IDABC
European
eGovernment Services

Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications

NATIONAL PROFILE POLAND

April 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Jerzy Peja• , Andrzej Ruci• ski, Unizeto Technologies S.A.

Company's name: Siemens - Lawfort

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°1

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6485/5938

Executive summary

The objective of the project is to analyse the requirements in terms of interoperability of electronic signatures for different eGovernment applications and services taking into account the relevant provisions of Directive 1999/93/EC on a Community framework for electronic signatures and their national implementation as well as the report on the Directive and the standardisation activities on the interoperability of electronic signatures.

This document does represent the current Poland situation regarding the use of eSignatures in Polish eGovernment applications.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	**Purchase Order No. ENTR/05/58-SECURITY/SC1 Date: 08.11.2006**

1.2 Reference Documents

[RD1]	eGovernment in the European countries – 6th edition, September 2006 http://europa.eu.int/idabc/en/document/5094/254
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf
[RD8]	Act on Electronic Signature from September, 18th, 2001 (Law Diary - Dz.U. 2001 no 130, pos. 1450) http://isip.sejm.gov.pl/prawo/index.html
[RD9]	Act of 17 February 2005 on activity informatisation of entities performing public tasks (Law Diary - Dz. U. no 64, pos. 565, with amendments)

	http://isip.sejm.gov.pl/prawo/index.html
[RD10]	The Act on taxes for goods and services, from March, 11th, 2004 (Law Diary - Dz.U. 2004 no 54 pos. 535, with later amendments) http://isip.sejm.gov.pl/prawo/index.html
[RD11]	The Act on tax system, from August, 29th, 1997 (Low Diary - Dz.U. 2005 no 8 pos. 60) http://isip.sejm.gov.pl/prawo/index.html
[RD12]	The Act on Public Procurement, from January, 29th, 2004 (Law Diary - Dz.U. 2004 no 19 pos. 177) http://isip.sejm.gov.pl/prawo/index.html
[RD13]	Act on social insurance system (from October, 13th, 1998; Law Diary - Dz. U. 1998 no 137, pos.887 with later amendments) http://isip.sejm.gov.pl/prawo/index.html
[RD14]	Act on National development Plan (from April, 20th, 2004; Law Diary - Dz.U. 2004, no 116 pos.1206 and later amendments) http://isip.sejm.gov.pl/prawo/index.html

2 Glossary

2.1 Definitions

In the course of this Questionnaire, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

  It should be noted that for the purposes of this questionnaire, only services which rely on eSignatures are relevant, and that the focus is on eGovernment applications offered to citizens and businesses (A2C and A2B, rather than A2A).

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions. However, PKI solutions are the principal focus of this questionnaire, and non-PKI solutions should only be included if no PKI solutions are in common use. It should also be noted that the questionnaire only examines eGovernment applications in which the eSignature is used to sign a specific transaction, and not where the signature is merely used as a method of authentication of the eSignature holder as defined below.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

- *Secure electronic signature*[1]: an electronic signature[2] which:

  (a) it is uniquely linked to the signatory;

  (b) it is created using secure-signature-creation devices and signature-creation data that the signatory can maintain under his/her sole control;

[1] Act on Electronic Signature of September 18th, 2001 (Law Diary - Dz.U. 2001 no 130, pos. 1450)

[2] According to Polish Act on Electronic Signature ***an electronic signature*** *means data in electronic form which are attached to or logically associated with other electronic data and which serve to confirm the identity of the signatory.*

(c) it is linked to the data to which it has been attached, in such a manner that any subsequent change of the data is detectable;

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[3].
- *Authentication*: the corroboration of the claimed identity of an entity and a set of its observed attributes (i.e. the notion is used as a synonym of "entity authentication"). It should be noted that the questionnaire is focused on the use of eSignatures as a method of signing a transaction, and not on their use as a method for authenticating the eSignature holder.
- *Relying party*: any individual or organisation that acts in reliance on a certificate (in a PKI solution) or a eSignature.
- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

2.2 Acronyms

A2A	Administration to Administration
A2B	Administration to Businesses
A2C	Administration to Citizens
CRL	Certificate Revocation Lists
EID	Electronic Identity
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
SCVP	Simple Certificate Validation Protocol
SSCD	Secure Signature Creation Device
TTP	Trusted Third Party

[3] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

3 Introduction

3.1 eGovernment structure

Poland has a three-level structure of local government, with 16 regions or ‘voivodeships’, 315 counties or districts, and around 2,500 municipalities. Local government is carried out by councils elected every 4 years at every level. A regional Governor (Voivode) represents the government and the state administration in each voivodeship. Governors act as "supervisors" of regional government but real power belongs to elected assemblies and to their chairmen who are the regions' chief executives.

As the result of such hierarchical administrative structure the most of systems and services built for eGoverment purpose are also very hierarchized. Moreover, in the case of eGoverment systems in Poland there is a tendency to make information centralized during collection, storage and processing.. That information is transferred from the communities and districts level to the regional administration authorities (the ‘voivodeship’ level), then the direct transfer from the voivodeship level to central administration authorities (ministries, departments) occurs. In such a situation actually it is the typical „vertical” integration of services accessible in eGoverment systems, i.e. they are separately closed inside the particular administrative sectors both, at a central administration level, and at the ‘voivodeship’ level as well. Practically there are no intersector public administration systems, nor regional/local government ones. It means there is a lack of a vertical integration and the horizontal one as well.. Therefore the citizen (or an organisation) has no possibility to gather information from one access point. He is enforced to use many portals and access points.

3.2 eGovernment co-ordination on national level

In Poland the minister designated for IT implementation is that one who is responsible for the development of intersector A2C and A2B IT solutions (the case of horizontal integration), and the responsibility for sector-specific IT solutions (the case of vertical integration) is delegated to the minister of an appropriate government administration department.

So there is no institution at the national level which would be responsible for development of all IT systems with digital signatures usage. IT Department of Home Affairs Ministry (MSWiA) is responsible for intersector IT projects. Usually IT systems departments inside any particular ministry are responsible for sector-specific IT systems development and roll-out. For instance, Department of Teleinformation Infrastructure in MSWiA supervises any IT implementation dedicated for public administration needs, including so called „state registers”. Similarly, in Ministry of Finances all matters concerning services of electronic tax documents are managed by two different Departments: Dept. of IT Systems Maintenance and Dept. of IT Systems Development.

3.3 eGovernment co-ordination on regional and local level

There are no independent initiatives for mature and universal roll-out of eGovernment systems at regional and local levels. Mainly the stage of implementation is obtained by those which are stimulated by central administration authorities, The confirmation of thesis stated above are Gateways of Malopolska, Opole, Podlasie and Pomerania, which are the parts of wider “Wrota Polski” (*Gateway of Poland*) project (http://www.mswia.gov.pl/index.php?dzial=267&id=3897), and portals named ePUAP, which are also the part of general Gateway of Poland concept (http://www.e-puap.mswia.gov.pl).

Nevertheless, due to the lack of complete implementation of „Gateway of Poland”, ePUAP, and because of gaps in common teleinformatic infrastructure, local public and community administration offices develop local informative portals only. Mainly it is the way to obtain C2A communication, very rarely it becomes the implementation of A2C communication idea.

At the regional and local levels internet Public Information Bulletins (Biuletyny Informacji Publicznej - BIP)[4] are rapidly developed. BIP is intended to transfer to citizens via WWW services any information concerning the State (its structures, procedures, finances, properties, etc.). It is an information enterprise mainly. Public administration subjects differently treat the role of BIP. Nevertheless it is the important mean in contacts with public administration, especially then, when information made accessible via BIP does not concern administrative issues only, but represents matters searched by citizens frequently, e.g.: public transport time-tables, education, health services.

3.4 Programmes, projects, initiatives

The project „Wrota Polski" (*Gateway to Poland*) begun on December 2002. At the beginning it was coordinated by Ministry of Science and Information Society Technologies, currently it is led by Ministry of Home Affairs and Administration. The main purpose of Wrota Polski project is the creation of an integrated platform for the provision of public services online. For citizens and business companies it is the portal for services made accessible by public administration. On the other hand, for public administration organs it is some kind of information highway for A2B and A2C common services, and for internal A2A services as well.

This concept is based on the assumption that in each organisation front office operations must be connected with a number of back office operations, which customers do not see. 'Back-office' is a term related to the 'front office' (i.e. Internet portal, palmtop, mobile phone, etc.). The back office receives and processes the information which the user of a service enters in order to perform and deliver the desired service. This may be done manually, or with the use of information and communications technologies (ICT)[5].

The following subsystems of eGoverment infrastructure are planned:

- ePUAP: integrated information platform (central, regional and local portals) supporting the provision of electronic public services for administration, citizens and business (front-office),
- STAP: internal network of Polish Public Administration (back-office infrastructure for eGovernment systems data exchange, TESTA Network Local Domain, secure access to Internet),
- EWD-P: European Information (U32) workflow for Polish Administration (system intended to improve activities of polish civil servants participating in European Union legislation procedures; it will be achieved by provision of EU documents' management mechanisms and appropriate support for working out official polish opinions and instructions).

The idea of ePUAP infrastructure is to create interactive services based on users identification and authentication, and electronic signatures as well.

The ePUAP portals are implemented according to requirements of services oriented architecture (SOA)[6].

[4] Rules for BIP functionality are defined in the act on public information accessibility (from September, 6th, 2001; Law Diary - Dz.U. 2001, no 112, pos. 1198 with later amendments)

[5] Ministry of Science and Information Society Technologies *eGovernment Action Plan for 2005 – 2006*, September 2004

[6] In computing, the term **service-oriented architecture** (SOA) expresses a perspective of software architecture that defines the use of loosely coupled software services to support the requirements of the business processes and software users. In an SOA environment, resources on a network are

3.5 General situation of electronic signatures

The first national-wide implementation of electronic signature in Poland has been roll out in 1998 (*Social Insurance Organisation* - Zak•ad Ubezpiecze• Spo•ecznych ZUS). Nevertheless, even if in 2001 regulations of „electronic signature act" became valid, up to date (i.e. 2006, October) there is a lack of clear and consistent concepts concerning the usage of electronic signatures in A2C and A2B communication.

Currently there are three qualified Certification Authorities in Poland: Certum (www.certum.pl), Sigillum (www.sigillum.pl.com.pl) and Szafir (www.kir.com.pl). They issue unqualified public key certificates as well. There are also IT systems in different administration sectors, which make avalaible certifcation services for sector-specific eneterprises. The ministry of Home Affairs and Administration (MSWiA) could be an example. Its Certification and Cryptographic Card Generation Center (CCiGK - Centrum Certyfikacji i Generacji Kart Kryptograficznych) provides certification services for accessible (via public IT network, i.e. Internet) data and information gathered in Information System of Central Register of Vehicles and Drivers (System Informatyczny Centralnej Ewidencji Pojazdów i Kierowców - SI CEPiK).

There is any subject for coordination of electronic signature development, including the issues of standardization and interoperability; so there is no activity concerning signature formats, certificate profiles, CRLs, tokens (e.g.: time stamping), etc. Partially qualified certification authorities offer the provision of necessary solution.

3.6 A specific strategy, a national framework or a technical solution already in place with regard to electronic signature interoperability, either on a national or international level

The Regulation of Ministry Council from August, 7th, 2002concerning technical and organisational requirements for qualified certification authorities, certification policies for qualified certificates issued by them, and technical requirements for secure signature creation and verification devices (Low Diary – *Dziennik Ustaw* – from August, 12th, 2002) accepts three basic electronic signature formats:

- ETSI TS 101 733 - Electronic Signature Format,
- ETSI TS 101 903 - XML Advanced Electronic Signatures (XAdES),
- PKCS#7 Cryptographic Message Syntax Standard.

The usage of other electronic signature formats is allowed, but they have to be officially registered before (in such a case mandatory Object Identifier should be assigned to the particular format).

The document stated above defines time stamping token format as well, it should be compliant with ETSI TS 101 861 - Time Stamping Profile.

All three mentioned above electronic signature formats are used practically; in the case of PKCS#7 format some small deviation from the standard could be met.

Even of official statements there is no strategy in Poland to ensure complete interoperability of electronic signature formats at neither national, nor international level.

Furthermore, there is currently no central e-identification infrastructure in Poland. The development of a 'Multifunctional Personal Document' (MPD) which could be used as an intelligent, PKI-ready smart card to replace the current plastic ID card is being studied. The Ministry of Home Affairs and Administration is responsible for the MPD project.

made available as independent services that can be accessed without knowledge of their underlying platform implementation (http://en.wikipedia.org).

It makes hard to standardize the logical structure of PKI-ready smart cards used as cryptographic keys carriers (technical components) in creation and verification of electronic signatures. As the result the usage of technical components provided by different producers requires to install different drivers in IT systems used for PKI services.

There is no PKI development programme in Poland for public and government administration purposes. No role is defined for qualified certification authorities, even if they are accredited by an appropriate ministry and act according to requirements of „the Act on Electronic Signature". It is essential issue in the case of ePUAP project.

There are no plans for electronic signature development compliant with European Interoperability Framework (EIF), though these problems are mentioned in different official government documents (e.g.: Strategic plan for eGovernment development 2005 – 2006. work out by Ministry of Science and Informatisation).

Signature creation applications are embedded in national-wide IT systems, and at regional/local levels as well. However the solutions are independent and there is a lack of connections among them, so it is hardly to evaluate their interoperability features.

4 eGovernment and eSignature regulations

4.1 eSignatures regulatory framework

European Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures was transposed into Belgian legislation through:

- Act on Electronic Signature from September, 18th, 2001 (Law Diary - Dz.U. 2001 no 130, pos. 1450)
- Act on changes of rules concerning publication of normative acts, some another legislative acts and the act on electronic signature from July, 21th, 2006 (Law Diary - Dz.U. 2006 no 145 pos. 1050)
- The Regulation of Ministry Council from August, 7th, 2002 on technical and organisational requirements for qualified certification authorities, certification policies for qualified certificates issued by them, and technical requirements for secure signature creation and verification devices (Low Diary –Dz.U. 2002 no 128, pos. 1094).
- The Regulation on a template and detailed scope of application form for register entry concerning qualified certification authorities providing electronic signature certification services (Law Diary - Dz.U. 2002 no 128, pos. 1097).
- The Regulation on maintenance of register of qualified certification authorities providing electronic signature certification services, register entries specification and detailed procedures for an entry assignment (Law Diary - Dz.U. 2002 no 128, pos. 1099).
- The Regulation on a detailed procedure for creation and issuance of public key certificates for qualified certification authorities providing electronic signature services (Law Diary - Dz.U. 2002 no 128, pos. 1101).

The Act on Electronic Signature (from September, 18th, 2001) defines the term „secure electronic signature”. The definition states that secure electronic signature is advanced electronic signature, under the assumption that it is created using secure signature creation devices that the signatory can maintain under his sole control, and data for electronic signature creation. It is clearly visible from the polish “Act on Electronic Signature” that the role of *„means”* from EU „*advanced electronic signature*” definitions is taken by secure devices.

Issuance services of public key certificates and time stamps and other electronic signature services can be made accessible by any subject providing certification services or qualified certification authorities. The last mentioned category of subjects covers those, who provides certification services and has its entry in qualified certification authorities register.

In Art.58, paragraph .2 of The Act on Electronic Signature the obligation is enforced for organs of public authorities to enable the users of certification services to apply and communicate in an electronic form. Due date for this Regulation is stated as August, 16th, 2006. Unfortunately, this Regulation has been time-shifted to May, 1th, 2008 („Act on changes of rules concerning publication of normative acts, some another legislative acts and the act on electronic signature” from July, 21th, 2006). The official reason was claimed as improper stage of readiness reached by public administration to fulfil that obligation.

Nevertheless, electronic signature usage (in secure and qualified form[7]) has been stated in many law regulations. The examples are given below.

4.2 eGovernment regulatory framework

The usage of secure and qualified electronic signature is legally enabled for A2C, A2B and A2A communication. Basic legislative acts defining areas of the usage are as follows:

- The Act on informatisation of entities activities for public tasks performance (Law Diary - Dz.U. 2002 no 169 pos. 1385),
- The Act on taxes for goods and services, from March, 11th, 2004 (Law Diary - Dz.U. 2004 no 54 pos. 535, with later amendments),
- The Act on tax system, from August, 29th, 1997 (Low Diary - Dz.U. 2005 no 8 pos. 60),
- The Act on Public Procurement, from January, 29th, 2004 (Law Diary - Dz.U. 2004 no 19 pos. 177).

