Aspect of data communication security in the Central Node of Poland's Schengen Information System and Visa Information System Component

G. BLIŹNIUK[A], R. KOŚLA[B], A. MACHNACZ[C]
e-mail: adres Grzegorz.Blizniuk@wat.edu.pl

Instytut Systemów Informatycznych
Wydział Cybernetyki, Wojskowa Akademia Techniczna
ull. S. Kaliskiego 2, 00-908 Warszawa

Abstract: Data communication security assurance in the Central Node of Poland's Schengen Information System and Visa Information System Component (in polish: Centralny Węzeł Polskiego Komponentu Systemu Informacyjnego Schengen i Systemu Informacji Wizowej – CW PK SIS i VIS) is crucial for building adequate trust of the operation of mechanisms of the Schengen agreement in Poland. Presented in this chapter are the security requirements, agreed by member states of the Schengen agreement, which fulfillment is subject to independent review during periodical SIS/SIRENE evaluations. The essence of law, organizational and technical role means have also been indicated for assuring a high level of SIS and VIS data communication security, which is higher than the standard level required by regulations on the protecting of personal data. Directions for further development of the implementation of the SIS and VIS in Poland have been presented in the conclusion.

Keywords: IT systems, ICT security, Schengen zone, Schengen Information System, Visa Information System

1. Introduction

Lifting border inspections between member states has entailed the necessity of implementing so-called "compensating instruments", which are to balance the ability of free flow of people between member states of the Schengen agreement in the range of citizens' security as well as crime-fighting effectiveness. Due to this, it was decided, among others, to create and implement the Schengen Information System (SIS), which goal is to assure a quick and safe exchange of data for border and internal control as well as police and justice system cooperation.

SIS comprises of a database that is constantly completed by authorized services and public authorities. It includes data of wanted people, undesirable people in given Schengen member states as well as sought for vehicles and entities. The SIS system is the most important of mechanisms for maintaining a high level of security in the area that comprises the free flow of people, which enables effective crime-fighting, especially on international terms.

The basis for the operation of SIS is Title IV of the Schengen Implementation Convention [2] (SIC – articles from 92 to 119), in which authorized personnel of member states are granted access to information concerning people and property through the procedure of automatic data searching.

In accordance with the initial intention of European Union member states, the expansion of the Schengen border area – in view of the necessity of increasing connection bandwidth and adding new features to the system and also the concept of building the Visa Information System (VIS) – was conditioned by the early launching of the second-generation SIS system (SIS II). Project delays arose due to the European Commission that caused a decision to be made on the meeting of Justice and Internal Affairs Council of Ministers in Brussels on the 5th – 6th of December 2006 to enable the ability to expand the Schengen border zone as established earlier, i.e. till the end of 2007, thanks to using a temporary solution that was proposed by the government of Portugal, i.e. SISone4ALL software package[1].

The fulfillment of the Portugal initiative consists of the acceptance by new EU member states and the adoption into their environment a copy of the system operating in Portugal and their connection to the presently operated first-generation Schengen Information System

[1] The SISone4ALL software package was forwarded to Poland in March 2006 at a meeting of ministers of home affairs in Lisbon on the basis of intergovernmental agreements concluded with Portugal, under which the Polish government acquired the right to freely use the software in order to meet the demands placed on the parties of the Schengen Implementation Convention. The Government Plenipotentiary Minister for SIS and VIS accepted the system on behalf of the Polish Government.

(SIS +1) enhanced with web services. The Portuguese solution is essential for assuring communication between national systems with the European central system in Strasburg (C.SIS). The necessity of waiting for the launch of the SIS II by the European Commission was avoided this way. However, in view of maintaining a high priority, which is the fulfillment of the building program of the SIS II system to replace the currently used SIS 1+ system, by the European Commission as well as individual member states, the necessity of synchronizing the implementation of two important data communication ventures arose that are to help in the realization of being a full member in the Schengen zone, i.e. SISone4ALL, SISII and VIS.

In view of the situation, during the period of January – September 2007 two physical and independent versions of the Central Polish Node SIS and VIS Component (CW PK SIS and VIS) were designed and implemented allowing authorized organs of the government, called institutional users (IU), cooperation with the currently used first-generation system as SIS 1+ is and also with second-generation systems, i.e. SIS II and VIS.

2. Security architecture in Central Node of Polish Component of SIS/VIS

The building of the Polish SIS and VIS Component, in view of the necessity of implementing SIS 1+, along with the simultaneous uninterrupted work on SIS II required that the accepted functional and technical structure of the SIS and VIS Central Node allowed easy integration of institutional users' systems with the SIS 1+ Central System (C-SIS) and afterwards with the SIS II (CS-SIS) and the VIS Central System (CS-VIS).

Presented further on in this article are the realizations of building CW PK SIS and VIS within the SIS and VIS Polish Component complying with European and national law, organizational and technical stipulation.

2.1. European context

Access to SIS and VIS information systems resources are regulated by laws of the European Union. Poland, by joining the EU on 1st of May 2004, which resulted in the signing of the Treaty of Accession, obliged to implement into Polish law the Schengen Implementation Convention [2]. This convention determines the basis of building and launching SIS. SIS is the largest extensive data communication system in Europe that enables current exchange of information between organs responsible for guarding external borders as well as police from countries belonging to the Schengen zone. It possesses criminal and judicial information as well as data concerning the free flow of people. The information in the SIS system allows authorized entities, among others, to:

- Identifying wanted persons and entities.
- Establishing reasons for searching.
- Defining priority actions in the case of finding a person or object.

