Project Administrative Reform in Eastern Ukraine II

being implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

співпраця з німеччиною
DEUTSCHE ZUSAMMENARBEIT

Виконавець:
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Evaluation of the Ukrainian Trust Services - eID legislation (Law 2155-VIII), and related implementing decisions in view of the eIDAS EU regulation

Version 15.3

Dr. Andy Dresviannikov

08.04.2019

Table of Contents

Preface - How to Read This Report

This report is divided into three logical parts:

The first part includes the context of studies, introduction into technical aspects in the context of Ukrainian legislation “Law on Trust Services and eID” 2155-VIII and implementing decisions. Later provides uderstanding of interoperability concept is important for further assessment of related Ukrainian Implementing acts as well as their correspondence with EU regulations and legal framework designed to ensure validity and proper usage of eID and Trust Services. It also includes the list of related EU projects / frameworks /ITC Systems. This part is written to give a reader an nunderstanding of the subject and ought to be understood without deep technical or legal knowledge.

The second part provides: **a)** methodology, sets criteria of assessment **b)** the main findings and conclusions on legal interoperability of the Law 2155-VIII and implementing acts **c)** list of recommendations.

The third part provides supporting documents in form of tables, with cosscomparison of terms used in the Ukrainian legislation 2155-VIII vs. eIDAS 910 Reg. Main purpose of this part is to provide evidence for the analysis, findings and the recommendations gived in the part 2 as well as the basis for the follow up on this report that can be conducted independently. The third part includes the documents as follows:

1. **Comparison table of main terms used in Ukrainian Trust Service Law vs. EU Reg. 910**
   Expected outcome - comparison table Ukrainian term (as in Ukrainian Legislation)/ wording of term explained (as in Ukrainian Legislation)/ referring term + term explained in Reg910 (Ukrainian translation) / referring term + term explained in Reg910 (English) / Conclusion on how terms and legal wording of the terms corresponds (identical \ somewhat identical \ not corresponds \ no equivalent)
   Location: (summary section 2 for details see comparison table in Annex 1)
2. **“by Article” matching of Law of Ukraine "On electronic trust services" according to the eIDAS Regulation 910.**
   Expected outcome – by article cross matching with references to eIDAS Regulation 910
   Location: Annex 1 and files attached)

List of Abbreviations Terms & Glossary

CAB - Conformity Assessment Body - (as defined in **Regulation (EC) No 765/2008 Article2 point (13))** body that performs conformity assessment activities including calibration, testing, certification and inspection

CC Common Criteria or **(**Common Criteria for Information Technology Security Evaluation**)** - Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements.

CCA (C3O) Central Certification Authority (Sentral'nyy Zasvidchuval'nyy Orhan (SZO) - in Ukrainian Latin transliteration https://czo.gov.ua/ - CCA is subordinated structure of Ministry of Justice of Ukraine
CCRA Common Criteria *Recognition Arrangement - details at* https://www.commoncriteriaportal.org/

CESG Assisted Products Scheme (CAPS) is the UK analogue of CC for cryptographic devices used only in the UK

CMU - Cabinet of Ministers of Ukraine

DCFTA - Deep and Comprehensive Free Trade Area (agreement)

DSM - Digital Single Market

EAL - Evaluation Assurance Levels are a category ranking (EAL1 through to EAL7) assigned to an IT product or system after a Common Criteria security evaluation. The level indicates to what extent the product or system was tested. A product or system must meet specific assurance requirements to achieve a particular EAL

eID Electronic Identification

ENISA - European Union Agency for Network and Information Security https://www.enisa.europa.eu/

ICT - Information and Communications Technology

***ProZorro* -** Ukranian Government Online Procurement System (hybrid electronic open source government e-procurement system created as the result of a partnership between business, government and the civil society) - https://prozorro.gov.ua/en

MoJ - Ministry of Justice of Ukraine (https://minjust.gov.ua/)
PKI Public Key Infrastructure - is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage **public-key** encryption implies formation of pair of key Public (sometimes referred to as Pair of Open and Private Keys)

QSCD Qualified Signature Creation Device

SARs Security Assurance Requirements - descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality

SSCSU State Special Communications Service of Ukraine (Administratsiya Derzhspetszv"yazku - in Ukrainian Latin transliteration) http://www.dsszzi.gov.ua - (can be shortened to DCZ)

TSPs Trust Service Providers

TOE - Target of Evaluation (referred to in context of **EAL** Evaluation Assurance Levels and **CC** Common Criteria

QTSP - Qualified Trust Service Providers (in terms of the Law 2155-VIII this term defined as "Qualified Providers of Electronic Trust Services")

FRAND - fair, reasonable and non-discriminatory principal - denotes a voluntary licensing commitment that standards organizations often request from the owner of an intellectual property right (usually a patent) that is, or may become, essential to practice a technical standard. Put differently, a FRAND commitment is a voluntary agreement between the standard-setting organization and the holder of standard-essential patents.