The first of acts stated above (the Act on informatisation) makes legally allowable:

(a) to address petitions and applications to public authorities in the form of an electronic document, including documents supplied with qualified electronic signatures,

(b) an electronic information exchange with public authorities confirmed by both communication parties with electronic signatures,

(c) a storage of archive electronic materials in state archives, taking into account the provision of their integrity and longterm validity,

(d) an electronic documents' transfer with data concerning ZUS (*Social Insurance Organisation*) insurance contribution payers, supplied with a qualified electronic signature by persons responsible for this,

(e) to publish normative acts and some other legislative acts in the form of electronic documents; the contents of an electronic document includes the confirmation of accordance with original and documents have to be supplied with secure electronic signature created by responsible signing entity.

The act on taxes for goods and services, from March, 11th, 2004, allows:

(a) to inform tax inspection authorities about an intention to use special VAT account settlement; this information should be supplied with a secure electronic signature verified with the usage of valid qualified certificate,

(b) invoicing and electronic transfer of invoices (as documents in an electronic form), their storage and presentation in the case of inspection performed by tax authority or tax control entity,

(c) to declare tax returns in an electronic form (in cases defined in paragraphs 1 and 2 i 8-11;the structure of tax returns is determined with respect to their security, credibility, nonrepudiation, inviolability and time stamping.

(d) VAT payers registration, including electronic application for registration and its revision, and declaration concerning the end of taxable activities,

[7] A qualified electronic signature is a secure electronic signature which requires the usage of qualified certifcate for proper verification

(e) to declare summary information and its corrigendum in an electronic form, with respect to their security, credibility, nonrepudiation, inviolability and time stamping.

The act on the tax system, from August, 29th, 1997, standardises tax obligations, tax information, tax procedures, tax inspection and control procedures, tax confidence. Particularly the following is stated:

(a) it is possible to make tax returns[8] via electronic communication means, supplied with electronic signatures; the Regulation of Minister of Finances on logical structure of tax returns, the way of transfer and the types of electronic signature they should be supplied with, from September, 11th, 2006, (Low Diary - Dz.U. 2006 no 168 pos. 1197) defines two legally accepted formats of qualified electronic signatures used: ETSI TS 101 903 - XML Advanced Electronic Signatures (XAdES) and PKCS#7 Cryptographic Message Syntax Standard,

(b) taxpayers can notify the head of Inland Revenue Service about the intention to perform tax returns via electronic means; notifications can be in the form of an electronic document supplied with a qualified electronic signature (the regulation of Minister of Finances on logical structure of tax returns, the way of transfer and the types of electronic signature they should be supplied with, from September, 11th, 2006, (Low Diary - Dz.U. 2006 no 168 pos. 1196),

(c) tax authorities can transfer the letters to taxpayers in the electronic form.

Quite new revision of the act on the tax system, from July, 13th, 2006 (Law Diary - Dz. U. from August, 10th , 2006 no 143 pos. 1031) cancels the obligation to make tax returns via electronic means, what was predicted earlier. The reason was claimed as unproper stage of readiness reached by inland revenue service systems to fulfil requirements of the act. Until the end of 2006 only those entities are allowed to send tax return information via electronic means, whose yearly netto incomes exceed the equivalence of 5 millions Euro.

The Act on Public Procurement, from January, 29th, 2004, allows to use an electronic signature in following cases:

(a) applying for participation in auction procedures,

(b) electronic tendering,

(c) electronic auction,

(d) procedures performed for establishment and order granting of dynamic procurement system.

Regulations presented above mean that currently it is possible to use electronic signatures in systems built up for public administration purposes (i.e. secure and qualified electronic signatures) for electronic invoicing, tax returns, petitions and applications transfer (e.g. by means of electronic delivery boxes), law regulations publication via Internet and electronic communication with public administration authorities. Additionally, the Regulation of Ministry of National Education and Sport Ministry on study documentation, from July, 18th, 2005, (Law Diary - Dz.U. 2005 no 149, pos. 1233) allows to issue electronic student cards. Identification data and validity period stored in card non-volatile memory are electronically signed using a qualified electronic signature.

An electronic signature will be also used by institutions supervised by Ministry of Justice. Proposed regulations changes concern:

- National Court Register (it will be allowed to apply via electronic means; applications will have to be supplied with electronic signatures verified with the usage of valid qualified certificate),
- Code of Civil Procedures (it will be possible to apply to register courts via electronic means, the same way will be allowed for court statements and acts delivery; in all the cases a

[8] There are lists and informations to notify which tax encashment personnel and taxpayers are obliged due to tax regulations.

qualified electronic signature is the basis; Code revision assumes the possibility to create notarial certifications and their copies, and send them to the courts via electronic means if these electronic documents are supplied with electronic signatures verified with the usage of valid qualified certificate),

- the Act on registered pledges and a pledge register (involved parties will be legally able to communicate electronically; that regulation will cover all type of information exchanged between entities and pledge register departments in regional courts and the central pledge register information office).

Nevertheless, everyday practice is far from conveniences offered due to mentioned above regulations. *IT reconstruction in public administration has begun from crucial decisions to delay some very important matters: – an introduction of electronic signatures to public administration, law regulations publishing via Internet and an electronic form of tax returns and dedarations. Official Government explanation of this delay was: appropriate offices have not been ready to fulfil duties stated in law regulations, only the one from every ten subjects have been able to introduce e-signature on time, i.e.: on August, 16th*[9].

4.2.1 Electronic identity card (e-ID)

An additional factor delaying seriously development of public administration IT systems is the lack of national electronic identity document (eID). Appropriate works are continued in Ministry of Home Affairs and Administration, but it is hard to predict the end even approximately. Probably public key certificates for the purpose of eID issuance will be issued by a newly established special Government Certification Authority. To delegate this role to commercial qualified certification authorities is another solution taken into account. The first solution would result in splitting of national CA network into few separate networks: existing qualified CA infrastructure (under the root supervised by Ministry of Economy) one or more CAs subject to Ministry of Home Affairs and Administration.

4.2.2 Commercial CA certificates

Qualified and unqualified certification authorities issue electronic identifiers to individual persons (they are not the same as eIDs mentioned in 4.2.1, and issued by appropriate public administration organs). Usually these identifiers are Integrated Circuit Cards with cryptocontroller and private cryptographic keys and public key certificates installed inside (obligatory solution used by qualified CAs) or software based tokens (cryptographic keys and certificates stored outside ICC's cryptographic modules). For eGoverment systems and applications mainly identifiers with qualified public key certificates are used (called "technical components in law regulations). Electronic signatures verified with unqualified certificates are used rather rarely. The scope of their usage is mainly limited to message authentication and authentication of servers, workstations and other IT equipment.

ICCs with different origin are issued by qualified CAs as technical components:

(a) Certum (www.certum.pl) - Philips Smart Card Controller P8WE5032V0G and operating system STARCOS SPK 2.3 v7.0 with Digital Signature Application v2.2 of Giesecke&Devrient

(b) Sigillum (www.sigillum.pl.com.pl) - operating system SetCos 4.4.1 with signature application SetEID v1.0 of Setec

(c) Szafir (www.kir.com.pl) - SetCos 4.4.1 with signature application SetEID v1.0 of Setec.

[9] Citation after „Rzeczpospolita" (no 249, 24.10.2006); *Unia daje pieni• dze, a informatyzacja stoi (EU gives money, but informatisation do not go forward)*

Another hardware and software platforms are offered as technical components by unqualified CAs. New auctions organised by public administration result in tenders with new technical solutions for technical components (contact and contactless0, including JavaCards. In such a situation no producer has preliminary advantage; on the other hand, it is serious barrier for creation of a consistent infrastructure for electronic identifiers services.

Let us notice that commercial electronic IDs disable unambiguous assignment of a unique identifier to the person – every CA has its own policy for electronic ID configuration. It is the main reason why they cannot be used as national electronic IDs[10].

The logical data structures of certificates are different also. There is no one national profile for certificates and CRLs. It is the fact that acceptable profiles are defined in an annex to the Regulation of Ministry Council from August, 7th, 2002 on technical and organisational requirements for qualfied certification authorities, certification policies for qualified certificates issued by them, and technical requirements for secure signature creation and verification devices (Low Diary – Dz.U. 2002 no 128, pos. 1094), but they are not sufficiently precise to enforce an uniform solution. Relatively good situation is in the case of qualified certificate. Fortunately, qualified CAs has agreed common rules for certificates issuance and contents interpretation.

There are two ICCs profiles in Poland:

(a) PKCS #15 Conformance Profile Specification,

(b) Unizeto Techologies S.A. Profile.

The first of them has been designed and registered by RSA Laboratories. It can be used for electronic signature creation in trusted environment, i.e. when it is not necessary to confirm an authenticity of technical components and/or signature creation systems/applications. Generally, this type of profile enables to create secure electronic signature in unpublic environment (e.g. the home or the office, where the individual or the company has direct control of the signature creation system).

In the case of public environment, especially if systems are distributed architectonically, an obligatory establishment of secure path and secure channel between technical component and signature creation application is required (see: regulations to the Act on Electronic Signature; see also: CWA 14170 *Security requirements for signature creation applications*). Unizeto Techologies S.A. Profile is compliant with requirements defined in CWA 14890-1 *Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements*. Consequently, it meets requirements of national law regulations and CWA 14170.

Three types of software interfaces are used for technical components (for signature creation process, and for component's data structure management as well):

- Microsoft Crypto API for application working under control of Microsoft Windows NT and Microsoft Windows XP,
- PKCS#11 (v2.11 or v2.20),
- proprietary interfaces at APDU level.

For Microsoft® standard applications, a so-called Cryptographic Service Provider (CSP) is created that implements the cryptographic operations from the smartcard. An application calls this implementation through a standard interface called Crypto API. CSP modules are provided by smart card producers and other companies involved in development of systems/applications using ICCs for cryptographic operations (electronic signature creation, data enciphering, etc.).

[10] It is possible to introduce subscriber's PESEL number or NIP number into a qualified certificate, but it is not obligatory – no such a numbers in certificates with subscriber's pseudonym.

The PKCS#11 interface is typically used in non-Microsoft applications, usually working under control of Unix-like operating systems. Custom applications can also make use of this interface instead of the Crypto API interface to develop applications working under control of Microsoft Windows NT and Microsoft Windows XP.

Some providers, e.g. Unizeto Technologies S.A., offer their own software libraries supporting smart cards and cryptographic mechanisms. Libraries are not free of charge and usually are dedicated for specific smart cards families provided by all qualified CAs.

Therefore there is no standard for smart card interface in Poland. Solution details are not published by commercial PKI services providers, or by government administration. However all producers provide software interfaces supporting CSP and PKCS#11 standards.

Public key certificates (usually stored in non-volatile memories of smart cards) can be issued by qualified and unqualified CAs providing certification services.

Unqualified CAs (e.g. www.certum.pl, www.sigillum.pl, Szafir - www.kir.com.pl, http://www.signet.pl, EuroPKI Polish Certification Authority - http://www.europki.pl, WTF Alfa - http://ca.alfatv.pl, EnergoCert - http://www.energocert.pl) create independent hierarchical CAs networks, each one with independent and separate root. Therefore it is hard to build trustworthy solution for users with certificates issued by different CAs. Currently only the one from polish acting CAs (www.certum.pl) has certification of compliance with WebTrust requirements and its root's certificate is embedded in following browsers: MS Internet Explorer, Opera, Mozilla, ThunderBird, Konqueror, TheBat!, Softerra and Netscape.

Qualified CAs providing certification services (Certum, Sigillum and Szafir) act in National Certification Center hierarchical structure (NCCert, http://www.nccert.pl); it consists of one root and three subject CAs mentioned above.

Certificates issued by qualified and unqualified CAs follow the X509v3 standard. It should be noticed that in the case of qualified certificate an attribute "serial number" in the field "subject" is set on the PESEL and/or NIP value (see below), assigned to the citizen by public administration before.

4.2.3 National register numbers

Every polish citizen is provided obligatory with two distinctive identifiers: PESEL number (an acronym from Powszechny Elektroniczny System Ewidencji Ludno•ci – General Electronic System for Citizens Evidence) and NIP (Numer Identyfikacji Podatkowej - *Tax Identification Number*).

PESEL number is assigned by ministry appropriate for public administration matters in the way of material-technical act. The legal foundation for PESEL numbers assignment is the Act on citizens evidence and identity documents, from April, 10th, 1974 (Art.46). Local public authorities are obliged to maintain citizens evidence in the form of communities evidence registers (Law Diary - Dz. U. z 2001,r. no 87 pos. 960 and later amendments).

PESEL number is assigned to:

(a) polish citizens with status of permanent stay or temporary stay within time period greater than 2 months, and applicants for issuance of an identity document as well,

(b) foreigners with status of permanent stay or temporary stay within time period greater than 2 months,

(c) polish citizens and foreigners who are covered by social or health insurance in Poland, excluding persons stated in pts. (a) and (b),

(d) polish citizens living abroad and applying for polish passport issuance.

PESEL numbers are stored in PESEL registers. PESEL numbers are not unique (incidents occurred in the past when different have been assigned to the same PESEL number). Among others it was the reason why MSWiA has started PESEL2 project for a new public registers implementation.

Tax Identification Number (NIP) is used for entities paying taxes in Poland. It is assigned by tax authorities according to regulations stated in the act on taxpayers evidence and identification form October, 13th, 1995 (uniform text: Law Diary - Dz. U. 2004, no 269, pos. 2681).

Obligatory evidence is relevant for individuals and legally registered entities; it concerns also other subjects who are obliged to pay taxes on the basis of separate law regulations. It includes the cases when the beneficent is Treasury and local communities as well. Additionally the evidence is obligatory for social and health insurance contribution payers.

NIP assignment is performed on the way of administrative decision, which the head of appropriate tax authority is responsible for.

With regard to the use of electronic signatures in eGovernment applications, the national registry numbers PESEL and NIP are particularly relevant because they can be used as the unique identifier in the certificate of the e-ID card (but not in commercial CA certificates). Furthermore, the national registry number PESEL and NIP can be also envisaged to become the identifiers to be used in the future for all back-office information exchanges in eGovernment applications regarding all persons who hold such a number.

Providers of applications based on national registry number are only allowed to use the national register number in certain cases upon authorisation from a sector committee, which is a subdivision of the General Inspector for the Protection of Personal Data (GIODO). Only certain categories of authorities and instances qualify for this permission. Nevertheless, regulation can determine the cases in which no authorisation is required. This is for instance the case for the exchange of information between institutions of social security.

Because the national registry number is included in the signature certificate (see above) compliance with the strict provisions on the use of this number become problematic. Therefore solutions are being proposed to encrypt the national registry number by means of a one-way function. This should solve possible conflicts between the validation of a certificate and the legal restrictions on the use of the national number.

5 eGovernment applications using electronic signatures

For an extensive list of eGovernment applications, we refer to the list in section 10. In the section below we will comment only the most significant eGovernment applications and the manner in which they rely on electronic signatures.

5.1 Public procurement

5.1.1 Application identification

The rules for public procurement are laid down in the Act of 29 January 2004 on public procurement (Law Diary - Dz.U. 2004 no 19 pos. 177). That act is adopted to requirements of Directives 2004/17/EC of and 2004/18/EC of 31 March 2004.

There are at least three procurement platforms in Poland (all founded on the basis of the act mentioned about):

– Polish Procurement Platform (PPP), managed by Polish Securities Manufactory S.A. (Polska Wytwórnia Papierów Warto•ciowych S.A.) in Warsaw, www.ppp.pwpw.pl

– Electronic Procurement Platform e-przetarg.pl (EPP), managed by SOLDEA Company, www.e-przetarg.pl

– Electronic Procurements (PE) managed by eTender Polska Company Ltd., www.etender.pl.

Existing platforms allow to provide electronically the following services:

(a) an electronic tendering (including applying for a permit to participate in auction/procurement procedures, questions and answers session, submission and opening of proposals), which can be used as a mechanism of a supplier choosing or allowing them to participate in an electronic auction (PPP, EPP and PE platforms),

(b) a leading of electronic auctions based on reverse electronic auctions; selected and tested suplliers log in to the system and as an answer for an opening bid more and more lower prices, down to the minimal benefit level accepted by them; Purchasers and suppliers have the possibility to observe the course of auction and current tenders in real time; it makes their competitiveness much greater (PPP, EPP and PE)

(c) a leading of electronic auctions using the forms published on an appropriate website; those forms allow to entry all necessary data during direct connection to the website; subsequent better tenders declared by suppliers are automatically classified (PPP and EPP platforms),

(d) catalogue purchases optimize purchasing processes in an organization due to the built-in electronic documentation circulation system; this service is based on a collection of information on goods and services offered by suppliers, which are taking part in the virtual market focused around the Polish Procurement Platform (only PPP).

