Biometric ID documents and system

System structure and inspection devices

Aleksej Makarov, Jelena Cvetković and Vojislav Lukić
R&D Centre Vlatacom
Belgrade, Serbia
aleksej@vlatacom.com

Abstract—**In this paper a general structure of an ID system is presented, together with its main subsystems, ranging from data enrolment to ID verification and document inspection. A special emphasis is given to data enrolment, ID verification and document inspection devices designed in Vlatacom Research and development Centre.**

Keywords – biometrics; smart ID documents; e-Government; pssport readers; automated fingerprint identification systems; passport readers; biometric data enrolmentt;

I. INTRODUCTION

The first years of the 21st century have been marked by security threats posed by international terrorism. Human trafficking has been a criminal activity of concern for a number of countries since a couple of decades. The convenient payment methods introduced in the last century such as credit cards and payments over internet have spurred a new sort of crime that can benefit international terrorism and organized crime: the identity theft. Our societies need to fight against identity theft by using state-of-the-art technology to protect rights of our citizens, residents, employees, social security beneficiaries, drivers, bank card holders and visitors.

In order to protect people's rights, identity protection and authentication need to be incorporated into ID documents, and used in everyday government, legal, commercial and business transactions. Secure means of identification are to be used in field, traffic and border control.

Edmond Locard, a French criminologist, defined, in 1909, identity as "the set of characteristcs by which a person can be distinguished from another". These characteristics as a means of verifying personal identity are nowadays referred to as biometrics. They are measurable patterns of either invariable characteristics of a person (physical biometrics) or of her behavioural characteristics such as voice, gait, signature.

In 1882, Alphonse Bertillon presented a set of 14 body measurements (height, head, foot, ear, nose, middle finger, arm, forearm) that was to be used as a quantitative measure of similarity together with the photograph of a person. However, the system turned to be flawed because the measurements for the same person could vary with age but would also differ when taken by different police officers. In order to remedy to these shortcomings, Parisian police added fingerprints to Bertillon's set of anthropometric measurements.

The 20th century brought the computer, the microchip and the telecommunications revolutions, and consequently new means of communicating, presenting, filing, classifying and searching personal identities. Face recognition became quantitative and independent of observer's interpretation.

New biometric characteristics such as iris have emerged as reliable, computationally identifiable patterns.

II. IDENTITY AND BIOMETRICS IN PRACTICE

Biometric features necessary for personal identification should be collected together with the personal data (demographics) from ID document applicants, and stored in a central database, usually referred to as a central or national identification register. The same data should be stored on ID document issued to the holder. This will allow later identity verification, i.e., a comparison of the holder's biometrics scanned for identity check with the ones initially stored either on the ID card or in the database.

A comprehensive biometric identity system consists of six main subsystems, as shown in Fig. 1:

- ID document enrolment stations
- central register of identity files: a database with demographic and biometric search engines
- Digital certificate issuing mechanism
- ID document production plant
- mobile and stationary devices for verification of identities and of identity documents

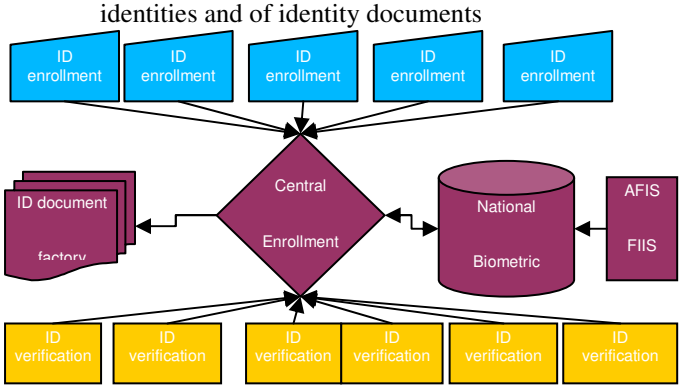

Figure 1. Block diagram of a national biometric system.

This work is partially supported by the following grant: "Innovative electronic components and systems based on inorganic and organic technologies embedded in consumer goods and products", Project No TR32016, Serbian Ministry of Education and Science.

A significant number of countries have introduced or are introducing biometrics in their ID documents: Malaysia (since 2001), Oman (since 2002), United Arab Emirates, Philippines, Spain, Italy, Great Britain, Netherlands, Germany, USA, etc..

The most complete set of biometrics to be stored in a central database was the one defined by the British Identity Cards Bill in 2006, consisting of the fingerprint, face and iris images stored in a central register and on ID cards. The system cost of about 160 dollars per capita was the reason to abolish this bill in 2011.

In 2003, a similar nationwide biometric identity system has been launched in Serbia, with the first biometric ID cards issued in 2008. The whole system, comprising of five major subsystems, costs about 15 dollars per capita.

