Privacy concept of Slovak national eID-model

LADISLAV HURAJ, GERMAN F. MICHAĽČONOK
Department of Applied Informatics
University of SS. Cyril and Methodius in Trnava
Nám. J. Herdu 2, 917 01 Trnava
SLOVAK REPUBLIC
ladislav.huraj@ucm.sk
german@ucm.sk

Abstract: European Commission has recognized the importance of eID in a multilingual and multi-legal environment and recommended for EU countries to implement electronic identification management, meeting national service needs, cultural traditions and personal data protection. Electronic identifiers are intended to facilitate ubiquitous access to electronic services.

Although national eIDs play a unique role in all identity management issues that are linked to a physical person, common specifications simplify the interoperable eIDM in the EU. The idea of the Slovak identification scheme has gone out from Austria identification model based on cryptographic operations. In our article the common and different features between the proposed Slovak and the existing Austrian model are described.

Key-Words: eID, Identification, Person Identifier, E-government

1 Introduction

Electronic or digital identifiers are key elements to identify the person in e-government scheme. The importance of electronic identity (eID) for e-government was also underlined in European document – *i2010 eGovernment Action Plan* [1]. EU countries should implement electronic identification management (eIDM), meeting national service needs, cultural traditions and personal data protection preferences, where electronic identification for public services is intended to ease access and offer personalised and smarter services.

Slovak proposal of national eID model is taking into consideration the main aim of the EU intent – to respect the different national approaches and solutions without creating a barrier to using public services across borders. Moreover, the principal objective of the Directive 95/46/EC [2], to ease data sharing – it provided regulations in terms of the "protection of individuals with regard to the processing of personal data", is considered for the Slovak identification scheme.

At present, in the Slovak Republic, Birth Number is used for the natural persons' identification in information systems. The main disadvantage of the use of Birth Number is the reflection of the date of birth and gender of the identified person, which does not correspond with EU legislation.

Some initial schemes for the Birth Number replacement were designed in 2005, e.g. [3,4]. But the requirements for the Unique Person Identifier from Ministry of Interior of the Slovak Republic have changed and design of a new scheme is inevitable.

The idea of the Slovak identification scheme has gone out from Austria identification model [5]. The Austrian model has already proved a justification of an application of cryptographic methods to identification systems. On the other hand, national differences in the Slovak identity management architecture imply a brand new model of the identification scheme.

The paper is organized as follows. In Sections 2 and 3, the Austrian and Slovak person identification models are described. In Section 4, two variants of Slovak Unique Person Identifier are presented and Section 5 gives the comparison of the Slovak and the Austrian scheme. Finally, Section 6 gives the preliminary conclusions and possible future work.

2 State of the Art – Austrian model

In this Section a short introduction to the Austrian person identification scheme [2,5,6,7,8] is presented. Austria was one of the first EU member states adopting the EU Signature Directive into domestic law in 2000. As a result of the Austrian e-government initiative, the Austrian e-government Act entered into force on March 1, 2004 [5,6].

2.1 Source Personal Identification Number

In Austria, each citizen is assigned a unique identification number held in the base registers – the Central Residents Register CRR and the Supplementary Register SR (for persons who do not have a registered address in Austria). However, public bodies are not allowed by law to use this unique number for e-government application. Instead of this, transformations of the unique identification number to different identifiers are used. The first transformation is based on a Triple-DES encryption and the derived number from the transformation is called "source personal identification number" (sourcePIN). SourcePINs are allowed to be stored on citizen cards only [7].

2.2 Sector Specific Personal Identification Number (ssPIN)

In order to prevent data abuse, the derived sourcePIN is also not used for the identification purpose. Instead of using the sourcePIN in different governmental applications, the second transformation based on one-way hash derivation of sourcePIN is applied and the sector specific personal identification number (ssPIN) is generated. The ssPIN is created by combining the sourcePIN with the sector specific alphanumerical code assigned to each government sector and then applying a cryptographic one way function. Due to the hash function, the sourcePIN is not revealed. Moreover, different ssPINs are thus generated for each governmental department based on the unique sourcePIN of a person and on particular alphanumeric code. It means that in practice, each sector uses different identifiers [2,6,7,8].