Note: The act on public procurement precises the terms „licytacja" and „aukcja"; they have the same equivalent in english language – an auction; the first case ("licytacja") concerns self-reliant procedure to place orders for strictly defined goods and services; the second one is associated with possible finalizing of some classic procedures (unlimited auctions, limited auctions, negotiations with publishing).

Electronic auctions are performed on the basis of electronic communication between the purchaser and the supplier. Valid tenders are claimed in the electronical form, and are supplied with secure electronic signature verified with a valid qualified certificate.

The scope of services provided currently by electronic procurement platforms do not cover all procurement services which are obtainable via electronic means; e.g.: services concerning electronic invoicing or electronic payment are outside of that scope.

5.1.2 eSignature details

5.1.2.1 Legal aspects

Electronic procurement platforms PPP, EPP and PE act on the basis of the act on public procurement, from January, 29th, 2004, the newest revision of which became valid on May, 25th, 2006.

In the revision of stated above act some novelties, concerning the usage of electronic means by public administration and business, have been introduced. Among others, a self-reliant auction ("licytacja") and new forms of finalizing of classic procurement (unlimited auctions, limited auctions, negotiations with publishing) (art. 91a) and so called „dynamic purchase system" (art. 102 - 109) have been allowed legally.

According to the act it is allowed to use electronic means (it concerns orders and contractors as well) to send declarations, notifications and information in procurement procedures. It also defines the cases when transferred data have to be supplied with a qualified electronic signature (i.e.: secure electronic signature verified with a qualified certificate).

5.1.2.2 Technical aspects

Polish Procurement Platform (PPP) enables to use secure signature creation devices for the purpose of qualified electronic signatures for subscribers of all three qualified certification authorities in Poland, i.e.: Certum, Sigillum and Szafir. Therefore none of qualified certificates issuer is discriminated, nor customers of stated above CAs.

Electronic Procurement Platform e-przetarg.pl (EPP) accepts and operates with secure signature creation devices provided by Unizeto Technologies S.A. (i.e.: Certum - qualified CA providing certification services), but it is possible to use the components offered by other qualified certificates issuers. There is no detailed information concerning Electronic Procurement platform (PE).

Communication between the users of procurement platforms and IT platform's systems is performed via standard WWW viewers. It is the reason why Internet Explorer communicates with smart cards using Cryptographic Service Provider (CSP) interface to enable a qualified electronic signature creation; for Netscape viewers PKCS#11 interface with Firefox is used.

WWW servers of all procurement platforms have certificates which allow to authenticate them and to establish cryptographically secure channel between the server and a user workstation; for both purposes SSL protocol is used.

5.1.2.3 Organisational aspects

Every procurement platform user has to be registered before the activity beginning; the unique identifier and the password should be assigned to them as well.

5.1.3 Interoperability

Electronic signatures are accepted only in particular procurement platform environment. Additionally, PPP platform provides qualified signature services for secure signature creation devices produced or delivered by all qualified CAs (Certum, Sigillum and Szafir).

5.1.4 Miscellaneous

From 2004 till November, 16th, 2006, Polish Procurement Platform (PPP) has organised about 170 electronic auctions, and Electronic Procurement Platform e-przetarg.pl (EPP) – over 90.

All platforms belong to A2B applications.

5.1.5 Assessment

All procurement platforms should allow to use any secure signature creation device compliant with the Act on Electronic Signature (from September, 18th, 2001) and associated regulations. This compliance should be confirmed by the compliance statement.

The customers of given procurement platform can participate in auctions managed by the others, but only in the case when they are registered users of this platform.

5.2 Public registers

The consequence of rules of the Act on activity informatisation of entities performing public tasks (from February, 17th, 2005, Law Diary - Dz. U. no 64, pos. 565, with amendments) are requirements concerning the obligation to ensure an access to information gathered in public registers via electronic means (this access should be enabled by public entities); another claimed issue is the possibility to exchange documents resulting from proceeding the matters from the scope of public entities activity; it should be obtainable with the usage of electronic data carriers and communication means.

One of the first public registers made accessible via electronic means is e-GIODO register; it is managed by General Inspector of Personal Data Protection (G•ówny Inspektor Ochrony Danych Osobowych) and enables bidirectional data transfer – to and from the register. Other public registers are just now at the design or concept creation stage (e.g.: PESEL[11], KEP[12], TERYT[13], KRS[14], REGON[15], EGIB[16] registers).

Public registers are registered by State Registry for IT Systems and Public Registers (Krajowa Ewidencja Systemów Teleinformatycznych i Rejestrów Publicznych - KESTiRP). Public Administration IT Enterprises Knowledge Management System (System Zarz•dzania Wiedz• o Przedsi•wzi•ciach Informatycznych w Administracji Publicznej - SZWPI) has been established for that purpose. SZWPI portal (https://szwpi.mswia.gov.pl) allows to apply for KESTiRP entry according to the regulation on KESTiRP maintenance and data exchange (issued by Ministry of Science and Informatisation).

[11] *Common Electronic Population Evidence System (Powszechny Elektroniczny System Ewidencji Ludno•ci)*

[12] *National Taxpayers Evidence (Krajowa Ewidencja Podatników)*

[13] *national Official Teritorial Division Register (Urz•dowy Rejestr Podzia•u Terytorialnego Kraju)*

[14] *National Judicial Register (Krajowy Rejestr S•dowy)*

[15] *National Official Register for State Economy Entities (Krajowy Urz•dowy Rejestr Podmiotów Gospodarki Narodowej)*

[16] *Ground and Buildings Evidence (Ewidencja Gruntów i Budynków)*

5.2.1 Personal data bases register

All answers to the questionnaire can be found at section 10.1.

5.2.1.1 Application identification

In the scope of General Inspector of Personal Data Protection is maintenance personal databases register and to inform about registered data bases (the Act on personal data protection, from August, 29th, 1997; Law Diary - Dz. U. 2002 no 101 pos. 926). Those registers are public and subject to requirements stated in the act on informatisation of entities activities for public tasks performance (Law Diary - Dz.U. 2002 no 169 pos. 1385). To fulfil that obligation, General Inspector of Personal Data Protection has established IT system named *Electronic Platform for Communication with* General *Inspector of Personal Data Protection (Elektroniczna platforma komunikacji z Generalnym Inspektorem Ochrony Danych Osobowych - e-GIODO)*.

e-GIODO has been developed due to EU Programme *„Sector Operational Programme for Enterprises Competitivness Growth 2004-2006"*. It is developed as the part of 1.5 activity stream of that programme, intended to develop an on-line system for contractors allowing an access to information and public services.

e-GIODO provides interactive communication with the Office of General Inspector of Personal Data Protection and allows:

(a) remote overview of Personal Data Bases Register contents, including the functionality of advanced search,

(b) interactive filling of an application form concerning personal data bases registration,

(c) signing of an application with qualified electronic signature by owners of qualified certificates, and signed application transfer to GIODO via electronic means.

5.2.1.2 eSignature details

5.2.1.2.1 Legal aspects

It is the obligation of a personal data base administrator to notify General Inspector of Personal Data Protection a personal database for registration. The notification should be compliant with the Regulation on a template of personal data base registration form, issued by Minister of Home Affairs and Administration on April, 29th, 2004 (Law Diary - Dz. U. 2004 no 100, pos. 1025), and a personal data base administrator's handwritten signature is required.

It is possible, on the basis of the act on activity informatisation of entities performing public tasks (from February, 17th, 2005, Law Diary - Dz. U. no 64, pos. 565, with amendments, art.14, clause 3), to notify personal data bases for registration purposes via electronic means. In such a case the notification should be supplied with a qualified electronic signature, and the signer is a personal data base administrator. That qualified electronic signature should be compliant with requirements of the act on electronic signature from September, 18th, 2001.

5.2.1.2.2 Technical aspects

Personal data base administrators, using the form presented in WWW service (http://egiodo.giodo.gov.pl), prepare the notification concerning personal data base for General Inspector of Personal Data Protection. Any errors and mistakes are signalized according with embedded verification rules.

The proper document in XML format is generated on the basis of input data. It is written into the file, and then (as a file) signed with the usage of a secure signature creation device provided by the one of acting qualified certification authorities (Certum - General Certification Authority - Unizeto Technologies SA, Szafir - National Clearing House C.o. or Sigillum - Polish Center of Electronic Certification).

Finally two files are sent to General Inspector of Personal Data Protection: one of them includes the notification contents, the value of a qualified electronic signature is placed in the second one.

WWW-server of e-GIODO system has a public key certificate, it enables to authenticate the server and to establish a cryptographic channel between the server and the user workstation. Authentication and cryptographic channel establishment are made on the base of SSL protocol.

5.2.1.2.3 Organisational aspects

e-GIODO is used directly by General Inspector for Personal Data Protection (as the recipient of signed data) and Personal Data controllers (as entities filling and signing application forms).

Indirect system users are three qualified certification authorities mentioned above. CAs provide signature creation devices and participate in qualified electronic signatures verification (it concerns subscribers with certificates issued by appropriate CA). In that case General Inspector for Personal Data Protection is a relying party.

5.2.1.3 Interoperability

The only one recipient of notification concerning personal databases is General Inspector for Personal Data Protection. Therefore interoperability is maintained due to the fact, that all electronic signatures in the system are created with the usage of secure signature creation devices provided by qualified CAs (Certum, Sigillum and Szafir).

5.2.1.4 Miscellaneous

In spite of XML format of notification files contents, XAdES format is not used for qualified electronic signatures creation.

e-GIODO system belongs to A2A, A2B and A2C application classes.

5.2.1.5 Assessment

e-GIODO system is convenient and fast form of personal data bases notification, and their modification as well. Notified personal databases are stored in the public register and are made accessible for all users who are interested in (if other rules do not exclude this possibility).

5.2.2 Central Register of Vehicles and Drivers - CEPiK

5.2.2.1 Application identification

Central Register of Vehicles and Drivers (Centralna Ewidencja Pojazdów i Kierowców- CEPiK) is an IT system with a central data base gathering any data and information about vehicles, their owners and persons authorized to drive.

The register is maintained in an IT system established on the basis of the Act on traffic rules, form June, 20th, 1997 (Law Diary - Dz. U. 2003 no 58, pos. 515, and later amendments). The act obliges Minister responsible for public administration to establish Central Register of Vehicles and Drivers (CEPiK). Functionality rules for CEPiK were defined by Minister of Home Affairs and Administration in the regulation on a central vehicles register (from September, 19th, 2001; Law Diary - Dz. U. 2001 no 106, pos. 1166) and in the regulation on registration fees (from June, 6th, 2005; Law Diary - Dz. U. 2005 no 103, pos. 870).

The following is stated in regulations mentioned above:

(a) the procedures for register maintenance,

(b) conditions and procedures for cooperation of entities sending the data and information to the register,

(c) the type of registered data and information, which can be made accessible,

(d) the value of payment for an access to registered data and information, and conditions for payment.

The following data and information are registered (among others): vehicle type, vehicle registration number, vehicle owner, incidents (e.g.: theft of vehicle and its recovery, chassis and body number striking, an assignment, a loss and finding of a registration book, registration plates, temporary permission, temporary registration plates, an arrestment of registration books or temporary permissions, a date of next technical inspection), a date of obligatory public liability policy contract.

Only authorized users can access CEPiK register, e.g.: police, military police, insurance agents, custom officers, border guard, municipal and community guards, court executive officers, governors.

5.2.2.2 eSignature details

5.2.2.2.1 Legal aspects

On the basis of the Regulation on a central vehicles register issued by Minister of Home Affairs and Administration (from September, 19th, 2001; Law Diary - Dz. U. 2001 no 106, pos. 1166) it is possible to transmit the data to CEPiK register in the form of an electronic document via computer networks.

5.2.2.2.2 Technical aspects

CEPiK register works with central data bases to which information is supplied by governors, police, military police, border guard, courts, public prosecutor's office, municipal and community guards, tax control authorities, custom offices, tax intelligence personnel.

The users communicate with CEPiK register using dedicated applications, allowing to prepare, sign and send to CEPiK IT system appropriate petition, request or query. Queries and answers can be also transferred via CEPiK internet portal (http://www.cepik.gov.pl).

Requests, queries and answers are enciphered.

Every authorized user of CEPiK system has to own a public key certificate issued by Certification and Cryptographic Card Generation Center (CCiGK - Centrum Certyfikacji i Generacji Kart Kryptograficznych), the part of CEPiK IT system. Keys are stored on smart cards, and a private key is unaccessible outside the card. Up to date, i.e.: until 2006 November) acceptance tests have been performed with cryptographic cards delivered by three providers:

(a) ENIGMA Information Protection Systems Co. Ltd. (Systemy Ochrony Informacji Sp. z o.o);

(b) UNICARD S.A.;

(c) UNIZETO Technologies S.A.

Certificates are used during an establishment of secure, mutually authenticated and enciphered channel (on the base of TLS protocol) and for verification of electronic signatures created by CEPiK system users and linked with messages/documents.

In the case of electronic signatures used in CEPiK system there is no need to be compliant with requirements of the act on electronic signature (from September, 18th, 2002). It is only required that private key carriers (integrated circuit(s) cards) have to be certified at least at ITSEC E3 High level.

5.2.2.2.3 Organisational aspects

Ministry of Home Affairs and Administration is responsible for CEPiK IT system management. "Voivodeship" IT centers are peripheral components of CEPiK IT system; they play a role of intermediates enabling an access to any information gathered in the system.

Signed information is transmitted only towards CEPiK system and authenticated information is transmitted to system users.

Especially for the purpose of CEPiK system Certification and Cryptographic Card Generation Center (CCiGK) has been established. This Center issues public key certificates on request of authorized users. The rules of certificate issuance are defined in Certification Policy for external entities using CEPiK IT system via public network[17].

CCiGK subscribers can be only physical persons providing goods and/or services individually, legal entities, public administration authorities or organisations without legal personality, which have an access to CEPiK system via CEPiK Internet Portal on the basis of law regulations.

End users certificates are issued for 2-years periods and can be used as follows:

(a) certificates for electronic signatures verification; these signatures are linked to requests and queries send to CEPiK system,

(b) certificates for data transmission protection in communication between Subscriber's communication server and CEPiK system,

(c) certificates for identification of users connecting to CEPiK system.

Certificates can be revoked and suspended (e.g.: in the case of private key compromising) by Subscriber or an authorized system representative (the head of Central Register of Vehicles and Drivers Department in Ministry of Home Affairs and Administration or the person appointed by him for that purpose).

5.2.3 Interoperability

CEPiK IT system is closed, i.e.: accessible for authorized users only. Electronic communiaction, including electronic signatures, are used only for the purpose of CEPiK system.

5.2.4 Miscellaneous

CEPiK system belongs to A2A, A2B and A2C application classes.

5.2.4.1 Assessment

CEPIK system is an example of public register providing services for public administration, business and citizens. It should bring legally valid electronic signatures (i.e.: compliant with the act on electronic signature from September, 18th, 2001) into general use and cover services provided by qualified and unqualified certification authorities. Establishment of closed certification systems will make an integration with another government administration systems harder in the future.

5.3 Social security

The polish social security sector was pioneer with the introduction of secure signatures for eGovernment applications. At the beginning of 1999 Social Insurance Organisation (Zak•ad

[17] See: http://www.cepik.gov.pl/portal/plik/Polityka%20certyfikacji%20v.1.3.pdf?id=75

Ubezpiecze• Spo•ecznych - ZUS) enabled the payers of social insurance fees to transmit insurance documents and declarations via electronic means.

All answers to the questionnaire can be found at section **Error! Reference source not found.**.

5.3.1 Electronic Transfer of Insurance Documents (EPDU)

5.3.1.1 Application identification

Design and implementation of EPDU system (*Elektroniczny Przekaz Dokumentów Ubezpieczeniowych – Electronic Transfer of Insurance Documents*) has been possible on the basis of the Act on social insurance system (from October, 13th, 1998; Law Diary - Dz. U. 1998 no 137, pos.887 with later amendments). That act allowed the payers to transmit insurance documents via electronic means.

EPDU system is the part of Complex Information System (Kompleksowy System Informatyczny ZUS - KSI ZUS).