For reasons of assuring an effective realization of the aforementioned actions the country services of the Schengen zone have to exchange information, which from the perspective of the citizen's interest, should be subjected to special protection, because they constitute a category of personal data [6]. The elementary requirements concerning SIS data communication security included in Art. 103 and 118 of the Schengen Implementation Convention [2]. Article 103 of the SIC obliges member states to register at least 10% of personal data transfer operations to national SIS components to achieve the requirement of accountability of administrators and operators actions. The logs that contain this data should be stored during a period no longer than 6 months. Art. 118 defines the minimal measures of protecting personal data processed in national SIS components, which must be used in order to:

- prevent any unauthorized person from having access to SIS installations used for the processing of personal data;
- prevent data media from being read, copied, modified or removed by unauthorized persons;
- prevent the unauthorized access to personal data processing in SIS;
- authentication authorization of SIS users;
- permission management of SIS users;
- SIS data protection during transmission;
- accountability operations on data in the SIS.

According to the requirements of the Schengen Implementation Convention member states have to agree upon measures of protecting data during their transfer through the data communication network and also assure the employment of qualified personnel that guarantees proper protection during data processing in the SIS. In connection with this, member states have agreed on the necessity of building a dedicated data communication

network with the name of SISNET to assure the ability of exchanging data between the SIS Central System and national components. The body in charge of building and maintaining the SISNET network on behalf of member states is the General Secretariat of the Council of the European Union and the C.SIS team is responsible for the current operation, which job posts are financed by the Ministry of Internal Affairs of France. The Infrastructure of the SIS Central System has been localized in Strasburg. Member states contribute annual contributions, which are proportionate to member contributions provided to the European Union for the maintenance of C.SIS and SISNET.

The requirements of the Schengen Implementation Convention were accepted by member states as insufficient from the SIS data communication security viewpoint due to their general nature. This is why in 1999 Finland took the initiative of elaborating "Guidelines for data security in connection with the Schengen systems"[3]. These recommendations were to assure the usage of identical procedures and protection measures in the SIS Central System and national components (N.SIS). Art. 103 and 113 of the Schengen Implementation Convention were accepted as a legal basis and recommendations were presented in the following order:

- Security planning – inter alia the necessity of elaborating a security policy,
- Security organization – inter alia identifying entities responsible for security management,
- Controlling system resources – inter alia cataloguing and documenting network and system resources,
- Personnel security – inter alia procedures permitting operators and system administrators as well as training in the range of data protection,
- Physical security – inter alia location security of national components, admittance control to buildings, limiting guest and external suppliers traffic around national components,
- Equipment protection – inter alia limiting access to the infrastructure of national components (especially servers and network equipment), fire protection and air-conditioned operation environment, backup electrical power source,
- Managing the operational environment – inter alia procedures of safe usage of equipment, protecting against malware, backup copies of data, network management, user access control, system monitoring, upgrading procedures and system software development, planning uninterrupted operation, legal regulations accordance control.

These recommendations were added to the Schengen Catalogue [4], which elaboration was undertaken by the Working Party on Schengen Evaluation in 2001 based on the EU Council mandate. The Schengen Catalogue comprises of four parts and the second part includes recommendations and best practices for the Schengen Information System as well as nation SIRENE offices[2], exchanging essential supplementary information, allowing the confirmation of identities of persons and entities. SIRENE offices, as coordinating units, have to operate in a non-stop mode (365/7/24), simultaneously meeting the functions of a single contact point for authorized SIS system users in a given member state as well as for SIRENE offices in other countries of the Schengen zone. The Schengen Catalogue is a textbook used during training personnel responsible for operating the SIS. The recommendations and good practices included are used as reference during a periodic evaluation carried out by countries of the Schengen zone and countries that are applying for membership in this zone. Evaluations are conducted by teams comprised of representatives of member states, General Secretariat of the Council of the European Union and the European Commission. The structure of the second part of the Schengen Catalogue has been developed in a form of a table, in which in one column recommendations were inserted and in the second column "good practices" for each issue involving the safe usage of SIS and the proper functioning of the SIRENE office. The basic recommendations concerning SIS indicate the necessity assuring the constant presence (24/7) of qualified technical personnel at the national SIS component location as well as real-time synchronizing data in the nation SIS copy with the SIS Central System. It is additionally recommended to have procedures of regularly comparing the national copy with the SIS Central System database. One of the key recommendations is that member states be vested in stable data communication networks, which will be used to exchange SIS data within the processes of entering new entries and entry-checking in SIS. Data communication networks

[2] SIRENE - Supplementary Information REquests at the National Entries

in member states should assure a response time from SIS no longer than 5 seconds.

Recommendations concerning SIS security are grouped in the Schengen Catalogue analogically as in the aforementioned initial 1999 document titled: "Guidelines for data security in connection with the Schengen systems". The structure and contents of the recommendations concerning SIS security in the Schengen Catalogue is noticeably very similar to the structure and contents contained in the 1995-published BS7799 British Standard titled: „A code of practice for information security management", which was later used to establish an international standard of data security management ISO/IEC 17799. Despite such extensively defined measures of data processing protection in SIS, the Schengen Catalogue does not make up a closed set of recommendations and good practices. It will certainly be modified with elements involving the usage of the second generation SIS II system.