If an authority requires an ssPIN from another sector for identification purposes, they can request it from the SourcePIN Register Authority. They send the ssPIN to the authority that requested it in encrypted form. It can be decrypted only by the public authority that is responsible for the foreign authority [5].

3 Slovak model

In this Section we describe current identification number of residents in the Slovak Republic. Definitions of new identifiers as well as their roles in on-coming identification system are described, too.

3.1 Current National identification number – Birth Number

In the Slovak Republic, National identification number based on birth date is currently used. The Birth Number is issued at birth by the civic records authority and recorded on the birth certificate as well as on an ID card. The Birth Number has a strict format: YYMMDD/XXXX with YYMMDD being the date of birth and XXXX being a semi-unique identifier. For females, the month of the date of birth is increased by 50. Full number is required to be divisible by 11. Nevertheless, this system does not provide a unique identifier – the numbers are repeated every century and there are mistakes in assignment of XXXX in the system. The Birth Number is moreover inconvenient to the Directive 95/46/EC of the European Parliament [9], because it has raised privacy concerns – age and gender of the owner can be decoded from the number. In the near future the Birth Number will be replaced by a meaningless identifier in the near future by a group of identifiers (BIFO, JIFO and SIFO), which will provide stronger level of data protection.

3.2 Meaningless Person Identifier – BIFO

BIFO is unique number allocated to the citizen in the Central Register of Residents. Confusion as to a person's identity can therefore be excluded. The size of BIFO is 12 alphanumerical values; there is request for shortness of BIFO because BIFO will be written in ID card and, what is more, it should be relatively easy to remember. Furthermore one BIFO will be assigned to a person for long period (usually for whole life). Longer Unique Person Identifier – JIFO is derived from a BIFO and is used for collaboration by e-government services.

3.3 Unique Person Identifier – JIFO

For the purposes of unique identification, all natural persons registered as resident in Slovakia as well as in the case of all other natural persons, will be allocated a unique identification number (JIFO) which is derived from the Meaningless Person Identifier BIFO in heavily encrypted form. The length of JIFO is bigger than BIFO in order to improve the resistance to brute-force attacks. JIFO is used for e-government services for collaboration among state authorities as main unique person identifier. We propose two variants of JIFO derivation described in Section 4.

3.4 Sector Person Identifier – SIFO

One fact that must be taken into consideration is that government public administration is divided into legally defined State sectors. The strong requirement for Slovak e-government is that different identifiers must be used for each sector to prevent of the synergic effects. For this purpose the Unique Person Identifier JIFO is uniquely transformed to respective Sector Person Identifier.

The transformation is based on strong encryption algorithm AES [10] in CBC (Cipher Block Chaining) mode. Diversity and uniqueness of the numbers is provided by respective sector key during the encryption process. In this case, the generated Sector Person Identifiers SIFOs from a JIFO are different for each sector and it is not possible to find the person information in a sector database knowing a SIFO from another sector. The authorities can use the same SIFO to retrieve the citizen's data saved within the same sector. However, authorities do not have access to SIFO from other sectors.

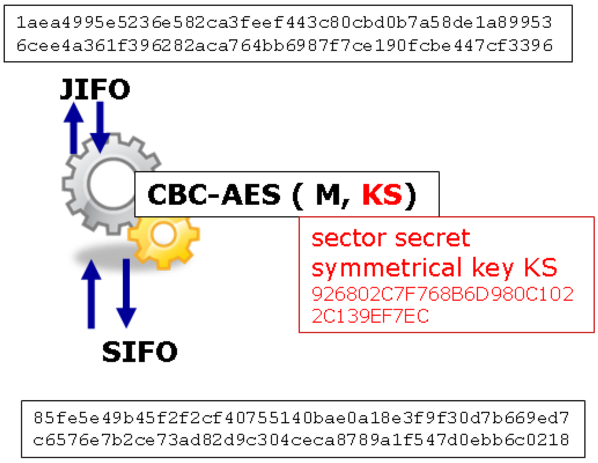
1aea4995e5236e582ca3feef443c80cbd0b7a58de1a89953
6cee4a361f396282aca764bb6987f7ce190fcbe447cf3396
JIFO
CBC-AES (M, KS)
sector secret
symmetrical key KS
926802C7F768B6D980C102
2C139EF7EC
SIFO
85fe5e49b45f2f2cf40755140bae0a18e3f9f30d7b669ed7
c6576e7b2ce73ad82d9c304ceca8789a1f547d0ebb6c0218

