

# Analysis of Problems Associated with Implementing Electronic Digital Signature in Ukraine

## Table of Contents

1. PRINCIPLES AND SPECIFIC ASPECTS OF BUILDING ELECTRONIC DIGITAL SIGNATURE SYSTEMS .....	2
1.1 WHAT IS AN ELECTRONIC SIGNATURE? .....	2
2. LEGAL STATUS OF A ELECTRONIC DIGITAL SIGNATURE .....	2
3. KEY CERTIFICATION CENTERS .....	4
3.1 GENERATING EDS KEYS .....	5
3.2 CERTIFICATION RULES .....	5
3.3 REINFORCED KEY CERTIFICATE .....	6
3.4 ACCREDITED KEY CERTIFICATION CENTER .....	6
3.5 CERTIFICATION OF A KEY .....	7
3.6 CENTRAL AUTHORIZING AGENCY .....	7
4. USING ELECTRONIC DIGITAL SIGNATURE .....	8
4.1 APPLICATION OF THE DIGITAL SIGNATURE .....	9
4.2 GENERATION AND OPERATION OF A DIGITAL SIGNATURE .....	9
5. STATUS AND PROSPECT FOR APPLICATION OF ELECTRONIC DIGITAL SIGNATURE IN UKRAINE .....	10
5.1 ELECTRONIC REPORTING WITH EDS .....	11
5.2 USE OF THE ELECTRONIC DIGITAL SIGNATURE IN DOCUMENT FLOW SYSTEMS .....	14
5.3 CREATION OF A UNIFIED CENTER FOR CERTIFICATION OF ELECTRONIC DIGITAL KEYS .....	15
6. CONCLUSIONS AND RECOMMENDATIONS .....	17

# 1. PRINCIPLES AND SPECIFIC ASPECTS OF BUILDING ELECTRONIC DIGITAL SIGNATURE SYSTEMS

## 1.1 WHAT IS AN ELECTRONIC SIGNATURE?

The Law of Ukraine “On Electronic Digital Signature” gives the following definition of the electronic digital signature: *Electronic digital signature is a (type of) electronic signature generated by cryptographic conversion of a set of electronic data, which is attached to (or logically combined with) this set of data and enables a user to confirm data consistency and identify its signer. The electronic digital signature is generated with a personal key and verified with a public key.*

Therefore, two security keys (which are stored at different locations) are used to run the electronic digital signature (EDS) system, namely:

- 1) Private (secret) key, which is kept by a signer (for example, on a floppy disk, Touch Memory, Smart card, etc.);
- 2) Public key which is usually available from a public or classified directory.

The private (secret) key is used to generate EDS whereas the public key is used to check the digital signature. The public key does not enable its holder to replicate the private key or generate the digital signature. The only thing she/she is able to do is to verify EDS. The private key of a signer is his/her property and cannot be transferred to a third party (even to the key certification center). Anybody may verify the digital signature with the public key only.

Attaching the electronic digital signature (signing) is an operation which is performed by document's sender (signer) with his/her private key. To perform this operation, the sender needs to run an appropriate application with a document to sign and his/her private key as parameters. With the private key, the application generates a unique block of data of a fixed size (essentially EDS) which is true only for the given private key and document. In other words, EDS is a distinctive “digital print of a private key and document”. As a rule, EDS is attached to an initial document (or entered in some field of the document) so that this combination (document + EDS) constitutes a secured electronic document.

Verification of an electronic digital document is an operation which is performed by a recipient of the secured electronic document with signer's (sender's) public key. In order to perform this operation, one has to have sender's public key (it may be available from a directory) and secured document (i.e. document data together with EDS data). A special application (software module) will check whether the digital signature complies with document and public key. The verification program will report on any modifications in the public key and document.

To ensure full-fledged operation of EDS system, recipients must have an access to senders' (signer's) public keys and be able to make sure that a given public key belongs to a certain signer. To this end, special protected directories of keys will be created and maintained by specialized institutions called key certification centers.

## 2. LEGAL STATUS OF A ELECTRONIC DIGITAL SIGNATURE

The Law “On Electronic Digital Signature” defines the legal status of electronic digital signatures and regulates relations arising from use of electronic digital signatures. However, this Law does not apply to relations arising from use of other types of electronic signature, including the digital image of a handwritten signature. According to Article 3 of Law of Ukraine # 852-IV dated May 22, 2003

“Legal Status of an Electronic Digital Signature”, the electronic digital signature is comparable to a handwritten signature (seal) by legal status when:

- Electronic digital signature is certified with a reinforced key certificate by reliable means of digital signature;
- Reinforced key certificate, which is valid as of the time of attaching the electronic signature, is used for verification purposes;
- Signer’s private key complies with the public key specified in the certificate.

The electronic signature cannot be found invalid just because it has an electronic form or it is not based on a reinforced key certificate.

The Ukrainian legislation envisages that five technologies of electronic identification can be used to sign electronic documents. These technologies, which are described below, feature various levels of legitimacy and legal regulation mechanisms.

1. Electronic-and-digit signature. While use of this type of electronic signature is envisaged by Article 207, Part 3 of the Civil Code, there is not a single clause in the current legislation which would regulate use of electronic-and-digit signatures.

2. Digital signature. Pursuant to Article 5, Part 7 of the Law on EDS, it is used in the banking sphere. Procedures for using digital signatures are specified by the National Bank of Ukraine, however, like in the previous case, the Ukrainian legislation fails to regulate it.

3. Electronic signature. According to Article 6 of the Law on electronic documents this should be interpreted as data in the electronic form which are attached to or logically associated with other electronic data and intended for identification of data’s signer. The electronic signature is a mandatory component of an electronic document and attaching it completes creation of the document. Despite Article 3, Part 5 of the Law on EDS says that *electronic signature may not be found invalid just because it has the electronic form and is not based on a reinforced key certificate*, lack of a direct applicability clause in the law precludes parties to civic relations from signing electronic documents with the electronic signature because the latter is not as valid as a handwritten signature.

4. Electronic digital signature is a set of data generated by cryptographic conversion of the content of an electronic document which makes it possible to confirm data consistency and identify a signer (Article 1.11 of the Law on payment system). This type of EDS is a mandatory component of electronic document. In terms of validity, it is comparable to the handwritten signature (Article 18.2-13.8 of the Law on Payment Systems). However, the Ukrainian legislation fails to define a procedure for using this type of electronic signature to sign electronic documents.

5. Electronic digital signature is a type of electronic signature generated by cryptographic conversion of a set of electronic data, which is attached to (or logically combined with) this set of data and enables a user to confirm data consistency and identify a signer (Article 1, Part 3 of the Law on EDG). This is the only type of the signature for which the law defines a procedure for using. By its legal status, it is comparable to the handwritten signature (seal) should it be confirmed by the reinforced key certificate with reliable means of digital signature.

Besides, this Law provides a list of participating entities in the area of EDG services, namely:

- Signer;
- User;
- Key certification center;
- Accredited key certification center;
- Central certifying authority;
- Certifying center of an executive authority or another government agency;

- Supervisory agency.