EIF - European Interoperability Framework

Context & Introduction

On October the 5ht 2017 Ukrainian Parliament passed the Law 2155-VIII "On electronic Trust Services". The regulation was designed with view of eIDAS (EU 910 regulation) and allowed one year to build underlying implementing decisions base and regulatory documentation. The Law is entered into force from 7th November 2018, however regulatory and implementing decisions in the area of responsibility of Ukrainian Government is still work in progress. By due date Ukrainian Government finalized drafting of ALL implementation legal acts **with seven out on nine** are signed and entered into force. **Remaining two are at the draft stage**.

It's excepted that completion of implementing framework on Trust Services and eID shall sets a predictable regulatory environment for Ukrainian citizens, business, and public administrations to confidently go digital through the use of electronic identification (eID) and trust services (e-signatures, e-seals, e-time stamping, e-delivery service and website authentication) as well as facilitate cross-border digital interactions, especially with EU Member States.

In the EU Member Etates formation of a Digital Single Market (DSM) is ongoing process with eIDAS regulation (910 Reg) had been already implemented across 27(28) countries starting from 2014. Furthermore, EU DSM concept implies that businesses can further benefiting from full electronic electronic data interchange(EDI), electronic procurement etc.

Digitalized government procurement it already had been implemented by Ukrainian Government via introduction of tendering system "Prozorro".

Following positive examples of digital transformation in EU Member States Ukrainian business and public bodies (both central government and municipalities) can increase efficiencies of their operations, reducing cost and save time (citizens and of staff). In particular public sector will be able increasingly offer online public services, allowing for more convenient, secure, and transparent service provisioning to citizens. On top of operational benefits for the civil society, public administrations and businesses, if get it right, can prepare themselves to alignment of Ukrainian national regulations with EU Regulation the is one of the requirement of Deep and Comprehensive Free Trade Area (*DCFTA*) Agreement. It also can create grounds of seamless integration of Ukraine into EU Digital Single Market (DSM) that forms win-win situation with economic benefits of both sides.

Creation of legal trust framework for eID and Trust Services is an important and necessary step on the way of digital transformation of Ukrainian society. Hereafter only legal and partially semantic aspects of interoperability are considered and assessed. It is good to note that by itself regulatory framework does not automatically lead to the realisation of its opportunities. As had been already demonstrated by EU member states (where a large market and interest exist for the use of eID and trust services), many parties, even after considerable time of 5+ years of implementations are still unaware of the opportunities and obligations flowing from the eID and Trust Services related regulation.

If the eID and trust services frameworks lakes certainty and interoperability , domestic users most certainly will be reluctant to increase their online interactions, let alone in a cross border aspects of it.

Technical Aspects

interoperability is the ability of organizations, public administrations (including but not limited to government) bodies to interact towards mutually beneficial goals, involving the sharing of information and knowledge between one another , through the business processes they support, **by means of the exchange of data between their ICT systems.** (ref EIF)

The following Interoperability layers are defined (as set in EIF European Interoperability Framework)

1. Interoperability governance
2. Integrated public service governance
3. Legal interoperability
4. Organizational interoperability
5. Semantic interoperability
6. Technical interoperability

Hereafter we shall consider legal interoperability and partially semantic interoperability of national legislative framework matching it against EU regulations.

Legal interoperability - The first step towards addressing legal interoperability, is to perform 'interoperability checks' (prime subject of this study) by screening existing Ukrainian legislation to identify interoperability barriers: for instance over-restrictive obligations to use specific digital technologies or delivery modes in public services provisions, sectoral or geographical restrictions in usage and storage of data, different and vague data licence models, contradictory requirements for the same or similar business processes, outdated security and data protection needs, etc.Coherence among legislations, in view of ensuring interoperability, should be assessed before adoption and through evaluating their performance regularly once they are put into application.

