NATIONAL IDENTITY CARDS

White Paper

JAN KREMER
CONSULTING SERVICES
# TABLE OF CONTENTS

1. INTRODUCTION .......................................................................................................................... 3

   1.1. DOCUMENT OUTLINE ................................................................................................................ 3

2. IDENTITY CARDS OVERVIEW ........................................................................................................ 4

   2.1. INTRODUCTION .......................................................................................................................... 4

   2.2. IDENTITY CARD IMPLEMENTATIONS ...................................................................................... 5

      2.2.1 Countries with compulsory identity cards .............................................................................. 5

      2.2.2 Countries with no identity cards ......................................................................................... 13

3. IDENTITY CARD PRINTING ............................................................................................................. 15

   3.1. USAGE OF PC CARD MATERIAL .............................................................................................. 15

      3.1.1 Introduction ........................................................................................................................... 15

      3.1.2 Unique Physical Characteristics ......................................................................................... 16

      3.1.3 Tamper Proof ......................................................................................................................... 16

   3.2. LASER ENGRAVING VERSUS D2T2 ....................................................................................... 18

      3.2.1 Print Technologies ................................................................................................................ 18

   3.3. SUMMARY ............................................................................................................................... 21

4. SECURITY & SMARTCARD BASED IDENTITY CARDS ....................................................................... 22

   4.1. INTRODUCTION ........................................................................................................................ 22

   4.2. HOW SECURE IS A SMARTCARD ........................................................................................... 24

      4.2.1 Solutions ............................................................................................................................... 25

      4.2.2 OS Security ............................................................................................................................ 26

      4.2.3 Software Security .................................................................................................................. 27

      4.2.4 Conclusions .......................................................................................................................... 27

   4.3. DATA ENCRYPTION ................................................................................................................... 28

   4.4. SMARTCARDS VERSUS SECURITY TOKENS ....................................................................... 29

      4.4.1 Token types and usage .......................................................................................................... 29

      4.4.2 Minimum requirement ......................................................................................................... 30

      4.4.3 Digital signature ................................................................................................................... 30

      4.4.4 Embodiments ......................................................................................................................... 30

      4.4.5 Disconnected tokens ........................................................................................................... 31

      4.4.6 Connected tokens ................................................................................................................ 31

      4.4.7 SmartCards .......................................................................................................................... 31

      4.4.8 Contactless tokens .............................................................................................................. 32

      4.4.9 Bluetooth tokens .................................................................................................................. 32

      4.4.10 GSM cellular phones ......................................................................................................... 33

      4.4.11 Single sign-on software tokens ......................................................................................... 33

      4.4.12 Related authentication technologies .................................................................................. 34

   4.5. SMARTCARDS WITH USB INTERFACE .............................................................................. 36

      4.5.1 ISO 7816-12 ......................................................................................................................... 36

      4.5.2 Solutions ............................................................................................................................... 37

      4.5.3 Cryptoflex Smart Card ......................................................................................................... 37
1. INTRODUCTION

This white paper provides an overview of Smartcard based Identity Cards technology.

For an overview of the Saudi Arabia Phase2 National Identity Card project and technology and the Malaysian Smartcard see my white papers “The Saudi Arabian Smartcard Summary” and “Malaysian Smartcard Summary”

1.1. Document Outline

Chapter 1 provides an introduction and outline of this document.

Chapter 2 provides an introduction to “what are National Identity Cards”, its usage and applications, countries with identity card implementations.

Chapter 3 provides an overview of “Card Printing Technologies”

Chapter 4 provides an overview Smartcard and Tokens security features
2. Identity Cards Overview

2.1. Introduction

Supporters advocate a national ID, not just for preventing terrorism, but for accessing government and healthcare services, conducting business transactions, and preventing underage drinking and smoking.

Detractors emphasize the privacy traps awaiting an implementation. They raise issues pertaining to data aggregation and matching, citing the historical “function creep” of the Social Security number and eliciting imagery of the ID as an enabler of persecution and discrimination based on religious or ethnic background.

An identity document can be used for many purposes. However, cost, complexity and resistance all rise in proportion to the number of functions supported by an ID. The United States is a large, populous country with great ethnic and religious diversity. Each proposed use for an ID must be scrutinized to determine its benefit and feasibility. Factors include costs, technological efficacy, and population dynamics and logistics, identity verification and issuance processes, and privacy implications.

To help fight terrorism, a national ID document must have the following characteristics:

- It must be issued to all who enter the country and remain for any period of time.
- The process for issuing the ID must include strenuous verification of identity prior to document issuance.
- The process must be distributed to serve the dispersed public and cover the vast number of entry points.
- The process must be free from corruption.
- The ID must uniquely identify the individual.
- All ID checkpoints must have access to information resources with the capability to link the identity to terrorist activity or potential terrorist activity.

Each of these characteristics faces tremendous pressure stemming from the country’s geographic vastness, the size of its population, its diversity and a Constitution that makes civil liberties paramount.
2.2. Identity Card Implementations

2.2.1 Countries with compulsory identity cards

According to Privacy International, as of 1996, around 100 countries had compulsory identity cards. They also stated that "virtually no common law country has a card."

The term "compulsory" may have different meanings and implications in different countries. The compulsory character may apply only after a certain age. Often, a ticket can be given for being found without one's identification document, or in some cases a person may even be detained until the identity is ascertained. In practice, random controls are rare, except in police states.

- Albania: Albanian Identity Card \textit{Letërnjoftimi}, is an electronic biometric ID card, compulsory upon 16 years old and costs 12000lek (€10).

- Argentina: Documento Nacional de Identidad (DNI) (Spanish Wikipedia). Issued at birth. Updated at 8 and 16 years old. Small booklet, dark green cardboard cover. The first page states the name, date and place of birth, along with a picture and right thumb print. It's a hand written form, and the newer models have an adhesive laminate for the first page. Next pages show address changes, wish to donate organs, military service, and vote log. Half of the pages have the DNI (a unique number), perforated through the first half of the book. Prior to DNI was the \textit{Libreta Civica} ("Civic booklet"), for women, and the \textit{Libreta de Enrolamiento} ("Enrollment Booklet"), for men. A few years ago there was a big scandal with the electronic DNIs that were going to be manufactured by Siemens, and it was decided that no private corporation could control the issuing of national identity. The federal police, also the same authority who can issue Argentinian passports, also issues an identity card called Cédula de Identidad that is valid sometimes instead of the DNI, which many people prefer to carry because after the loss of DNI there is a long process (caused only by bureaucratic reasons) in which the person is limited in some situations which require the DNI. Random controls cannot be made without a judge's order, except in situations such as military border checkpoints.

- Belarus: Passport (Belarusian: Пашпарт). Compulsory at 16. Reissued at 25, 45 and 100. Can be used to travel to other countries. Could be issued before 16 for travelling purposes.

- Belgium: See Belgian ID Card and State Registry (in Dutch, French and German). The card is first issued at age 12, compulsory by 15. Since the beginning of 2005 the eID (electronic IDentity-card) has been issued to Belgian citizens who apply for a new identity card. Apart from being a form of identification, the card also is used for authentication purposes. Future usages include using the eID as a library card, keycard for restricted areas or chatrooms and the digital signing of documents. In 2009 all Belgians now have an eID card.. The identity cards for Belgians living abroad are not electronic cards like those issued in Belgium. They
are, however, equally valid and are accepted and used in the same way as the electronic identity card.