Article 17 of the Law says that foreign key certificates issued pursuant to the legislation of issuing countries are found valid in Ukraine according to the procedure established by the law.

The electronic digital or just digital signature (DS) are to be attached to electronic documents (ED) which are, generally speaking, a set of data that could be represented as a number. Needless to say, these are not “ordinary” numbers but sequences of digits which can be pretty long. The content of these document may be text, graphic, video/audio data, digital data etc. In other words, to attach the digital signature to an electronic document means to combine one number with another. In so doing, a concrete digital signature must be uniquely associated with both electronic document and person who used this signature. That is, any changes in the document content or improper attachment of the document to the signature must be identified as inadequacy of the digital signature to the electronic document.

Realization of these features of the digital signature and electronic document is based on application of cryptographic algorithms which use two mandatory parameters (numbers) called keys. One of them (private/secret) is used to sign a document whereas the other one (public) is used to verify DS.

Naturally, software, hardware or both, which are used by certain entities to attach or verify digital signatures should be based on the same cryptographic algorithm with certain fixed parameters, specifically, a fixed length key. Cryptographic algorithms, in turn, must be approved by relevant state standards or be recommended for application by an authorized government agency.

According to the Law “On Electronic Documents and Electronic Document Flow”, software, hardware, information security tools, and electronic and digital signature tools are subject to certification and expert examination pursuant to a procedure established by the authorized government agency. The Law specifies which government agency is responsible for certification of such systems. At the moment, these matters fall under competence of the Department for Special Telecommunication System and Information Security within the National Security Service of Ukraine.

### 3. KEY CERTIFICATION CENTERS

A key certification center (KCC) is one of entities emerging in the process of using DS, which is vested with certain authorities and responsible for verifying data of an open key holder and issuing protected electronic documents of a special form – public key certificates containing a public key and verified information on the key holder. Public key certificates are to be signed with the electronic digital signature of a key certification center. Therefore, having only one electronic document – a legally received certificate of a key certification center – enables its holder to verify authenticity of any certificate issued by this key certification center. Activities in organization and operation of such centers fall in the area of cryptographic protection of information.

A key certification center is an individual entrepreneur or legal entity of any ownership form which is duly licensed to provide digital signature services and maintain reinforced key certificates, receive and verify information required to register a user and generate a key certificate directly at the place of an individual, legal entity or representative thereof.

Key certification centers are the only entities in the EDS system which provide services in certification of public keys directly to end users. KCC functions include:

- Generating the own key pair (private and public keys);
- Registering (identifying) end users;
- Certifying users’ public keys (the process for generating public key certificates for end users);

- Distributing certificates through public directories to provide end users with an access to these certificates;
- Ensuring certificate withdrawal (blocking or canceling certificates at the onset of certain circumstances);
- Ensuring verification of certificate legitimacy (distributing lists of withdrawn certificates);
- Archiving certificates;
- Generating keys for users;
- Ensuring impossibility of refusal from using EDS;
- Administering certificate “history”;
- Putting timestamps;
- Making notary certification;
- Settling conflicts

Relations between customers of the EDS system and certification centers will be built on a contractual basis. This is specified by Article 5 of the Law of Ukraine “On Electronic Digital Signature”. A contract for key certification services is a possible legal form of using EDS as a legal equivalent of the handwritten signature. Only key certification centers are allowed to provide such services.

According to Item 5 of the “Regulation on using electronic digital signatures by government authorities, local governments, enterprises, institutions and state-owned organizations” approved by Cabinet of Ministers Decree # 1452 dated October 28, 2004, ... *an entity shall receive services associated with electronic digital signatures from an accredited key certification center on a contractual basis. In so doing, this institution may receive such services only from one accredited key certification center. Signers may not use private keys if corresponding public keys have been certified by other accredited key certification centers.*

This means that only keys issued by an accredited key certification center which is recommended by one or another government agency can be used to exchange documents with this agency. In other words, if a user is willing to exchange documents with a multiple government agencies, he/she has to obtain keys from all key certification centers recommended by these agencies.

### 3.1 GENERATING EDS KEYS

Generation of the private and public keys of an electronic digital signature is the initial procedure a user needs to accomplish prior to the procedure of certifying the public key. This is done with a specialized software program, a key generator, provided by a key certification center.

To accomplish certification of the public key, one needs to furnish the certification center with:

- Application for public key certification, a special electronic document containing the public key and electronic card with key holder’s details. The application is generated by a special program, key generator;
- Set of documents proving key holder’s identity (in case of entity officer’s key additional documents are required to prove that this officer is authorized to act on behalf of this legal entity).

### 3.2 CERTIFICATION RULES

Certification rules is a document describing rules for verifying information in a certificate which are specific for each center. That is, not all key certification centers operate by the same rules and follow the same requirements when they verify documents proving key holder’s identity (these rules are also called “certification policy”).

A number of checks and how detailed these checks are may vary across key certification centers. Many centers pursue multiple certification policies i.e. they issue certificates of various confidence levels (these confidence levels are sometimes referred to as “certificate classes”). Existence of various certificate classes is conditioned by the costs difference: the higher confidence level – the more checks, the more checks – the more work, the more work – the higher cost).

Certification rules and certificate class directly affect the level of confidence to key certificates issued by key certification centers. That is to say, confidence in a public key certificate depends not only on the very fact of certification but also on who (which certification center) certified it and by what rules (certification policy and certificate class).

### **3.3 REINFORCED KEY CERTIFICATE**

Generally speaking, certification policy and list of certificate classes are specific for each certification center. To standardize processes in this industry, many countries (including Ukraine) introduce a legislated concept of the “Reinforced key certificate” i.e. a certificate issued pursuant to certain standardized and legislated requirements and rules (including rules for certifying identify of a key holder). To become eligible for issuing certificates of this type, certification centers need to undergo an accreditation procedure i.e. a procedure for certification of compliance with statutory requirements. An accredited certification center has the right to issue reinforced key certificates. The responsibility for maintaining a list of accredited certification centers rests with the Central Certifying Agency.

By its order, the Department for Special Telecommunication System and Information Security within the National Security Service of Ukraine approved the Reinforced Certification Rules applying to accredited key certification centers. These Rules define organizational, technical, and technological requirements to accredited key certification centers with regard to the processes of servicing reinforced key certificates and ensuring proper use of these certificates. This Order was registered with the Ministry of Justice on January 27, 2005, # 104/10384, and enacted effective February 7, 2005.

According to Article 9 of Law of Ukraine # 852-IV dated May 22, 2003 “On Electronic Digital Signature”, accredited key certification centers will provide EDS services and maintain exclusively reinforced key certificates.

### **3.4 ACCREDITED KEY CERTIFICATION CENTER**

Another entity in the digital signature area – accredited key certification center – provides EDS services and maintains exclusively reinforced key certificates, receives and verifies information required to register a signer and generate a reinforced key certificate. An accredited KCC is a certification center which underwent a voluntary certification procedure which proved its capability of meeting commitments to service (maintain) reinforced certificates. In addition to statutory responsibilities and requirements, accredited KCCs must use only reliable EDS tools in the process of providing DS services.