The cost efficiency of Serbian biometric ID system can be partially explained by the choice of technologies and contractors. Technologically, Serbian system supports face and fingerprint based identification, but not iris recognition. Serbian government has partially relied on local software and hardware designers. The existing national identity register containing demographic but not biometric information of citizens may have also contributed to the cost efficiency of the Serbian solution.

Here below are summarized the aforementioned subsystems and illustrated by examples provided by Serbian biometric ID system and Vlatacom products.

A. ID Enrolment Stations

These stations consist essentially of computers, with peripherals allowing for acquisition of biometric features (in Serbia, a camera, a fingerprint scanner and a signature pad), and connected to the central identification register over a private or a cryptologically protected public telecommunications network, as shown in Fig. 2.

Figure 2: The acquisition equipment of different vendors controlled by Vlatacom enrolment application software. The passport scanner shown in the left-hand side is optional and serves for acquisition of demographic data from a previously issued ID document (either passport ot ID card).

The introduction of biometric ID documents is accompanied by modified enrollment procedures, and often by tight deadlines for issuance of new ID documents, resulting in long lines in front of enrollment offices. In order to increase the system efficiency with the same man-power, the equipment in Fig. 2 can be assembled within a self-service biometric enrollment kiosk controlled by slightly modified software, as in a Vlatacom product [4] shown in Fig. 3. Thus, instead of having one enrollment officer per station, optimally four enrollment stations can be supervised by a single operator.

Figure 3: Self-service biometric kiosks multiply the efficiency of enrollment officer by four. The kiosk in the bottom contains all functional components shown in Fig.2, while the one on the top has a signature pad installed instead of the ID document reader. With a different software, this kiosk is used for verification.

Figure 4: Central identification register, the appropriate searching engines (such as AFIS) and the digital certificate issuing and verification mechanisms (such as Certificate Authority and Certificate Revocation List) form the central part of a biometric identity system.

B. Central identification register

The identification register is the heart and brain of the biometric identity system. It consists of a database containing millions of biometric identity files. The files can be searched by either textual, i.e., demographic queries such as name, city, sex, height, or by biometric queries (an image or a processed description of a fingerprint, face, iris). The search engines are powerful parallel computers specialized for various types of submitted queries. In Serbia, biometric search engines consist of an Automated Fingerprint Identification System (AFIS) and Facial Image Identification System (FIIS).

C. ID document production plant

This facility produces smart cards. It inserts security features on the card bodies (such as rainbow, micro, infrared or ultraviolet prints, optical variable ink, hologram or kinegram) and personal information of the document holder. The personal information has been provided from the identity file stored in the central identification register. A part of the personal information, such as name and photograph, is printed on the card body. A microchip is embedded in a specially prepared hole on the card body. Complete biometric and textual information is downloaded to the chip, together with cryptographic functions to be used for protecting these data. Such an identity document is often referred to as eID.

Vlatacom has carried out the installation of entire ID document plants, but its development focus is on eID chip personalization software and on implementation of cryptographic functions.

D. Digital certificates - Public Key Infrastructure

The final stage of eID production is the chip personalization (downloading holder's demographic and biometric data onto the chip) and generation of signature and authentication keys. This stage can take place in the ID production plant, but also at the site where the eID is issued to the citizen.

Namely, electronic ID documents (eID) contain cryptographic functions which allow their holders to remotely sign legal documents, to authenticate themselves to e-government servers and to encrypt the contents of the information they exchange. Public key infrastructure (PKI) and digital certificates are used to enable signature, authentication and encryption functions using keys stored on the chip.

1) Signing with eID

An ID document must allow its holder to irrevocably prove his or her identity in order to execute his or her legal rights and assume legal responsibility with regard to the government and other citizens. Legal responsibility is related to the notion of "non-repudiation" of signature, i.e., to the fact that a citizen cannot deny his or her signature on a given document. This is implemented through the signature keys.

Signature keys are generated in pairs, consisting of a private and a public key, on the eID embedded microprocessor. The private key is stored in protected memory that cannot be read from outside the chip. Consequently, only the eID holder can use it. The public signature key is a part of a digital certificate released to government institutions, allowing them to verify the authenticity of documents the eID holder signs. When such a document is signed (e.g., on a web browser), the hash image derived from it (i.e., a unique fixed-length sequence to which the document has been mapped according to a pre-determined rule) is sent to the smart card (by the browser, via PKCS#11 or CSP interface installed on the computer).

The hash can be viewed as a message digest, mainly used in order to keep the encryption time and the encrypted data sequence length as short as possible, while preserving the integrity of the original document content (if the document is altered, its hash changes). The embedded microprocessor encrypts the hash image using the stored private key of the holder, and returns it encrypted to the computer (i.e., to the web browser). The eID holder usually activates the signing process by entering a PIN code on the computer or eID reader keyboard. The activation represents the deliberate will of the eID holder to sign a document.

