Toward a Unique Person Identifier Model in the Slovak Republic

LADISLAV HURAJ
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

Abstract: A national identification number of natural persons is used by the governments of many countries in various ways. The main objective is to improve security in online services and unify authentication. In the Slovak Republic, National identification number based on birth date is currently used, which does not correspond with EU legislation.
In our article we describe our new prototypes of Unique Person Identifier prepared on the basis of request of the Ministry of Interior of the Slovak Republic. The scheme is based on the idea of the Austrian system. Moreover, an introduction of proposal of an electronic system for identity management (IDM) in the Slovak Republic is presented.

Key-Words: Identification, Unique person identifier, Sector-specific personal identifier, Meaningless identifier

1 Introduction

A national identification number of natural persons (citizens, permanent residents, and temporary residents) is used by the governments of many countries for taxation, work, government benefits, health care, and other governmentally-related functions. The identification number usually appears on an identity card issued by a country. Implementation of such system depends on the countries, but in most cases, for a citizen a number is issued at birth or when they reach a legal age. For non-citizens such numbers are issued when they enter the country.

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. [5,6]. But the requirements for the Unique Person Identifier from Ministry of Interior of the Slovak Republic have changed and a design of a new scheme is inevitable. The main change lies in relation between two main identifiers in the scheme, the Meaningless Person Identifier and the Unique Person Identifier. Whereas in previous scheme the Meaningless Person Identifier was derived from the Unique Person Identifier, the new requirement changes the order, i.e. the Unique Person Identifier should be derived from the Meaningless Person Identifier.

The idea of the Slovak identification scheme has gone out from Austria identification model [1]. The Austrian model has already proved a justification of an application of cryptographic methods to identification systems.

Moreover, the principal objective of the Directive 95/46/EC [10], to ease data sharing – it provided regulations in terms of the "protection of individuals with regard to the processing of personal data", was considered for the Slovak identification scheme. Moreover, the European Directives requires for data protection [16]:

- Personal data shall be processed fairly and lawfully and the amount of personal data gathered should be adequate, relevant and not excessive in relation to the purposes for which they are processed.
- Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in a way incompatible with those purposes, and shall be accurate and up-to-date. Inaccurate or incomplete personal data shall be erased or rectified, and personal data shall be preserved in a form, which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.
- Security measures shall be implemented to protect personal data from unintended or

unauthorized disclosure, destruction or modification.

The paper is organized as follows. The next section consists of brief information about identity management and basic terms. In Section 2, the Austrian person identification model is described. In Section 3, we give three variants of generating and using of Unique Person Identifier and Section 4 gives the comparison of the scheme in taxonomy of government approaches. Finally, section 5 gives the preliminary conclusions and possible future work.

1.1 Identification and Authentication

Tsiakis et. al. described in [17] six fundamental security requirements for electronic communication. These are:

- Identification and authentication – the ability to identify (uniquely) an entity
- Authorization – the ability to control the actions of the entity based on its identity
- Confidentiality – the ability to deter unauthorized disclosure of information
- Integrity – the ability to assure that data has not been modified
- Non-repudiation – the ability to prevent the denial of actions by the entities
- Availability – the ability to provide an uninterrupted service.

As can be seen from the previous list, the unique identification holds first position in the security requirements.

Academic experts have invested considerable effort to review the extent to which a digital identity may be different compared to physical identity. Greenwood in [18] presents a useful typology of different forms of identity in relation with government:

1. Digital identity (e.g. username, IP, email address);
2. Physical identity (e.g. passport, drivers license, birth certificate); and
3. Dual or "converged identity", a combination of digital and physical identity (e.g. a 'chipped' person or animal, biometric passport)

In our article we deal with person identity as digital identity defined in [13] as "a message which is received about a person through digital information either as such or in combination with other information of that person (characteristics, habits)".

1.2 Identity Management

The concept of identity is closely connected with the concept of identity management. The term of identity management can be understood as "the set of business processes, and a supporting infrastructure for the creation, maintenance, and use of digital identities" [19] or more closely as "a process of representing and recognizing entities as digital identities in computer networks" [20].

1.3 e-Government

E-government can be defined in various ways. In [15] several definitions of e-government are collected, e.g. "using the Internet and the world-wide-web for delivering government information and services to citizens", "information and communication technologies to optimize government service delivery, constituency participation and internal government processes" or "e-government refers to government's use of information technology to exchange information and services with citizens, businesses, and other arms of government."