Fig. 1 Reversible derivation of the Sector Person Identifier from the Unique Person Identifier JIFO

Moreover, the scheme satisfies the second main requirement from the Ministry of Interior of the Slovak Republic – the reversibility is feasible in the system. The JIFO can be transformed back from the Sector Person Identifier SIFO with knowledge of the sector secret key. Government bodies from different sectors often have to co-operate together, they need to consolidate data that is stored in different sectors under different SIFO. For this purpose the scheme uses the reversibility between JIFO and SIFO. If an authority requires data from different sector they can request it by JIFO. The authority transfers back its SIFO to the Unique Person Identifier JIFO, the JIFO is sent (in encryption form based on asymmetrical encryption) to requested authority and respective Sector Person Identifier SIFO of the requested authority can be computed. The reversibility is the main difference between Slovak and Austrian scheme.

4 Variants of Unique Person Identifier

Considering the above mentioned requests for a unique person identifier from the Ministry of Interior of the Slovak Republic we prepared two variants of generating and using of Unique Person Identifier (JIFO).

4.1 Variant the 1st – JIFO as hash value

JIFO is generated by a cryptographic hash computation as a 384-bits output of SHA-384 hash function [11] from BIFO, Figure 2. It can therefore be generated at any moment by anyone who knows the BIFO value. This is an irreversible cryptographic derivation, i.e. the BIFO cannot be identified from the derived identifier.

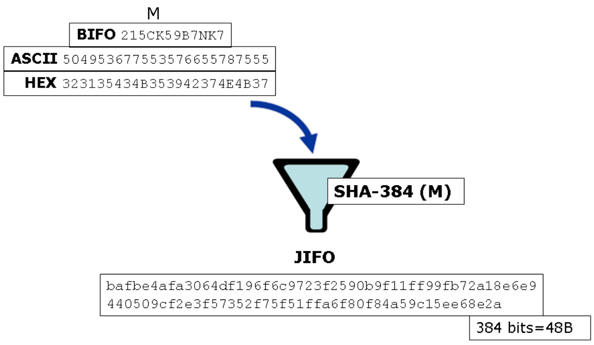
M
BIFO 215CK59B7NK7
ASCII 504953677553576655787555
HEX 323135434B353942374E4B37
SHA-384 (M)
JIFO
bafbe4afa3064df196f6c9723f2590b9f11ff99fb72a18e6e9
440509cf2e3f57352f75f51ffa6f80f84a59c15ee68e2a
384 bits=48B

Fig. 2 – JIFO generating as hash value

Whereas because of Birthday Paradox, a 50 % probability that two outputs of different inputs are equal for the SHA-384 function is equal $1/2^{192}$. Although the probability is extremely low the system should check up each BIFO after its generating for the JIFO unique. If there is a JIFO duplicity, the BIFO is marked as useless.

4.2 Variant the 2nd – JIFO as HMAC value

Analogically with the previous variant, a JIFO is generated from a BIFO by a cryptographic HMAC computation as a 384-bits output of HMAC SHA-384 function [12], where the function incorporates BIFO together with a secret key from Central Register of Residents, Figure 3. It makes a possibility only for a holder of the secret key to generate a JIFO. HMAC is again an irreversible cryptographic derivation, i.e. the BIFO cannot be identified from the derived identifier.