It is worth stressing the fact that the data in the SIS system are not admittedly secret information subjected to special signification and protection in accordance with regulations on the protection of secret information. However, their high sensitivity and potentially negative effect on interests of citizens caused member states to make a decision of using advanced cryptographic protection measures, i.e. IP ciphers, which assure data confidentiality transferred through telecommunication connections leased for the needs of the SISNET network. The same requirements concerning the use of IPS ciphers were introduced to the non-functional requirements specifications of the SIS II system, in which the SISNET network was replaced with a dedicated IP network that is in accordance with the sTESTA network specification.

2.2. Connecting the C.SIS with national components

As mentioned earlier, the concept of building the Polish Central Node SIS Component and VIS (in polish: CW PK SIS and VIS) within the Polish SIS and VIS Components is based on the solution proposed by the Portuguese government along with maintaining accordance with the European Commission's and Member States' program of building the SIS II and VIS systems (see: fig. 1). The Portuguese solution enabled new member states of the European Union, including Poland, to have access to SIS 1+ during their transition period, i.e. before the European Commission's initiation of the newer SIS II system that enables the entering and searching of entries of people and entities in the SIS database in the scope of Schengen Implementation Convention by authorized institutional personnel[3].

The exchange of information in SIS occurs through the medium of an updated Central SIS System of each member state that is connected to national SIS components with the help of a dedicated SISNET network. The national SIS copy[4] can also be a part of the national component. Data transferred from any member state are first transferred to the other member states belonging to the Schengen zone. This means that they are always in possession of the same set of acquired data in national copies, because the update of data in each national copy occurs on-line, which assures immediate data update and assures identical search results of every member states' system in the Schengen zone. The operation of the system is based on an automatic process of searching for data. This process can return one or two kinds of answers for a given query:

– The search in SIS generates a positive result; a hit, which means that the data searched can be found in the system,
– The search in SIS generates a negative result; a no hit, which means that the searched data in the system cannot be found.

In case of a hit, necessary actions are conducted that are foreseen for a specific type of hit. It can be, for example an arrest of a person or detaining a vehicle or documents, etc. If during a specific action it is necessary to attain, so-called supplementary information, then they are delivered by the SIRENE office. Such an event takes place in a situation when it is necessary to arrest somebody. In Poland, The National Police Headquarters is responsible for the operation of the SIRENE office and for the implementation of the Polish Central SIS and VIS Component Node (CW PK SIS and VIS).

[3] Poland was added to the paneuropean ongoing cooperation in the framework of the SISone4ALL system in September 2007.

[4] In order to increase the reliability of the implementation of PK SIS and VIS, the solution of using the national copy has also been adopted in Poland. Not all countries of the Schengen zone have applied their own national copies.

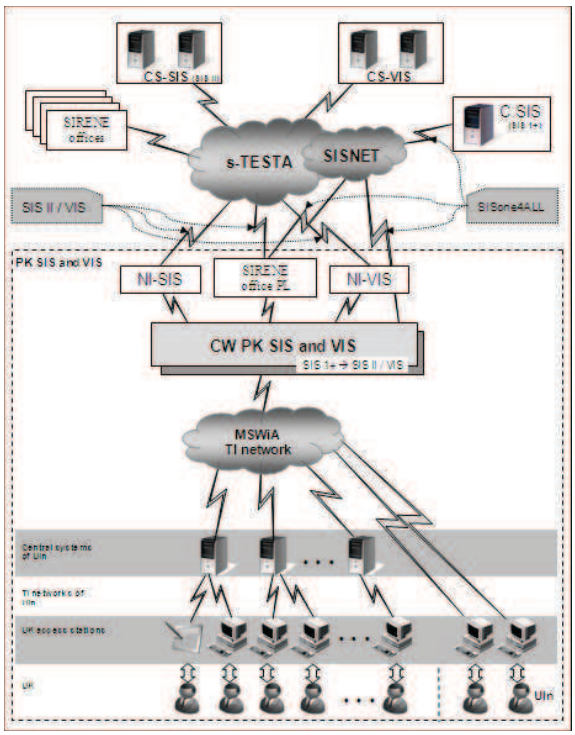

Fig. 1. Architecture of Polish Component of SIS/VIS

According to the scheme in figure 1, the following elements are distinguished in PK SIS and VIS:

- End users (UK) and individual users (UIn) that possess certain access rights bestowed by a instituational user to the SIS and VIS within the scope of possessed authority by law and using the access stations to the SIS and VIS,
- UK and UIn access stations allowing access to applications, including applications provided by CW PK SIS and VIS, allowing the entering of entries in the SIS and VIS, and making checks in the SIS and VIS,
- Data communication networks of institutional users as a medium of communication for secure data transmission between the UK and access stations UIn and central systems,
- Central systems, performing the functions of processing data falling within the competence of institutional users, including data for the purposes of the SIS and VIS as well as functions related to ensuring accountability, integrity and confidentiality of data, with particular attention to ensure the security of personal data,
- MSWiA (Ministry of Interior and Administration) data communication network[5] (MSWiA TI Network) performs functions of a secure communications medium for data transmitted between central systems, individual users, and CW PK SIS and VIS system as well as the SIRENE data communication office,
- CW PK SIS and VIS carries the functions of technical and organizational infrastructure, ensuring the flow of information between the C-SIS (in the future between the CS and CS-SIS-VIS using the NI-SIS and the NI-VIS), and central systems of institutional users and SIRENE data communication infrastructure office,
- SIS II and VIS national interfaces (NI-SIS, the NI-VIS[6]) enabling the integration of CW PK SIS and VIS with CS-SIS and with CS-VIS to cooperate with end-users of SIS II and VIS,
- Polish SIRENE Office (SIRENE PL Office) performing the functions as a contact point for matters relating to the practical use of the SIS, including those arising from the responsibility of validating data transferred to the C-SIS (in the future to the CS-SIS for SIS II) and associated with the transmission of supplementary data, required by the procedures for cases of positive checking results.

Each of the above-mentioned elements performs a specific role in the process of fulfilling the provisions of Title IV of CIS and in the future cooperation with VIS. The following are also important for the full functioning of the system:

- Member States in their respective areas of their SIRENE offices, as well as physical safety and maintenance of buildings, which copy is placed of the SIS as well as NI-SIS and NI-VIS[7],
- France in the scope of C.SIS and SISNET,
- European Commission in the scope of CS-SIS, CS-VIS, s-TESTA as well as NI-SIS and NI-VIS.

2.3. National context

The adoption of the Portuguese initiative regarding the construction of the SISone4ALL system, which allowed the new Member States to abolish checks at internal borders of the Schengen area on December 21, 2007, also

[5] Warsaw city SDH (Synchronized Digital Hierarchy) network, also known as the MSWiA teletransmission network.

[6] The abbreviation "NI" means: National Interface (Narodowy Interfejs).

[7] In the case of Poland the Chief Commissioner of Police is responsible for the mentioned elements of the system.

resulted in a new situation from a legal point of view. In order to assess the ability of formally launching the SISone4ALL in Poland, a detailed analysis of the legal order was carried out. As a result of this task a document was elaborated entitled: "Legal opinion on the formal and material conditions for adjusting the legal system of the Republic of Poland to participate in the Schengen Information System on the basis of the SISone4ALL concept and legislative action to ensure full implementation and compliance with European regulations in this subject." This document was prepared by the Legal Advisor of the European Programs Implementation Authority, acting close to the Ministry of Interior and Administration and providing legal, organizational and technical for the Plenipotentiary of the Government for SIS and VIS. The analysis demonstrated the lack of a complete legal basis for access and the transfer of information of all authorized government administration bodies to the SIS1+ system resources database through the SISone4ALL system. In the opinion of the Legal Adviser there was a need for a special law regulating the operation of the SISone4ALL system, while indicating that, the optimal regulatory from the point of view of preparing a comprehensive solution would be regulated by law in the functioning of elements of SISone4ALL (SIS1+), SIS II and VIS systems in Poland.

Therefore, on behalf of the Government Plenipotentiary for SIS and VIS a draft law on the participation of the Republic of Poland in the Schengen Information System and Visa Information System [5] was prepared in April 2007. The Act came into force in September 2007. On the basis of it the following institutions in Poland received access to the CW PK SIS and VIS:

- The Internal Security Agency,
- Foreign Intelligence Agency,
- The Government Protection Bureau,
- The Central Anticorruption Bureau,
- Inspector General for the Protection of Personal Data,
- Ministry of Finance (through Customs and tax control offices)
- Ministry of National Defence,
- Ministry of Interior and Administration (through the voivodes (governors), prefects (local authorities), SIS and VIS Office in the European Programs Implementation Authority)
- Ministry of Foreign Affairs (through the consulates)
- Ministry of Justice (through the public prosecutor's office and courts)
- Polish National Police,
- Military Intelligence Service,
- Counterintelligence Military Service,
- Border Guard,
- Head of the Office for Foreigners,
- Polish Military Police.

Moreover, the Act provides delegations to issue the following implementation regulations by the Ministry of Interior and Administration:

- On the making of SIS data entries and updating, deleting and searching the data by the SIS National Information System,
- On the detailed registering of cases, in which access to data or data were used in another way by the National Information System,
- On the mode of access to the National Information System,
- On the mode of handing over to the Police persons or entities found as a result of access to SIS data, as well as the responsibilities associated with the Police,
- On the entry card designs and exemplary query papers asking for data from the Schengen Information System and on the method of filling them out.

In parallel with the legislative work, based on the shared solution SISone4ALL by Portugal since February 2007 work was conducted for the construction of the SIS 1 + national component. It should be noted that the CW CK SIS and VIS is a result of the expansion of existing infrastructure hardware-software system for the National Criminal Information Center (KCIK[8], see Figure 2) and the independent implementation of hardware-software infra-structure for the SIS II and the VIS (see: Figure 3). Such a solution of CW CK SIS and VIS implementations, for both the SIS 1 +, and the SIS II, aimed at ensuring:

- A reliable point of access to SIS resources allowing the flow of information between the C-SIS (in the future, the CS-SIS), and central systems of the competent authorities,
- The flow of information between the telecommunication infrastructure of the SIRENE Office, and central systems of the competent authorities,
- Node sharing a dedicated software application that enables users to benefit

[8] In this case, physical and logical databases KCIK and SIS were separated.

from the SIS, directly without the participation of legitimate authority of the central system, to its access rights,
- The uniqueness of data entered into the SIS by authorized users,
- Full accountability of users' actions, including their authentication and authorization.