Only those EDS tools are considered reliable which are either duly certified or backed by a positive conclusion based on the state expert examination in the area of cryptographic protection.

The Regulation on accreditation and requirements to accredited key certification centers are approved by Cabinet of Ministers Decree # 903 dated July 13, 2004 pursuant to Article 9 of the Law of Ukraine “On Electronic Digital Signature”.

This Regulation specifies a procedure for accrediting key certification centers, conditions on which centers provide EDS services, requirements to personnel and information security. Information on

accrediting key certification centers and terminating their operation is subject to disclosure by the Central Certifying Agency through its web site and printed media.

### 3.5 CERTIFICATION OF A KEY

A standard procedure for certifying a key is as follows:

- An applicant prepares documents, a list of which depends on the key type, and print out a form of contract for providing EDS services. Then the applicant receives key generation software and certificate of a specialized key certification center (SKCC) and fills out the application for key certificate. Once the two keys have been generated, the private key and application for certificate are saved on a floppy disk. Later on, the applicant prints out the key registration form and certificate of data in the key registration form and submits the above documents and materials to SKCC.
- SKCC operator certifies the public key (this stage consists of preparation and verification). The entire process consists of reading the application file from the floppy disk, verification of EDS shown on the application form, calculation of the actual ID number of the public key from the application file with a hash function, visual verification of the public key identifier from the application file with public key identifier on the paper key registration form, visual verification of details of application file with details of the paper key registration form.
- SKCC operator verifies documents proving information in the application file. SKCC operator certifies applicants public key with SKCC software by saving on applicant's floppy disk the public key certificate, key certificates of SKCC and Data Processing Center (DPC). SKCC operator writes down the date and series number of the certificate on the paper key registration form and signs it. Once the applicant has signed the paper key registration form in the "Key is certified" field, he/she receives the first copy of the key registration form. The application also receives his/her floppy disk (with applicant's certificate and certificates of DPC and SKCC saved on it). The other copy of applicant's registration form is sent to SKCC archive. At the completion of this technological cycle (at least once per business day) information on issued certificates is entered in the SKCC database.
- The subscriber (applicant/key holder) places its key certificate in the public key directory; in so doing, the subscriber uses SKCC master key for verification.
- SKCC sends information on certified public keys to DPC. At the next communication session, SKCC sends the updated database together with information on certificates' status (valid, blocked or cancelled) to DPC. Periodicity of reporting to DPC is specified by KSC's rules of procedure and contract between KSC and DPC. SKCC discloses information on blocked and cancelled certificates by posting it on its web site on a regular basis. Besides, the rules of procedure envisage withdrawal, blocking, voice authentication, cancellation and resuming of subscribers' public key certificates.

### 3.6 CENTRAL AUTHORIZING AGENCY

According to the Law "On Electronic Digital Signature", the responsibility for registering key certification centers and issuing key certificates of these centers rests with the Central Authorizing Agency.

The Cabinet of Ministers of Ukraine, by Decree # 1451 dated October 28, 2004 and pursuant to the Law of Ukraine "On Electronic Digital Signature", approved the Regulation on the Central Authorizing Agency. At the moment, the Ministry of Transport and Communication performs functions of the Central Authorizing Agency. A Coordination Council was set up to coordinate activities of the Central Authorizing Agency; members of the Coordination Council were appointed.

Cabinet of Ministers Decree # 1454 dated October 28, 2004 approved the Regulation on Mandatory Provision of Documented Information.

This Regulation determines a mechanism for mandatory provision of the Central Authorizing Agency or authorizing center of reinforced certificates with public keys and documented information for safekeeping by an accredited key certification center in the event of shutting down.

This is done to make it possible to verify an electronic digital signature of a signer whose public key is certified by an accredited center which seizes its operation. The Regulation specifies the algorithm for providing information and content of this information.

Regulation on the Central Authorizing Agency established legal grounds for provision of services in EDS registration. Pursuant to this Regulation, a buyer of EDS may use it at his/her own discretion.

The Cabinet of Ministers, by its Decree # 1453 dated October 28, 2004, approved the Standard Procedure of electronic document flow within executive authorities.

This Standard Procedure establishes general rules for documenting administrative activities of executive authorities electronically and regulates all operations with an electronic document from the time its created or received up to the time of sending it (to executive authority's archive).

Executive authorities perform all other operations with electronic documents pursuant to requirements to paper documents determined by internal rules.

The Standard Procedure applies to all electronic documents which are created or received by executive authorities. In particular, the Standard Procedure defines how to organize processing of incoming, internal, and outgoing electronic documents as well as processes for agreeing on and safekeeping of electronic documents.

#### **4. USING ELECTRONIC THE DIGITAL SIGNATURE**

Use of electronic digital signature is based on two major processes/tools:

- Encryption with the public key;
- Hash-value of a document.

Document hash-value is a checksum or, in other words, digital digest which is calculated with a hash-function so that each document has a unique hash-value. Should even minor modifications be made in the document (even if a single comma is shifted/deleted) its hash-value will be modified. From technical perspective, the electronic digital signature looks like document hash-value calculated with a known algorithm and encrypted with sender's private key; in so doing, the electronic digital signature should include a reference to the hash-value calculation method (hash-function). Therefore, a recipient of the document may decipher with public key the hash-value specified by the sender and verify it with the actual hash-value of the document. Equality of both indicates that the document was signed by the holder of the given private key and that the document was not modified in the transmission process.

Needless to say, all these operations are performed by a special program. A text document or a portion thereof may be signed with the electronic digital signature.

A signed document together with the digital signature may be printed out, saved on a magnetic medium or sent via web. If an entire file is signed with the electronic digital signature (this may be text or graphic file), then, traditionally, the electronic digital signature is generated as a separate file (the electronic digital signature file) which is attached to the signed file.

#### 4.1 APPLICATION OF THE DIGITAL SIGNATURE

Digital signatures are used to make sure that a message has come from a given sender on the condition that this sender is the only holder of the private key matching his/her public key.

Digital signatures are also used to put **timestamps** on documents. A party in which we trust signs a document containing the timestamp with his/her private key, thus, confirming that the document was existent at the time showed by the timestamp.

Digital signatures may be also used **to certify** that a document belongs to a certain person. Namely, the public key and information on whom this key belongs to are signed by a trustee. In so doing, our trust in the signer may be based on that the signer's (trustee's) key has been signed by a third party. Therefore, the trust hierarchy emerges. Obviously, someone's key needs to be the root of hierarchy (i.e. we trust this "someone" not because his/her key is signed by somebody else but simply because we a-priory believe that this person/entity can be trusted). There is a few root keys of the web **in the centralized key infrastructure**, for example, **certification authorities**. There is no need to have universal keys for all root keys in an extensive web; therefore, each party may trust its set of root keys, say, its own key and keys signed by it. Such a concept is called **web of trust** and realized, for instance, in Pretty Good Privacy (PGP).