Insurance documents are transmitted using „the Payer" („P•atnik") application or via three internet access points:

(a) https://www.sdwi.gdansk.zus.pl

(b) https://www.sdwi.warszawa.zus.pl

(c) https://www.sdwi.wroclaw.zus.pl

„The Payer" application is free of charge and can be downloaded from http://www.platnik.info.pl.

5.3.1.2 eSignature details

5.3.1.2.1 Legal aspects

Article 46 of the Act on social insurance system (from October, 13th, 1998; Law Diary - Dz. U. 1998 no 137, pos.887 with later amendments) states that payment declarations, submitted by payers monthly, have to include handwritten or electronic signature of the payer. Additionally (art. 47a, clause 2a), it makes obligatory to sign insurance documents electronically. It concerns applications for social insurance, nominative monthly reports defined in art. 41 clause 3, payment declarations defined in art. 46 clause 4, and other documents necessary for accounting and corrigenda; the signature has to be a secure electronic signature verified with the usage of a valid qualified public key certificate (according to the act on electronic signature, from September, 18th, 2001. That signature should be created by the person responsible for the transfer of those documents to ZUS.

Currently this requirements are neither met by payers, nor by ZUS itself. It is the result of revision of article 58, clause 2 (the act on electronic signature); due date for public authorities to enable all kinds of data exchange with them via electronic means has been shifted to May, 1st, 2008. It is the reason why (up to date) insurance documents are signed with the usage of electronic signatures not compliant with mentioned about act.

Cryptographic keys for an electronic signature creation are stored on floppy discs, USB memories, CDs, etc. It requires to download the private key to workstation operational memory and for signing purpose every time the signature is created.

Public key certificates, used for electronic signatures verification, are issued for payers (legal personalities or other).

5.3.1.2.2 Technical aspects

Public key certificates are issued by CA established only for that application; it is CERTUM for ZUS (http://www.cc.unet.pl).

System *Electronic Transfer of Insurance Documents* (EPDU) accepts only certificates issued by CA CERTUM for ZUS.

The payer, „equipped" with the private key and the certificate issued by CERTUM for ZUS, using „the Payer" application, prepares the collection of documents concerning insured persons and then signs it (the Signer is an authorised person), encrypts and sends to ZUS. As an answer ZUS replies with an electronic confirmation of delivery.

EPDU system accepts certificates from different certification services providers, including qualified CAs.

An electronic signature format is compliant with PKCS#1.

5.3.1.2.3 Organisational aspects

Social Insurance Organisation (ZUS) is responsible for management of EPDU system. Based on the relevant contract between ZUS and Unizeto Technologies S.A. (http://www.unizeto.pl), the second of mentioned parties is responsible for CA CERTUM for ZUS functionality.

Rules and procedures accepted by CA CERTUM for ZUS are described in "Certification Policy for CERTUM for ZUS services" (ver. 4.3) and „Code of Certification Practice for CERTUM for ZUS services" (ver. 4.3).

End users certificates are issued for 1 year period of validity. End users (subscribers) are for instance: insurance fees payers, Open Retirement Funds (Otwarte Fundusze Emerytalne – OFE) and other external entities, ZUS organisational units, communication servers for data exchange between payers and ZUS. ZUS is the sponsor of all issued certificates.

ZUS is the recipient of all signed documents and it sends electronically signed confirmation of delivery in every case. Confirmations are addressed to payers or authorized legal entities. ZUS can also send to the payer signed information concerning inexactitudes found in delivered documents. All electronic signatures are verified inside certification domain CERTUM for ZUS.

5.3.1.3 Interoperability

EPDU system is closed and limited to the known users supported by „the Payer" application. Signatures, formatted according to PKCS#1, should be recognized by their systems.

Currently the system does not allow to use certificates issued by another CAs, including the qualified ones.

5.3.1.4 Miscellaneous

EPDU system belongs to A2A and A2B application classes.

5.3.1.5 Assessment

EPDU system is the only one in Poland using electronic signatures and electronic data transfer so widely. Currently there are ca. 200 000 users (the estimation based on the number of active certificates issued by CA CERTUM for ZUS).

It is highly probable that at the due date of the obligation to sign documents for ZUS with qualified electronic signature EPDU system will accept certificates issued by other CAs. That fact could be important for meaningful growth of interest in the usage of qualified signature in Poland.

5.3.2 Financial Support Service System (SOD)

5.3.2.1 Application identification

Financial Support Service System (System Obs•ugi Dofinasowa• - SOD) is used by employers to apply electronically for financial support in the case of disabled workers salaries and to report account settlements monthly as well. Applications and reports are transmitted to the State Fund for Disabled persons Rehabilitation (Pa• stwowy Fundusz Rehabilitacji Osób Niepe•nosprawnych - PFRON).

The legal basis for it is Article 26c, clause 2, of the act on professional and social rehabilitation, and disabled persons employment (from August, 27th, 1997; Law Diary - Dz.U. 1997 no 123 pos. 776). An employer who wants to exchange documents electronically, should be registered in SOD system, and is obliged obtain a qualified or an unqualified public key certificate and a private key for the purpose of electronic signatures creation.

5.3.2.2 eSignature details

5.3.2.2.1 Legal aspects

Applications and reports concerning financial support of disabled persons salaries send from employers to PFRON in the electronic form have to be supplied with electronic signatures. It results from Article 9, clause 1, of the regulation on financial support of disabled persons salaries, issued by Minister of Economy, Employment and Social Policy (from December, 30th, 2003; Law Diary - Dz.U. 2003 no 232 pos. 2330). Qualified and unqualified signatures are allowed in this case.

5.3.2.2.2 Technical aspects

Qualified public key certificates used in SOD system are issued by qualified CAs providing certification services in Poland. Unqualified public key certificates are issued by a specially established internal CA of PFRON. Rules the last mentioned CA acts according to, are not publicly known.

A user of SOD system has to prepare an electronic document firstly (it is made in off-line mode using Java applet downloaded free of charge from http://www.pfron.org.pl/zwi/zwi.nsf/graph?OpenFrameset), and transmits it on-line using appropriate website (https://www.sod.pfron.org.pl).

An electronic signature is created using off-line SOD Java applet. That applet also enables to generate key pairs and to prepare request for an unqualified certificate issuance.

5.3.2.2.3 Organisational aspects

Qualified certificates are issued according to certification policies and Certificate Procedure Statement (CPS) approved by the minister relevant to informatisation. Those certificates are issued outside SOD system. The rules of unqualified certificates issuance are unknown.

Certificates are issued for employers of disabled persons applying for financial support of salaries. PFRON is the relying party and the one who verifies and accepts electronic signatures.

5.3.2.3 Interoperability

SOD system is closed and accessible only for employers acting on the territory of Poland.

System does not allow to serve certificates issued by other commercial unqualified CAs (it concerns certificates issued abroad as well).

5.3.2.4 Miscellaneous

There is a lack of data concerning a current number of SOD system users.

5.3.2.5 Assessment

SOD system supports all activities which can be managed with the usage of electronic documents. There is a lack of basic information about the way the documents are signed. Therefore it is hard to perform relevant assessment.

5.3.3 e-PFRON system

5.3.3.1 Application identification

e-PFRON is intended to accept payment declarations and information concerning an employment, an education and activities for disabled persons benefit. It is the obligation of those employers, who are obliged to pay for PFRON account.

e-PFRON system allows to serve documents compliant with templates published in the regulation on a declarations templates establishment for the purpose data exchange between PFRON Head Office and employers obliged to do it (Minister of Economy, Employment and Social Policy; from June, 6th, 2003; Law Diary - Dz.U. 2003 no 105 pos. 989), (Dz. U. Nr 105, poz. 989), and in the regulation on monthly and yearly reports templates establishment for information concerning an employment, an education and activities for disabled persons benefit (Minister of Economy, Employment and Social Policy; from May, 29th, 2003; Law Diary - Dz. U. no 104, pos. 969).

e-PFRON fulfils requirements defined in Article 49, clause 2, of the act on professional and social rehabilitation, and disabled persons employment (from August, 27th, 1997; Law Diary - Dz.U. 1997 no 123 pos. 776, with later amendments), and allows employers to prepare and to send documents in the electronic form via electronic means.

5.3.3.2 eSignature details

5.3.3.2.1 Legal aspects

Declarations and information submitted by obliged employers to PFRON have to be supplied with electronic signatures. There is no relevant regulation indicating such an obligation. However this requirement is compliant with conditions defined in Article 58, clause 2, of the act on electronic signature (from September, 18th, 2001) where the obligation for public administration authorities is stated to allow recipients of certification services to petition and to apply in the electronic form whenever law regulations require to prepare applications and petitions in the relevant form or according to defined templates.

5.3.3.2.2 Technical aspects

e-PFRON system consists of two parts: e-PFRON OffLine local application and http://www.pfron.org.pl/zwi/zwi.nsf/WWW/AC7E10357EC3E04FC1256EAC00381624?OpenDocumente-PFRON OnLine internet applicationhttp://www.pfron.org.pl/zwi/zwi.nsf/WWW/F10A420A0DC296B3C1256EAC003886B3?OpenDocument. Such a division allows to separate time-consuming preparation of documents from the act of data transmission itself. It minimizes the time required for internet connection.

e-PFRON OffLine application allows e.g.: documents' preparation and signing. It is made accessible free of charge in PFRON Office in Warsaw and in all Fund Departments. It can be also downloaded from Information Service (http://www.e-pfron.pl). Using that application it is possible to generate key pair and to prepare a request for an unqualified public key certificate issuance. e-PFRON OffLine allows an authorized person to transmit this request to the internal CA. CA issues those certificates with two years period of validity.

e-PFRON OnLine allows documents transfer, electronic correspondence reception, downloading of archival documents and reports. An application is obtainable at: https://www.e-pfron.pl.

5.3.3.2.3 Organisational aspects

The rules of unqualified certificates issuance are unknown.

Certificates are issued for employers of disabled persons applying for financial support of salaries. PFRON is the relying party and the one who verifies and accepts electronic signatures.

The rules of unqualified certificates issuance are unknown.

5.3.3.3 Interoperability

Certificates created in e-PFRON system can be used only for communication with PFRON. A system is not prepared for an acceptance of certificates issued by commercial entities providing certification services.

5.3.3.4 Miscellaneous

There is a lack of data concerning a current number of e-PFRON system users. It has been design to serve 60 000 users (there is a number of employers in Poland, who are obliged to fulfil requirements mentioned in 5.3.3.1).

5.3.3.5 Assessment

There is a lack of basic information about the way the documents are signed and the signatures format as well. Therefore it is hard to perform relevant assessment of system security.

5.4 Tax

On the basis of the Act on Electronic Signature (from September, 18th, 2001; art. 58, clause 2), the act on taxes for goods and services (from March, 11th, 2004; art. 99, clause 16) and the act on tax system (from March, 29th, 1997; art. 3a) companies and individuals should transmit tax returns via electronic means.

Ministry of Finances has decided to establish **e-podatki** (**e-tax**) system to enable taxpayers fulfil stated above requirements. An electronic system for taxpayers service **e-podatki** (**e-tax**) is one of the strategic enterprises in the scope of Ministry of Finances activity. The goal is to improve citizens tax service and to implement new quality in tax authorities functionality, similarly to solutions implemented in many others EU countries (e.g. in Belgium).

The project e-Deklaracje (e-declarations) is developed as the part of the wider e-podatki (e-tax) project. European funds from European Fund for Regional Development are involved (1.5 activity stream of EU Programm „*Sector Operational Programm for Enterprises Competitivness Growth*). The main task of the project is to create the system for direct electronic communication between external entities and tax administration. It should cover electronic data exchange for all documents stated in relevant law regulations. It is planned to start the system at the beginning of 2008.

From August, 16th, 2006, Ministry of Finances made accessible for some taxpayers the solution named „e-poltax system". It is some kind of temporary solution, intended to revise and verify functional, legal and organisational requirements, and then to select a final solution for e-Deklaracje (e-declarations) project.

5.4.1 e-poltax system

5.4.1.1 Application identification

e-poltax system is intended to enable fulfilment of requirements stated in the act on tax system (from March, 29th, 1997, with later amendments). It allows tax administration to manage electronic documents, i.e.: reception and service of tax returns and other tax related documents in an electronic form.

e-poltax system is set up as an internet service, accessible at https://e-poltax.mf.gov.pl. There are three functional components:

(a) an application for electronic documents exchange with Inland Revenue Service,

(b) an off-line application enabling to sign and to send electronic tax returns to Inland Revenue Service,

(c) an electronic documents schemes repository.

The usage of the system is allowed for those entities whose yearly netto incomes exceed the equivalence of 5 millions Euro. Those entities (about 7 500) can use the system according to "the rule of good will". Other companies will wait until 2008 year, when complete rollout of e-Deklaracje system is planned.

Polish Securities Manufactory S.A. (Polska Wytwórnia Papierów Warto•ciowych S.A.) is the producer of the basic version of e-poltax system.

From August, 16th, 2006, e-poltax system enables the transfer of fourteenth forms, e.g. PIT-4 (for employee paying in earnest income tax for his employees monthly) and PIT 8-A (declaration concerning income tax in a lump). Subsequent forms will be obtainable according to the time schedule accepted by Ministry of Finances.

5.4.1.2 eSignature details

Electronic documents (declarations and petitions) sent to e-poltax system have to be supplied with a secure electronic signature verified with a first category valid qualified certificate. According to the annex 2 of the regulation on technical and organisational requirements for qualified certification authorities, certification policies for qualified certificates issued by them, and technical requirements for secure signature creation and verification devices (from August, 7th, 2002, Low Diary –Dz.U. 2002 no 128, pos. 1094), first category qualified certificate consists at least the following attributes: the name of state, surname and name (names), serial number (certificate owner's NIP or PESEL number).

e-poltax system requires a secure electronic signature (verified with a valid qualified certificate issued by the qualified CA, i.e.: Certum, Sigillum or Szafir) for every petition or declaration.

Signature formats are compliant with the act on electronic signature (from September, 18th, 2001).

5.4.1.2.1 Legal aspects

Allowed formats of qualified electronic signatures used in e-poltax system for signing tax returns or notifications by taxpayers are defined in the Regulation of Minister of Finances on logical structure of tax returns, the way of transfer and the types of electronic signature they should be supplied with (from September, 11th, 2006; Low Diary - Dz.U. 2006 no 168 pos. 1197) in the regulation of Minister of Finances on logical structure of tax returns, the way of transfer and the types of electronic signature they should be supplied with (from September, 11th, 2006; Low Diary - Dz.U. 2006 no 168 pos. 1196) appropriately.

Those regulations indicate two electronic signature formats:

(a) ETSI TS 101 903 - XML Advanced Electronic Signatures (XAdES),

(b) PKCS#7 Cryptographic Message Syntax Standard.

Both formats are accepted in e-poltax system.

5.4.1.2.2 Technical aspects

Tax declarations and notifications can be submitted by the means of:

1. a website accessible via internet viewer at https://e-poltax.mf.gov.pl; any submission should be preceded by a completion of the form published on that website and XML document signing,

2. an application installed locally at the user's client workstation; it can be downloaded from https://e-poltax.mf.gov.pl; HTTPS protocol is used for transmission;

3. web-service accessible at https://e-poltax.mf.gov.pl.

In cases 1 and 2 e-poltax system includes components enabling to create a qualified signature in XAdES format; certificates issued by any qualified CA are accepted. The content of document is located in ds:Object element.

In case 3 it is assumed that document supplied with a secure qualified electronic signature is created according to PKCS#7 standard.

In cases 1 and 2, the authorized person responsible for e-declaration submission should be equipped with a qualified certificate, a cryptographic card and appropriate interface device.

In case 3 the user should additionally install a relevant application for signatures creation or relevant software components.

e-poltax system is the second one in administration (the first one was GIIF system) where qualified certificates, issued by qualified CAs (providing certification services on the basis of the act on electronic signature from September, 18th, 2001) are accepted. Those CAs provide technical components (IICs) and interface devices.

5.4.1.2.3 Organisational aspects

Only registered users can use e-poltax system. For that purpose a user submits the notification concerning the intention of declaration submission via electronic means to the relevant Inland Revenue Service. This intention has to be confirmed by signed electronically notification via https://e-poltax.mf.gov.pl portal. The last can be done only by owners of qualified certificates issued by qualified CA providing certification services in Poland.

5.4.1.3 Interoperability

As explained above, there are only three recognised commercial CA certificate issuers. Interoperability with other certificates is not being examined at this stage.