Communication between the central systems of institutional members and CW PK SIS and VIS is assured through by the Ministry of Interior and Administration's data communications network. This network was built with the mutual efforts of the Ministry of Interior and Administration and the Police in 2000-2001, it was also incorporated into the *Regional telecommunications network with integrated ISDN services,* Decision No. 121 of the Minister of Interior and Administration of 6 June 2002. Originally, a system based on the use of synchronous SMA terminal equipment made up the teletransmission platform for the simultaneously built digital commutation systems for the needs of the Ministry of Interior and Administration as well as the National Police Headquarters and the Metropolitan Police Headquarters. With the ongoing computerization process of the so-called Ministry of Interior and Administration group, new needs for data transmission arose. In connection with this, an IP subnet was launched, inter alia, on the SDH platform, providing the exchange of information between the administrations of the European Union, the so-called access point to the global network called the "Eurobramą" (Euro Gateway). To this end, throughput of main nodes forming a ring to the level of STM-16 (2.5 Gbit / s) was increased and other network nodes were built and launched. Presently, the Warsaw SDH teletransmission network includes 55 nodes, i.e. 350 E1 - 2 Mbit/s links and 40 Ethernet links. In the area of Warsaw, it is a platform for transmitting, in particular, the so-called TESTA network of national domain, on which other systems work, inter alia, the EURODAC system, AIM, CECIS, STAY, PASSPORT and EMERYT. Ultimately, the running of about 30 different applications is planned on the basis of this network, including, inter alia, the national components of the SIS 1 + as well as the SIS II and VIS, police and government commutation systems, PESEL-NET, CEPIK and many others. Warsaw SDH network is already a large urban network, and prospects for its growth reach more than 200 nodes in the area Warsaw. SDH Infrastructure was, moreover, included in a Ministry of Interior and Administration proposed so-called Department Data Communication Network (Resortowa Sieć Teleinformatyczna – RST) and the gradually implemented Public Administration Data Communication Network (in polish: Sieć Teleinformatyczna Administracji Publicznej – STAP[9]).

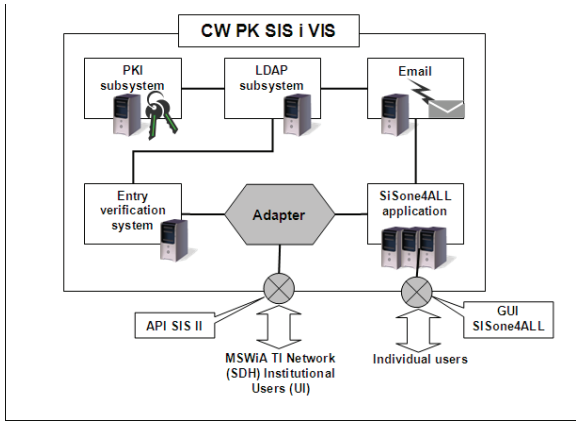

Fig. 2. CN architecture for the needs of the SIS 1+

At present, Police, in accordance with the already mentioned decision no. 121, are responsible for the operating and maintenance of the SDH network. The Ministry of Interior and Administration takes on the role of network administrator and manages the network of the national domain of the TESTA network. Currently under development, for the needs of SIS II and VIS as well as, are modernization works, which will ensure increased flowability between major nodes to the level of STM-64 (10 Gbit/s), as well as the acquisition of Ethernet ports scalability, redundancy at the level of connectivity and streams and traffic prioritization (Ethernet traffic). The possibility of sharing bandwidth channels in the streams will also be obtained. Given the continuous development of data communication systems of the public administration and the associated increase in demand for network resources, while simultaneously seeking to reduce costs of maintaining data communication networks of the Ministry of Interior and Administration, future plans include the modernizing the network to MPLS technology.

Returning to the SIS and VIS, the basic components of CW PK SIS and VIS that ensures cooperation with the C-SIS (see: Fig. 2) are:
- PKI subsystem authentication and authorization process, as well as controlling access to data and services,

[9] Assumptions for STAP have been accepted by the Council of Ministers on 25.01.2005.

- LDAP subsystem storing information on authorizations,
- E-mail for the SIRENE office,
- The Portuguese SISone4ALL application as a graphical user interface,
- Entry verification system, allowing the analysis of entry registration accuracy made in the system,
- Adapter carrying out two-way announcement translation services in SIS 1 + and SIS II formats.