Identification of persons as well as identity management play a key role in each e-government.

2 State of the Art – Austrian model

In this Section a short introduction to the Austrian person identification scheme [1,7,8,9,10] 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. It establishes the Source Identification Number (sourcePIN) to identify natural and legal persons and other data subjects unmistakably based on using strong cryptography [1,7].

2.1 Source Personal Identification Number (sourcePIN)

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 [8].

Only a central governmental department called SourcePIN Registration Authority is allowed to create these sourcePINs. The derivation of sourcePIN is done by adding a secret seed-value to the unique identification number and by applying a cryptographic encryption (Triple-DES) using an authority's secret key, Fig. 1 [9].

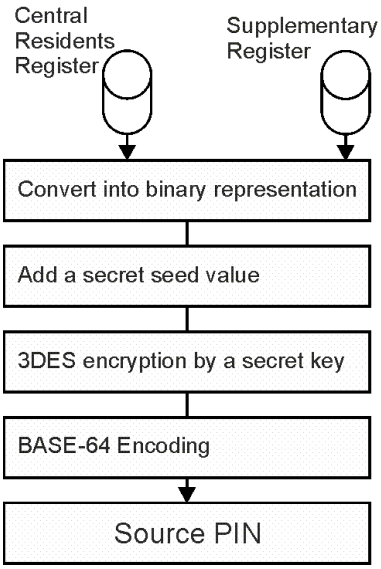

Fig. 1: Source PIN generation [9]

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. In data files of controllers in the public sector, the identification of natural persons is to be represented only in the form of an ssPIN, derived from the sourcePIN [7,8,9,10].

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 [1].

In figure 2 the creation process of the ssPIN as well as workflows between sectors are illustrated.

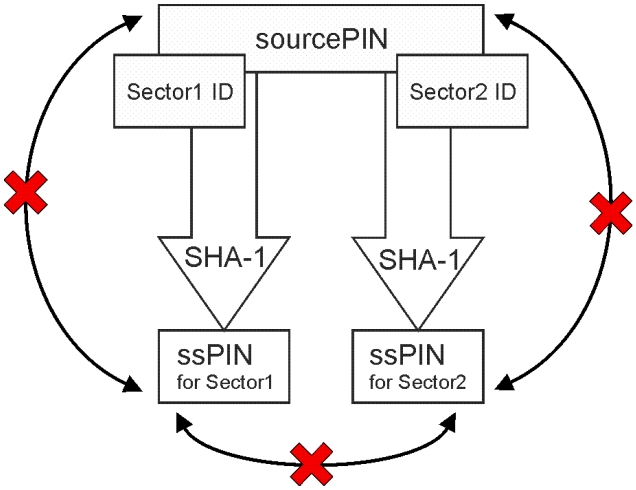

Fig. 2: Workflow to create ssPINs based on a given sourcePIN; it is neither possible to calculate the underlaying sourcePIN nor any other sector's ssPIN from a given ssPIN [9]

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 (Slovak: Rodné číslo) 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 [11], 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 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 three 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 the synergic effects. For this purpose, the Unique Person Identifier JIFO is uniquely transformed to respective Sector Person Identifier SIFO.

The transformation is based on strong encryption algorithm AES [3] 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, e.g. if they need, to the citizen's records or use it to pre-fill forms. However, authorities do not have access to SIFO from other sectors.

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.

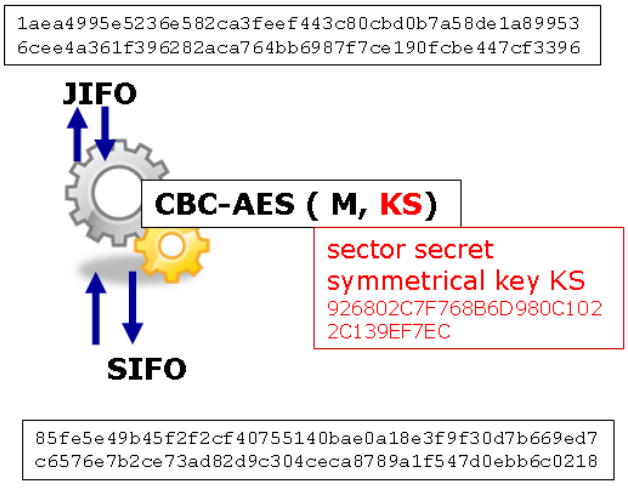

Fig. 3 Reversible derivation of the Sector Person Identifier SIFO from the Unique Person Identifier JIFO

