 2006, an e-mail chain letter hoax circulated that claimed a reverse PIN duress code system is in place universally. *American Banker* reported on January 2, 2007 that no PIN-reversal duress code is used on any ATM as of that date. In July 2008 the hoax was still circulating in Australia with the text:

If you should ever be forced by a robber to withdraw money from an ATM, you can notify the police by entering your PIN in reverse. For example if your PIN is 1234 then you would put in 4321. The ATM recognizes that your PIN is backwards from the ATM card you placed in the machine. The machine will still give you the money you requested, but unknown to the robber, the police will be immediately dispatched to help you. This information was recently broadcasted *[sic]* on TV and it states that it is seldom used because people don't know it exists. Please pass this along to everyone possible. Australian Federal Police.

The same kind of e-mail chain letter hoax is still circulated in India and other parts of the world.

Were the system implemented, PINs that are reversible such as 5555 or 2112 then would be unavailable so that false alarms would not occur. Moreover, PINs that are semi-reversible such as 5255 or 1241, where the first and last numbers are the same, would be something to avoid as well so that accidental alarms would not be triggered by mistakenly switching the middle numbers.

Diebold, a manufacturer of ATMs, states on their website that no such emergency alerting system is currently in use. They cite an article in the St. Louis Post-Dispatch which claims bankers oppose the reverse-PIN system out of concerns that "ATM users might hesitate or fumble while trying to enter their PINs backwards under duress, possibly increasing the chances of violence." Diebold further states that they would be willing to support such technology if their customers (presumably banks) request it.

2009 bill

A bill making the reverse emergency PIN system mandatory on all ATMs in the state of Illinois was proposed on February 10, 2009. Subsection (i) is the new bill.

i) A terminal operated in this State must be designed and programmed so that when a consumer enters his or her personal identification number in reverse order, the terminal automatically sends an alarm to the local law enforcement agency having jurisdiction over the terminal location. The Commissioner shall promulgate rules necessary for the implementation of this subsection (i).

Los Angeles City Councilman Greig Smith announced his intention to make the ReversePIN system mandatory on all ATMs in the city.