#### 4.2 GENERATION AND OPERATION OF THE DIGITAL SIGNATURE

As a rule, the digital signature of a document is created in the following way: the **message digest** is generated first and then information on document signer, timestamp, etc. is added. Next, this information line is encrypted with signer's private key and some algorithm. The generated set of bits represents a signature. Signer's public key is usually attached to the signature. First of all, a recipient decides whether he/she is sure that the public key really belongs to the given person. Then the recipient decipheres the signature with the public key. If the signature has been deciphered normally and its content matches the document (digest, etc.) the message is found confirmed (certified).

- On the whole, the EDS system operates as follows: an individual or legal entity willing to become a participant in the system (in terms of the Law – signer), applies directly to an (accredited) key certification center or its authorized representative which in the registration process with a certain confidence level identifies the applicant and its/his/her data needed to generate the certificate (reinforced certificate);
- KSC generates user's public key certificate and certifies it with its signature;
- The new certificate is entered in the KSC database of valid certificates, thus, it becomes available to all users through public communication links.

Now, a sender sends his/her certificate together with a signed document. On receiving a message, a recipient sends a query to the database of certificates, gets sender's certificate based on his/her identification data, checks the status of this certificate (valid, blocked, cancelled). If the certificate is valid as of the time verification of EDS, the recipient extracts sender's public key from the received certificate and verifies sender's signature.

Generation of EDS on the electronic document and follow-on verification of EDS by users go beyond responsibilities of a key certification center. Normally, such services are provided with special software products. It should be noted that client software which ensures generation and verification of EDS is automated and absolutely transparent for users.

## 5. STATUS AND PROSPECT FOR APPLICATION OF ELECTRONIC DIGITAL SIGNATURE IN UKRAINE

As a matter of fact, some Ukrainian agencies and organizations have been using EDS for a long time. For example, the National Bank of Ukraine (NBU) uses EDS in the electronic payment system (EPS). NBU did not wait for enabling legislation to be passed to implement its own EDS system. All commercial banks are bound to use EDS. Ukrainian banks use electronic documents within the state system of electronic payments and through various Client-Bank systems. Clearing operations in the banking sphere are regulated by the Law of Ukraine “On Payment Systems” which defines the notion of “electronic document”. However, application of electronic documents in the Ukrainian banking system is limited. The Law fails to provide a comprehensive definition of “electronic signature” and rules for using it. The current banking clearing system in Ukraine is legislated due to passage of the Laws “On Electronic Digital Signature” and “On Electronic Document and Electronic Document Flow” which define electronic document flow as electronically generated information that includes mandatory fields, in particular, electronic signature, needed to identify document author or signer.

Currently, international payment systems are in the process of transferring to DS-based electronic information processing standards (public key infrastructures, **PKI**), namely, **SWIFT**, **VISA** and **Europay** system. Very soon ES technologies will work up a major segment of electronic technologies market in the client service industry. This is evidenced by rapid development of **Identrus**, an international PKI bank consortium, which includes more than 60 strong financial institutions from 160 countries. These technologies are intended to secure electronic payments and electronic commerce.

UN and EU passed enabling legislation on electronic documents, namely, UN standard law on electronic signatures (2001); Directive 1999/93/EU of the European Parliament and Council dated December 13, 1999 on the electronic signature system; Resolution of the European Commission and Council 2000/709/EU dated November 6, 2000 on minimal criteria in the area electronic signature recognition. National legislation of EU member contraries was adapted to EU statutory requirements. There are principal differences in basic terms and ideology between the Law of Ukraine on EDS and EU legislation. For instance, under the Ukrainian legislation the electronic signature is intended to identify document author whereas the EU Directive envisages that electronic signature would be used for data certification which include both author identification and verification of authenticity/consistency of signed data (to make sure that the data were not modified after the signature was attached to the data).

Discrepancy in basic terms defined by the Ukrainian Law and EU Directive results in even bigger differences in definitions of the status of EDS or ES as an equivalent of the handwritten signature and associated notion of “signature reliability”. The Ukrainian law sets three criteria of equivalence to the handwritten signature: (a) EDS is certified with a valid reinforced key certificate (as of the time of generating EDS); (b) Signature is generated with reliable EDS tools; (c) private key complies with the certified public key.

At the same time, the EU Directive (Article 5) defines a different criterion of handwritten signature equivalence – an enhanced electronic signature which is based on a valid certificate and generated with secure signature generation tools. Since Ukraine pursues the EU accession strategy, such differences and inconsistencies constitute a real problem of Ukraine’s European integration. Among other commitments, Ukraine needs to harmonize the national legislation with the legislation of EU member countries.

Since the Law of EDS does not specify any special procedure for registering key certification centers, any legal entity of any ownership and institutional form may become a key certification center on the condition that its public key is certified by the Central Certifying Agency or certifying

agency. Today, the number of registered key certification centers, which offer EDS and electronic document flow services, keeps growing. Key certification centers provide EDS services to individuals and legal entities on a contractual basis. Generally, key certification centers charge fees for generating key certificates and follow-on maintenance of certificates (blocking, cancellation, resuming of validity, etc.).

As far as users are concerned, EDS allows them to keep the costs of a transactions down due to making transactions via Internet and conversion of document flow into electronic document flow. Electronic document flow gains particular significance in view of Ukraine's joining international trade systems.

The Law on electronic signature enables individuals and legal entities to use the electronic signature for certification of materials and documents sent electronically. Today, use of electronic document flow tools is a pressing issue for the organized securities market. Use of electronic documents will allow brokers from remote regions to conclude contracts directly from their offices. Such contracts can be sent via Internet to the depository for immediate execution. This will be a significant progress as compared to the situation when contracts concluded in the electronic trade system have to be also delivered on paper via regular post service or courier.

Today, securities custodians have an opportunity to transfer from cumbersome flow of paper documents to/from clients to the electronic one. Therefore, management of securities accounts will be more efficient and convenient for clients; execution of clients' instructions will be sped up.

## **5.1 ELECTRONIC REPORTING WITH EDS**

Electronic reporting is the most important area where application of EDS is feasible. Users benefit from reporting electronically with EDS tools in many way:

- There is no need to complete, print out, sign, and stamp paper reporting forms;
- Enterprises save funds due to reduction of costs of paper, equipment, transport. Most importantly, executives and accountants save their work time;
- There is no need to physically visit institutions which enterprises report to;
- Less time is needed to process reports and correct errors in reports.

Electronic reporting is a convenient and streamlined process consisting of the following stages:

- Generating a electronic report by specialized software;
- Generating EDS;
- Sending the electronic report by digital communication links (Internet, e-mail, modem connection, etc.) or delivering it on a physical medium;
- Verifying EDS;
- Accepting and processing the report.

The ultimate objective of using DS systems is authentication of information i.e. protection of participants in information sharing processes from fake information, detection of modifications of information which is transmitted or saved, securing that information is authentic, and identification of authorship. The EDS system assumes that each web user has his/her own private key, which is used to generate the signature, and matching public key available to other web users and intended for verification of the signature. The digital signature is generated based on sender's private key and document (file) content. One of users may be selected as a "Notary public" so that he/she is responsible for certification of any document with his/her own private key. The other users may verify his/her signature i.e. make sure that a received document is authentic. The algorithm for generating the digital signature is designed in such a way that knowing the public key does not enable anybody to fake the signature. Any user having the public key issued by the same key

certification center is able to verify the signature including an independent arbiter who is authorized to settle disputes on document/message authorship.