5.4.1.4 Miscellaneous

e-poltax system belongs to A2B applications. 242 entities (from about 7 500 having netto incomes exceeding 5 millions Euro) claimed the will to use electronic means for purpose of accounting with tax authorities (the situation on November, 23th, 2006).

5.4.1.5 Assessment

e-poltax system development works are continued and mainly they are focused on an extension of the accepted electronic documents set (declarations, notifications concerning VAT and CIT). nevertheless it is temporary solution and will be replaced by e-declarations system in 2008.

5.5 Finance

5.5.1 Data transfer to General Inspector of Financial Information (SI GIIF)

5.5.1.1 Application identification

The Act on counteraction against introduction of illegal assets (with illegal or unknown origin) into a finance turn and terrorism financial support (from November, 16th, 2000; Law Diary - Dz.U. 2000 no 116 pos. 1216) enforces many entities to report monthly all transactions exceeding 15 000 Euro. Due date is July, 1st, 2004, and reports have to be sent to General Inspector of Financial Information (Generalny Inspektor Informacji Finansowej - GIIF). GIIF is the special authority designated for gathering and analysing the data concerning suspected financial transactions.

IT system for General Inspector of Financial Information (SI GIIF) allows, according to art. 11 of mentioned above act, to transmit via electronic means the data concerning financial transactions by institutions obliged to do it. Transmitted data have to be supplied with a secure electronic signature.

The obligation to inform GIIF about any transaction with amount exceeding 15 000 Euro, or transactions suspected to be illegal/hidden originated, concerns many so called **obliged institutions**. There are for instance: banks, brokers, entities managing bets and lotteries, insurance offices, investment funds and notary offices.

5.5.1.2 eSignature details

5.5.1.2.1 Legal aspects

Electronic data formats required for communication with GIIF are defined in the revised Regulation of Minister of Finances on the template of transaction register, the procedures of transaction register maintenance and the way of registered data transfer to GIIF (from May, 20th, 2003; Law Diary - Dz.U. 2003 no 101 pos. 935). Clause 1 of this regulation states that data transmitted in the electronic form have to be supplied with a secure electronic signature (in the meaning of the act on electronic signature, from September, 18th, 2001). This signature is created by the person designated for obligations defined in the act from November 16th, 2000 (Law Diary - Dz.U. 2000 no 116 pos. 1216).

It should be noticed that the signature does not need to be a qualified electronic signature, but has to be created with the usage of a secure signature creation device. The format of an electronic signature is compliant with the regulation of Ministry Council from August, 7th, 2002 on technical and organisational requirements for qualified certification authorities, certification policies for qualified certificates issued by them, and technical requirements for secure signature creation and verification devices (Low Diary – Dz.U. 2002 no 128, pos. 1094). In practice, it means compliance of that format with qualified signature formats supported by CAs providing certification services.

5.5.1.2.2 Technical aspects

Electronic data transfer to GIIF is possible using GIIF website (https://www.giif.mofnet.gov.pl/giif/), allowing obliged institutions to perform all formalities related to data exchange with General Inspector of Financial Information. The transfer is possible after a successful login procedure. It can be done by these, and only these obliged institutions, which have a qualified certificate issued by the one of three qualified CAs providing certification services according to rules stated in the act on electronic signature, from September 18th, 2001.

GIIF IT system accepts certificates with categories I and II, according to the regulation of Ministry Council from August, 7th, 2002 on technical and organisational requirements for qualified certification authorities, certification policies for qualified certificates issued by them, and technical requirements for secure signature creation and verification devices (Low Diary – Dz.U. 2002 no 128, pos. 1094).

To send reports to GIIF it is necessary to be equipped with so called „secure signature creation set". The components of such set are: a qualified certificate, a cryptographic card (a technical component) and an interface device (a card reader/writer). It enables to create qualified electronic signatures.

5.5.1.2.3 Organisational aspects

Qualified certificates and secure signature creation devices are provided by qualified CAs providing certification services. They act according to the act on electronic signature (from September, 18th, 2001; Law Diary - Dz. U. 2001, no 130, pos. 1450 and later amendments) and procedures defined in Certificate Practice Statement.

An authorized person from the obliged institution, equipped with a qualified certificate and a secure signature creation device, signs the data and transfers them to GIIF via appropriate website mentioned above.

5.5.1.3 Interoperability

GIIF IT system is only used by obliged institutions and General Inspector of Financial Information. Therefore the system ensures operational compatibility at the level of qualified CAs Subscribers and at the signature formats verification level. However the system does not allow any data exchange with other systems currently.

5.5.1.4 Miscellaneous

GIIF IT system belongs to B2A application class.

5.5.1.5 Assessment

The users of GIIF IT system use qualified certificates and secure signature creation devices provided by all three qualified CAs. Even if the regulation of Minister of Finances (from May, 20th, 2003; Law Diary - Dz.U. 2003 no 101 pos. 935) does not enforce the usage of a qualified signature, implemented solution enables to use the system interfaces by all of entities who have or will have qualified certificates. Another advantage is the uniform user interface.

5.5.2 SIMIK system

5.5.2.1 Application identification

Information System for Monitoring and Financial Inspection of Structural Funds and Integrity Fund (Informatyczny System Monitorowania i Kontroli Finansowej Funduszy Strukturalnych i Funduszu Spójno•ci - SIMIK) is the tool for management, monitoring, inspection and implementation assessment of sector operational programs and regional operational programs financed partially from UE funds.

The system allows to monitor and to manage projects from the moment the application is submitted. It gathers any information necessary to perform assessment works, monitors inspection activities and enables to monitor every fund and programme individually. SIMIK system is coordinated and implemented by Department for Supporting Funds Service in Ministry of Finances.

The legal foundations of the system are:

(a) the Act on National development Plan (from April, 20th, 2004; Law Diary - Dz.U. 2004, no 116 pos.1206 and later amendments),

(b) Directive 1999/1260/EC of 21 June 1999 laying down general provisions on the Structural Funds

(c) Directive 2001/438/EC of 2 March 2001 laying down detailed rules for the implementation of Council Regulation (EC) no 1260/1999 as regards the management and control systems for assistance granted under the Structural Funds,

(d) Directive 2002/1386/EC of 29 July 2002 laying down detailed rules for the implementation of Council Regulation (EC) No 1164/94 as regards the management and control systems for assistance granted from the Cohesion Fund and the procedure for making financial corrections.

Regulations mentioned above allow to transfer electronically the data concerning realization of projects financed from EU structural funds. Institutions relevant for given operational programme are recipients of those data.

SIMIK system consists of three decentralized applications: Application Generator, Application Verifier and Payment Request Generator. Electronic signatures are used only in the case of Application Verifier. Documents generated by Application Generator and Payment Request Generator are not signed.

Application Verifier is used when there is no direct communication between an institution directly involved in structural funds usage (the one responsible for application reception and formal evaluation) and the central database of SIMIK system (located in Ministry of Finances).

5.5.2.2 eSignature details

5.5.2.2.1 Legal aspects

Public key certificates and electronic signatures used in SIMIK system are not qualified ones (in the meaning of the act on electronic signature, from September, 18th, 2001).

5.5.2.2.2 Technical aspects

All applications and requests, generated with the usage of Application Generator or Payment Request Generator, is transferred in the form of XML document to the institution relevant for given operational programme. Authorized persons verify submitted applications. There are three possible results of verification (and they are assigned to the application as the status of verification): application accepted, uncompleted or rejected. The decision (status information) is signed electronically by a verifier or a person checking a document.

Signed applications are transmitted to the central database of SIMIK system (managed by Ministry of Finances).

5.5.2.2.3 Organisational aspects

Cryptographic keys and public key certificates are issued by internal CA of SIMIK system. Request for certificate is authorized by an application verifier. Cryptographic keys are stored in non-volatile memories of Integrated Circuit Cards.

There is a lack of information enabling to state what kind of electronic signature formats are used in the system; the same concerns general rules of public key certificates issuance.

The system users are for instance: Voivodeship Employment Offices, State Fund for Disabled Persons Rehabilitation, Ministry of National Education, Implementation Office for European Structural Funds and Civil Services Office.

5.5.2.3 Interoperability

An electronic signature is used for the purpose of SIMIK system only.

5.5.2.4 Miscellaneous

SIMIK system belongs to A2A applications. Over 3000 users (applicants) have used SIMIK system till October 2006.

5.5.2.5 Assessment

Applications, submitted to SIMIK system by users interested in financial support of their projects, should be electronically signed as well.

SIMIK system is the next example of the system where a proprietary CA has been established and implemented, in spite of commercial CA services usage.

The system is permanently modified. The system implementator claims that permanent changes proponed by Ministry of Finances are the reason. On the other hand, users indicate many faults and errors requiring an essential improvement of the system. All these circumstances invoke the necessity of software upgrades. Ministry of Finances is going to audit the system to state what is really necessary to improve.

5.6 Customs

Polish customs law allows to prepare custom documents using electronic data processing mechanisms. That possibility is indicated in Article 19, clause 1, of the act on customs law (from March, 19th, 2004; Law Diary - Dz. U. no 68, pos. 622). That act is compliant with EU law, for instance with requirements for New Computerised Transit System (NCTS).

Polish Customs use three following basic systems supporting a circulation of electronic customs documents:

(a) CELINA system – designed to serve basic source documents concerning foreign trade controlled by Polish Customs;

(b) INTRASTAT system – providing statistic data about trade circulation between EU member states.

(c) New Computerised Transit System (NCTS) – allowing economy subjects to submit declarations concerning transit in an electronic format; data concerning transit operations are exchanged as messages transmitted in real-time between customs offices and authorities and economy subjects; the system has been implemented in 29 EU countries and EFTA members;

There is possibility to sign electronic documents in every mentioned system (CELINA, INTRASTAT and NCTS). However that possibility is theoretical, because currently polish customs do not use electronic signatures for customs documents frequently. Nevertheless such a possibility is realistic and the case of OPEL Polska company confirms it. From October 25th, 2004, OPEL Polska can use an unqualified electronic signature to submit customs documents. Only customs offices in Gliwice and Krakow are ready to accept these documents.

5.6.1 CELINA System

5.6.1.1 Application identification

CELINA system supports customs authorities activity during customs declaration service, i.e. accelerates and simplifies service procedures for documents submitted by economy subjects, enables to collect notified information in an electronic form and to transfer them to external systems, e.g.: ZEFIR system (System for Tax-Customs and Finance-Accounts Clearing). Moreover, the system validates documents automatically and in the same manner selects declarations for customs inspection, registers and processes data from electronic INTRASTAT declarations, i.e. statistical declarations concerning trading between EU states.

CELINA system acts in every customs office and department.

Electronic customs documents are created in XML format. For every type of customs declaration exists detailed XML specification (so called public specification), therefore software-houses can adopt applications dedicated for that sector. Those specifications can be downloaded from website http://www.krakow.uc.gov.pl/celina.htm.

5.6.1.2 eSignature details

5.6.1.2.1 Legal aspects

Electronic customs documents used in CELINA system (allowed on the basis of Article 19 of the act on customs law; from March, 19th, 2004; Law Diary - Dz.U. no 68, pos. 622) can be signed with the means of an unqualified electronic signature.

It results from EEC Directive 2913/92 from October, 12th, 1992, establishing EEC Customs Code (articles 61 and 77) and EEC Directive 2454/93 from July, 2nd, 1993, establishing executive regulations for the first one (articles 4a, 4b and 199). In article 4b and article 199, clause 2, of the last mentioned directive it is stated, that in the case of data processing systems usage customs authorities can allow to replace hand-written signatures by other identification techniques, e.g.: based on the codes usage.

In CELINA system an electronic signature is not required, nor recommended. Moreover, the compliance with requirements of the act on electronic signature from September 18th, 2001, is not obligatory.

5.6.1.2.2 Technical aspects

An electronic signature included in XML electronic customs documents is optional. However if the document is signed electronically, then the following requirements should be fulfilled:

(a) an electronic signature format has to be compliant with W3C/IETF Recommendation (February 2002): *XML-Signature Syntax and Processing*,

(b) an electronic signature should be inserted in an additional element „<ds:Signature …",

(c) an element „ds:Signature" should be placed as the last one subelement of the main element,

(d) an electronic document has to be signed completely; i.e. it is not possible to sign selected parts of the document only.

Electronic data exchange with notifying entities is arranged via websites CELINA WEB-CEL (https://www.celina.krakow.uc.gov.pl/AppCel/index.jsp for standard procedures) and CELINA OPUS (https://www.celina.krakow.uc.gov.pl/Celina/index.jsp for simplified procedures).

Electronic customs documents are prepared using relevant applications outside CELINA system. The users have the possibility to send documents directly to CELINA OPUS (simplified procedures) or to CELINA WEB-CEL, it means that an application connects with CELINA system self-reliantly, transmits a document in XML format and receives an answer from the system. Application user can write XML document into the file and send it via an internet viewer. Some examples of applications are mentioned below:

(a) WinSADIB / WinSADEU application designed by Huzar Software (http://www.huzar.pl) for customs documents SAD and SAD BIS management,

(b) AGENT CELNY (CUSTOMS AGENT) application designed by Studio Oprogramowania FRAKTAL (Software Studio FRAKTAL) (http://www.fraktal.com.pl) for customs documents SAD, SAD BIS and DWC management.

An electronic document supplied with an electronic signature is prepared by any entity notifying a customs document and provided with an unqualified public key certificate (certificate issuance has been performed earlier). Certificates are issued by the internal Center of Secure Transmission for Customs Systems (Centrum Bezpiecznej Transmisji Systemów Celnych - CBTSC, https://cbt.celina.pl), managed by Customs Authority in Krakow. Signing keys and related public key certificates can be generated by CBTSC and send to the user in the form of a token compliant with PKCS #12 standard, or the user can generate the keys inside GemSafe card (GemPlus) alternatively.

Requests for certificates are send to relevant registration points; there, after a verification of requester identity, requests are approved or rejected (a corporal appearance of requestors is required).

A special application for customs documents signing (*Podpisywanie dokumentów XML – XML Documents Signing*), is available at https://cbt.celina.pl/program/Kontrolka_AX_podpisu_XML.exe. It works only with certificates issued by CBTSC and allows to sign customs documents created with the usage of WinSADIB / WinSADEU or AGENT CELNY (CUSTOMS AGENT) applications.

5.6.1.2.3 Organisational aspects

Public key certificates are issued by internal CBTSC (see: above). There is one CA in the system.

CBTSC has no Certificate Procedure Statement (CPS).

5.6.1.3 Interoperability

According with regulations, an unqualified electronic signature created with the means of a private key and linked to a certificate issued by CBTSC, *will be treated equivalently to a handwritten signature of the person, who placed that signature on SAD document or SAD document rectification, and in the case of some decisions of the Head of Customs as well.* Unfortunately, it is not possible to use in CELINA systems qualified, nor unqualified certificates issued by other CAs providing certification services.

5.6.1.4 Miscellaneous

The only one known user of an electronic signature in CELINA system is OPEL Polska company. There is a lack of information concerning the number of electronic signatures created by representatives of this company. The same concerns the number of public key certificates issued by CBTSC.

5.6.1.5 Assessment

The serious defect of this electronic signature usage concept is that only subscribers with certificates issued by CBTSC can use CELINA system. The main reason for such a solution was the price of one public key certificate. In the case of CBTSC it is 0 zloty (it is true, but under the assumption the costs of IT infrastructure maintenance are neglected), and in the case of other CAs – few hundreds zloty.

Currently (i.e.: on November 2006) an implementation of electronic signatures in Customs have been adjourned for unknown time period.

5.6.2 INTRASTAT subsystem

5.6.2.1 Application identification

INTRASTAT system is designed for gathering and providing statistic data about trade circulation between EU member states. In Poland Customs is the body responsible for data gathering, processing, controlling and transferring. In that case it is subjected to Ministry of Finances.

INTRASTAT is subsystem of CELINA system.

The legal foundations for INTRASTAT system functionality are as follows:

(a) Directive 2004/638/EC of the European Parliament and of the Council on Community statistic data concerning trade circulation, from March, 31th, 2004, cancelling EEC Directive 3330/91 (Law Diary - Dz. Urz. WE no L 102, from April, 7th, 2004);

(b) the act on customs law, from March, 19th, 2004 (Law Diary - Dz. U. 2004 no 68, pos. 622) - Clause 8 (articles 97 - 102 of the act) entitled "registration and statistics concerning trade circulation between EU member states";

(c) the regulation of minister of Finances on ITRASTAT declarations, from April 21th, 2004 (Law Diary – Dz. U. 2004, no 89, pos. 846).