- Bolivia: Cédula de identidad, is compulsory at 18. Rarely required by police.
- Bosnia and Herzegovina: "Lična karta / Osobna iskaznica / Лична Карта", compulsory at 16.
- Brazil: Carteira de identidade. Compulsory to be issued and carried since the age of 18 (though it can be substituted by a series of equivalent documents, see below). It is usually issued, for civilians, by each state's Public Safety Secretary, but other state departments — including the Armed Forces, the Police and some professional councils — can issue alternate identity cards too. There is a national standard, but each state can include minor differences (usually numbering scheme, font, printed seal and background pattern. The front has a picture (with an electronic stamp on it), right thumb print and signature (for illiterate people the phrase "não assina" — cannot sign — is printed in its place). The verse has the unique number (RG, registro geral), expedition date, full name of the person, name of the parents, place (town, state) and date of birth, CPF number and other optional information. It is green and plastified, officially 102 × 68 mm,[4] but lamination tends to make it slightly larger than the ISO/IEC 7810 ID-2 standard of 105 × 74 mm, resulting in a tight fit in most wallets. Only recently the driver's licence received the same legal status of an identity card in Brazil. There are also a few other documents, such as cards issued by the national councils of some professions (doctors, accountants, dentists, engineers, lawyers etc.), which are considered equivalent to the national identity card for most purposes.

- Bulgaria: Bulgarian identity card лична карта in Cyrillic alphabet (or "lichna karta" in Latin transliteration) is first issued and is compulsory after turning the age of 14. The new Bulgarian ID cards were introduced in 1999. They follow the general pattern in the EU and replaced the old, Soviet-style "internal passports", also known as "green passports". During the socialism period (1945–1989), to receive an "international passport", especially one allowing traveling to a Western country, was considered an achievement. Not all Bulgarian citizens had the right to travel abroad, and those who travelled outside the Soviet bloc underwent strict investigation for possible links with political enemies of the regime. Since January 1, 2007, the Bulgarian identity card can be used to travel within the European Union. Since 29 March 2010 new Bulgarian identity cards were introduced with embedded chip with personal data.

- Chile: Cédula de identidad. First issued at age 2 or 3, it is compulsory at 18.
- People's Republic of China: First issued at school age, the Resident Identity Card (PRC) (Chinese: 居民身份证 Pinyin: Jūmín Shēnfènzhèng) becomes compulsory at 16.
- Republic of China (Taiwan): Republic of China National Identification Card (Guomin Shenfenzheng/國民身份證).
Colombia: *Tarjeta de identidad*. First issued at age 2 or 3, then it's changed at 18 for another identity card called *Cedula de Ciudadania*. It is only renewed afterwards if stolen or lost.

Croatia: The *Croatian identity card* is compulsory at 16.

Cuba: *Carné de identidad*

Cyprus: All Residents aged 12 and up are required to carry an official ID card (http://moi.gov.cy/content.php?subid=180)

Czech Republic: *Občanský průkaz*, compulsory at 15.

Egypt: Personality Verification Card (بطاقة تحقيق الشخصية) is compulsory to issue at the age of 16. Issued by the Civil Registry Office which is subordinate to the Ministry of Interior. Not carrying the ID card is only penalized by fine not exceeding 200 EGP.

Estonia: See id.ee (in Estonian), id.ee (in English)

Germany: *Personalausweis* (German Wikipedia): It is compulsory for all German citizens age 16 or older to possess either a "Personalausweis" (identity card) or a passport, but not to carry it. While police officers and some other officials have a right to demand to see one of those documents, the law does not state that one is obliged to submit the document at that very moment. Fines may only be applied if an identity card or passport is not possessed at all, if the document is expired or if one explicitly refuses to show ID to the police. If one is unable to produce an ID card or passport (or any other form of credible identification) during a police control, one can (in theory) be brought to the next police post and detained for max. 12 hours, or until positive identification is possible. However, this measure is only applied if the police have reasonable grounds to believe the person detained has committed an offense. As driver's licences are not legally accepted forms of identification in Germany, most persons actually carry their "Personalausweis" with them.

Greece: In Greece, the biggest change in Identity Documents Law happened in 2000, when some fields of the Police Identity Card (as Greeks call it) were rejected. These fields included religion, addresses, biometric characteristics and fingerprint. Oppositely, some fields were added. These are Latin transliterations of name and surname, blood type and Rhesus of the owner. Under this law, all Greeks over 12 years old must go to a police office to ask for an Identity Card. In Greece, there are many everyday things you cannot do without an ID. In fact, according to an older law, the Police ID is the only legal identity document and no one has a right to ask for more identity documents. Since the 1980s all legal services in Greece must be done with this ID. Also, you can travel within the EU with a Greek National ID card. Carrying the ID is not compulsory, however during routine police checks, if you are found without an ID, the police officer may take you to the nearest police station for further investigation.

Hong Kong: See main article *Hong Kong Identity Card*. Identity cards have been used since 1949, and been compulsory since 1980. Children are required to obtain
their first identity card at age 11, and must change to an adult identity card at age 18.

- **Hungary**: It is compulsory to possess an ID or passport from the age of 14. A driving license can be also used for identification from the age of 17. Private entities however, are legally required to accept passport or driver's license for proof, but often do not accept them, only the ID card, thus in effect almost all citizens have the ID card. Police has the legal power to stop people on streets at random and ask for ID paper only if they have any proof that the person was involved in a crime, or is a witness. If the person has no proof for identification he/she can be detained for maximum 24 hours. It is a common misconception in Hungary that the Police can ask for your ID at any time, but since 1990 this is not the case.

- **Indonesia**: *Kartu Tanda Penduduk* for Indonesian citizens and the KITAP's or permanent residents card holder. This card is compulsory for people at age 17 or has been married.

- **Iran**: The *Iranian national identity card* is compulsory for permanent residents, age 15 and over.

- **Israel**: The *Teudat Zehut* is first issued at age 16 and is compulsory by 18.

- **Jordan**: First issued at age 16 and is compulsory by 18.

- **Kenya**: Issued at age 18 and is compulsory. Carrying the ID is not compulsory; however it's easier to get through police checks if you have one.

- **Lithuania**: *Asmens tapatybės kortelė*, compulsory at 16.

- **Luxembourg**: First issued at age 15 and only issued to Luxembourg citizens, who are required by law to carry it at all times.

- **Latvia**: An identity card or passport is the mandatory personal identification document for a citizen of Latvia or a non-citizen who lives in Latvia and has reached 15 years of age. However, ID cards are still not being issued; the ID card project is a concept, even though the legislative base is present.

- **Madagascar**: *Kara-panondrom-pirenen'ny teratany malagasy* (*Carte nationale d'identité de citoyen malagasy*). Possession is compulsory for Malagasy citizens from age 18 (by decree 78-277, 1978-10-03).

- **Malaysia**: *MyKad*. Issued at age 12, it is updated at 18.

- **Malta**: *Karta ta’l-Identità* Issued at 14, updated at 16, compulsory at 18.

- **Morocco**: The national identity card is the ID of the citizens of Morocco (in Arabic: *بطاقة التعريف الوطنية*). This is an official document which allows any citizen to prove his identity and therefore it is valid, his Moroccan nationality. It is compulsory for all citizens aged over 18 years, but it can be obtained from the age of 16. A new version of the card is now out, it has the form of a credit card. The Directorate General of National Security (DSMS) of Morocco announced Sunday,
March 30, 2008 it will proceed on 1 April 2008 to issue new national identity card Electronic (NIEC). The current national maps will be gradually replaced in four years. The NIEC is biometric and provides citizens of the presentation of life certificate, residence certificate, extract of birth and citizenship certificates.