As a biometric alternative to the PIN code entered on an ordinary card reader, one can use a device designed by Vlatacom, which integrates the smart card reader with a fingerprint scanner. In this implementation, the eID holder scans his or her fingerprint by the device, which then sends it to the eID microprocessor. In the smart card CPU, the scanned fingerprint is compared with the one stored in the protected memory of the chip ("match-on-chip"). The signature is activated when these fingerprints match.

The organization or government institution that needs to verify the authenticity of the signature and the integrity of the signed document (i.e. that the content of the document has not been altered) must possess a valid digital certificate. This certificate contains the eID holder's name, the public signature key, the algorithm used to create hash images, the period of validity and the authority which has generated it (e.g., the Ministry of Internal Affairs) with its own signature.

If the smart card is stolen, the thief will still need the owner's PIN code or finger to generate a digital signature. The eID loss may be detected by its owner and the corresponding certificate can be immediately revoked.

2) Authenticating with eID

Signature keys can be also used for accessing government servers. In this case, they are referred to as authentication keys. Thanks to these keys, the ID card holder can access servers across the web and retrieve or submit information considered confidential. e.g. in order to check his or her tax return status, request a civil record or vote. The web site server sends a random challenge to the holder's web browser, which in turn asks the holder to start the authentication process by entering the PIN or scanning the fingerprint. This way the eID holder reconfirms he or she trusts in this web site and is willing to exchange data with it. When the PIN or fingerprint is correct, the browser sends the hash map of the challenge to the eID, which is returned encrypted (signed), together with its public key certificate (i.e., digital certificate) through the browser to the web site. Provided the digital certificate has not expired or been revoked, the web site retrieves the public key from the digital certificate, applies it to the signed hash map of the challenge, obtains the decrypted hash and verifies whether it corresponds to the original challenge. If it does, the web site established the true identity of its remote user to whom it can grant the access to confidential data. In some cases, authentication keys are generated separately from signature keys and can be activated by a different PIN code. This depends on the security policy of the issuing authority.

3) Encrypting with eID

The last cryptographic function is encryption. The encryption relies on a pair of asymmetric keys (private encryption and public encryption keys) and on an internally generated symmetric encryption key. The symmetric encryption key is generated randomly by the smart card CPU to encrypt the confidential information whenever needed. The same key is used for encrypting and decrypting. The result of these symmetric operations will be obtained more quickly and will take less bits. The sender typically uses the recipient's public encryption key to encrypt the symmetric encryption key prior to sending it over the network. Thus, only the recipient can read the symmetric encryption key thanks to his or her private encryption key stored on the chip. In case of loss of the ID card, the holder can still retrieve the encrypted archived message since the encryption private key is generated and backed up by an external mechanism (i.e., the Certificate Authority).

Figure 5: Vlatacom biometric access device is a smart card reader with integrated fingerprint scanner and security access module. The device allows the eID holder to authenticate him- or herself to e-Government servers, sign electronic documents and exchange confidential information by using his or her finger instead of the PIN code. The smart cards used with this device possess the "match-on-card" capability, performing the comparison of the scanned with the enrolled fingerprint on the chip. Otherwise, the risk of identity theft would have occurred as a result of the upload of the fingerprint to the computer.

4) eID middleware: a bridge between the card and the PC

The communication between the computer and eID cryptographic functions is implemented through the software libraries provided by smart-card vendors complying to the PKCS#11 standard. These libraries have to be installed on the computer. They are platform independent, though some OS specific applications use OS specific libraries. For example, the CSP API is also supported by smart card vendors for MS-Windows specific applications such as Internet Explorer.

To summarize, the user can use his eID, a smart-card reader and the eID middleware installed on his or her computer in order to log in to specific e-government websites. The smart card reader can integrate the fingerprint scanner as shown in Fig.4.

E. ID document verification devices

The United Nations' International Civil Aviation Organization (ICAO) recommends the face, fingerprint or iris image of a holder to be stored on a contactless chip embedded in his or her passport [7]. Most border crossings nowadays are equipped by readers capable of reading biometric and textual data from national ID cards, visas and any machine-readable passports. In addition, these readers are capable of checking security features visible under white, ultraviolet and infrared lights. Such readers are manufactured by Vlatacom [5] and are deployed in Serbia, Bosnia and Herzegovina, Moldavia, Nigeria and elsewhere.