0
JIFO
1aea4995e5236e582ca3feef443c80cbd0b7a58de1 a899536cee4a361f396282aca764bb6987f7ce190f cbe447cf3396 (384 bits = 48 bytes)
1
sector secret symmetrical key KS
926802c7f768b6d980c1022c139ef7ec
2
SIFO – AES encryption in CBC mode, hexadecimal
85fe5e49b45f2f2cf40755140bae0a18e3f9f30d7b6 69ed7c6576e7b2ce73ad82d9c304ceca8789a1f547 d0ebb6c0218 (384 bits = 48 bytes)

Table 1: Process of derivation of the Sector Person Identifier SIFO from the Unique Person Identifier JIFO

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 three 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 [2] from BIFO, Figure 5. 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.

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 and it is not used.

0
BIFO
215CK59B7NK7 (12-digit decimal number)
1
Binary representation – data for the hash calculation
323135434b353942374e4b37 (hexadecimal number)
2
JIFO – Hash value with SHA-384(M), hexadecimal
bafbe4afa3064df196f6c9723f2590b9f11ff99fb72a 18e6e9440509cf2e3f57352f75f51ffa6f80f84a59c1 5ee68e2a (384 bits = 48 bytes)

Table 2: Variant 1: Derivation of a JIFO as hash SHA384

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 [4], where the function incorporates BIFO together with a secret key from Central Register of Residents, Figure 6. 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.

0
BIFO
215CK59B7NK7 (12-digit decimal number)
1
Binary representation – data for the hash calculation
323135434b353942374e4b37 (hexadecimal number)
2
secret key K_h from the Central Register of Residents
4142434445464748494a4b4c4d4e4f50515253545 5565758595a
3
JIFO – HMAC value with SHA-384(M,K_h), hexadecimal
42d6eb1aa04a939b0bda07e5e949f4b8d2872a0f7 a53934923972dc809c27f36a19006956093e54d90 037d82830e6b8a (384 bits = 48 bytes)

Table 3: Variant 2: Derivation of a JIFO as HMAC SHA384

4.3 Variant the 3rd – without JIFO (straight from BIFO to SIFO)

In this scheme the JIFO is emitted from the system and the Sector-specific Personal Identifier SIFO is derived directly from BIFO and particular sector code (e.g. Ministry of Interior of the Slovak Republic = MVSR), Figure 7.

The size of SIFO is in contrast to previous variants not 384-bits long, its length is 128 bits. Therefore the used mode of AES symmetrical algorithm is here ECB (Electronic codebook) that operates only one block of 128-bits data.

0
BIFO
215CK59B7NK7 (12-digit decimal number)
1
Sector abbreviation
MVSR
2
Binary representation – data for the encryption {96 bits +32 bits = 128 bits}
323135434b353942374e4b374d565352 (hexadecimal number)
3
sector secret symmetrical key KS
9b3d64f79a5330ad694c535c59c4499c
4
SIFO – AES encryption in ECB mode, hexadecimal
2016b84305a5a7ab95d364538f7d5700 (128 bits=16B bytes)

Table 4: Variant 3: Derivation of SIFO without JIFO (straight from BIFO to SIFO)

5 Comparisons

Because of synergetic effect, the Unique Person Identifier JIFO is not stored in any database. Each sector stores its own different unique sector identifiers SIFO. For co-operation among particular sectors, the Unique Person Identifier JIFO is transformed to respective sectors' SIFO. Even during this process the JIFO is not stored in any store. Moreover, the issuing Central Register of Residents does not need to hold a copy of the JIFO created either.

This section categorizes our new model into existing taxonomy regarding the previous conditions.

5.1 Taxonomy

In [12] authors present a taxonomy of government approaches towards online Identity Management. The taxonomy identifies three essential approaches: a decentralized, a federal, and a centralized type.

(i) In the decentralized approach, each government agency develops its own identity registration systems and accompanying policies to suit its own needs. An identifier issued to a citizen will be unique to the agency, but the citizen will find the identifier of no use for accessing other government services online.