In the concept of implementing the CW PK SIS and VIS for SIS 1 + it was assumed that, given the advanced technical and financial preparation, that has already been made by institutional users in Poland during the process of adapting their branch systems to cooperate with SIS II as well as the transitional nature of functioning of the Portuguese proposal, CW PK SIS must be made available to individual institutions that have built their branch systems in newer standards foreseen for SIS II and VIS. For this reason, in October 2006 the representative of government for SIS and VIS proposed the implementation of the so-called translator (otherwise: adapter, see: fig. 3), which ensures effective integration of the central node system with data communication systems of individual institutions. Implementing the adapter allows two-way translating of bulletins between SIS II and SIS 1+ formats. Using such a genuine EU-wide implementation solution helped avoid costly and time-consuming adapting of branch systems working in SIS II formats to the limited, when it comes to the period and scope of operation, SISone4ALL format, which is based on SIS I+ formats. SIS institutional users in Poland have already been obliged earlier to adapt their central systems to the technical requirements of SIS II. So, thanks to the translator, CW PK SIS did not have altered preparatory work schedules of individual institutions in Poland, which also significantly facilitated the future transition to the target version, i.e. SIS II and VIS, making it a big challenge in the near future.

To ensure collaboration with the CS and CS-SIS-VIS the basic components of CW PK SIS and VIS (see: Fig. 3), should include:

- Security subsystem using PKI technology to ensure transaction incontestability and the process of authentication and authorization, as well as controlling access to data and services, including implementing the functionality of the issuing of digital certificates and managing their life cycle,

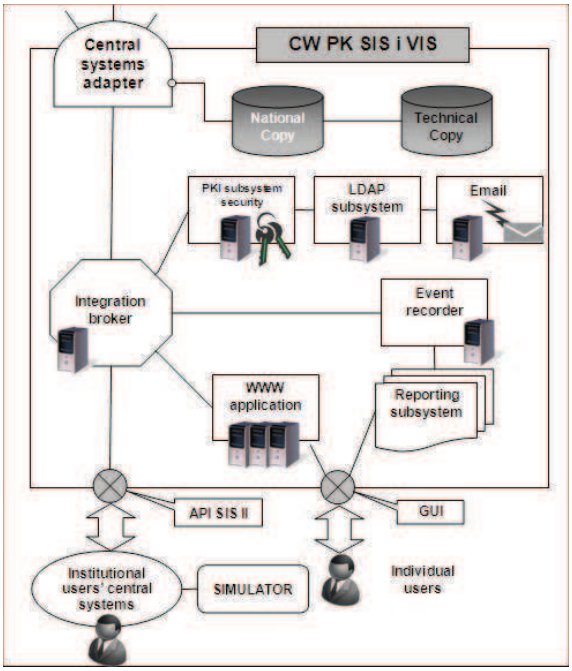

Fig. 3. CN architecture for the needs of the SIS II and VIS

- Subsystem LDAP storing information about entitlements,
- The integration broker, to ensure the implementation of business processes (the flow of data) in SOA technology,
- Central systems adapter, enabling CW PK SIS and VIS communication with CS-SIS and the CS-VIS (the so-called Steria Interconnecion Box),
- Web application, enabling interaction with SIS II and VIS for individual users,
- Reporting subsystem, which provides summaries and statistics on the functioning of the system,
- A national and technical copy providing local access to data stored in the CS-SIS,
- Operating database to ensure the functioning of the integration broker, web applications and reporting subsystem,
- E-mail subsystem, enabling CW PK SIS and VIS communication with institutional users via e-mail,
- Simulator, providing an alternative test bed for SIS II and VIS services.

2.4. Applied mechanisms of security

An important element, especially given the need to ensure compliance with the provisions governing the protection of personal data [6], in the area of action in the building of CW PK SIS and VIS, are the measures of protection, covering issues of incident and network management as well as physical, personal,

equipment and data security, and also security features[10] such as: accountability, accessibility and reliability, and data access control collected in SIS and VIS, and shared services.

Access from central systems of institutional users (SC UI) to the CW PK SIS and VIS is carried out through secure connections, using IPSec VPN technology in a SDH network. Bilateral authentication and authorization devices, taking part in conjunction occurs on the basis of digital certificates issued by the PKI system subsystem of CW PKP SIS and VIS.

Identity management, including the process of authentication and authorization of individual users, is based on a simplified model of "user name and password" in the case of implementing SIS 1+, and on the basis of a digital certificate in the case of SIS II and VIS. All messages exchanged between the individual and institutional users and CW PK SIS and VIS, are digitally signed and time marked, in accordance with the XAdES-T standard. For example, incoming messages from institutional and individual users of CW PK SIS and VIS are recorded and verified by checking the correctness and validity of digital signatures.

Given the temporary nature of the implementation of SIS 1+ and the planned replacement of this solution by SIS II for CW PK for SIS 1 + a centre-based technology cluster was built. Databases use the Oracle 10g engine in RAC mode. Application servers work in clusters based on JBoss technology, and access servers (proxy) work in Apache farms and load-balancing equipment. Network infrastructure is built on the basis of redundant equipment.

In accordance with the decision of the SIS and VIS Government Plenipotentiary on January 4th 2006 for CW PK SIS II and VIS two processing centres were launched. The primary centre is located in the resources of the National Police Headquarters, while the backup center in the resources of the Border Guard Command Headquarters. The backup centre acts as a backup, called the "Hot reserve system" and at anytime it can take the role of the main centre. Both centres in the layer of application servers work in an Active-Active mode, while the layer of database servers in an Active-Passive mode. Databases are run by the Oracle 10g engine in the RAC mode, and switching centers is done through HP ContinentalCluster. The data between centres are replicated on the EVA matrix level using ContinousAccess technology. Application Servers work in BEA WLS clusters or Oracle iAS, and access servers (proxy) work in the farm-based Apache technology and load-balancing equipment. Network infrastructure is built on the basis of redundant equipment in each centre. The centers are connected using DWDM technology by two independent optical fibre wires. Each of them have independent and redundant electrically powered lines and an adequate physical and electromagnetic security zone.