Today, all these opportunities and capabilities are of paramount importance for the State Commission for Regulation of Financial Services Markets, State Securities Commission, and Pension Fund of Ukraine. These agencies make consistent efforts to use electronic document flows in relations among participants in securities market.

For example, the State Commission on Securities and Stock Market is in the process of designing fundamentals of the legislative and regulatory frameworks so that electronic documents with the certified electronic digital signature are used in legal relationship among participants in the securities market and electronic signature is used to certify transactions with securities in the non-documentary form.

The Pension Fund of Ukraine has implemented and currently operates the Electronic Report system intended for automated download of reports. This system is a component of the global system of remote reporting by employers. The centralized monitoring of the Electronic Report system ensures versatile functionality of the Pension Fund. The system is intended for both legal entities and individuals reporting to the Pension Fund of Ukraine electronically and using EDS.

The state enterprise Information Center for Personified Record Keeping (ICPRK) has been set up within the Pension Fund of Ukraine which issues electronic digital signatures. It does not generate keys for electronic digital signatures but concluded a contact with the Kiev enterprise State Information Security Center (SISC) which is licensed for issuing and certifying keys for electronic signatures.

When a payer of contributions to the Pension Fund of Ukraine (either individual or legal entity) is willing to obtain the electronic digital signature, he/she/it needs to apply to a local PFU office and provide it with a package of documents according the list in Attachment 1. The applicant is offered to conclude two contract for yearly services:

- Contract with SISC for issuing certificates for using electronic keys (UAH 270 per year);
- Contract with ISPRK for using the Electronic Report system and maintenance of this system during a year (UAH 198).

Once the contracts are signed and yearly fees (totally, UAH 468) are paid, the applicant receives two floppy disks with electronic keys, software, and user's manual. The applicant (contribution payer) is registered in the Electronic Report system i.e. his/her/its keys are entered in relevant registers.

At the time of reporting to the PFU, the contribution payer generates the report electronically in the form of a number of files with ARM-R, a pension reporting program. Then the files are encoded with the Electronic Report system with user's individual electronic digital signature and sent to the PFU via Internet or on a floppy disk or CD.

Once the report has been received, the local (or central if the report has been sent via Internet) office of the PFU:

- Verifies validity of EDS and sends the acceptance report to the sender;
- Processes the reports and sends the verification report to the sender.

Therefore, a contribution payer has to pay UAH 468 each year for using EDS for reporting purposes. For the time being, not more than 300 contribution payers, primarily those residing in Donetsk and Luhansk regions, have obtained electronic signatures from SISC. Obviously, the EDS system is at the initial stage of development and the number of EDS users will be increased. However, most payers can hardly afford paying the UAH 468 for using EDS. That is why this yearly fee should be regarded as a factor hampering development of the EDS system. It is planned

to involve insured individuals on the electronic data sharing process so that future pensioners are able to access latest information on the status of their pension accumulation accounts.

The State Tax Administration of Ukraine faces a similar situation with use of the electronic digital signature. Almost all reports to the State Tax Administration (around 200 reporting forms) can be generated electronically with the BEST-Zvit program. To make these report legitimate, they need to be printed or encoded with EDS. The State Administration does not accept reports with electronic digital signatures obtained from those certification centers which are not associated with the BEST-Zvit developer.

Effective July 1, 2005, the Tax Administration requires from tax payers to report only electronically. However, even tax inspectors do not believe that this requirement will be met because many tax payers just do not have computers whereas many computerized tax payers do not have an access to Internet. Yet those who have both are not willing to pay fee for using of EDS and opt for generating reports without EDS.

Transfer to corporate electronic document flow system rather than electronic reporting systems looks more feasible and significant. This approach was used as a basis of a pilot project of the State Customs Service of Ukraine. In order to streamline the procedure of customs clearing of goods and vehicles involving submission of an electronic cargo custom declaration, the State Customs Service conducted the experiment to test electronic declaration form from September 2004 through January 2005. Specifically, temporary rules for custom checks and custom clearing of goods and vehicles envisaged use of electronic digital signatures in electronic documents with involvement of an accredited key certification center on a contractual basis pursuant to the Law of Ukraine “On Electronic Digital Signature”. The temporary rules defined EDS as a mandatory component of electronic documents. A document not certified with the EDS could not be accepted for customs clearing. In so doing, when accepting electronic documents customs houses had to adhere to the predefined EDS verification procedure realized through a software program capable of certifying consistency and authenticity of electronic documents. The temporary rules applied exclusively to entities of foreign economic activities participating in the experiment on the condition that they agreed to take part in the experiment and concluded a relevant contract.

Confirmation of consistency of data which were accepted, processed, saved and sent to customs authorities as well as confirmation of signer’s identity were certified with EDS. The mechanism for attaching and verifying EDS was realized through special software programs. Custom clearing and custom inspection of goods and vehicles were made with an automated informational system for processing electronic data. A special regulation determined organizational conditions for using EDS, in particular, processes for generation, saving, use, deletion of personal keys belonging to officials of foreign economic activity entities and/or customs authorities which were used to attach EDS to electronic documents as well as procedures for generating, canceling, blocking, and resuming certificates of public keys.

The software program for preparing, editing, and sending customs declarations to custom authorities, which was used in the experiment, featured the following capabilities:

- Data generation;
- Verification of the format of information on goods and vehicles;
- Generation and import of customs declaration forms;
- Verification of prepared declarations to make sure that they comply with the requirements to the data structure and form set out by Order of the Customs Service of Ukraine # 628 dated August 30, 2004 “On Approving Specifications for Sharing Data”;
- Attachment of EDS to customs declarations (EDS was attached to an electronic document as either integral part thereof or separate file depending on specifics of a given EDS tool which was used to attach EDS);

- Sending of declarations to customs offices;
- Verification of EDS on electronic messages received from customs authorities.

Authenticity of EDS attached to an electronic document was checked by verification of EDS with the public key certificate of an official who put his/her signature, verification of validity of the public key certificate of an official who put his/her signature at the time of attaching EDS, and verification of the public key certificate of the key certification center. If an electronic document with attached EDS did not meet those requirements, the EDS was found invalid.

The computer center of the customs office automatically checked validity of EDS and compliance and then either rejected the declaration or accepted it for further processing. The software-and-hardware key certification system featured the following capabilities:

- Generating key certificates for officials of foreign economic activity entities and custom authorities;
- Distributing key certificates to customs authorities and entities subject to customs clearing (applicants);
- Canceling, blocking, and resuming key certificates;
- Maintaining the database of generated key certificates.

Once verification has been completed successfully, the customs computer center registered the electronic declaration and assign it a unique number. A notification showing this number (or a list of errors detected if the application was rejected) was generated and sent to the applicant.

Based on verification results, a customs official may decide to inspect declared goods and vehicles.

While outcomes of the experiment are still being processed, the very fact of this pilot suggests that implementation of the electronic signature and electronic document flow is an urgent task and both will become a common practice in the Ukrainian Customs Service soon.