(ii) Under the federal approach, a group of government agencies enter into a trust federation and agree using shared policy and technology standards and protocols to accept each others identifiers to allow citizens to access each others online services.

(iii) Under centralized approach, a central government agency manages and stores citizen identities in a single location, and all government bodies are required to connect their online services to the central identity provider [12].

Though models, Austrian as well as new Slovak model, belong to centralized type, their executions are different. The Austrian model is strictly centralized, i.e. when an authority identifies a person for the further co-operation with other sector authority it needs to contact the Central identity registration service. In the new Slovak model, the sector authorities can co-operate together without the Central identity registration service knowing the Unique Person Identifier JIFO. However, the Unique Person Identifier JIFO is never stored in any databases, the encrypted form for particular sector is applied.

In light of previous case, the taxonomy should be expanded to four types regarding the new Slovak model, e.g. "centrally cooperating".

We shortly prove that new model does not belong to any of the previous categories. In the decentralized type (i), the new model does not fit the requirement: "The citizen will find these credentials of no use for accessing other government services online [12]" because one sector identifier can be transformed to other sector identifier and the citizen can use it for other government services. In the federal approach (ii) it does not fit the requirement "to accept each others identity credentials to allow citizens to access each others online services [12]" because each sector uses only its own identifier and does not know the identifier from the other sector.

Finally, the centralized approach (iii) requires that "a central government agency manages and stores citizen identities in a single location (at least logically), and all government agencies are required to connect their online services to the central identity provider [12]". This approach fits to the Austrian model. But in Slovak model the sector authorities can co-operate without connection of the central provider. Moreover, the centralized approach carries its own set of disadvantages. Because every citizen's identity is stored in one place, the impact of a security breach can be high. There are potentially great threats to privacy in case such a security breach does happen. Several high-profile cases in which much citizen data was lost illustrate that the occurrence of a security breach is not at all improbable [12]. We must note, that in the Austrian model if attacker obtained a sourcePIN it is easy to compute particular ssPIN.

In new model there is no central store for all identities. Moreover, it is not possible to derive the sector identifier directly only from the Unique Person Identifier JIFO, the secret sector key is needed.

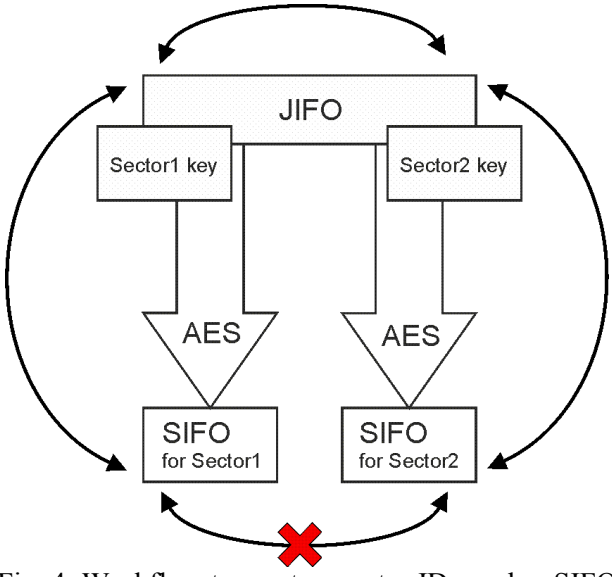

Fig. 4: Workflow to create a sector ID number SIFO based on a given Unique Person Identifier JIFO; it is possible to calculate the underlying JIFO and from JIFO (only if the Sector2 key is known) other sector's SIFO without a central provider

6 Preliminary conclusions and future work

The paper introduced three approaches of 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 how to generate the JIFO
  - 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.

Variant the 3rd – without JIFO (straight from BIFO to SIFO)

- absence of JIFO as middle element among authorities
- SIFO is shorter than in the previous variants.

Moreover, we presented that our new model invokes a necessity to expand existing taxonomy of government approaches.

In the future it is necessary to take into account two main topics based on chosen variant.

The first of these is the possibility of unjustified, unauthorized or intermeddled use of citizen's data by government bodies. There may be strict

government guidelines as to which agency can use which part of the identity store for which reasons.