2.5. Poland's rated readiness to participate in SIS – results of SIS/SIRENE evaluation missions

Poland's readiness to participate in the SIS, including the Polish SIS 1+ Component data communication security, was the subject of an evaluation carried out on September 17-21, 2007 by representatives of EU member states, the General Secretariat of the EU Council and the European Commission. The positive outcome of the evaluation was approved at a meeting of the SCH- EVAL group on October 25, 2007. During the discussion on the results of the SIS/SIRENE evaluation in Poland it was stated that:

- The used data communication technologies are among the most modern,
- Integration of national systems with the Schengen Information System is great - thanks to which all available data is made available both in the SIS, as well as national systems in response to a query,
- Entering entries will be done through a data warehouse - a significant increase in the number of entries entered by Poland is noticeable every day,
- Poland has developed an original solution, which is a SIS1+/SIS II translator- thanks to which it is better prepared than other countries to migrate from first to second-generation SIS system, i.e. SIS II,
- The Border Guard application was very well-developed - a high level of user interface transparency,
- The dynamic approach on solving technical problems identified by the evaluation teams made a big impression - practical changes in the application functionality at the Police were entered the day during the evaluation.

[10] These mentioned security features are in accordance with the standard PN-I-02000: 2002 "Technika informatyczna" (Information Technology).

2.6. Information system national audit

The national SIS component, functioning under the National Information System, in accordance with Article 29, paragraph 2 of the Act from September 24, 2007 on the participation of the Republic of Poland in the Schengen Information System and Visa Information System, was subject to checks carried out by the minister responsible for interior affairs. The audit was carried out by experts from the European Programs Implementation Authority on January 04, 2008. This was after notification by the Chief Commissioner of Police of the readiness to launch the National Information System. The scope of inspections was related to NIS's compliance with requirements set out in Art. 92 paragraph 2 of the Schengen Implementation Convention. In particular, it was examined whether:

- NIS is compatible with the Central SIS System,
- NIS provides fast and efficient transfer of data from the central SIS in direct transmission mode (on-line), so that the file of the national data module (national copy) contains identical information,
- NIS provides data for the purpose of conducting an automatic search for authorized institutional users,
- Data available through NIS, which has been removed, will only be stored for the period stated in the regulations (one year - according to SIC, from one year to 3 years - according to [Council decision 2007/533/WSiSW]);
- Within the required period deleted data will be available only for consultation and for further verification of their accuracy and whether the data were entered legally,
- Data available through NIS after the expiry of this period will be destroyed,
- All cases are recorded, in which access to SIS data achieved for purposes of controlling whether the search is permissible, monitored, whether data processing is consistent with the law, for automatic monitoring and to ensure the proper functioning of N.SIS, as well as the data integrity and security,
- Records are kept containing the history entries, the date and time of data transfer, the data used for searching, a reference to data transferred as well as the name of the competent authority and the surname of the person responsible for processing the data.

It should be noted that the result of the aforesaid control showed that the National Information System meets the requirements set out in Article 92 paragraph 2 of the Schengen Implementation Convention.

3. Conclusion and directions of further work

Building the Schengen Information System and the Visa Information System was a major legal, technical and organizational undertaking. The price for the free flow of people, without border controls, was the need of collecting, processing and exchanging data on missing persons, wanted for questioning or detention as a witness, unwanted on the territory of the Schengen zone, as well as information on stolen or lost identity documents and weapons.

Such extensive data communication systems, which are without doubt the SIS and VIS, require an adequate implementation of appropriate legislative, organizational and technical measures in order to ensure a level of security agreed by Member States. Belonging to the standard of security services of confidentiality, integrity and availability they need to be fully implemented in all components of the SIS and VIS – both in central systems (C-SIS, the CS-SIS, the CS-VIS), as well as national components (N.SIS and N.VIS). When examining the priorities of implementing data communication security services of SIS and VIS, it can certainly be said that due to high demands for short-time response to a query to the SIS (recommendation – up to 5 seconds) and the requirement to maintain the quality of data entered into the system, implementing the availability of services is the most important and then integrity. Moreover, regulations for the protection of personal data in line with EU the directive applied by all Member States, impose a duty to protect the confidentiality of personal data processed – the service is performed in SIS at the level corresponding to the protection of classified information, which constitutes to official secrecy. This is so, because of, inter alia, the use of strong cryptographic mechanisms to encrypt transmitted data and user authentication and accountability.

The need for constant synchronization of data between the Central SIS System, which in May 2008 nearly 25 million entries were stored (and this number is gradually rising), and the national copies as well as the need to ensure uninterrupted access to the central database system in the case of countries, which do not

have a copy of the national SIS influenced the decision to build a separate SISNET communication network. For SIS II and VIS SISNET it will be replaced with dedicated sTESTA network subnets. Availability requirements of SIS II and VIS as well as sTESTA network were set at to the level of 99.95%.