- **Montenegro**: The *Montenegrin identity card* (Lična karta/Лична карта) is compulsory at the age of 16. It is issued only to Montenegrin citizens with permanent residence in Montenegro. While it is the most often used official identification document, three other hold the same status — Passport, Driver's license and Refugee ID card.

- **Mozambique**: *Bilhete de identidade*

- **Netherlands**: *Identiteitsbewijs* (Dutch Wikipedia): Since 1 January 2005 identification is compulsory at 14. Legal proof of identity is a Dutch or other European identity card or a passport. A Dutch driving license is valid while other driving licenses are not valid for identification. It is not compulsory to carry a proof of identity, but it is compulsory to show it to the authorities when they ask such under certain circumstances. Such circumstances include suspicious behavior, committing any offense, or if a person is interviewed as a witness of a crime. Identity checks at events where the public order may be in danger are also allowed. Otherwise random identity checks by the police are not allowed in principle but can happen in certain areas such as a train station or doubtful areas i.e. red-light district and a fine for not showing proof of identity may be successfully challenged in such cases. The fine for not being able to show proof of identity when legally required is € 50. Proof of identity is also required when opening a bank account and when entering an employment contract.

- **Panama**: Cedula de Identidad. Required at 18. Panamanian citizens must carry their Cedula at all times.

- **Pakistan**: Computerized National Identity Card (CNIC). First made at the age of 18, not compulsory to carry all the time. The card is mandatory for opening bank accounts, for passport and almost all substantial monetary transactions from car, land to high value assets.

- **Peru**: Documento Nacional de Identidad.

- **Poland**: Polish National Identity Card The card is compulsory at 18. Those who do not comply with the relevant law are denied passports.¹

- **Portugal**: *Bilhete de identidade*: The card is compulsory at 10, but can be issued before if needed.

- **Romania**: The *Carte de identitate* is compulsory at 14.

- **Russia**: *Internal passport* is compulsory at 14 (but there is no penalty for not having one until the age of 16) and reissued with a new photograph at 20, 45. Although there are no laws in Russia requiring to carry a proof of identity, in certain places, such as Moscow, it is sensible to carry a passport at all times as
lack of an ID during ad-hoc police checks is sufficient grounds for detention. A passport is also required for travel by long-range trains and airlines. There are a couple of operations that require an internal passport, (e.g. all notarial operations, land to high value assets).


- **Serbia**: The *Lična karta* (Лична карта) is compulsory at the age of 16, but it can be obtained when a person turns 10. It is issued only to Serbian citizens with permanent residence in Serbia. While it is the most often used official identification document, three other hold the same status — Passport, Driver's license and Refugee ID card.

- **Singapore**: It is compulsory for all citizens and permanent residents to apply for the *National Registration Identity Card* from age 15 onwards, and to re-register their cards for a replacement at age 30. It is not compulsory for bearers to hold the card at all times, nor are they compelled by law to show their cards to police officers conducting regular screening while on patrol, for instance. Failure to show any form of identification, however, may allow the police to detain suspicious individuals until relevant identification may be produced subsequently either in person or by proxy. The NRIC is also a required document for some government procedures, commercial transactions such as the opening of a bank account, or to gain entry to premises by surrendering or exchanging for an entry pass. Failure to produce the card may result in denied access to these premises or attainment of goods and services. In contrast to other countries, the NRIC also states the bearers' race. [Immigration & Checkpoints Authority](https://www.ica.gov.sg)

- **Slovakia**: *Občiansky preukaz* (Citizens card) is compulsory at the age of 15. It serves the purpose of general identification towards the authorities. It features a photograph, date of birth and the address. Every card has a unique number.

- **Slovenia**: The *Osebna izkaznica* is compulsory for citizens of Slovenia who have a permanent residence in Slovenia, are at least 18 years old, and do not have a passport. It can be issued to citizens under 18 on request by their parent or legal guardian.

- **South Africa**: An Identity Document (ID) is issued at age 16 to all citizens; and permanent residents. Although passports and driver's licenses are also acceptable forms of identification, banks only accept IDs. Your ID has a barcode, a photo, and your unique ID number. Information (including age and gender but excluding race) is referenced under your ID number: accounts, criminal record, voting history, driver's license etc. You need an ID in order to apply for a passport, bank account, driver's license or tertiary studies, as well as to register to vote. In most cases employers will also request a photocopy of your ID in order to process your appointment. Your voting history as well as any firearm licenses is documented in your ID booklet. As one's ID may be required for some of the functions listed
above, some SA permanent residents, may elect to keep their ID document on
their person.

- **South Korea**: Korean citizens are issued a national ID card when reaching
  adulthood (typically when he/she reaches the age of 19 under East Asian age
  reckoning). The first six numbers indicate the citizen's date of birth, while the last
  seven numbers includes information such as where the birth was registered. This
  number is used by Korean citizens for all forms of record-keeping, including
  online.

- **Spain**: The Documento Nacional de Identidad (DNI) (Spanish Wikipedia) is
  compulsory at 14, can be issued before if necessary (to travel to other European
  countries, for example). By law, it has to be carried at all times, and it is routinely
  used for identification, and it is often photocopied by private and public bureaus.
  Credit-card purchases cannot be made without showing this ID. Since 2006, it is
  being replaced by the Electronic DNI.

- **Sri Lanka**: All citizens over the age of 16 needs to apply for a National Identity
  Card (NIC). Each NIC has a unique 10 digit number, in the format 000000000A
  (where 0 is a digit and A is a letter). The first two digits of the number are your
  year of birth (e.g.: 88xxxxxxxx for someone born in 1988). The final letter is
  generally a 'V' or 'X'. An NIC number is required to apply for a passport (over
  16), driving license (over 18) and to vote (over 18). In addition, all citizens are
  required to carry their NIC on them at all times as proof of identity, given the
  security situation in the country. NICs are not issued to non-citizens, but they too
  are required to carry some form of photo identification (such as a photocopy of
  their passport or foreign driving license) at all times.

- **Thailand**: National ID card is compulsory for all citizens at the age of 15.

- **Turkey**: The Nüfus Cüzdanı is compulsory right after birth without photograph, at
  the age of 15 a photograph must be sticked on. It has to be carried at all times and
  it is often photocopied by bureaus, banks, etc.

- **Ukraine**: Internal Ukrainian passport is compulsory (to possess but not to carry) at
  age of 16.

- **Venezuela**: In Venezuela it is called Cédula de Identidad, it is mandatory at the
  age of 10 and is renewed every 10 years

- **Vietnam**: Known as giấy chứng minh nhân dân (“people's proof document”), it is
  compulsory for all Vietnamese citizens over 14.
1.1.1 Countries with non-compulsory identity cards

These are countries which have national identity cards, but they are not compulsory by law. Some kind of identity card is usually needed anyway for e.g. bank transactions.