And the second is technical problem, the amount as well as the functionality of shared registers and databases. E.g. some most important registers for Austrian model can be found in [7] and are as follows:

- Central Register of Residents – contains domicile and personal data of every person living in Austria
- Supplementary Register for Natural Persons – contains natural persons not living in Austria, but in contact with Austrian authorities, e.g. abroad citizens or citizens of foreign states not living in Austria but in contact with Austrian authorities
- SourcePIN Register – Contains the source identification number derived from the person's registration number in the Central Register of Residents or in the Supplementary Register
- Register of Company Names
- Central Register of Associations
- Supplementary Register for legal persons – contains legal persons not contained within the Register of Company Names or within the Central Register of Associations, which are in contact with Austrian authorities, e.g. consortia of natural or legal persons
- Real Estate Database, buildings and domicile register, register of valid addresses
- Other registers, e.g. central trade register, register of industrial plants, passport register, driving licence register, weapons register and criminal records.

A databases' design for the Slovak Republic will be based on the chosen model of JIFO transformation.

Moreover, for example Diaconita et al. in [14] presents several additional services for quick access to citizen information, e.g. Generic systems, XML Transformation, Metadata processing, Integration processes. The design of the services depends on chosen model as well.

The above mentioned Slovak prototypes are now under discussion and they will be tested before their application in practice.

An open issue is also the integration of proposed methods with others European identification schemes. But as shown in [9], it could not be a problem to transfer the Slovak ID number to e.g. Austrian scheme. In [9] authors show a web service which offers the possibility to request for an Identity Link based on a subsourcePIN generated by using a foreign citizen card. As a result, the requester is enabled to use e-governmental applications with the Austrian e-ID just having been created. The whole application can be done with one contact to the authority, using possible communication channel like the Internet.

References:

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

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

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

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

[5] 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

[6] 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.

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

[8] 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.

[9] 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.

[10] 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

[11] 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

[12] Seltsikas, P., Heijden, H.: A Taxonomy of Government Approaches Towards Online Identity Management, In: *43rd Hawaii International Conference on System Sciences (HICSS-43 2010)*, IEEE Computer Society, pp.1-8, January 2010, Koloa, Kauai, HI, USA 2010

[13] Saärenpaä A., The constitutional state and digital identity, Paper available on the website of *the World Congress for Informatics and Law II*, Spain, September 23rd–27th, 2002 http://www.ieid.org/congreso/ponencia_i.htm

[14] Diaconita, V., Botha, I., Bara, A., Lungu, I., and Velicanu,M.: Two Integration Flavors in Public Institutions, In: *WSEAS Transactions on Information Science and Applications*, Volume 5, Issue 5, May 2008, pp. 806-815

[15] Spremic, M., Hrvoje, B.: Comparative Analysis of e-Government Implementation Models and Progressive Services. In: *WSEAS Transactions on Business and ECONOMICS*, Vol. 5, Issue 5, 2008, pp. 260-269.

[16] Zorkadis, V. and Karras, D.A.: Privacy - enhancing digital rights management systems, In: *Journal of WSEAS Transactions on Communications*, Vol. 2, No. 2, 2003, pp.160-165.

[17] Tsiakis, T., Evagelou, E., Stephanides, G., Pekos, G.: Identification of trust requirements in an e-business framework, In: *WSEAS Transactions. on Communications*, Issue 2, Volume 3, pp. 670-674, 2004.

[18] Greenwood, D., Dempster, A.P., Laird, N.M. and Rubin, D.B.: The context for Identity Management Architectures and Trust Models, In: *Proceedings of the OECD Workshop on Digital Identity Management*, 2007.

[19] Scorer, A., Identity Directories and Databases, Birch, D. G. W., Ed., *Digital Identity Management*, 41-52, Gower Publishing Ltd., 2007.

[20] Jøsang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, S.: Trust requirements in identity management. In: *ACSW Frontiers '05: Proceedings of the 2005 Australasian workshop on Grid computing and e-research*, pp. 99–108, Darlinghurst, Australia, Australia, 2005. Australian Computer Society, Inc.., Jan. 2005.