In Poland every flow of EU goods, omitting exceptions defined in law regulations, is registered in INTRASTAT system appropriately as:

(a) export of goods – when registration is made by Poland as member State exporting goods (declaration INTRASTAT – EXPORT (WYWÓZ)),

(b) import of goods - when registration is made by Poland as member State importing goods (declaration INTRASTAT – IMPORT (PRZYWÓZ)).

An entity obliged to provide information (for the purpose of registration and statistics of INTRASTAT system) can be any physical or legal individuality, and an organisation entity unit, who participates in trade circulation with EU Member States, is registered as VAT-payer, and exceeds export/import value relevant for basic statistic export/import threshold appropriately.

5.6.2.2 eSignature details

5.6.2.2.1 Legal aspects

In the case of INTRASTAT system, which is the independent part of CELINA system, the same law regulations apply which allow an electronic exchange of customs documents in CELINA system (see: clause 5.6.1.2.1).

5.6.2.2.2 Technical aspects

Similarly as in the case of CELINA system, electronic reports are created in XML format. Format specification is accessible at

http://www.mf.gov.pl/_files_/sluzba_celna/intrastat/ist_dek_tch_xmlw1r1_13pl.zip.

Electronic documents in INTERSTAT system can be generated using the following applications:

(a) ist@t, accessible free of charge by Customs Authority in Krakow (http://www.mf.gov.pl/_files_/sluzba_celna/intrastat/ist_dek_tch_xmlw1r1_13pl.zip),

(b) WinSADIB / WinSADEU designed by Huzar Software company (http://www.huzar.pl),

(c) Intrastat++ designed by Studio Oprogramowania FRAKTAL (Software Studio FRAKTAL) (http://www.fraktal.com.pl).

The format of an electronic signature is the same as the format used in CELINA system; the same application is used for signing, and the signer has to be the owner of an unqualified certificate issued by CBTSC (details, see: clause 5.6.1.2.2).

Prepared electronic documents are transferred via website CELINA WEB-CEL (https://www.celina.krakow.uc.gov.pl/AppCel/index.jsp), directly from application for documents generation, or via an internet viewer.

5.6.2.2.3 Organisational aspects

See: clause 5.6.1.2.3.

5.6.2.3 Interoperability

See: clause 5.6.1.3.

5.6.2.4 Miscellaneous

See: clause 5.6.1.4.

5.6.2.5 Assessment

An assessment presented in clause 5.6.1.5 is valid in the case of INTRASTAT system as well.

5.6.3 NCTS Poland subsystem

5.6.3.1 Application identification

The New Computerised Transit System (NCTS) is a European wide system, based upon electronic declaration and processing, designed to provide better management and control of CT. It involves all EU Member States and the EFTA countries.

Each country's own NCTS processing system is connected, through a central domain in Brussels, to all of the other countries. Since NCTS Mandation on the 1 July 2005, paper transit documents will only be accepted from private travellers (with goods in excess of allowances) and during NCTS fallback.

NCTS system in polish NCTS domain is used to exchange information concerning transit operations in real time; electronic messages are transmitted among all customs offices at the whole country area. It is used by customs officers during customs declaration processing and monitoring, and by companies during customs declaration submission, revocation, securing submission, goods for transit releasing, transit operation finalizing in a destination customs office and closing the operation in a source customs office.

The legal foundations for NCTS system functionality are as follows:

(a) Directive of the EEC Council 2913/92, from October, 12th, 1992, on an establishment of EEC Customs Code (Law Diary - Dz. Urz. WE L 302, 19.10.1992, page 1, and later amendments; Law Diary - Dz. Urz. UE – polish special edition, clause 2, vol. 4, page 307),

(b) Directive 2454/93/EEC, from July, 2nd, 1993, on an establishment of executive regulations to execute Directive of the EEC Council 2913/92, from October, 12th, 1992, on an establishment of EEC Customs Code (Law Diary - Dz. Urz. WE L 253, 11.10.1993, page 1, and later amendments; Law Diary - Dz. Urz. UE – polish special edition, clause 2, vol. 6, page 3).

5.6.3.2 eSignature details

5.6.3.2.1 Legal aspects

In the case of NCTS system the same law regulations apply which allow an electronic exchange of customs documents in CELINA system (see: clause 5.6.1.2.1).

5.6.3.2.2 Technical aspects

In NCTS system, similarly as in the case of CELINA system, electronic reports are created in XML format. Format specification is accessible at

http://mofnet.gov.pl/_files_/ncts/ncts3_2_specxml_pwkw1r1pl.zip.

Electronic documents in NCTS system can be generated using the following applications:

(a) Minimal Common Core (MCC) software developed centrally by the Directorate-General for Taxation and Customs Union and Eurostat (DG Taxud),

(b) WinSADIB / WinSADEU designed by Huzar Software (http://www.huzar.pl),

(c) NCTS++ designed by Studio Oprogramowania FRAKTAL (Software Studio FRAKTAL) (http://www.fraktal.com.pl).

The format of an electronic signature is the same as the format used in CELINA system; the same application is used for signing, and the signer has to be the owner of an unqualified certificate issued by CBTSC (details, see: clause 5.6.1.2.2).

Electronic customs declarations for transit procedures are submitted to NCTS systems via e-mail. Declarations should be sent to pwk@ncts.mofnet.gov.pl

System is designed in client/server architecture and consists of the central node (located in Lodz and intended to manage and administrate at the whole polish territory) and users network. The users are customs officers. User interface, i.e. MCC application, is installed only on the computers in customs offices, and companies willing to communicate with NCTS system use commercial software created on the base of XML specification made accessible by customs administration.

NCTS system is integrated with other systems, i.e. CELINA and Zefir systems (Zefir system enables the customs and tax payments clearance globally).

5.6.3.2.3 Organisational aspects

See: clause 5.6.1.2.3.

5.6.3.3 Interoperability

Polish domain NCTS servers located in Lodz are an access gate for common European NCTS system. Even of NCTS messages compatibility the polish part of NCTS will not enable interoperability at the electronic signature level (see also: clause 5.6.1.3).

5.6.3.4 Miscellaneous

See: clause 5.6.1.4.

5.6.3.5 Assessment

An assessment presented in clause 5.6.1.5 is valid in the case of NCTS system as well.

5.7 Education

5.7.1 SELS – electronic student card

5.7.1.1 Application identification

The electronic student card (ELS) replaces the paper student card used in Poland up to date. The legal foundation for an introduction of SELS is the regulation of Ministry of National Education and Sport on the course of study documentation, from July 18th, 2005 (Law Diary - Dz.U. 2005 no 149 pos. 1233).

Electronic student cards are managed by Electronic Student Card System (System Elektronicznej Legitymacji Studenckiej - SELS), which allows for instance to personalize cards, to issue new cards and to prolongate/revocate issued cards as well.

There are local systems dedicated for individual universities or the groups of them. The users are dean's offices of high schools mostly, because they are responsible for student cards management. Nevertheless, to enable common recognizing of the cards, some of technical details are universal and allow at least students identification at the national level.

5.7.1.2 eSignature details

5.7.1.2.1 Legal aspects

Due to the regulation, the student card is an electronic microcontroller card with contact interface defined in ISO/IEC 7816-2 and ISO/IEC 7816-3 standards. An additional usage of contactless interface is not precluded.

It is stated in Annex 3 being an integral part of the regulation on the course of study documentation, from July, 18th, 2005 (Law Diary - Dz.U. 2005 no 149 pos. 1233) that an electronic student card has to include (in non-volatile memory) the data structure named SELSInfo, supplied with an electronic signature compliant with the technical specification ETSI TS 101 733 (it is indicated in Article 49, clause 2, subclause 3, of the regulation of Ministry Council from August, 7th, 2002 on technical and organisational requirements for qualified certification authorities, certification policies for qualified certificates issued by them, and technical requirements for secure signature creation and verification devices (Low Diary – Dz.U. 2002 no 128, pos. 1094). An electronic signature has to be a qualified signature, verified with the usage of a qualified certificate (the term defined in the act on electronic signature, from September, 18th, 2001).

5.7.1.2.2 Technical aspects

Every SELS system is equipped with the module allowing secure electronic signature creation. The providers of those modules are qualified CAs: Certum (www.certum.pl), Sigillum (www.sigillum.pl.com.pl) and Szafir (www.kir.com.pl).

The providers of SELS systems are for instance:

(a) Unizeto Technologies S.A. (http://www.unizeto.pl) - with its own module for qualified signatures creation,

(b) Computerland (http://www.computerland.pl) – with the module for qualified signatures creation provided by PWPW (Polish Securities Manufactory S.A. - Polska Wytwórnia Papierów Warto•ciowych S.A. – the owner of qualified CA Sigillum)

(c) OPTeam S.A. (http://www.optimus-comfort.com.pl) - with the module for qualified signatures creation provided by PWPW (Polish Securities Manufactory S.A. - Polska Wytwórnia Papierów Warto•ciowych S.A. – the owner of qualified CA Sigillum).

5.7.1.2.3 Organisational aspects

In SELS system qualified signatures are created by authorized employees of universities dean's offices. Every one of them has to be equipped with a technical component (with cryptographic keys for the purpose of qualified signatures creation installed) and a qualified public key certificate. Qualified certificates are issued by qualified CAs providing certification services (Certum (www.certum.pl), Sigillum (www.sigillum.pl.com.pl) and Szafir (www.kir.com.pl)) according with requirements defined or resulting from the act on electronic signature, from September, 18th, 2001.

Every qualified certificate issued for SELS system purposes has to include in „subject" field an attribute "common name" with the following value: "the person authorized for student cards issuance" ("osoba upowa• niona do wystawiania legitymacji studenckiej").

5.7.1.3 Interoperability

The format of a signature for SELSInfo data structure (compliant with ETSI TS 101 733 technical specification) and the format of SELSInfo itself are standardized well; therefore they should be recognized by all applications where student cards will be used in. Currently there is no such an application in Poland.

SELS systems do not interoperate with external applications.

5.7.1.4 Miscellaneous

It is predicted that for the purpose of SELS systems different high schools will issue about 1 million electronic student cards in next years. The number of qualified electronic signatures will be two times more (one qualified signature for every semester of education). Just now about 10 thousand electronic student cards are used.

ICCs, which electronic student cards have to be based on, should to be choosed at the auction organized by Technical University of Poznan.

5.7.1.5 Assessment

SELS systems are able to accept only dedicated public key certificates, defined in the relevant law regulation.

The tendency is observed to introduce the solution provided by one producer/provider – this solution could be cheaper one, but is contradictive with competitiveness rules.

5.8 Local applications

Regional and community authorities very rarely decide to implement application and systems supporting A2B and A2C communication. In contradiction to portals mentioned in an introduction (they make accessible static information, e.g.: templates of official documents or confirmations of administrative decisions only), the one advanced group of systems for C2A and B2A communication occurred in 2006. It is an electronic delivery box – the form of service allowing the transfer of electronic documents to administration with confirmation of receipt (nonrepudiation of receipt).

5.8.1 Electronic delivery box (ESP)

5.8.1.1 Application identification

The Act on activity informatisation of entities performing public tasks (from February, 17th, 2005, Law Diary - Dz. U. no 64, pos. 565, with amendments) obliges all public administration entities to receipt petitions and applications via electronic means. The way the relevant electronic documents are delivered are precised in the regulation of the Prime Minister on organisational and technical conditions for electronic documents delivery to public entities (from September, 29th, 2005; Law Diary - Dz. U. no 200 pos. 1651). According to the contents of that regulation, electronic documents can be delivered to public administration IT systems via electronic delivery boxes. The only requirement is that they meet requirements defined in the regulation of Ministry Council on minimal requirements for IT systems (from October, 11th, 2005; Law Diary - Dz. U. 2005 no 212 pos. 1766).

An electronic delivery box is any publicly accessible mean of an electronic communication which can be used for electronic data transfer to a public administration entity with the usage of commonly accessible IT networks.

After the delivery of an electronic document to a delivery box – public administration IT system creates an official confirmation of receipt automatically[18] and send it back to the electronic document sender. This official confirmation of receipt has to be supplied with an electronic signature (the regulation from September, 29th, 2005, does not precizes if it has to be a qualified or an unqualified signature).

Electronic delivery boxes are made accessible by different public administration entities (government institutions, regional administration and communities administration as well). Therefore it is no one unique system/application, but the whole family of products providing electronic delivery box services.

5.8.1.2 eSignature details

5.8.1.2.1 Legal aspects

According to the act on administrative procedures code (from June, 14th, 1960; Law Diary - Dz.U. 1960 no 30 pos. 168) it is necessary to ensure the possibility of petition submission in the electronic form with the usage of an electronic signature (Article 63, clause 3a). Any petition can be submitted by petitioners to IT system of a public entity (administrative unit). They also receive as an answer official confirmation of receipt supplied with an electronic signature (according to Article 6.1 of the regulation from September, 29th, 2005, see: clause 5.8.1.1).

5.8.1.2.2 Technical aspects

Electronic delivery box systems are implemented as client-server architecture or web service. Each of public administration entities makes its IT system accessible in such a way, that receipts petitions in an electronic form (obligatory supplied with a qualified electronic signature) and response with official confirmations of receipt automatically. That confirmation should be generated with the usage of a cryptographic module (HSM - *Hardware Security Module*), certified at least at FIPS PUB 140-2 Level 3.

Qualified certificates used for verification of signed electronic petitions are issued by qualified CAs providing certification services: Certum (www.certum.pl), Sigillum (www.sigillum.pl.com.pl) and Szafir (www.kir.com.pl). On the other hand, unqualified certificates (used for verification of official confirmations of receipt) are issued by unqualified CAs providing certification services (e.g.: Certum (www.certum.pl), Sigillum (www.sigillum.pl.com.pl), Szafir (www.kir.com.pl), Signet (http://www.signet.pl)).

An official confirmation of receipt can be provided by any public administration entity self-reliantly or by the third party, which intermediates between petitioners and public entities. In the second case the third party is authorized by a public entity to provide such services. In other obtainable solution, CA

[18] Electronic data added to an electronic document (delivered to public administration IT system) or joined with that document in such a manner that any later document changes (especially after reception) are recognized.

providing certification services receipts petitions, creates confirmation of submission, then redirects both sends both components to a relevant public administration entity.

Electronic delivery box services can be provided by the following systems:

(a) Electronic Delivery Office (Elektroniczny Urz•d Podawczy - EUP), developed by Unizeto Technologies S.A. (http://www.unizeto.pl): a qualified PKI service provided by CERTUM – Powszechne Centrum Certyfikacji (Public certification Center) (http://www.certum.pl); it can be integrated with a portal of public administration entity (relevant forms for documents are obtainable there) and enable petitioners to create qualified electronic signatures; EUP provides confirmations of petition submission and confirmations of receipt;

(b) Electronic Delivery Chamber (Elektroniczna Kancelaria Podawcza - EKP) developed by Unizeto Technologies S.A. (http://www.unizeto.pl): a special version of EUP system intended for use by public administration entities;

(c) Centaur WER developed by ENIGMA Information Protection Systems Co. Ltd. (Systemy Ochrony Informacji Sp. z o.o.) (http://www.enigma.com.pl): dedicated server with HSM (i.e. ICC certified at FIPS PUB 140-2 level 3), providing official confirmations of receipt;

(d) Electronic Delivery Box (Elektroniczna Skrzynka Podawcza) ESP E-STUDIO developed by E-STUDIO company (http://www.estudio.lublin.pl/),

(e) Electronic Delivery Box (Elektroniczna Skrzynka Podawcza) Sigillum-ESP (http://www.sigillum.pl) - details unknown.

Different formats of an electronic signature are used for petition signing, and for confirmations of receipt provision as well.

In EUP and EKP systems ETSI TS 101 903 (XAdES) format is used for petitions, and PKCS#7 format for confirmations of receipt (included in S/MIME messages).

Centaur WER system accepts petitions supplied with electronic signatures in formats supported by qualified CAs providing certification services. Confirmations of receipt are compliant with ETSI TS 101 733 format.

In ESP E-STUDIO system PKCS#7 format is used in bidirectional documents exchange. Moreover, a qualified signature for petitions and confirmations of receipt is required.

5.8.1.2.3 Organisational aspects

Qualified certificates used in electronic delivery box systems are issued by qualified CAs providing certification services. On the other hand, unqualified certificates (used for verification of official confirmations of receipt) can be issued by unqualified CAs providing certification services. In both cases certificates sholud be issued according to requirements of the act on electronic signature (from September, 18th, 2001).