- **Austria**
- **Canada**: Citizenship and Immigration Canada (CIC) issues the Canada Permanent Resident Card to permanent residents of Canada. A Citizenship Certificate can be given to any citizen that choose to apply, but is automatically issued to naturalized Canadian citizens.
- **Finland**: National identity cards exist, but commonly people use their driving licenses or national social security cards as ID. When making purchases with a credit card, ID card will usually be asked for.
- **France** (see extended discussion below)
- **Iceland**: The National Register of Persons ("Þjóðskrá") issues national identity cards ("Nafnskírteini") to all teenagers in the year they become 14 years old. People in Iceland are required to present identification if asked by police, but it doesn't have to be this particular card as driving licenses and various other ID cards are considered valid.
- **Italy**: Carta d'Identità (Italian Wikipedia) May be issued to anyone (either Italian citizen or foreigner) who resides in Italy, and to Italian citizens living abroad. It is issued after the 15th birthday. It's not compulsory to have it or to carry it along, unless expressed ordered by public security authorities.
- **Mexico**: The Federal Electorate Institute ("Insituto Federal Electoral") issues a Voting card (Credencial para votar) for Mexican citizens when they become 18 years old. The card is compulsory in order to participate in Federal level elections, and is the defacto ID for most legal transits.
- **Sweden** (see extended information below)
- **Switzerland**
- In the European Union, a national identity card complying to certain standards can be used by European citizens as a travel document in place of a passport.
- In the United States, the Passport card is issued to its citizens upon request. Although it’s main purpose is for land and sea travel within North America, under the REAL ID Act, the passport card will also be accepted for domestic air travel.
2.2.2 Countries with no identity cards

- **Australia**: In 1985, there was a failed proposal to create an **Australia Card**. In 2006 the Australian Government announced the introduction a non-compulsory **Access Card** that would act as a gateway to services administered by **The Department of Human Services**. This project, however, was terminated in November 2007. Class A identification documents in most Australian states include Driver’s License (issued by the state government), 18+ Card (issued by the state government), Australian Passport (issued by the Federal government), foreign passport, or Residency/Citizenship documents (issued by the Federal government).

- **Denmark**: No national identity card, but other identity cards exist which are needed e.g. in the bank if not using a passport.

- **India** (*India* is currently piloting an ID card system, see **Multipurpose National Identity Card (India)**)

- **Ireland**: There is no requirement for Irish or UK citizens to identify themselves in Ireland. Citizens who are born in Ireland or the UK are allowed to travel within the **Common Travel Area** without producing a passport, but should be able to provide photographic identification on demand. All others are required to show a passport, or National Identity card in the case of **EEA** nationals. There is a voluntary **Aoischéarta Náisiúnta / National Age Card** available to residents over 18, showing name, date of birth, sex, photograph, and unique card number. It is aimed at young people to prove they are legally allowed to buy alcohol, it is a "proof of age card" not an "identity card"

- **Japan**: There are no national identity cards for Japanese citizens, but all resident foreigners must get a Certificate of Alien Registration (外国人登録証明書 **Gaikokujin Tōroku Shōmeisho**). Non-Japanese citizens must be able to show that they have the right to stay in Japan (using a Certificate of Alien Registration if the person entered the country more than 90 days ago; or either a Certificate of Alien Registration or a passport with a valid landing permission if the person entered the country up to 90 days ago). Driving licenses, National Health Insurance Cards (国民健康保険証 **Kokumin Kenkō Hoken Shō**), Certificates of Alien Registration and passports containing a registration for a Certificate for Alien Registration are used as ID for most purposes. Note that the insurance card doesn't contain any photo of the person in question.

- **New Zealand**: There are no national identity cards, however the New Zealand driver license is the de facto national identity card used as a legal document to certify a person's identity or age when purchasing alcohol, authorizing bank transactions and at other situations when identification is required. They do not show citizenship status and therefore a passport, or birth certificate in conjunction with a driver license must be presented when required to show citizenship.

- **Norway**: No national identity card, but other identity cards exist which are needed e.g. in the bank if not using a passport.

- **Philippines**: In an effort to hasten application for government services, the government is now issuing the Unified Multi-Purpose ID (UMID) as the single
identity card for the four main government agencies namely, the Social Security System (SSS), Government Service Insurance System (GSIS), Philippine Health Insurance Corporation (PhilHealth) and the Pag-IBIG Fund.

- **United Kingdom**: Though introduction of voluntary cards began in 2009, legislation was introduced to cancel the scheme in 2010. See main article: British national identity card.

As noted above, certain countries do not have national ID cards, but have other official documents that play the same role in practice (e.g. driver's license for the United States). While a country may not make it de jure compulsory to own or carry an identity document, it may be de facto strongly recommended to do so in order to facilitate certain procedures.
3. **Identity Card Printing**

3.1. **Usage of PC Card Material**

3.1.1 **Introduction**

What sets polycarbonate apart from other materials is the fact that it is non-delaminable. When used in pure form and not mixed with other plastics, the different layers of polycarbonate that make up the identity document fuse together to form a single, solid card body. All security features, including irreversible laser-etched personalization information, are safely located within and protected by the 100% polycarbonate card body.

In addition to traditional security features, such as security printing, screen-printing with optically variable inks (OVIs), holograms and diffractive optically variable image devices (DOVIDs), polycarbonate is unique in supporting highly fraud-resistant level-one security features; that is to say those visible to the naked eye. These features, which are easily authenticated by the relevant authorities, include changeable laser images (CLIs), clear windows and irreversible laser-etched information personalization.

Moreover, polycarbonate’s durability allows for the production of long-lifespan identity documents, which can last for over ten years, and it is available in a choice of interfaces including chipless, contact, contactless and dual interfaces (whether with one shared or two distinct microprocessors).

Polycarbonate has won the trust of governments around the world and is used in the production of at least 14 national identity card programs, ten national passport programs and 13 national driving license programs. In addition, the majority of national electronic identity cards deployed worldwide are made from Polycarbonate.
3.1.2 Unique Physical Characteristics

Polycarbonate is a type of thermoplastic with excellent molding and thermoforming properties. It is exceptionally robust and is used to make bulletproof glass. Its optical properties are excellent as its percentage light transmission stands at 90%, higher than that for many traditional glasses. Polycarbonate is employed for a variety of purposes, including the manufacture of indestructible eyeglasses and protecting the surfaces of DVDs. In terms of identity documents, polycarbonate makes it possible to incorporate a significant number of additional security features, including CLIs; clear-windows-transparent windows inside the card body similar in effect to watermarks on banknotes; and positive and negative embossing, which are used for tactile recognition.

One property unique to polycarbonate is that it is non-delaminable. It is impossible to separate layers of polycarbonate that have been fused together using temperature and pressure, rather than glue. During lamination, the constituent molecules in polycarbonate layers fuse together to form a homogeneous mass. The result is a single, solid card body. In identity documents, this solid card body serves to trap, and thus protect, all security features printed or positioned on its various constituent layers. It should, however, be noted that only documents made entirely from polycarbonate are non-delaminable. Hybrid documents – those made from a mixture of polycarbonate and other plastics – do not share this property.

Polycarbonate documents contain special layers of carbon-enriched polycarbonate. When these layers are exposed to a laser beam, the carbon reacts to form a permanent black mark, trapped inside the material. Even at temperatures as low as -100°C or as high as +135°C, polycarbonate conserves its physical and optical properties, making it ideally suited to the normal conditions of use of identity Documents.

3.1.3 Tamper Proof

A polycarbonate identity document, such as an ID card, is created by fusing together multiple layers of polycarbonate in a glue-free process, using temperature and pressure.

Each layer has a specific role:

- The central layer is generally opaque and white. It can house an antenna to enable contactless reading of an electronic chip.
- Intermediate layers carry the security imprint and specific security features, such as holograms and screen-printed OVIs.
- A carbon-enriched intermediate layer supports laser-personalization.
- The outer layer bears the tactile embossing and the CLI.
A polycarbonate electronic identity card can be contact, contactless or dual-interface – functioning in both contact and contactless mode. Dual-interface cards may have a single shared microprocessor, or one separate microprocessor for each interface. The security and durability of the polycarbonate card body are not dependent on the electronic system.