## **5.2 USE OF THE ELECTRONIC DIGITAL SIGNATURE IN DOCUMENT FLOW SYSTEMS**

Today, the process of transferring to legislated electronic document flow systems is hampered by a number of reasons. One of them is insufficient funding for purchase of software. However, lack of experience in using EDS and electronic document flow systems outweighs financial problems. Meantime, important requirements to security and authenticity of electronic messages (documents) need to be met as soon as possible. For example, ordinary e-mail and networks fail to provide any security mechanisms. Any message can be easily read by strangers. A copy of the message is saved in the cache memory of internet-provider's server. Office network servers also keep a copy of the message. Besides, copies of the message are saved on all servers through which the message is routed to the recipient. System administrators of intermediary servers may read the message and forward it to whomever they like. Special services of powerful nations usually scan e-mail to find and check suspicious key words and phrases.

Usually, an encryption system does not solve the information security problem for 100 percent. Here one should rather talk about ensuring authenticity and confidentiality of information. This is, in fact, what the electronic signature is intended for.

Almost all Ukrainian enterprises are planning to use electronic document flow systems and, specifically, electronic digital signatures in the future. They are in the process of setting up relevant functional units, learning document flow technologies, and even implementing some solutions. As it turns out, however, most organizations are not ready to switch to the total document flow and even are not aware of how they will really benefit from it. That is why high fees for accomplishing not an urgent task make organizations postpone implementation of document flow system sine die. To change this situation, it would be reasonable to implement a model of corporate document flow and EDS, identify its specifics, test processes, and only then decide on feasibility of legislating and

implementing legislated electronic document flow systems. Such a model could be easily realized based on freeware, for example, GnuPG. GNU Private Guard is a free non-commercial analog of PGP which is also based on OpenPGP IETF standard. Software development under auspices of GNU Privacy Project is funded by the German Federal Ministry of Economy and Technologies. These software development tools are an open source i.e. they are absolutely free for both commercial and non-commercial use.

For instance, you can use GPG to encode a message, sign a letter electronically and certify not only authorship but also content of the letter. On receiving the letter, its recipient will verify your electronic signature to make sure that you are the sender and the message was not modified after you signed it. These two principles of using GPG apply to files which are saved on a computer or sent via network.

GPG is based on the Public Key Infrastructure Principle i.e. there are two keys: the private key is used for signing and encrypting whereas the public key is used for deciphering and verifying the signature.

First, a pair of keys needs to be generated. The process begins with selection of the key size, duration of key validity, selection of private information to be used to identify the new key and key phrase. Then the pair of keys is generated. Generated keys may be used for attaching EDS to messages and encrypting data. Most e-mail client programs support encryption and EDS; users have just to configure the Security fields properly. Ciphering and deciphering of an ordinary file is accomplished with the gpg utility, which is included in the GPG package. If you need to attach EDS to the file, the signature will be either inserted in the file if this is a text file or saved in a separate file if the file is binary. In doing so, the content of the file will remain unchanged. Any attempt to make even negligible changes will invalidate the signature.

Once the keys have been generated, other people's public keys need to be linked to your set of keys. This can be done by placing your key on a special PGP/GPG server intended for safekeeping of public keys. The key may be also saved on your own site. If someone has sent you his/her public key, you may import this key. Should there be a need in automated detection of authenticity of public keys, a confidence web has to be created.

The GPG open protocol is in no way worse than similar commercial products and may be used to accomplish all tasks associated with document flow and EDS.

For practical application of the above solution, an organization needs to develop a friendly client module, for example, thin Internet client, deploy the corporate server from which clients will be able to obtain EDS, and create a special PGP/GPG server for saving public keys. Later, this technology could be offered to all interested entities; in such a way a confidence web will be created. This solution could also serve as a basis for creation of a unified center for certification of electronic digital keys for government agencies.

### **5.3 CREATION OF A UNIFIED CENTER FOR CERTIFICATION OF ELECTRONIC DIGITAL KEYS**

As it has been pointed out, each government agency may choose a key certification center (KSC) at its own discretion and require from entities which send it electronic documents to use only those keys which are issued by this KSC. As the State Commission for Regulation of Financial Services Markets, State Securities and Stock Market Commission, and Pension Fund of Ukraine are committed to accomplish similar tasks in the process of implementing electronic document flow and EDS systems for participants in the Ukrainian financial stock market, it would be feasible to set up a unified center for certification of electronic digital keys for these entities (market participants). Naturally, each of these entities may pursue its own EDS implementation policy pursuant to the Ukrainian legislation, for example, use services of intermediaries like it is done in the PFU or set up their own centers of key certification. Fees charged by intermediaries increase costs borne by users

of EDS. Should entities in the financial and stock market use services of a unified key certification center, EDS would be more attractive to clients, at least, this solution would be more cost-effective. Besides, existence of the unified key certification center would streamline implementation of electronic document flow systems by financial and stock market participants. It should be noted that the level of fees for generating key certificates depends on a number of factors including duration of certificate validity, key length, etc. Charges for certification of EDS keys vary across key certification centers; the average fee for key certificate is roughly UAH 250 for individual and UAH 300 for a private entrepreneur. The digital stamp costs UAH 350 for a private business and UAH 450 for a legal entity. The key combined with digital stamp for legal entity's official costs some UAH 550. However, a client may purchase KSC services through an intermediary rather than directly like it happens in the PFU. In this case client's costs almost double.

Therefore, from conceptual and economic perspectives, it is feasible to set up the unified center for certification of electronic digital signatures for participants in the Ukrainian financial and stock market (in the future – for all legal entities and individuals exchanging electronic documents with government agencies). This would make it possible not only to unify **use of private keys by signers** but also pursue an agreed pricing policy, thus, making use of EDS more attractive to Ukrainian residents.

Taking into account experience gained in this area by the Tax Administration, Pension Fund, and other government agencies, such center could be set up on the basis of an existing KCS, say, the State Information Security Center (SISC).

Such a certification center will play an important role in the system of reporting by participants in the Ukrainian stock market. It will ensure proper administration of security keys in the secured electronic document flow system. In this system, document will be transmitted via public communication links with encryption and EDS mechanisms to ensure consistency and confidentiality of information. In the future, this center could be used in (personal and collective) document flow systems of any level complexity (centralized, decentralized, mixed systems) to administer keys intended to secure confidential information.

The unified center for certification of electronic digital keys for participants in the Ukrainian financial and stock market may be created on a phased basis with unification of the reporting system at the first stage and parallel design of the concept of the center, development of specifications for technological communications, and creation of a web portal.