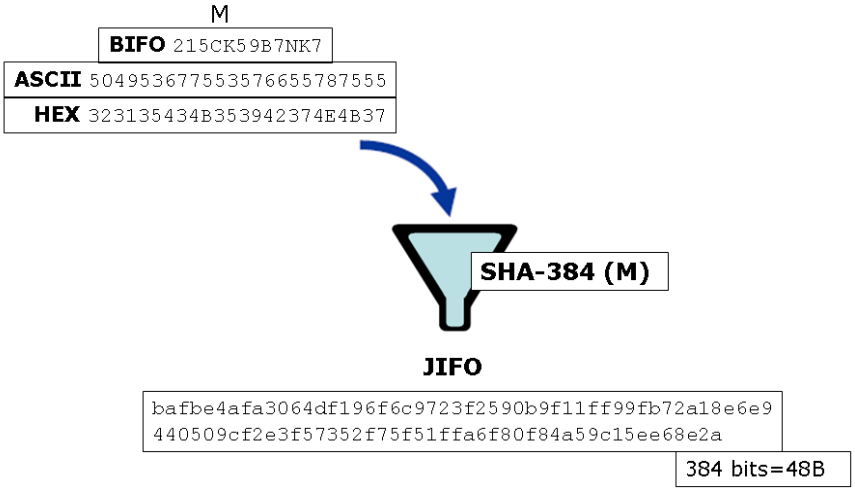

Fig. 5 – JIFO generating as hash value

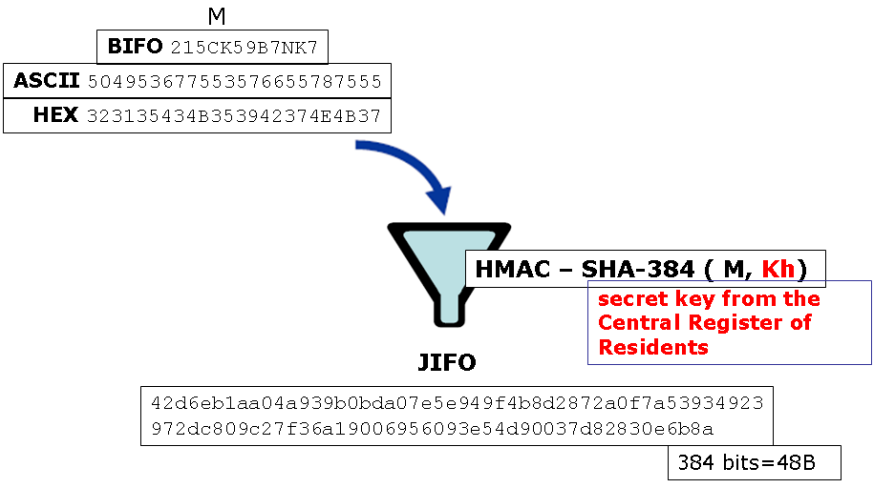

Fig. 6 – JIFO generating as HMAC value

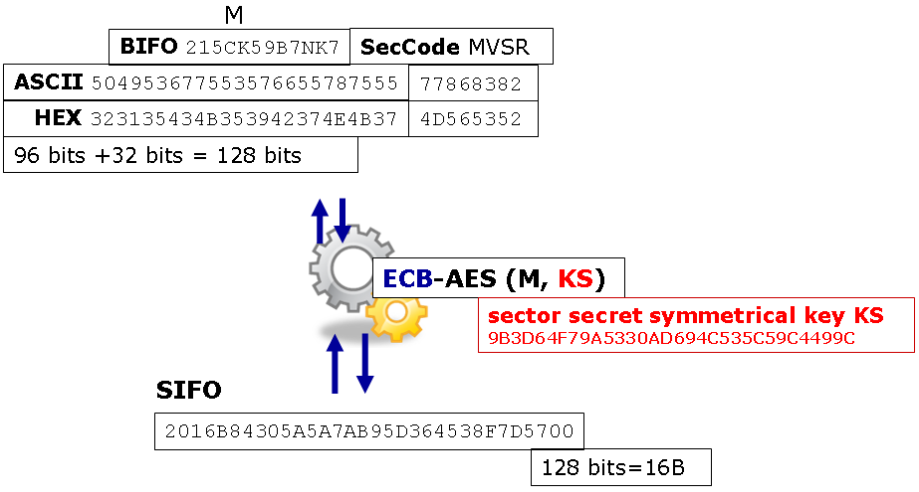

Fig. 7 – Using the system without JIFO