Communication between petitioners and public administration entities can be performed with and without intermediation of trusted third parties. EUP system is an example of the second solution.

5.8.1.3 Interoperability

EUP, EKP and Centaur WER systems approve those petitioners signatures which can be verified with the usage of qualified certificates issued by any polish qualified CA. Therefore any owner of a qualified certificate can send an electronic petition to any public administration entity (if such a possibility is obtainable for petitioners). In the case of confirmation of receipt the situation is worse due to the fact, that they can be verified using certificates issued by different CAs. Therefore petitioners can have some problems with correct verification of signatures.

Electronic delivery box systems can interoperate with internal systems for documents circulation management of public administration entities.

However the basic interoperability problem is the need to recognize different templates of electronic petitions (XML, PDF, MS Word formats, etc.). It results in difficulties in data exchange between different public administration entities and in data processing in IT systems of petition recipients.

5.8.1.4 Miscellaneous

Already a few dozen public administration entities make accessible electronic delivery boxes via their portals. It concerns local, regional and central administration as well (an electronic delivery box of Ministry of Regional Development could be an example: https://esp.mrr.gov.pl). The rapid development of this C2A and B2A communication for has been disturbed by the last decision of polish Government. It was decided to adjourn (May, 1st, 2008) the obligation of public authority organs to allow the submission of petitions and applications in an electronic form; it concerns the other electronic communication forms as well.

5.8.1.5 Assessment

A variety of solutions present on the market, the lack of unique standard for a confirmation of receipt, different interpretations of the regulation of Ministry Council on minimal requirements for IT systems (from October, 11th, 2005; Law Diary - Dz. U. 2005 no 212 pos. 1766), all of these invokes many doubts concerning the possibility to arbitrate in the disputes between petitioners and public administration entities. The courts can have the problems with unambiguous interpretation of a force of evidence in the case of confirmations of receipt submitted by parties. The problem should be solved by an introduction of third trusted party as an intermediate in data exchange between petitioners and public administration entities. However it requires to accept legal validity of evidences issued by trusted third parties.

6 General Assessment

Despite of establishment of the act on electronic signature (September, 18th, 2001), a development of electronic signature usage in B2A and C2A electronic communication is very slow. The following is the main reason: administration is not ready for that. It is the result of delays in an informatisation of public administration entities. Nor of complex projects from government *Polish Republic Informatisation Strategy for 2004-2006 ePolska* has been finalized; many of them are seriously delayed. There are the following examples:

(a) Gateway of Poland (Wrota Polski): an integrated internet platform for administration – primary due date has been predicted for the first half of 2005;

(b) e-PUAP: an electronic platform for public administration services – implementation in 2006 - 2008;

(c) STAP: IT network for public administration – due date at the end of 2007;

(d) e-Declarations: electronic tax returns for bussiness – due date before the half of 2008;

(e) CEPiK: Central Register of Vehicles and Drivers – the project still will be continued in 2007.

An essential drawback for an implementation of the act on electronic signature (from September,18th, 2001) by public administration, particularly in the case of an obligation to receipt and accept documents transferred via electronic means, is the lack of definitions and terms concerning the structure of electronic documents (or the lack of consistence). The act on activity informatisation of entities performing public tasks (from February, 17th, 2005, Law Diary - Dz. U. no 64, pos. 565, with amendments) could be an example. It states that the minister relevant for informatisation should issue:

(a) the regulation on indispensable elements of electronic documents structure for archivisation purposes (Article 37);

(b) the regulation on structure of official documents and the way to arrange them in an electronic form, and organisational and technical conditions for their submission (Article 36).

The first one has been published (Law Diary – Dz.U. 2006, no 206, pos. 1517). The second one still waits for publication. There is no necessity to define documents structure in many regulations. It is enough to standardize the process of documents' structure; it could be done in Polish Committee for Dstandardizing for instance.

Another barrier in wider implementation of electronic signatures in public administration is the lack of coordination in ministries, regional and local administration activities. Consequently, where authorities representatives note benefits obtained due to an electronic document and signature usage (e.g.: an improvement of information delivery and processing), there such a systems are implemented. In other cases regional and local authorities wait for centralized decisions and solutions.

An analysis of systems and applications presented in section 5 indicates the following: any kind of an electronic signature system will be not developed till then a relevant law regulation exists. Such an approach, correct from the legal point of view, makes it hard to decide when an electronic signature can be used, and when not. It seems that a general rule is needed for all of electronic signatures applications focused on public administration.

Currently the implementation of an electronic signature became slower than few years ago. It is the result of delayed public administration obligations concerning for instance:

(a) to allow the submission of petitions and applications in an electronic form, and to perform other activities using an electronic form: previous due date – September, 16th, 2006; current due date – May, 1st, 2008,

(b) to publish „Monitor Polski B" (official source of information concerning legislative decisions of Government) in the electronic form: previous due date – July, 1st, 2006; current due date – probably May, 1st, 2008,

(c) to allow submit tax declarations electronically (e-Declarations): previous due date – August, 16th, 2006; current due date – April 2007 (only "big" tax payers can use this possibility from August, 16th, 2006).

Despite of facts mentioned above, the number of systems and applications for communication with public administration entities, which an electronic signature is used in, increase day by day. Their great number and variety kindly surprise authors of this report.

The serious fault of existing systems and applications is their weak interpretability. The situation is relatively good there, where qualified electronic signatures are used. Qualified CAs providing certification services try to obtain an acceptance for qualified signature and certificates in the case of any project implemented for the purposes of public administration. The situation is worse in the case of unqualified signatures usage. Usually they are used in closed systems, implemented for particular purposes and encompassing limited users populations. The tendency to establish more and more internal certification authorities for Public administration IT systems purposes is another serious mistake. Therefore it is hard to obtain interoperability in public administration systems themselves, but most of all it is the great problem for communication with external systems. For that problem two solutions could be considered: to use certificates issued by commercial CAs only, or to establish one or few CAs only for public administration purposes[19].

All systems and applications examples described in clause 5 are based on internal modules for electronic signatures verification; for that purpose CRLs are mainly used. It requires to design universal signature verification modules whenever certificates from many issuers are accepted. It is a difficult and time-consuming task (for instance, it requires to gather many CRLs published by different CAs in one system). The solution could be specialized and trusted providers of electronic signature verification services. An example of such a service is electronic signature verification service made accessible in national NCCert domain by Unizeto Technologies S.A. That service is based on DVCS protocol (RFC 3029) and allows to verify signatures from other countries, e.g.: Russia.

All CAs acting in Poland on the base of the act on electronic signature (from September, 18th, 2001) are obliged to archive data indispensable for electronic signature verification purposes (CRLs, certificates). Theoretically it should be satisfied solution for signatures verification. In practice it could be not the case, e.g.: in the situation when an electronic signature algorithm is broken. Many companies in Poland have noticed the issue of long-term electronic documents storage. There are developed archives and PKI services not only for the storage, but for maintenance of force of evidence as well. However the lack of standards can be serious drawback in common acceptance of those solutions, particularly in the case of international data exchange.

[19] An establishment of such an authority is predicted in e-PUAP project (e-Signature Certification Center for Public Administration).

7 Operational and planned applications

Interesting applications mentioned in the tables below have been further elaborated above with information on the actual usage of the applications. It should be noted that the list is not exhaustive.

7.1 Applications at the national level

	Application	Scope	Reference	Contact	Signature
1.	Polish Procurement Platform (PPP)	Letters of inquiry and offers, electronic auction, electronic catalogue	https://www.ppp.pwpw.pl	http://www.ppp.pwpw.pl/Kontakt	Qualified signature
2.	Elektroniczna Platforma Przetargowa e-przetarg.pl (EPP)	Electronic auction	https://www.e-przetarg.pl	http://www.e-przetarg.pl	Qualified signature
3.	Przetargi Elektroniczne (PE)	Electronic auction	https://ww.etender.pl	http://www.etender.pl/kontakt.php	Qualified signature
4.	Platforma Marketplanet	Electronic auction	https://www.marketplanet.pl	http://www.marketplanet.pl	Qualified signature
5.	E-GIODO	Submission of personal databases to General Inspector of Personal Data Protection for registration	https://egiodo.giodo.gov.pl	http://www.giodo.gov.pl/	Qualified signature
6.	CEPiK	Central register of vehicles and Drivers	https://www.cepik.gov.pl	http://www.mswia.gov.pl	Non-qualified signature, internal CA
7.	EPDU	Electronic transfer of insurance documents by payers to Social	http://e-inspektorat.zus.pl	*http://zus.pl*	Non-qualified signature,

	Application	Scope	Reference	Contact	Signature
		Insurance Organisation (ZUS)			internal CA
8.	SOD	Financial support service system used by employers to apply electronically for financial support in the case of disabled workers salaries and to report account settlements monthly as well	https://www.sod.pfron.org.pl	http://www.pfron.org.p	Non-qualified and qualified signature, commercial CA
9.	e-PFRON	System used to accept payment declarations and information concerning an employment, an education and activities for disabled persons benefit	http://www.e-pfron.pl	http://www.pfron.org.p	Non-qualified signature, commercial CA
10.	e-poltax	Reception and service of tax returns and other tax related documents in an electronic form	https://e-poltax.mf.gov.pl	http://www.mf.gov.pl	Qualified signature
11.	SI GIFF	System for report sending to General Inspector of Financial Information about all transactions exceeding 15 000 Euro	https://www.giif.mofnet.gov.pl/giif	http://www.mf.gov.pl	Qualified signature
12.	SIMIK	Tools for management, monitoring, inspection and implementation assessment of sector operational programs and a regional operational programs financed partially from UE funds	https://www.simik.gov.pl	http://www.mf.gov.pl	Non-qualified signature, internal CA
13.	CELINA	Supporting customs authorities activity during customs declaration service	https://www.celina.krakow.uc.gov.pl/AppCel/index.jsp (for standard procedures) https://www.celina.krakow.uc.	http://www.mf.gov.pl/sluzba_celna	Non-qualified signature, internal CA Under

	Application	Scope	Reference	Contact	Signature
			gov.pl/Celina/index.jsp (for simplified procedures)		development
14.	INTRASTAT	Gathering and providing statistic data about trade circulation between EU member states	https://www.celina.krakow.uc.gov.pl/AppCel/index.jsp	http://www.mf.gov.pl/sluzba_celna	Non-qualified signature, internal CA Under development
15.	NCTS Poland	System used to exchange information concerning transit operations in real time; electronic messages are transmitted among all customs offices at the whole country area	http://www.lodz.ic.gov.pl/	http://www.mf.gov.pl/sluzba_celna	Non-qualified signature, internal CA Under development
16.	SELS	Electronic evidence of an electronic student card validity	http://www.menis.gov.pl/prawo/wszystkie/rozp_361.php	http://www.mnisw.gov.pl/mein	Qualified signature

7.2 Applications at the local level

	Application	Scope	Reference	Contact	Signature
	ESP	The delivery of an electronic data (e.g. application) to a public administration entity with the usage of commonly accessible IT networks	e.g.: https://esp.mrr.gov.pl http://www.katowice.uw.gov.pl/urzadkatowice.php?urzad/esp	http://www.enigma.com.pl, http://www.unizeto.pl	Non-qualified and qualified signature, commercial CA

8 Annex A: Contact details of National Correspondents

Contact Information of the person(s) completing the questionnaire. The person(s) will be contacted for any queries related to this questionnaire.

8.1 Primary Contact

Country	Poland
Name	Jerzy Peja•
Organisation	Szczecin University of Technology

8.2 Alternative Contact

Country	Poland
Name	W•odzimierz Chocianowicz
Organisation	Szczecin University of Technology

9 Annex B: National Regulations Details

In the table below we include references to the legal sources that they have used during writing this report. This includes references to laws, other regulations, and doctrine, in such a manner that a legal expert with knowledge of the national legal system would be able to retrieve the sources.

National regulation title	National regulation translated title (English title)	Relevant links to on-line resources
Ustawa o podpisie elektronicznym z dnia 18 wrze•nia 2001 r. (Dz.U. 2001 Nr 130, Poz. 1450)	Act on Electronic Signature from September, 18th, 2001 (Law Diary - Dz.U. 2001 no 130, pos. 1450)	http://isip.sejm.gov.pl/prawo/index.html
Ustawa z dnia 21 lipca 2006 r. o zmianie ustawy o og•aszaniu aktów normatywnych i niektórych innych aktów prawnych oraz ustawy o podpisie elektronicznym (Dz.U. 2006 nr 145 poz. 1050)	Act on changes of rules concerning publication of normative acts, some another legislative acts and the act on electronic signature from July, 21th, 2006 (Law Diary - Dz.U. 2006 no 145 pos. 1050)	http://isip.sejm.gov.pl/prawo/index.html
Rozporz•dzenie w sprawie okre•lenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów •wiadcz•cych us•ugi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urz•dze• s•u••cych do sk•adania i weryfikacji podpisu elektronicznego. (Dz.U. 2002 Nr 128, Poz. 1094)	The Regulation of Ministry Council from August, 7th, 2002 on technical and organisational requirements for qualified certification authorities, certification policies for qualified certificates issued by them, and technical requirements for secure signature creation and verification devices (Low Diary –Dz.U. 2002 no 128, pos. 1094)	http://isip.sejm.gov.pl/prawo/index.html
Ustawa z dnia 11 marca 2004 r. o podatku od towarów i us•ug (Dz.U. 2004 nr 54 poz. 535, z pó•niejszymi zmianami)	The Act on taxes for goods and services, from March, 11th, 2004 (Law Diary - Dz.U. 2004 no 54 pos. 535, with later amendments)	http://isip.sejm.gov.pl/prawo/index.html
Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa (Dz.U. 2005 nr 8 poz. 60)	The Act on tax system, from August, 29th, 1997 (Low Diary - Dz.U. 2005 no 8 pos. 60)	http://isip.sejm.gov.pl/prawo/index.html
Ustawa z dnia 29 stycznia 2004 r. Prawo zamówie• publicznych (Dz.U. 2004 nr 19 poz. 177)	The Act on Public Procurement, from January, 29th, 2004 (Law Diary - Dz.U. 2004 no 19 pos. 177)	http://isip.sejm.gov.pl/prawo/index.html