All security imprints and security features are embedded and protected within the solid, polycarbonate card body, formed by the fusion of layers. Any attempt to tamper with the document will leave clearly visible marks.

Polycarbonate identity documents support all traditional security features, including guilloches, rainbow printing, screen-printing, OVIs, transparent and metallic holograms, ultraviolet inks and taggants.

The first differentiator for polycarbonate is that all these security features are protected inside a single solid block. The second difference is that polycarbonate allows exclusive, difficult to counterfeit level-one security features.

Polycarbonate identity documents are secure and reliable. Their quality resides in the exceptional optical and physical properties of polycarbonate. They are non-delaminable, and their personalization by laser engraving is irreversible. They incorporate easy-to-authenticate level-one security features.

The security industry is constantly engaged in research and development activities aimed at developing new and innovative security features using polycarbonate. Most new-generation identity documents, particularly driving licenses and electronic national identity cards, now use Polycarbonate.
3.2. Laser Engraving Versus D2T2

3.2.1 Print Technologies

3.2.1.1 Laser Engraving

Performing laser engraving on a polycarbonate identity document results in the formation of a permanent black mark. This mark is precise and non-reversible.

This technique is used to personalize a blank document with the holder’s information using text and a photograph of the holder.

The letters and figures are deep black, and may have a distinctive texture. The photo is black and white, with shades of grey and high contrast.

Personalized engravings are made within the solid polycarbonate card body frame and are therefore irreversible.

The Laser Sealer process combines guilloches and a photograph in such a way that any attempt to perform additional laser engravings subsequent to the official personalization of the document is easily detected.

This technology has been used in Europe for more than a decade for high security documents.
3.2.1.2 **D2T2**

**Dye Sublimation** (sometimes called dye diffusion thermal transfer – or D2T2) uses heat to transfer dyes to a substrate. Used for high quality color printing, the process creates continuous tone colors by varying the amount of heat applied. Typically a 3- or 4-color ribbon (cyan, magenta, yellow and black) is passed under a thermal print-head and heat is applied to deposit dye. Ribbon dyes can be applied:

a. **Direct** - printed directly to a card surface; or,

b. **Retransfer** - printed to the backside of a clear retransfer ribbon which is then fused to the card surface. Frequently used to personalize smart cards which may have irregular surfaces.

![3-Panl Ribbon Diagram]

A disadvantage of this technology is the supply cost for the multi-panel ribbon. Another limitation is that the dyes need to be protected from degradation that may result from chemical or ultraviolet radiation attack. The required protection called lamination is another added cost factor as well as an issue as to the life cycle duration (delamination) of the card.

3.2.1.3 **Black & White Photo**

Laser Engraving text and Photo Images is limited to Black & White. A combination of Laser Engraving and D2T2 (for a color photo) is technically feasible but extremely expensive and less secure. It would require additional D2T2 printing units, consumables, lamination (protection of the color photo) and is not used in any of the international implementations of Electronic Identification Documents (e-ID) in the World. Below is a list of e-ID implementations (not complete) that include Laser Engraving on Polycarbonate with Black & White Photo’s. In addition it should be
noted that almost all e-Passport implementations include Laser Engraving with Black & White Photo.

List of e-ID implementations with Laser Engraving and B&W photo:

- Belgium
- India
- Hong Kong
- Finland
- Sweden
- Lithuania
- Portugal
- Netherlands
- Switzerland
- Austria
- Estonia
- Macao
- Singapore
- Albania
- Bosnia
- Croatia
- Bulgaria
- Hungary
- Poland
- Slovakia
- United Kingdom (residents)

Total 21 countries with Laser Engraving AND Black and White Photo
3.3. Summary

Of all the countries in Asia and Europe having a National Identity Card (total 26) 21 countries use Laser Engraving with Black and White Photo’s. Saudi Arabia is the only GCC Country that has implemented their National Identity Card based on this latest and most secure technology.

The vast majority of countries having issued secure national identity cards and countries planning to issue one have decided on the most secure manner of personalization of data on this ID card by using laser engraving for text and photo. Color photos can only be achieved with current technology using D2T2 and this document using international white paper data provided by international experts clearly states that D2T2 is not feasible solution for Identity cards being National Id or Drivers License.

D2T2 personalization is not appropriate for national identification or driving licenses. It's possible to remove and replace personalization data without affecting the background design of the card how can this ever be used for documents of value like identification documents? Additionally it is well known that PVC card material simply does not last for the length of time that is needed in National Identity schemes.

Although future laser engraving schemes will support color text and photo’s it will take time before this new technology will have an acceptable cost-benefits solution for high quantity ID card requirements.

With the current technology available the usage of Polycarbonate and Laser Engraving provides by far the most secure and cost effective solution which is supported by the worldwide technology providers for cards, card printing and card encoding.
4. Security & Smartcard based Identity Cards

4.1. Introduction

Unlike alternative, less secure ID card technologies (such as magnetic stripe, printed bar code, optical, or RFID), smart card technology supports numerous unique features that can strengthen the security and privacy of any ID system.

**Strong Identity Authentication.** One essential characteristic of a secure ID system is the ability to link the individual possessing an identity document securely to the document, thus providing strong authentication of the individual’s identity. Smart card technology supports PINs, biometric factors, and visual identity verification. For example, the REAL ID Act requires that each person applying for a driver’s license or identification card be subjected to a facial image capture. This facial biometric factor can be stored directly in the secure chip in the smart card and used to verify that the individual presenting the card is the individual to whom the card was issued.

Other biometric factors (for example, fingerprints), the biometric that is captured when the cardholder applies for the card (or is enrolled in the identification system) can be stored securely on the card. It can then be matched either on or off the card (in a reader or against a database) to verify the cardholder’s identity. In addition, states can establish databases to achieve the goal of “one credential, one record, and one identity.”

**Strong Credential Security.** Protecting the privacy, authenticity, and integrity of the data encoded on an ID is a primary requirement for a secure ID card. Smart cards support the encryption of sensitive data, both on the credential and during communications with an external reader. Digital signatures can be used to ensure data integrity and authenticate both the card and the credentials on the card, with multiple signatures required if different authorities create the data. To ensure privacy, applications and data must be designed to prevent information sharing.

**Strong Card Security.** When compared to other tamper-resistant ID cards, smart cards represent the best balance between security and cost. When used with technologies such as public key cryptography and biometrics, smart cards are almost impossible to duplicate or forge. Data stored in the chip cannot be modified without proper authorization (a password, biometric template, or cryptographic access key). Smart cards also help deter counterfeiting and thwart tampering. Smart cards include a wide variety of hardware and software capabilities that can be used to detect and react to tampering attempts and counter possible attacks. When smart ID cards will
also be used for manual identity verification, visual security features can be added to a smart card body.

Adding a smart card chip to a Real ID would exponentially increase the difficulty of making a fraudulent ID card. The vulnerabilities of printed plastic ID cards are well known—fake state IDs are readily available for purchase over the Internet or in rogue ID card facilities. Smart cards deter forgers and can ensure that only the person to whom the card is issued will be able to verify themselves when the card is presented. No other technology can offer such secure, trusted, and cost-effective identification capabilities.