Bearing in mind that long term preferences to provide public services in Ukraine (as well as European) are via digital channels, ICT must be considered as early as possible in the law-making process. In particular, proposed legislation should undergo a 'digital check':

• to ensure that it suits not only the physical but also the digital world (e.g. the internet);

• to identify barriers to digital exchange (**interoperability)**

• to identify and assess its ICT impact on stakeholders

This can facilitate interoperability between public services at lower levels (semantic and technical) and increase the potential for reusing existing ICT solutions, therefore reducing cost and implementation time. This also may require additional agreements between Ukraine and EU Member States to overcome differences in the implementation of the Trust Services and eID related legislation (for instance: Standards Recognition, *Common Criteria* Recognition Arrangement (*CCRA***)**.

EU is multilingual area with 24 officially recognized languages Article 12(6) of 910 Reg requires the use of the English language, for the purposes of the notification of electronic identification schemes therefore Englih considered to be a default languge set by eIDAS regulation acros EU**.** On the other hand EU includes two languages that use Cyrillic/Greek semantics in this regard it has relevance as Ukraine has_cyrillic alphabet and it makes semantic interoperability and correct terms transliteration an important point to pay attention too.

Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'. The semantic aspect refers to the meaning of data elements and the relationship between them. It includes developing vocabularies and schems to describe data exchanges, and ensures that data elements are understood in the same way by all communicating parties. On the side of semantic interoperability assessment this study will be restricted by alignment of the main terms used in Ukrainian eID and Trust Services regulation (Law 2155-VIII) vs. eIDAS (910 reg)

Technical interoperability covers the applications and infrastructures linking systems and services. Technical interoperability includes interface specifications, interconnection of services, data integration services, data presentation and exchange, and secure communication protocols. (not the subject of this study)

Additional outcome of this report can be assessment as to what extend eIDAS EU regulations complements or challenges domestic Ukrainian initiatives.

Related EU projects / frameworks /ITC Systems

Listed below are just few examples of e-services and EU –wide frameworks that increase efficiency and create Digital Economy. Ukraine can benefit either directly from taking part in those EU initiatives or by drawing analogies.

STORK is a set of pilot projects, which aims to establish a European eID interoperability platform by testing the interoperability of the existing technical solutions. First pilot have successfully proved the interoperability between participants. (STORK 2012)

e-CODEX is an operational ITC system that provide means of digitally exchange legal information between the Member States of the EU. The goal of e-CODEX is to improve the cross-border access of citizens and businesses to legal means and to improve interoperability between legal authorities within the EU. (e-CODEX 2014)

SPOCS is a large-scale pilot attempting to provide seamless electronic procedures by building cross -border solutions which are interoperable with the existing systems. The goal is to help businesses of EU Member States to overcome complications with apllying for licenses and permits, and completing other administrative procedures. (SPOCS 2012)

PEPPOL (Pan-European Public Procurement On-Line)is a set of artifacts and specifications enabling cross-border eProcurement. The use of PEPPOL is governed by a multi-lateral agreement structure that enables trading partners to exchange standards-based electronic documents over the PEPPOL network (based on a 4-corner model). These documents include e-Orders, e-Advance Shipping Notes, eInvoices, eCatalogues, Message Level Responses, https://peppol.eu

Joinup - is a collaborative platform created by the European Commission and funded by the European Union via the Interoperability solutions for public administrations, businesses and citizens (ISA2) Programme. It offers several services that aim to help e-Government professionals share their experience with each other. We also hope to support them to find, choose, re-use, develop and implement interoperability solutions. https://joinup.ec.europa.eu/

PART2

Executive Summary

Objectives of the assessment

- Extend of alignment of Ukrainian national legislation “Law on Trust Services and eID” 2155-VIII with EU eIDAS Regulation (EU 910)
- How well implementation acts that support “Law on Trust Services and eID” 2155-VIII reconciled with the Law itself and reality on the ground.
- Assess clarity of legal definitions of implementation acts (how well defined and split responsibilities of different bodies bodies, sequences of action, contingencies, and responsibilities in case of breaching the regulations)

Methodology

Ukrainian regulations and the Law (10 documents in total) are screened by means of interoperability checks, to identify existing and potential barriers to: **a)** regulations implementations **b)** interoperability **c)** compatibility with EU. For interoperability checks purpose the following criteria of assessment of the Law and implementation acts ware used**:**

- **Legal Certainty**
- **Technological neutrality**
- **Non-discrimination**
- **Interoperability**
- **Cross-border recognition**

Legal certainty is a principle in national and international law which holds that the law must provide those, who subject to it, with the ability to regulate their conduct. Legal certainty is also defined in terms of maximum predictability of officials' behaviour and ability of the subject to the law, to organise their affairs in such a way that does not break the law.