According to the chronology of events, Poland gained access to the resources of the first generation Schengen Information System (SIS1+) on September 1st, 2007, since then, the exchange of information takes place both using the Portuguese SISone4ALL software, as well as through the SIS I+ <-> SIS II two-way communications translator created in Poland. With the implementation of the translator there weren't any interruptions during the process of preparing institutional users in Poland to participate in the SIS II, despite delays by the European Commission to start the SIS II, which was originally planned for September 2007. It is also worth mentioning that the translator significantly facilitated the migration of Poland from SIS1+ to SIS II, because it will only require a software update used in institutional users' systems, rather than developing an entirely new software[11]. For this reason, Poland has been highly rated for innovation and high-level of implemented national systems.

The participation of Poland in SIS and VIS will contribute positively to the level of citizens' safety and allow more effective cooperation between police forces and border guards in search of missing persons, wanted in connection with the European Arrest Warrant, the search for stolen items, the prevention of illegal emigration. The tasks related to the supervision of the functioning of the National Information System, whose main elements are components of the Polish SIS II and VIS will be carried out in accordance with the laws by:

- Minister of Interior and Administration, through the so-called SIS and VIS Office – in the technical supervision of the functioning of the National Information System, and in particular the availability of its resources for authorized institutional users,
- General Inspector for the Protection of Personal Data –protecting personal data processed in the National System of Science.

The entry of Poland into the Schengen zone on December 21, 2007 does not mean the end of the implementation of the Preparation of State Administration Bodies Programme to cooperate with the SIS and VIS. In 2008-2009, Poland must continue to work towards building national components of the Schengen Information System (SIS II) and building the Visa Information System (VIS) in the project coordinated by the European Commission. Many innovations were introduced into the design of the SIS II in comparison to the SIS 1+. These include the use of biometric data for facial photographs and fingerprint images and the so-called tying entries. It is to enhance the capabilities of the SIS reliability. Moreover, new categories of data will be introduced; the functionality and work ergonomics with the system will be enhanced. Launching the Visa Information System (VIS) will streamline the process for issuing and checking visas to enter the member countries of the Schengen zone[12]. The relevant authorities of the Member States will have a complete overview of all visa applications submitted for entering into the Schengen zone. The new functionality of SIS II will be available for use, among others, thanks to a change in the infra-structure of the network (from SISNET to sTESTA).

The continuation of the CW PK SIS II and VIS project will provide opportunities for collecting, processing and transmitting data using the electronic flow of information and decisions between the central SIS II (CS-SIS), a national copy of SIS II and the central VIS system, with central systems of institutional users and data communication infrastructure of the SIRENE office. Over 2,000 individual users and authorized operators registered in data communication systems of institutional users will be able to benefit from the services of CW PK SIS and VIS. This system will provide, as in the case of the implementation of CW PK SIS and VIS for the SIS 1+, uninterrupted service of 30 operations per second, 7 days a week, 24 hours a day, and timely responses from the standard query system will not exceed an average of 5 seconds.

The full success of these IT ventures can only be stated when the smooth migration of data communication systems will be conducted in Poland, which make up components of PK SIS and VIS of the current version of SISone4ALL working in SIS I+ technology to the target version of the Schengen zone systems,

[11] The other countries of the Schengen zone, which did not apply the concept of a translator like in the Polish model, have to take into account the need of developing completely new software.

[12] So-called "Schengen visas"

what are SIS II and VIS. In this case, the key is that in the years 2006-2007 conceptual and technological foundations were prepared in Poland for a relatively easy method of that migration, which is optimistic for the years 2009-2010, when we have already achieved full operational capability to work in the target version of the second generation Schengen Information System and the Visa Information System.

4. Bibliography

[1] Schengen Agreement of June 14, 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (with changes) (Journal of Laws UE.L.2000.239.13);
[2] Implementation Convention of June 19, 1990 to the Schengen Agreement;
[3] Guidelines for data security in connection with the Schengen systems - 6124/1/02 REV 1 SIS 10 COMIX 98 i 8946/02 SIS 32 COMIX 320,
[4] EU Schengen Catalogue, The General Secretariat of the Council of the European Union, 2002
[5] The Act dated June 24, 2007 on the participation of the Republic of Poland in the Schengen Information System and in the Visa Information System (Journal of Laws 2007.165.1170);
[6] The Act dated August 29, 1997 on the protection of personal data (Journal of Laws 2002.101.926)

[A] Grzegorz.Blizniuk@wat.edu.pl, Military University of Technology, Faculty of Cybernetics, Institute of Systems Engineering, Warsaw. In the years 2005-2007, Undersecretary of State in the Ministry of Interior and Administration and the Plenipotentiary of the Polish Government for SIS and VIS, and also responsible for Poland's IT preparation for accession into the Schengen zone.
[B] Robert.Kosla@microsoft.com, Defense Industry Manager, Public Sector, Microsoft Central and Eastern Europe HQ. Munich. In the years 2006-2008 Deputy Director of European Programs Implementation Authority, Head of the Office of the Government Plenipotentiary for SIS and VIS, responsible for handling the work of the Plenipotentiary of the Government and with current coordination of activities in the area of the SIS and VIS.
[C] A.Machnacz@policja.gov.pl, Director of IT Projects Centre in the Ministry of Interior and Administration. In the years 2005-2008 Director of Communications and Information Technology Bureau at the National Police Headquarters, Warsaw, responsible for implementing and operating the Polish Central Node SIS and VIS Component.