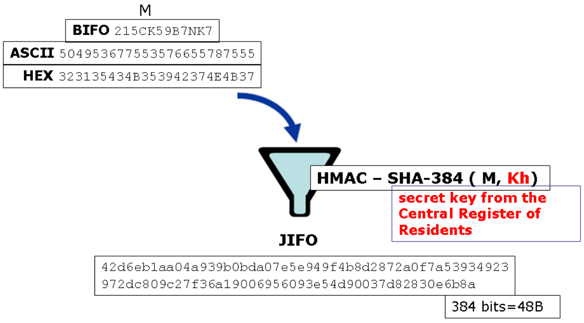
M
BIFO 215CK59B7NK7
ASCII 504953677553576655787555
HEX 323135434B353942374E4B37
HMAC – SHA-384 (M, Kh)
secret key from the Central Register of Residents
JIFO
42d6eb1aa04a939b0bda07e5e949f4b8d2872a0f7a53934923
972dc809c27f36a19006956093e54d90037d82830e6b8a
384 bits=48B

Fig. 3 – JIFO generating as HMAC value

5 Comparison with Austrian model

Common features in both models, Slovak and Austrian, are:

- in both cases the component data for the eID come from a civil registry where citizens have to register by law
- an identifier which is attributable to a data subject to be unambiguously identified and which also serves as the basis for generating sector-specific personal identifiers
- use of strong cryptography.

Although the Slovak and the Austrian schemes use different cryptographic algorithms for generating of particular identifiers, it is not the main contrast between them. The main difference of the schemes is in cooperation among sectors' bodies. In Slovak scheme, the central point is not included in the cooperation process and the bodies should communicate directly without intermediate entity. From this reason, there is reversibility from sector identifier back to the Unique Person Identifier JIFO in the scheme.

In figure 4, the creation process of the ssPIN as well as workflows between sectors in the Austrian scheme is illustrated. On the other hand, figure 5 presents reversible workflow in the Slovak identification scheme.

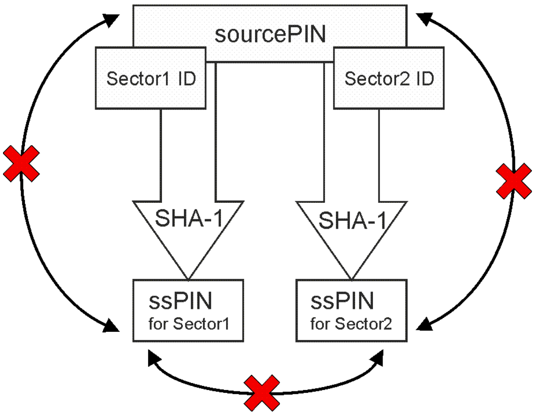

Fig. 4 – Workflow to create ssPINs based on a given sourcePIN; it is neither possible to calculate the underlying sourcePIN nor any other sector's ssPIN from a given ssPIN [8]

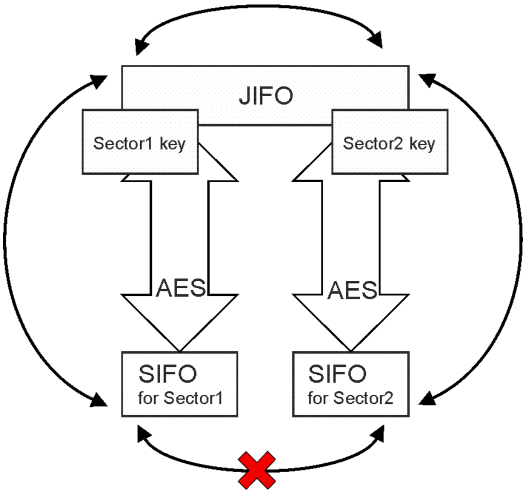

Fig. 5 – Workflow to create a sector ID number SIFO based on a given Unique Person Identifier JIFO; it is possible to calculate the underlying JIFO and from JIFO (only if the Sector2 key is known) other sector's SIFO without a central provider

6 Preliminary conclusions and future work

The paper introduced two approaches integrating professional representation into Slovak e-government scheme.

Each of proposed prototypes has its own advantages as well as disadvantages of the implementation or of the robustness as well as from the security point of view.