Rozporz• dzenie Ministra Finansów z dnia 11 wrze• nia 2006 r. w sprawie struktury logicznej deklaracji, sposobu ich przesy•ania oraz rodzajów podpisu elektronicznego, którymi powinny by• opatrzone (Dz.U. 2006 nr 168 poz. 1197)	Regulation of Minister of Finances on logical structure of tax returns, the way of transfer and the types of electronic signature they should be supplied with, from September, 11th, 2006, (Low Diary - Dz.U. 2006 no 168 pos. 1197)	http://isip.sejm.gov.pl/prawo/index.html
Rozporz• dzenie Ministra Finansów z dnia 11 wrze• nia 2006 r. w sprawie trybu sk•adania oraz struktury logicznej zg•oszenia upowa• nienia podatnika lub osoby upowa• nionej przez podatnika do sk•adania deklaracji w formie elektronicznej i podpisywania deklaracji podpisem elektronicznym, Dz.U. 2006 nr 168 poz. 1196	Regulation of Minister of Finances on logical structure of tax returns, the way of transfer and the types of electronic signature they should be supplied with, from September, 11th, 2006, (Low Diary - Dz.U. 2006 no 168 pos. 1196)	http://isip.sejm.gov.pl/prawo/index.html
Rozporz• dzenie Ministra Edukacji Narodowej i Sportu z 18 lipca 2005 r. w sprawie dokumentacji przebiegu studiów (Dz.U. z 2005r. Nr 149, poz. 1233)	Regulation of Ministry of National Education and Sport Ministry on study documentation, from July, 18th, 2005, (Law Diary - Dz.U. 2005 no 149, pos. 1233)	http://isip.sejm.gov.pl/prawo/index.html
Ustawa z dnia 17 lutego 2005 r. o informatyzacji dzia•alno• ci podmiotów realizuj• cych zadania publiczne (Dz. U. Nr 64, poz. 565, z pó• , zm.)	Act of 17 February 2005 on activity informatisation of entities performing public tasks (Law Diary - Dz. U. no 64, pos. 565, with amendments)	http://isip.sejm.gov.pl/prawo/index.html
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101 poz. 926)	Act on personal data protection, from August, 29th, 1997 (Law Diary - Dz. U. 2002 no 101 pos. 926)	http://isip.sejm.gov.pl/prawo/index.html
Rozporz• dzenie Ministra Spraw Wewn• trznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie wzoru zg•oszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. z 2004 r. Nr 100, poz. 1025)	Regulation on a template of personal data base registration form, issued by Minister of Home Affairs and Administration on April, 29th, 2004 (Law Diary - Dz. U. 2004 no 100, pos. 1025)	http://isip.sejm.gov.pl/prawo/index.html
Ustawa prawo o ruchu	Act on traffic rules, form June,	http://isip.sejm.gov.pl/prawo/ind

drogowym z dnia 20 czerwca 1997 r. (Dz. U. z 2003 r. Nr 58, poz. 515 z pó• n. zm	20th, 1997 (Law Diary - Dz. U. 2003 no 58, pos. 515, and later amendments)	ex.html
Rozporz• dzenia Ministra Spraw Wewn• trznych i Administracji z dnia 19 wrze• nia 2001 r. w sprawie centralnej ewidencji pojazdów (Dz. U. z 2001 r. Nr 106, poz. 1166)	Regulation on a central vehicles register issued by Minister of Home Affairs and Administration (from September, 19th, 2001; Law Diary - Dz. U. 2001 no 106, pos. 1166)	http://isip.sejm.gov.pl/prawo/index.html
Ustawa z dnia 13 pa• dziernika 1998 r. o systemie ubezpiecze• spo•ecznych (Dz. U. z 1998 r. Nr 137, poz.887 z pó• n. zm.),	Act on social insurance system (from October, 13th, 1998; Law Diary - Dz. U. 1998 no 137, pos.887 with later amendments)	http://isip.sejm.gov.pl/prawo/index.html
Ustawa z dnia 16 listopada 2000 roku o przeciwdzia•aniu wprowadzeniu do obrotu finansowego warto• ci maj• tkowych pochodz• cych z nielegalnych lub nieujawnionych • róde• nieujawnionych • róde• oraz o przeciwdzia•aniu finansowaniu terroryzmu (Dz.U. 2000 Nr 116 poz. 1216)	Act on counteraction against introduction of illegal assets (with illegal or unknown origin) into a finance turn and terrorism financial support (from November, 16th, 2000; Law Diary - Dz.U. 2000 no 116 pos. 1216)	http://isip.sejm.gov.pl/prawo/index.html
Rozporz• dzeniu Ministra Finansów z dnia 20 maja 2003 r. zmieniaj• ce rozporz• dzenie w sprawie okre• lenia wzoru rejestru transakcji, sposobu jego prowadzenia oraz trybu dostarczania danych z rejestru Generalnemu Inspektorowi Informacji Finansowej (Dz.U. 2003 nr 101 poz. 935)	Regulation of Minister of Finances on the template of transaction register, the procedures of transaction register maintenance and the way of registered data transfer to GIIF (from May, 20th, 2003; Law Diary - Dz.U. 2003 no 101 pos. 935)	http://isip.sejm.gov.pl/prawo/index.html
Ustawy z dnia 20 kwietnia 2004 r. o Narodowym Planie Rozwoju (Dz.U.04.116.1206 z pó• niejszymi zmianami)	Act on National development Plan (from April, 20th, 2004; Law Diary - Dz.U. 2004, no 116 pos.1206 and later amendments)	http://isip.sejm.gov.pl/prawo/index.html

10 Annex C: Filled-in questionnaires

10.1 Electronic platform for the communication with General Inspector for Protection of Personal Data (e-GIODO)

10.1.1 Application identification

Application/Service Classification	
Application/Service Name	*e-GIODO (http://egiodo.giodo.gov.pl)*
Application/Service Type	*A2A, A2B or A2C*
Concerned sector	*Protection Personal Data*
Application/Service Cross-Border Type	*None*
Level of Online Sophistication Type	*Stage 4: Transaction: Case handling; decision and delivery*
Intended "clients"	*Personal data controllers, citizens*
Abstract Description	*Using dedicated forms, the personal data administrators are obligated to register the databases that contain the personal (citizens) data. The form is supported to facilitate filling it in and then makes easer its formal validation.* *Citizens may obtain information about personal databases systems registered by the administrators, theirs purposes and the scope of information being processed.*
Identification of Application/Service Entities	*General Inspector for the Protection of Personal Data (GIODO) + Personal Data Administrators*
Procedural Details	*Using dedicated application, the administrator shall fill in the electronic notification form submitted by the General Inspector for Personal Data Protection, create the qualified signature and send all to GIODO information system. GIODO sends confirmation of application acceptance and verifies data in order to establish applicant's identity and further tracking of the ongoing case that is to be dealt with.*
Current status	*Operational since August 2006*
Expected future developments	*Including the time stamp to the confirmation of form receiving that will be sent to sender*

Responsible Organisation	
Organisation Name	*General Inspector for Personal Data Protection:*
Organisation Type	*National*
Date of interview	*10/11/2006*

Application/Service System Details	
Communications Information	*Internet + Internal workflow system + Personal data file systems register*
External interface	*Webform to fill out (with series of consistency controls) – Result can be printed, signed manually and sent by post or signed electronically (qualified electronic signature) and sent electronically to GIODO*
Data structures processed by the application	*Data are entered into XML forms, extracted and further processed in Workflow and Register systems. For the preview the data are transformed to the html format*

10.1.2 eSignature details

Legal aspects	
Does the system rely on a simple / advanced / qualified / other signature?	*The system relies on qualified signature provided by Certum General Certification Authority - Unizeto Technologies SA, National Clearing House C.o. or Sigillum Polish Center of Electronic Certification*
Is the signature required/recommended?	*Required (for sending application in electronic form)*
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	*There are no specific plans for this yet.*
What is the legal basis (law, decree,…) for this application?	*The Act of 18 August 2001 on Electronic Signature (Journal of Laws of 2001 No 130 items 1450)* *Act of 17 February 2005 on activity informatisation of*

	entities performing public tasks (Law Diary - Dz. U. no 64, pos. 565, with amendments)
How is liability/responsibility regulated? Does the national legal framework regulate more than the minimum demand of the directive 1999/93 EC?	*The Act of 18 August 2001 on Electronic Signature which states that documents with a secure electronic signature shall be legally recognised as equivalent to documents with handwritten signatures. This Act specifies also the requirements that should be met by certification-service-providers and public administration authorities: during the four years from the date of the Act was entered into force the certification service customers should be able to submit applications and requests as well as other actions in the electronic form, in the cases when the law requires that they shall be made in a specified form or according to a specified specimens (Article 58 paragraph 2).* *The Act of 17 February 2005 on activity informatisation of entities performing public task among others things regulates also the rules for exchanging information by electronic means between public and nonpublic organizations. In Article 14 paragraph 3 the Act obligates public authorities which maintain electronic registers in IT systems to provide information about that register and make it available by electronic means*

Technical aspects	
What are the parties involved in the signature process?	*Parties authorized to grant qualified certificates by the Minister of Economy*
What kind of token or credentials are used (smart cards, software certificates, paper tokens …)?	*Person, which is using electronic signature, has a private key and certificate on a smart card.* *Certified applications are used as a signature creation device.*
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	*An approved ID smartcard reader*
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	*Windows and middleware delivered by qualified signature issuers (Certum General Certification Authority - Unizeto Technologies SA, National Clearing House C.o. and Sigillum Polish Center of Electronic Certification)*
What information is signed by the user and what is the objective of the signature?	*The notification of a personal database system registration by the General Inspector for Personal Data Protection; this notification is signed by the personal data administrator*
Is this an application with multiple signatures for the same data and, if	*No*

yes, what is the relationship between the signatures?	
What are the relevant policies (CPS, certificate policy, signature policy)?	*Certification policies issued by each of qualified certification providers. Certification policies should be accepted by Minister of Economy*
How are the signature/certificate presented to the application?	*User is filling-in his notification in electronic way, then write it as a data file in XML format on his local computer, signs this data file using qualified digital signature and puts signed file into the form and presses button for sending*
What information is included in the certificate, and what is the role of this information in the functioning of the application?	*When using the qualified digital signature certificate, the full name and national register number is required*

Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)? If yes, describe the framework in the country general profile.
If no, specify which standards have been implemented in the eSignatures application? Depending on the signature type, this may include standards regarding certificates, signature formats, signature algorithms, token formats, other information security standards, etc.
	The application for digital signature should use currently the following standards:
	ETSI TS 101 733 - Electronic Signature Format issued by European Telecommunications Standards Institute;
	ETSI TS 101 903 - XML Advanced Electronic Signatures (XAdES), issued by European Telecommunications Standards Institute;
	PKCS#7 Cryptographic Message Syntax Standard, issued by RSA Security;

How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	*Digital signature is verified using software delivered by qualified certificate issuers. Each qualified certificate issuer delivers own dedicated software.*
What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP…)	*For validation electronic certificate can be used CRLs or OCSP*
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	*The validity of the signature is verified at the time of its receiving*.

Organisational aspects

Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	*General Inspector for Personal Data Protection (as the recipient of signed data), Personal Data administrators (as the creator of the filing application) and three listed below providers responsible for issuing qualified certificates for digital signature (Certum General Certification Authority - Unizeto Technologies SA, National Clearing House C.o. and Sigillum Polish Center of Electronic Certification)*
Who are the relying parties[20]? Describe the context?	*Inspector General for Personal Data Protection as the recipient of signed data. Personal data administrators can fulfil his obligation of registration by using delivered platform of electronic communication.*
Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	*For issue/manage credentials are responsible qualified certificate providers pointed by Minister of Economy*
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	*The qualified certificates are issued for 1 or 2 year period. Condition for revoking or suspending credentials are regulated by certification policies issued by providers.*

[20] « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

10.1.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	*No*
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	*No*

10.1.4 Miscellaneous

Miscellaneous	
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	*17 electronic notification were made from August to November 2006*
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	*The application in not widely used because of not widely usage of digital signature. The Polish government not support business and citizens for gaining qualified digital certificates. The cost of qualified certification issued by three mentioned above providers is relatively high.* *The disadvantage of this application is necessity to use different application for verification digital signature. The application for verification is different for each of qualified certificate service providers.*
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	*Not now*

10.1.5 Assessment

Assessment	
Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses).	*The Polish Government has not indicated tools that should be used by the citizens or businesses for the generation of electronic signature. There are also no clear guidelines for private entities offering electronic signature services. Therefore, each of qualified certificates providers use it own*

Take this opportunity to bring any fruitful information that was not addressed by previous questions.	*tools for verification of signature.*

10.2 Electronic transfer of social insurance documents

10.2.1 Application identification

Application/Service Classification	
Application/Service Name	*Electronic transfer of social insurance documents*
Application/Service Type	*A2B*
Concerned sector	*Social insurance*
Application/Service Cross-Border Type	*No*
Level of Online Sophistication Type	*Stage 3: Two-way Interaction: Processing of forms including authentication*
Intended “clients”	*Social insurance fees payers*
Abstract Description	*The payers are obliged to submit insurance documents to ZUS via electronic means. Completing the forms and their electronic transfer is performed with the usage of P• ATNIK (PAYER) application via internet to one of the following addresses:* https://www.sdwi.gdansk.zus.pl https://www.sdwi.warszawa.zus.pl https://wroclaw.sdwi.zus.pl *The collection of completed forms is signed electronically by the payer of fees or the person authorized to submit them, then data are enciphered with session key and transferred to ZUS. ZUS delivers the payer an electronical confirmation of receipt. Electronic transfer of social insurance documents is an element of ZUS Complex Information System*
Identification of Application/Service Entities	*Social Insurance Organisation (ZUS) + payers of fees*
Procedural Details	*Authentication and electronic signatures use RSA algorithm and SSL protocol; public key certificates are issued for ZUS and payers by CERTUM for ZUS on the contractual base.*

Current status	*Active from February 1999*
Expected future developments	*There are the plans to create secure electronic signatures for collections of electronic insurance documents.*

Responsible Organisation	
Organisation Name	*Social Insurance Organisation - Zak•ad Ubezpiecze• Spo•ecznych (http://zus.pl)*
Organisation Type	*National*
Date of interview	*October 2006*

Application/Service System Details	
Communications Information	*Internet + intranet of Complex Information System KSI ZUS*
External interface	*P• ATNIK (PAYER) application made accessible at http://e-inspektorat.zus.pl . This webservice enables to use electronic services bythe selection of required service.*
Data structures processed by the application	*XML formatted data transmitted by P• ATNIK application are processed by KSI ZUS applications.*

10.2.2 eSignature details

Legal aspects	
Does the system rely on a simple / advanced / qualified / other signature?	*Unqualified electronic signature compliant with PKCS#1 format is used in the system; it ensures the integrity of signed insurance documents. An authentication of the Signer is ensured due to SSL protocol and public key certificates of ZUS and payers.*
Is the signature required/recommended?	*An electronic signature is required.*
Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?	*It is planned to replace current unqualified signatures with qualified ones.*
What is the legal basis (law,	*The act on social insurances system (Law Diary - Dz. U.*

decree,…) for this application?	*1998 no 137, pos. 887, and later amendments).*
How is liability/responsibility regulated? Does the national legal framework regulate more than the minimum demand of the directive 1999/93 EC?	

Technical aspects	
What are the parties involved in the signature process?	*ZUS, fees payers, CERTUM for ZUS*
What kind of token or credentials are used (smart cards, software certificates, paper tokens …)?	*Cryptographic keys (RSA) for payers are generated using P• ATNIK application. Public keys are certified free of charge by CERTUM for ZUS (http://cc.unet.pl) and then registered in P• ATNIK application and in an internet viewer. Private keys are stored on the floppy discs (secured by passwords).*
What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?	*PC with MS Windows and P• ATNIK application, public key certificate*
What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?	*PC with MS Windows and P• ATNIK application, public key certificate*
What information is signed by the user and what is the objective of the signature?	*The collection of electronic insurance documents.* *Integrity and non-repudiation of transmitted documents.*
Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?	*No. There is one electronic signature for many completed forms.*
What are the relevant policies (CPS, certificate policy, signature policy)?	*Certification policy (http://cc.unet.pl)*
How are the signature/certificate presented to the application?	*After insurance documents (forms) are completed and collected – P• ATNIK applications requests for an electronic signature creation; A private key of the payer/authorized person is stored on the floppy disc (secured by a password).*
What information is included in the certificate, and what is the role of this	*A certificate, based on X.509 v.3 standard, includes all information enabling payer's identification. A certificate is*

information in the functioning of the application?	*used for an electronic signature creation, session keys enciphering and SSL authentication. The structure of certificates is presented in:* *"New certificate and CRLs profiles for ZUS, ver. 1.4"*
Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)? If yes, describe the framework in the country general profile. If no, specify which standards have been implemented in the eSignatures application? Depending on the signature type, this may include standards regarding certificates, signature formats, signature algorithms, token formats, other information security standards, etc.	*No. RSA and SHA1 for signatures and SSL authentication, 3DES for session encryption.*
How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?	*Signatures are verified by KSI application receiving the collection of electronic documents with payer/authoried person public key certificate. Signature Verification Application uses certificates issued for payers by CERTUM for ZUS and CRL.*
What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP…)	*CRLs*
How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?	*The signature is valid for certificate validity period only. A signature verification is performed just after the documents collections reaches the receiving application.*

Organisational aspects	
Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?	*Fees payers, ZUS, CERTUM for ZUS*
Who are the relying parties[21]? Describe the context?	*Social Insurance Organsation (ZUS) as the recipient of signed documents responsible for social insurance in Poland.*

[21] « Relying Party » :shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature

Who issues/manages credentials (e.g. certificates)? Describe the conditions and the procedure for the issuance of the credentials.	*CERTUM for ZUS (http://www.cc.unet.pl)*
What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?	*The validity period of ZUS and payers certificates is 1 year.* *Certificate revocation: the end of economic activity, private key compromising.* *Certificate suspension is not possible.*

10.2.3 Interoperability

Interoperability aspects	
Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?	*The system is addressed for all entities acting economically in Poland.*
What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?	*There are plans to adopt the system for acceptance of certificates issued in EU Member States.*

10.2.4 Miscellaneous

Miscellaneous	
Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?	*1 050 000 certificates have been issued from February, 1st, 1999.* *200 000 certificates are active.*
Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application;	*There are no difficulties regarding electronic signatures.*
Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature *for this specific eGovernment application* (e.g. through an awareness programme)?	*The act on electronic signature.* *The act on informatisation of entities activities for public tasks performance.*

10.2.5 Assessment

Assessment	
Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses). Take this opportunity to bring any fruitful information that was not addressed by previous questions.	*It is my personal opinion that the implementation of described system is a great success of ZUS. ZUS is the first entity in Poland which have decided to implement electronic signatures massively.*