## 6. CONCLUSIONS AND RECOMMENDATIONS

1. Enactment of the Laws “On Electronic Documents and Electronic Document Flow” and “On Electronic Digital Signature” effective January 1, 2004 defined the legal status of the electronic digital signature and settled relations emerging from use of the electronic digital signature. A series of Cabinet of Ministers decrees approved regulations and procedures binding for parties to relations arising from use of EDS. That pushed hard on development of information technologies and services in Ukraine. One can state that legal fundamentals for using the electronic digital signature in Ukraine do exist despite some inconsistencies in the legal framework and lack of some enabling laws and regulations.
2. According to the Laws of “**On Electronic Digital Signature**” and “**On Electronic Documents and Electronic Document Flow**”, an electronic document is defined as electronically generated information which includes compulsory fields of a document. In so doing, the electronic signature is a mandatory field intended to identify document’s author or signer. Most enterprises have to implement EDS as they state their intention to transfer to electronic document flow systems in their development programs.
3. In view of Ukraine’ strategic plan to join the European Union, the major task of the Legislator is to bring the Ukrainian laws on EDS, electronic document, and electronic document flow in compliance with the EU legislation. In the context of Ukraine’ European integration such harmonization will eliminate barriers hampering implementing a regime of mutual recognition of electronic signatures existing in EU and Ukraine. Most probably, new laws need to be drafted based on the existing laws while other laws and, in the first place, the Civil and Criminal Code need to be revised.
4. There is a positive trend in Ukraine: the number of Ukrainian users of Internet has been increased by 40 percent recently, which is close to the average European rate (50 percent to 55 percent). Given the international experience one may project that in the nearest future electronic signature technologies will work up a significant segment of the electronic technologies market in the client servicing field. Hence, there is an urgent need to ensure reliability and security of electronic payments and electronic commerce.
5. Article 8 of the Law of Ukraine “On Electronic Digital Signature” clearly defines that *a key certification center is any legal entity irrespective of its ownership form or individual entrepreneur which/who provides electronic digital signature services and has certified its/his/her public key with the Central Certifying Agency or certifying center pursuant to the requirement of Article 6 of this Law*. Therefore, the Law does not define a special procedure for registering key certification centers. Due to that any legal entity regardless of its ownership and institutional form may become a key certification center on the condition that its public key is certified by the Central Certifying Authority or certifying center, Ukraine sees a growing number of registered key certification centers offering services in EDS and electronic document flow.
6. Implementation of EDS-based electronic document flow systems will help users to speed up many commercial transactions; reduce the volume of book keeping paper documents; save employees’ time; minimize costs associated with execution of contracts, delivery of payment documents, reporting to supervisory agencies, obtaining certificates from government agencies, registration, licensing, etc. Transfer to corporate electronic document flow system rather than electronic reporting systems looks more feasible and significant.
7. On the part of businesses, EDS is considered as an ordinary good for sale. Accordingly, businesses will not set up key certification centers and apply for due licenses unless they are

- able to get profit. Unfortunately, for lack of pilot projects it is practically impossible to project how this industry will development. Such situation hampers modernization of the banking structure and trading via Internet in Ukraine. Creation and operation of the unified center for certification of electronic digital keys for participants in the Ukrainian financial and stock market could demonstrate advantages of electronic document flow systems and bring EDS-based technologies closer to businesses.
8. Implementation of the EDS system is not the end in itself. EDS should be considered exclusively in the context of concrete tasks. One of these tasks is to implement the electronic document flow system in Ukraine. Accomplishing this task involves high costs of equipment, training, creation of proper structures, purchase of EDS keys, etc. Many enterprises lack funds to switch to the electronic document flows or are not aware of advantages of this system. In this connection, it would be feasible to implement a pilot project under which enterprises could be able to get EDS keys for free or for a very small charge so that they are able to implement their own document flow systems. This would enable Ukraine to implement a corporate model of the EDS-based document flow system, identify its specifics and test processes and later decide on feasibility of legislating and implementing legislated electronic document flow system. Such pilot project is easy to implement with available freeware, namely GNU Privacy Guard, a non-commercial analog of PGP. From practical perspective one needs to develop a friendly client module, for example, thin Internet client, deploy the corporate server from which clients would be able to obtain EDS, and create a special PGP/GPG server for saving public keys. Later, this technology could be offered to all interested entities; in such a way a confidence web will be created. This solution could also serve as a basis for creation of a unified center for certification of electronic digital keys for government agencies.
  9. Despite the current legislative framework is sufficient for implementing EDS, laws and regulations contain only general provisions. Today, EDS is perceived by government agencies as a technical means of information security rather than a realistic alternative to paper document flow. The Law on EDS must upgrade the government document flow by creating the legislative framework for industrial implementation of electronic technologies. Corporate awareness of EDS advantages in such areas as reporting, customs clearing, and electronic document flow needs to be improved through intensive public education campaigns, in particular, regular seminars, information Internet portals, etc.
  10. According to Item 5 of the “Regulation on using electronic digital signatures by government authorities, local governments, enterprises, institutions and state-owned organizations” approved by Cabinet of Ministers Decree # 1452 dated October 28, 2004, ... *an entity shall receive services associated with electronic digital signatures from an accredited key certification center on a contractual basis*. Since the entity may receive such services only from one accredited key certification center, it is conceptually and economically feasible to set up a unified center for certification of electronic digital keys for both participants in the Ukrainian stock market and Ukrainian government agencies.
  11. Creation of the unified center for certification of electronic digital keys for Ukrainian government agencies will make it possible not only to unify use of private keys by signers by also to pursue an agreed pricing policy, thus, making use of EDS more attractive to Ukrainian residents.

## Introduction

Over the past ten years, the use of electronic documents exchange has become a significant part of government reporting landscape. The concept of e-filing, e-reporting etc. has become a prominent technique for communications between various governmental agencies, individuals and business enterprises. The development of these techniques was inevitable, given the information technology advancements during the same period.

It is important to understand that e-commerce, e-reporting and electronic commerce, in general, should be considered a desirable goal from a public policy perspective. It is a positive development for the economic health and advancement of a countries economy. From a macro perspective, e-commerce improves efficiency and productivity by eliminating barriers and costs inherent in traditional transaction methods. It also opens the economy to commerce and transactions with more advanced information economies.

From a micro perspective, it can improve the efficiency of an agency by reducing the cost of data collection. Clearly, a government agency that can collect it's data electronically can reduce the expense of data collection. In some cases, it can reduce the cost of data collection by as much as 80%. So, it is highly desirable to encourage constituents and customers to use electronic means of reporting rather than "hard copy" submissions.

These advancements in the electronic reporting field have accelerated due to several major advancements in technology. The most important developments of the past ten years has been the advancement and deployment of the Internet, broadband connection and the wide acceptance of email.

The introduction of electronic processing of information has been accompanied with a reduction of personal, face to face contact. As people rely more on the Internet and e-mail the need to meet or the opportunity to meet face to face is reduced. This is one of the benefits of electronic commerce – people don't have to travel to conduct business. There is a down side to this impersonal environment. It becomes easier to mask ones identity and therefore the possibility of identity theft increases.

Identity theft and all its ramifications is not a new phenomemon. In the past, one could mask one's identity over the telephone or via post. In some cases, identity theft could even be accomplished face to face. But clearly it is easier to steal an identity when the environment is electronic or "virtual" and there is no physical contact between parties.

To promote electronic commerce and yet combat the possibility of identity theft in a virtual environment people have been employing several techniques to insure identity. One popular method is the use of a password to insure identity. For example, the access to a bank account will be controlled by a unique user ID and a password. It is assumed that if one knows the ID and the password this can prove the authenticity of the person. This is very effective against the casual identity thief. Of course, this will not stop a dedicated thief.