* Strong Support for Privacy.* the use of smart cards strengthens the ability of a system to protect individual privacy. Unlike other identification technologies, smart cards can implement a personal firewall for an individual’s data, releasing only the information required and only when it is required. The card’s unique ability to verify the authority of the information requestor and the card’s strong security at both the card and data level make smart cards an excellent guardian of a cardholder’s personal information. Unlike other forms of identification (such as a printed driver’s license), a smart card does not reveal all of an individual’s personal information (including potentially irrelevant information) when it is presented. Information embedded on the chip can be protected so that it cannot be surreptitiously scanned or skimmed, or otherwise obtained without the knowledge of the user. Personal information stored on the smart card can be accessed only through user-presented PINs and passwords or by biometric matches at the place of use. By allowing authorized, authenticated access to only the information required for a transaction, a smart card-based ID system can protect an individual’s privacy while ensuring that the individual is properly identified.

**Flexibility as a Secure Multi-Use Credential.** The driver’s license is currently a multi-use credential. It not only indicates that the cardholder has driving privileges, it also serves as the default credential for establishing that the cardholder can board an aircraft, engage in age-related retail purchases, establish banking relationships, complete retail point-of-sale transactions, and apply for employment. Smart card technology can support these current uses along with any additional applications that enhance citizen convenience and/or government service efficiency. For example, smart cards provide the unique capability to easily combine identification and authentication in both the physical and digital worlds. This capability can generate significant savings for states. A smart card-based driver’s license or ID card could not only indicate privileges and allow physical access to services, it could also allow individuals to file taxes, request official papers (e.g., birth certificates) online, or access secure networks. Multiple applications (with their required data elements) can be stored securely on the smart ID card at issuance or added after the card is issued, allowing functionality to be added over the life of the driver’s license or ID card.
Standards Based Technology. Smart card technology is based on mature international standards (ISO/IEC 7816 for contact smart cards and ISO/IEC 14443 for contactless smart cards). Cards complying with standards are developed commercially and have an established market presence. Multiple vendors can supply the standards-based components necessary to implement a smart card-based ID system, providing buyers with interoperable equipment and technology at competitive prices.

Cost Effective and Flexible Offline Verification. In addition to the privacy and security benefits afforded by smart cards, the technology also delivers features that support cost-effective offline verification and efficient use of the ID card once the card has been issued.

Verification of a cardholder’s identity is often required at multiple locations or at points that do not have online connections. A smart card-based ID system can be deployed cost-effectively at multiple locations by using small, secure, and low-cost portable readers that take advantage of the smart card’s ability to provide offline identity verification. For example, verifying a cardholder’s identity with biometrics would not require access to an online database: the smart card can securely hold the necessary biometric identifier, with the secure chip on the card comparing it to the live biometric. The credential on a card can be authenticated by a reader using digital signatures contained on the ID card, making it a trusted credential-online or off.

4.2. How Secure is a Smartcard

All data and passwords on a card are stored in the EEPROM and can be erased or modified by an unusual voltage supply. Therefore some security processors implemented sensors for environmental changes. However, since it is difficult to find the right level of sensitivity and there is a voltage fluctuation when the power is supplied to the card, this method is not widely used. Other successful attacks methods include heating the controller to a high temperature or focusing the UV light on the EEPROM, thus removing the security lock. Invasive physical attacks are the most destructive when the card is cut and processor removed. Then the layout of the chip can be reverse engineered.
Differential Power Analysis (DPA), is a statistical attack on a cryptographic algorithm which compares an hypothesis with a measured outcome and is often capable of extracting an encryption key from a smart card or other computing device. Simple Power Analysis (SPA), the direct analysis of the recorded power data to determine actions and data, is also useful.

4.2.1 Solutions

Several technologies have been developed to protect Smart Cards. These are technologies such as of STMicroelectronics against SPA/DPA attacks:

- **Technology barrier.** Advanced 0.6 micron technology greatly reduces the size and power consumption of cards as well as the relative variations in their operating parameters. This makes it very hard for external SPA/DPA methods to distinguish between normal card fluctuations and data-related fluctuations.

- **Clock fluctuation.** A special Clock Software Management facility, when properly used, results in highly variable software timing when the embedded application program is executing.

- **Unpredictable behavior.** A built-in timer with Interrupt capability and an Unpredictable Number Generator is used to impose unpredictable variations on software execution behavior, with consequent changes in the pattern of power consumption.

- **Robust design.** A modular design allows new hardware variations, including custom variations, to be produced quickly and efficiently, thereby allowing fast response to new attack scenarios.

- **Memory control for multi-applications.** An enhanced Memory Access Control system provides secure operating system support for multi-application cards.

- **Security mechanisms and firmware functions.** An enhanced set of security mechanisms and firmware functions allow the application to detect and respond appropriately to the occurrence of conditions that might indicate an attack. These conditions include invalid operating conditions, bad opcodes, bad addresses and violations of chip integrity; the possible responses include interrupts, program reset, and immediate erasure of all RAM data and flash programming of the entire EEPROM array.
Data on Smart Cards is organized into a tree hierarchy. This has one master file (MF or root) which contains several elementary files (EF) and several dedicated files (DF). DFs and MF correspond to directories and EFs correspond to files, analogous to the hierarchy in any common OS for PCs. However, these two hierarchies differ in that DFs can also contain data. DF’s, EF’s and MF’s header contains security attributes resembling user rights associated with a file/directory in a common OS. Any application can traverse the file tree, but it can only move to a node if it has the appropriate rights.

Attributes (Access Rights)

There are five basic levels of access rights to a file (both DF and EF). Some OS provide further levels.

Basic levels can be categorized, increasingly in security, as follows:

1. **Always (ALW)**: Access of the file can be performed without any restriction.
2. **Card holder verification 1 (CHV1)**: Access can only be possible when a valid CHV1 value is presented.
3. **Card holder verification 2 (CHV2)**: Access can only be possible when a valid CHV2 value is presented.
4. **Administrative (ADM)**: Allocation of these levels and the respective requirements for their fulfillment are the responsibility of the appropriate administrative authority.
5. **Never (NEV)**: Access of the file is forbidden.

However, presenting a CHV2 does not suffice to access a file requiring CHV1. CHV1 and CHV2 correspond to the two security PINs stored in the card: one is common user identification PIN and the other is a specific unblocking PIN pre-stored in the card.
4.2.2.2 The PINs

The PINs are stored in separate elementary files, EF\textsubscript{CHV1} and EF\textsubscript{CHV2} for example. The OS blocks the card after a wrong PIN is entered several consecutive times. The number of times is fixed and depends on the OS. Once blocked, the card can only be unblocked with a specific unblocking PIN stored in the card. The unblocking PIN can become blocked in the same way. If this happens, card is said to be in irreversible blockage and may have to be scrapped for security reasons.

If the PIN is blocked, the attribute of every file is changed to require CHV1. After the unblocking PIN is presented, the file attributes are returned to normal, the counter for the PIN is set back to its maximal value and the counter for the unblocking PIN is decremented. If the latter counter reaches zero, it cannot be used for unblocking the PIN any more. This provides additional security for the card.

4.2.3 Software Security

Software producers also contribute to the Smart Card security - they should provide their products with properly encrypted data and transfers. To help them achieve this goal, hardware-based or OS-based instructions and libraries supporting advanced cryptographic algorithms have been developed.

4.2.4 Conclusions

Most attacks today are classified as class 3 attacks, which means that either the costs associated to break the system are far more than the cost of the system itself, or that the cracker has to spend several or hundred years of computing power to break into a single transaction. Technology is developing faster than cracker methods. Therefore, each new generation of technology usually prevents attacks that the previous generation was vulnerable to.
4.3. Data Encryption

None of the data stored on identity cards in the European Union is encrypted, according to a study by the European Network and Information Security Agency.