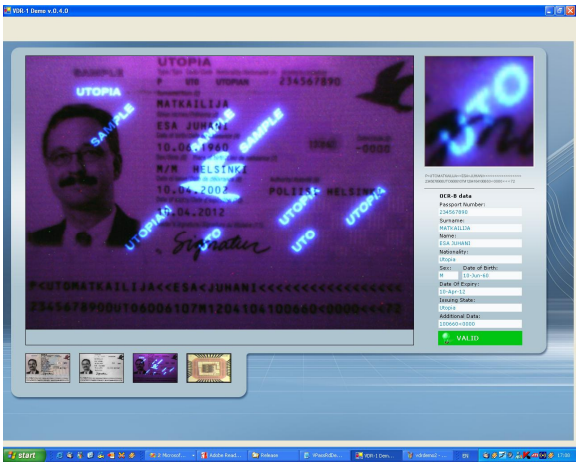

Figure 6. The first Vlatacom travel document reader VDR-1 (top) reads electronic chips (middle) and machine-readable zones from passports, visas and ID cards. In addition, optical security features can be zoomed and checked against ultraviolet (bottom) and infrared light.

Figure 7. The electronic gates (eGates) retrieve demographic and biometric data from international passengers' passports and perform biometric verification of their holders. Used essentially in self-service mode (one officer per security area of four gates), they increase the border control efficiency at international airports.

Figure 9. The hand-held travel document reader and biometric authenticator VDR-H produced by Vlatacom basically performs all functions as does the large biometric verification kiosk

Figure 10. VDR-H is equipped with wireless or PMR modem and encryption functions. Thus, it can be used in the lines of cars at the border crossing, which reduces the queues and the waiting time. Alternatively, the train passengers can be checked while the train is still in motion.

Mobile devices can be used for field checks of ID cards. Vlatacom has developed devices, which, in addition, are to our best knowledge the only portable document readers capable of performing all inspection functions on the document ([1][2][3][6]) as do the bulky desktop devices shown in Fig. 2 (without the camera), Fig. 3 (the bottom part when used for verification) and Fig. 6 (where a computer and fingerprint reader have to be added to complete the inspection system) .

With VDR-H, the citizen's identity can be checked even when no ID card is physically present, by transmitting biometric data over a telecommunication network, if the national laws provide for such a possibility.

III. Conclusion

Security threats to our societies impose a rapid deployment of comprehensive national biometric ID systems. Many ID card projects worldwide have shown that the biometric ID technology is mature but slow to introduce because of incurring costs. Serbian case study shows that a comprehensive biometric identity system can be cost-efficient and that the confidence given to the domestic industrial partners pays off in the increasing number of work places, taxes collected and the level of technology necessary to maintain the public safety and keep in pace with the world.

References

[1] Jelena Cvetković, Ilija Popadić, Saša Vujić, Aleksej Makarov, "Universal Battery Management System in a Handheld Device", Proceedings of the 16th IEEE Mediterranean Electrotechnical Conference, Medina Yasmine Hammamet, Tunisia, 25-28 March 2012J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Nikola Balaban, Aleksej Makarov, Vujo Drndarevic, "Photoelectronic system for reliable detection of document presence", Proceedings of the Tenth International Scientific – Professional Symposium INFOTEH®-JAHORINA 2011, Vol. 10, Ref. C-6, pp. 263-267, Jahorina, Bosnia and Herzegovina, 2011.

[3] Jelena Cvetkovic, Sasa Vujic and Aleksej Makarov, "Multiple Sensors' Lenslets for Secure Document Scanners", Proceedings of the Tenth International Scientific – Professional Symposium INFOTEH®-JAHORINA-2011, Vol. 10, Ref. E-VI-11, p. 892-896, Jahorina, Bosnia and Herzegovina, March 2011

[4] Vlatacom, assigned patent 50469 with Zavod za Intelektualnu Svojinu Republike Srbije, Biometrijski kiosk za akviziciju, 3.3.2010.

[5] Vlatacom, assigned patent 50179 with Zavod za Intelektualnu Svojinu Republike Srbije,, citac putnih i licnih dokumenata, 7.5.2009

[6] Vlatacom, assigned patent 51531 with Zavod za Intelektualnu Svojinu Republike Srbije, Rucni prenosni uredjaj za proveru putnih iI licnih dokumenata, ocitavanje biometrijsih podataka i prepoznavanje lica koja nose te dokumente, 1.7.2011.

[7] ICAO Doc 9303, Machine Readable Travel Documents, Part 1 : Machine Readable Passports, Volume 2 : Specifications for electronically enabled passports with biometric identification capability, Sixth edition, 2006.

[8] ICAO Supplement to Doc 9303, Machine Readable Travel Documents, ISO/IEC JTC1 SC17 WG3/TF1 for ICAO-NTWG, Release 11 (final), November 17, 2011

[9] ICAO TAG MRTD/NTWG, Machine Readable Travel Documents (MRTDs): History, Interoperability and Implementation, Draft 1.4, March 23, 2007.