Variant the 1st – JIFO as hash value

- everyone can generate the JIFO everywhere; JIFO is "in principle" known to everyone who knows the BIFO

- BIFO cannot be identified from the JIFO; but because of BIFO shortness there is a possibility to use brute-force attack for this purpose
- application of JIFO is also open for private sector
- overhead of testing of the JIFO unique after a BIFO generating.

Variant the 2nd – JIFO as HMAC value

- JIFO can be generated only by a holder of the secret key; JIFO is known only to the state authorities
- there are two possibilities of JIFO generation:
  - only in the Central Register of Residents, i.e. overhead with communication to Register on each occasion
  - on the side of an authority – key distribution problem
- application of JIFO only for the state sectors
- analogically an overhead of testing of the JIFO unique after a BIFO generating.

The Slovak prototypes and their implementations are now under discussion and they are tested from different points of view e.g. [13] before being applied in practice.

Although new national Slovak identification scheme has gone out from Austria identification model and uses similar cryptographic methods, the philosophy of its application is different.

Acknowledgements: This work was supported in part by the University of SS. Cyril and Methodius in Trnava under project 69/10.

References:

[1] EUROPEAN COMMISSION (EC), *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*, COM (2006) 173 final, Brussels: EC, 2006.

[2] Austrian Federal Chancellery, ICT Strategy Unit: *Administration on the Net - An ABC Guide to E-Government in Austria*, Official Report, Austria, June 2004

[3] FIPS PUB 180-2 (Federal Information Processing Standards Publication), *Secure Hash Standard*, National Institute of Standards and Technology, August 2002

[4] FIPS PUB 197 (Federal Information Processing Standards Publication) *Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, 26 November 2001.

[5] FIPS PUB 198 (Federal Information Processing Standards Publication) *The Keyed-Hash Message Authentication Code (HMAC)*, National Institute of Standards and Technology, 6 March 2002.

[6] Ministerstvo financií Slovenskej republiky: *Identifikátor fyzických osôb [Identifier of natural persons]*, Čiastková štúdia uskutočniteľnosti projektov prioritnej osi 1 Elektronizácia verejnej správy a rozvoj elektronických služieb OPIS, Information Risk Management, Ministry of Finance of the Slovak Republic, November 2008

[7] Sasinek, M.: Návrh zásad vytvárania BIFO v podmienkach SR [Design of principles of the BIFO creating in SR] *Řešení problematiky identifikátoru občana v oblasti zdravotnictví v ČR a SR*, česko-slovenský seminář, Prague, April 2005.

[8] Makolm, J.: Registers as part of back office integration: the Austrian experience. In Electronic Government, Proceedings: Lecture Notes in Computer, EGOV 2004, Zaragoza, Spain, Sept. 2004, Springer-Verlag, Heidelberg

[9] Tauber, A., Rössler, T.: Professional Representation in Austrian EGovernment, In: Proceedings of the 8th International Conference EGOV 2009, Springer Verlag: Heidelberg et al, LNCS # 5693, 2009.

[10] Hayat A, Posch R, Rössler T. Giving an interoperable solution for incorporating foreign eIDs in Austrian e-Government. In: IDABC-conference 2005: cross-border e-Government services for administrations, businesses and citizens Brussels, Belgium; 2005.

[11] Otjacques, B., Hitzelberger, P., Feltz, F.: "Identity Management and Data Sharing in the European Union," hicss, vol. 4, pp.70a, Proceedings of the 39th IEEE Annual Hawaii International Conference on System Sciences (HICSS'06) Track 4, IEEE Computer Society, Washington, DC, USA, 2006

[12] European Union (EU), "Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data", Official Journal of the European Communities of 23 November 1995 No L. 28

[13] Tanuska, P., Moravcik, O., Vazan, P.: The base testing activities proposal. In: *Annals of DAAAM and Proceedings of DAAAM Symposium*. ISSN 1726-9679, Vol. 20, No. 1 Annals of DAAAM for 2009 & Proceedings of the 20th international DAAAM symposium, November 2009, Vienna, Austria. DAAAM International Vienna, ISBN 978-3-901509-70-4, pp. 371-372.