Governments in 11 EU countries use electronic identity cards (eID) to authenticate citizens for access to government services, the European Network and Information Security Agency (Enisa) said in a report this week. The cards hold personally identifiable data, such as names and addresses, but this data goes unencrypted in all the countries.

Enisa does not see the lack of encryption as a cause for worry, as the cards have access control mechanisms on them.

"There is, in fact, absolutely no concern about [unencrypted data storage]," an Enisa spokesperson told ZDNet UK on Friday. "From a technical perspective it is absolutely fine to use access control mechanisms; depending on the implementation it is usually even better [than storing encrypted data on the card]."

Access control mechanisms include PIN access (where the user authenticates their identity using a personal identification number), symmetric key-based access (where frequently identical, secret keys are used for encryption and decryption) and certificate-based access control (which uses public keys).

Cambridge University security expert Richard Clayton said that access-control cryptography can, in general, be trusted to maintain data integrity. However, it is possible to "sniff", or remotely read the chip, on cards and passports using symmetric key systems, if the chip inside is designed for contactless use, he said.

"If I have a big antenna, I can capture the information from across the room," Clayton told ZDNet UK on Friday.

The information on eID cards usually includes names and birthdates, which are used as the basis for symmetric keys. If those names and birthdates are known, it's possible to guess the keys, Clayton said.

It is also possible to compromise machines that read symmetric keys. "If all card readers can decrypt the cards, someone will [compromise] the readers and get hold of the keys," he said.

However, if personal data on electronic cards is encrypted, it might have an effect on public trust in the cards, Clayton suggested. "If there is an encrypted blob, the conspiracy people would run around saying it doesn't contain your name but some other data," he said.
Saudi Arabia Phase 2 Identity Card uses a public key system, rather than symmetric keys and does not support contactless access.

Furthermore it is compliant with relevant international standards and uses Public Key Infrastructure (PKI) to ensure that the data within the chip retains its integrity through cryptographic protection.

4.4. Smartcards versus Security Tokens

A security token may be a physical device that an authorized user of computer services is given to ease authentication. The term may also refer to software tokens.

Security tokens are used to prove one's identity electronically (as in the case of a customer trying to access their bank account). The token is used in addition to or in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access something.

Hardware tokens are typically small enough to be carried in a pocket or purse and often are designed to attach to the user's keychain. Some may store cryptographic keys, such as a digital signature, or biometric data, such as a fingerprint minutiae. Some designs feature tamper resistant packaging, while others may include small keypads to allow entry of a PIN or a simple button to start a generating routine with some display capability to show a generated key number. Special designs include a USB connector, RFID functions or Bluetooth wireless interface to enable transfer of a generated key number sequence to a client system.

4.4.1 Token types and usage

There are four types of tokens:

1. Static Password.
2. Synchronous Dynamic Password
3. Asynchronous Password
4. Challenge Response

This article currently focuses on Synchronous Dynamic password tokens.

The simplest security tokens do not need any connection to a computer. The client enters the number to a local keyboard as displayed on the token (second security factor), usually along with a PIN (first security factor), when asked to do so.

Other tokens connect to the computer using wireless techniques, such as Bluetooth. These tokens transfer a key sequence to the local client or to a nearby access point.

Alternatively the new form of tokens that are coming into mainstream are mobile device which are communicated with out-of-band channel (like voice, SMS, USSD)
that also make the authentication and identity protection much stronger when compared to conventional simple Synchronous Dynamic Password tokens.

Still other tokens plug into the computer. For these one must:

1. Connect the token to the computer using an appropriate input device
2. Enter the PIN if necessary

Depending on type of the token the computer OS will now either:

- read the key from token and perform cryptographic operation on it or
- ask the token's firmware to perform this operation

- A related application is the hardware dongle required by some computer programs to prove ownership of the software. The dongle is placed in an input device and the software accesses the I/O device in question to authorize the use of the software in question.

### 4.4.2 Minimum requirement

1. Option 1: (for zero installation and excluded tokens): The minimum requirement of any token is at least an **inherent unique identity** in a protected memory that cannot be tampered with and preferably is not openly accessible to applications other than those offered by the token vendor or another trusted organization.

2. Option 2: (for out of band tokens): The minimum requirement of this form of token is connectivity from another medium like mobile network for USSD, SMS and voice. All you need a registered telephone / mobile number.

### 4.4.3 Digital signature

Trusted as a regular hand-written signature, the digital signature must be made with a private key known only to the person authorized to make the signature. Tokens that allow secure on-board generation and storage of private keys enable secure digital signatures, and can also be used for user authentication, as the private key also serves as a proof for the user’s identity.

For tokens to identify the user, all tokens must have some kind of number that is unique. Not all approaches fully qualify as digital signatures according to some national laws. Tokens with no on-board keyboard or another user interface cannot be used in some signing scenarios, such as confirming a bank transaction based on the bank account number that the funds are to be transferred to.

### 4.4.4 Embodiments

Tokens can contain chips with functions varying from very simple to very complex, including multiple authentication methods. Commercial solutions are provided by a variety of vendors, each with their own proprietary (and often patented)
implementation of variously used security features. Token designs meeting certain security standards are certified as FIPS compliant. Tokens without any kind of certification are sometimes viewed as suspect, as they often do not meet accepted government or industry security standards, have not been put through rigorous testing, and likely cannot provide the same level of cryptographic security as token solutions which have had their designs independently audited by 3rd party agencies.

4.4.5 Disconnected tokens

![Disconnected token image]

When using a disconnected token the number must be copied into the PASSCODE field by hand. Disconnected tokens have neither a physical nor logical connection to the client computer. They typically do not require a special input device, and instead use a built-in screen to display the generated authentication data, which the user enters manually themselves via a keyboard or keypad. Disconnected tokens are the most common type of security token used (usually in combination with a password) in two-factor authentication for online identification.

4.4.6 Connected tokens

Connected tokens are tokens that must be physically connected to the client computer. Tokens in this category will automatically transmit the authentication info to the client computer once a physical connection is made, eliminating the need for the user to manually enter the authentication info. However, in order to use a connected token the appropriate input device must be installed. The most common types of physical tokens are smart cards and USB tokens, which require a smart card reader and a USB port respectively.

4.4.7 SmartCards

Many connected tokens use SmartCard technology. SmartCards can be very cheap (around ten cents) and contain proven security mechanisms (as used by financial institutions, like cash cards). However, computational performance of SmartCards is often rather limited because of extreme low power consumption and ultra thin form-factor requirements.
4.4.8 Contactless tokens

Contactless tokens are the third main type of physical tokens. Unlike connected tokens, they form a logical connection to the client computer but do not require a physical connection. The absence of the need for physical contact makes them more convenient than both connected and disconnected tokens. As a result, contactless tokens are a popular choice for keyless entry systems and electronic payment solutions such as Mobil Speedpass, which uses RFID to transmit authentication info from a keychain token. However, there have been various security concerns raised about RFID tokens after researchers at Johns Hopkins University and RSA Laboratories discovered that RFID tags could be easily cracked and cloned.[3] Another downside is that contactless tokens have relatively short battery lives; usually only 3–5 years, which is low compared to USB tokens which may last up to 10 years. Though some tokens do allow the batteries to be changed, thus reducing costs.

4.4.9 Bluetooth tokens

Bluetooth tokens are often combined with a USB token, thus working in both a connected and a disconnected state. Bluetooth authentication works when closer than 32 feet (10 meters). If the Bluetooth is not available, the token must be inserted into a USB input device to function.