The concept of an electronic signature is another attempt to increase trust and predictability in electronic commerce and reporting. Again, it is used to insure the authenticity of identity. It is the application of a "traditional" technique (i.e. signature) into the "virtual" arena.

The signature concept (a person signing a document with their name) has been in existence for centuries. It is obvious to everyone, what the purpose of a signature on a document is, but it is useful to review this concept for the purposes of understanding its application to the technique of electronic signature. In general, a signature can:

- indicate that the person has created the document. (i.e. the signer is the author). An example is a personal letter with a signature at the bottom.
- indicate the person agrees with the contents of the document. An example of this is a contract between two parties.
- indicate that the person supports the position of the contents of a document. An example of this may be a petition being circulated for signatures.
- It can indicate that the signer is guaranteeing the contents of the document. An example of this may be a check or IOU.

In an ideal world a signature would be adequate to establish identity. However, in reality a signature does not always guarantee authenticity of identity. First, a signature can be a forgery. It is possible that a very accurate forgery can be achieved on a handwritten signature. Thus giving the indication that the signer has assented to a document.

To diminish the risk of forgery, we have developed the concept of a Notary Public who is warranted to examine the identity of the individual and attest that the person signing is in fact who they say they are. In some cases a stamp is affixed to the document to further attest to the authenticity of the document. It is assumed that a signature may be easy to forge, but a stamp or press may be more difficult to forge. Of course, if people are determined they can circumvent almost any method of verifying or authenticating a document.

Authenticating electronic documents have many of the same problems that authenticating paper documents have with some additional challenges. Since an electronic document is created via a keyboard, it is impossible to affix a free-hand signature to the document. Thus, the typing of the name of the signer can be forged with little effort. Therefore there is little or no validity to a typed name on an electronic document.

It is important to understand that in many cases a signature is a mere formality and may not be needed to verify authenticity. For example, an invoice from a company may not need a signature since the receiver may be well aware of the bill and there is no doubt who sent the invoice. Likewise, a personal letter may also not need a signature as it is again obvious who is sending the letter. In these cases, the signature may just be a formality.

It is only in a situation where the signature is necessary for proof of authenticity that a signature is needed. In these cases, the signature is a second line of defense against unauthorized or illegal use of a person's name or identity.

As mentioned, in many cases a signature is not necessary and the authenticity of a document is not in question. The lack of an electronic signature has been used as an excuse for delaying the implementation of electronic reporting. It is important, in all cases, to decide if a signature of any type is truly required or if merely typing the name of a responsible person or company is adequate.

In addition, creative methods can be found to avoid the need and complication of an electronic signature. For example, a password system can be developed which will require an initial set-up and then from that point on a signature is no longer necessary. The benefits of e-reporting are worth the effort to develop a workable method of electronic signature or its substitute.

## Legal Framework for Electronic Signature:

The concept of an electronic signature has been around for several years. However, the laws governing the use of electronic signatures have been fairly recent. In the U.S., electronic signature laws have been established only since 1995. The initial legislation was developed at the state level. Many states have only established laws in this regard since the late 1990's or early 2000's. The Electronic Signatures in Global and National Commerce Act (often referred to as the e-signature bill) specifies that in the United States, the use of an electronic signature is as legally valid as a traditional signature written in ink on paper. This is a Federal Law and has been in effect since October 1, 2000. The law is technology neutral, in that it does not specify any particular methodology or technology must be used.

The European Union's primary law (or directive) related to electronic signature was EU directive 1999/93 on "practical uses of electronic signature and related services". The function of this directive was to facilitate the use of electronic signature and to contribute to its legal recognition among member states. It also attempts to create a structure for the legal framework and to facilitate implementation of electronic signature. It is important to note that the directive is again technology neutral in that it does not attempt to mandate any particular technology. However, because of the nature of the EU, the actual implementation of electronic signature legislation will reside within the individual member countries. The directive's main purpose is to insure harmony of electronic signature rules among the members and avoid prejudicial or predatory practices by members. (i.e. one country not accepting an electronic signature from another country or requiring the registration of an electronic signature from a home countries certifying authority).

## Certification Process

As mentioned, the concept of a notary public or some form of additional verification of a person's identity has been developed long before electronic signature. The need to establish an independent, unbiased and reliable method of guaranteeing authenticity of a signature was developed long before computers or electronic commerce. A similar need exists in the electronic arena.

In the electronic arena, there is a need to establish the identity of the individual or enterprise at the beginning of the process. Without this step, electronic ID's could be obtained falsely and there would be little control over its illegal use. Therefore, the concept of "certifying" the identity of the person prior to issuance of an electronic ID has been developed. The certification process is somewhat equivalent to the notary public, in that it is an independent verification of identity.

Unlike the notary public, who must attest to the signature each time a document is signed, the certification process only occurs at the time of issuance of an ID. At some future time, there may be a need for an electronic notary public, but at current one does not exist.

In addition to the verification of identity, the certifying organization must also handle the "mechanics" of issuing an electronic ID. As will be seen later, this involves the issuance of a public and private "key". The technical issues will be discussed later, but it must be understood, that this process involves a few steps and is not trivial. In any event, it involves some knowledge of computers, cryptographic concepts, etc. Because of this, there is some expense associated with the distribution/certification process.

One of the major issues related to electronic signature is the transparency of the certification process. As will be discussed later, the technology involved in electronic signature generation and

usage can be complex. Since obtaining an electronic signature can involve several steps, there is some expense associated with the process. It is reasonable to expect some cost to be born by the recipient/consumer for this. Establishing a fair price for this is an important task in implementing electronic signature.

The most significant cost in the process is the certification of an individual or enterprise. That is the process of establishing the identity of the individual and issuing a public and private key. The cost of establishing a key certification center is usually determined by the electronic signature legislation. In the Ukraine, the process is controlled rather closely by the government. This is not the case in the U.S. where the certification process is generally left up to the marketplace.

Of course, when the marketplace is free to compete the price for a good or service is usually less. In the U.S. an electronic signature key can cost from \$15.00 to \$40.00 for an individual per year. The prices can be more for a company, and can range from \$100.00 to \$150.00 from a reputable certification center.

In the EU, where regulation and government intervention tends to be greater than in the U.S. , the cost of certifications vary considerably. The cost in Germany for an electronic signature for an individual is 30 eu. per year. This is considered by many people to be too high a price to pay for the service and it has been regarded as a major deterrent to the wider adoption of electronic signatures in Germany.

Poland is another country with experience in implementing electronic signatures. The costs in Poland are more expensive than Germany. The average cost of purchase for an individual private key is around \$ 75.00 (U.S.) for one year. Again, this is considered an obstacle to the implementation of electronic signatures on a broad scale.

Another factor affecting cost is the acceptance by all parties (government and non-government) of electronic signature certifications. Even if an electronic signature certificate is reasonably priced, it is a major deterrent to consumers if the certificate is not accepted by all government agencies. It is highly undesirable to force consumers to purchase multiple electronic signatures for different agencies.