In the USB mode of operation sign of required care for the token while mechanically coupled to the USB plug. The advantage with the Bluetooth mode of operation is the option of combining sign-off with a distance metric. Respective products are in preparation, following the concepts of Electronic leash.
4.4.10 GSM cellular phones

A new category of T-FA tools allows users to utilize their mobile phone as a security token. A Java application installed on the mobile phone performs the functions normally provided by a dedicated token. Other methods of using the cell phone include using SMS messaging, instigating an interactive telephone call, or using standard Internet protocols such as HTTP or HTTPS.

Such a method can simplify deployment, reduce logistical costs and remove the need for separate token devices. In the case of SMS options, there is trade-offs: users may incur fees for text messages or for WAP/HTTP services.

4.4.11 Single sign-on software tokens

Some types of Single sign-on (SSO) solutions, like enterprise single sign-on, use the token to store software that allows for seamless authentication and password filling. As the passwords are stored on the token, users need not remember their passwords and therefore can select more secure passwords, or have more secure passwords assigned.
4.4.12 Related authentication technologies

4.4.12.1 Two-factor authentication (T-FA or 2FA)
Security tokens provide the "what you have" component in two-factor authentication and multi-factor authentication solutions. Some tokens provide up to three factors of authentication, or allow you to combine different factors to create multifactor authentication.

4.4.12.2 One-time passwords
A one-time password is a password that changes after each login, or changes after a set time interval.

4.4.12.3 Mathematical-algorithm-based one-time passwords
Another type of one-time password uses a complex mathematical algorithm, such as a hash chain, to generate a series of one-time passwords from a secret shared key. Each password is unguessable, even when previous passwords are known. The open source OATH algorithm is standardized; other algorithms are covered by U.S. patents.

4.4.12.4 Virtual Tokens
Virtual Tokens are a new concept in multi-factor authentication first introduced in 2005 by the security company Sestus. Virtual tokens work by sharing the token generation process between the internet website and the user's computer and have the advantage of not requiring the distribution of additional hardware or software. In addition, since the user's device is communicating directly with the authenticating website, the solution is resistant to man-in-the-middle attacks and similar forms of online fraud. However, during recent investigations of Virtual Tokens the question was asked, "What about the man in the browser attacks?" No answer was given to this inquiry, though the problem was acknowledged. Problems are usually not at the bank, credit card institution, etc. Large companies and banks have high tech IT departments and a staff to assure security on the institutional side. Most institutions like banks also have analysts that monitor their side of all online transactions that are done. The real problem is that the average consumer does not have the same high tech luxuries. Most consumers are barely protected with antivirus software. These software packages don't usually stop intrusions at the consumer's computer. This, in short, means that until this issue is addressed, it appears that virtual tokens cannot stop "man in the browser" intrusions, exposing consumers to potential loss.

4.4.12.5 Time-synchronized one-time passwords
A time-synchronized one-time passwords change constantly at a set time interval, e.g. once per minute. To do this some sort of synchronization must exist between the client's token and the authentication server. For disconnected tokens this time-
synchronization is done before the token is distributed to the client, other token types do the synchronization when the token is inserted into an input device. The main problem with time-synchronized tokens is that they can, over time, become unsynchronized.[citation needed] However, some such systems, such as RSA's SecurID, allow the user to resynchronize the server with the token, sometimes by entering several consecutive passcodes. Most also cannot have replaceable batteries and only last up to 3 years before having to be replaced - so there is additional cost.

4.4.12.6 Event-based Token
An event based token, by its nature, has a longer life span. They work on the one-time password principle and so once used, the next password is generated. Often the user has a button to press to receive this new code via either a token or via an SMS message. All CRYPTOCard's tokens are event-based rather than time-based.

4.4.12.7 Smart Card Based USB tokens
Smart-card-based USB tokens which contain a smart card chip inside provide the functionality of both USB tokens and smart cards. They enable a broad range of security solutions and provide the abilities and security of a traditional smart card without requiring a unique input device. From the computer operating system's point of view such a token is a USB-connected smart card reader with one non-removable smart card present.
4.5. Smartcards with USB interface

4.5.1 ISO 7816-12

According to its abstract, it specifies the operating conditions of an integrated circuit card that provides a USB interface. An integrated circuit card with a USB interface is named USB-ICC.

ISO/IEC 7816-12:2005 specifies:
- the electrical conditions when a USB-ICC is operated by an interface device - for those contact fields that are not used, when the USB interface is applied;
- the USB standard descriptors and the USB-ICC class specific descriptor;
- the data transfer between host and USB-ICC using bulk transfers or control transfers;
- the control transfers which allow two different protocols named version A and version B;
- the (optional) interrupt transfers to indicate asynchronous events;
- status and error conditions.

ISO/IEC 7816-12:2005 provides two protocols for control transfers. This is to support the protocol T=0 (version A) or to use the transfer on APDU level (version B). ISO/IEC 7816-12:2005 provides the state diagrams for the USB-ICC for each of the transfers (bulk transfers, control transfers version A and version B). Examples of possible sequences which the USB-ICC must be able to handle are given in an informative annex.

The USB CCID device class defines a standard for communicating with ISO/IEC 7816 smart cards over USB.
4.5.2 Solutions

For comfortable and unhindered e-commerce activities the usual smartcards (as security tokens) are not an optimal solution. Their use requires the availability and use of an appropriate card reader. This results in debates regarding who has to pay for the reader (especially in broad, low cost use). Such a reader is uncomfortable in handling (at least for mobile use) and can obstruct a required serial connector on the PC already used for other devices, or the drivers cannot be loaded. Alternatively, modern information and communication equipment (like PC, Laptops or future mobile phones) have already a fast and easy to use USB connector with the according drivers an SW support.

Microchip providers such as Atmel provide Microchip solutions which support both the ISO-7816-1 through 4 (Contact Reader) as well as the ISO7816-12 (USB ICC) interface.

ATMEL AT83C5127 is an example of such a solution.

See attached PDF Datasheet for details

4.5.3 Cryptoflex Smart Card

The smart card for e-transactions and trusted services

- Portable digital credential management
- Integrates into Public Key Infrastructures
- Also available with USB communication interface (Cryptoflex e-gate)

Security Purposes
CryptBot Smart Card™, named Cryptoflex™, was supplied by Schlumberger, one of the world-leading smart card companies, and customized and modified by CryptBot™'s Team for specially using with all CryptBot™ applications, especially for generating PKI key pair inside smart card's chip and then securely retrieve it to scramble with a targeted sensitive data. This is one of the best ways to securely generate and protect your key pair according to the transaction and digital signature laws.

Features & Functions
- Portable security over networks

Companies need solutions to ensure information security and
confidentiality over public networks. Cryptoflex makes it easy to carry your digital identity with you, ready to use with any secure system that requires authentication, digital signature and data ciphering. The card enables secure logon, e-mail, access to proprietary and confidential web sites, or single sign-on to intranets. Cryptoflex can be integrated into an existing government or corporate badge system to add functions such as network security, physical access and company management applications.

- **Cryptographic functions**
  Cryptoflex incorporates a crypto-processor dedicated to security enhancement - implementing security industry functions based on public key cryptography directly onto the card, eliminating the risk of sending secret unprotected data across a network. The card provides maximum security and flexibility of system integration thanks to administrative functions such as secure key loading, on-card key generation and ciphering of imported/exported data.

- **e-gate ready**
  Cryptoflex is also available with built-in e-gate smart card technology - enabling it to communicate directly with the computer's USB communication interface (USB v2.0 compliant) without the need for a smart card reader.