Technological neutrality is one of the key principles of the European regulatory frameworks for electronic communications. It means that the same regulatory principles should apply regardless of the technology used. Technology neutrality – sometimes referred to as (**Technology agnostic**) also means that regulators should refrain from pushing the market toward a particular structure that the regulators consider optimal. Since 2011, technology neutrality is recognized as a key principle for Internet policy (OECD, 2011)

Non-discrimination principle in application to eID and Trust Services implies equal legal effects and admissibility of electronic documents and another forms of documents (usually paper-based) in legal proceedings whan qualified electronic signature is used it has the equivalent legal effect of a handwritten signature. Non-discrimination principle of electronic documents is regulated at EU level by eIDAS (910 Reg) Article25 (2)

Interoperability is the ability of organizations, including but not limited to public administrations and government bodies, to interact towards mutually beneficial goals, involving the sharing of information and knowledge

between one another, through the business processes they support, by means of the exchange of data between their ICT systems. (definition taken from EIF)

Cross-border recognition – implied as potential of cross-border recognition of Ukranian domestic norms and proceeding accepted in another country. May be considered as one of the main goals of this study.

Analysis of Ukrainian regulation and implementing decisions related to Trust Services and eID was conducted in view of the following EU Implementing decisions:

Implementing decisions	CELEX number	link
On electronic identification:		
Commission Implementing Decision (EU) 2015/296 on procedural arrangements for MS cooperation on eID;	32015D0296	https://goo.gl/kxzNTW
Commission Implementing Regulation (EU) 2015/1501 on interoperability framework;	32015R1501	https://goo.gl/H5qB8q
Commission Implementing Regulation (EU) 2015/1502 on minimum technical specifications and procedures for assurance levels for electronic identification means;	32015R1502	https://goo.gl/YA3tJu
Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining thecircumstances, formats and procedures of notification	32015D1984	https://goo.gl/Efx8yL
On electronic trust services:		
Commission Implementing Regulation (EU) 2015/806 on the form of the EU Trust Mark for Qualified Trust Services;	32015R0806	https://goo.gl/AW9mot
Commission Implementing Decision (EU) 2015/1505 laying down technical specifications and formats relating to trusted lists;	32015D1505	https://goo.gl/7nGpkQ
Commission Implementing Decision (EU) 2015/1506 on formats of advanced electronic signatures and advanced seals.	32015D1506	https://goo.gl/TeFdbo
An additional Implementing Decision (2015/1984) on the notification of eID schemes to the Commission by the Member State for which there is no obligation but is complementary to reach interoperability was adopted on 3 November 2015. - original title - Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (notified under document C(2015) 7369) (Text with EEA relevance)	32015D1984	https://goo.gl/9wt5AG
Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014	32016D0650	https://goo.gl/rQQNQ6

Main Findings

Legislation Analysis (Law 2155-VIII – on Trust Services and eID)

The purpose of the Law 2155-VIII is to regulate the electronic identification (eID), and to set principles and means of functioning of the institute of Trust Services. The overall structure of the legislation resembles eIDAS regulation (EU Reg.910). Law 2155-VIII contains 38 Articles logically grouped in seven Chapters. Outcomes of the review are provided thereafter with emphasis on the correspondence of the legislation (Law 2155-VIII) with eIDAS EU 910 Regulation.

CHAPTER **I** comprise of four Articles devoted to:

Provisions of Article 1 Definition of terms - defined list of terms, in the area of eID and Trust Services numbered 44.

Provisions of Article 1 lists terms relevant to eID and Trust Services that had not been determined in other regulation – such as 4- "Open Key" 6- "Trust List" 7-"Electronic Trust Service" 10- "electronic timestamp", 21- "Interoperability", and 42 -"Technological Neutrality of technical solutions" On the critical side, however, it should be noted that definitions related to Public Key Infrastructure (PKI) namely definitions used in the foolowing Articles **2,4,14,30,33,35,38,39)** - may be considered as such that are in breach of Technological Neutrality Principal.

In-depth term comparison analysis presented in the form of comparison table in Annex 1

Provisions of Articles 2 (Scope of the Law) – define the area and the scope of the Law application (no obections or comments)

Provisions of Articles 3 (Legislation in the areas of electronic trust services and electronic identification) - lists other Laws and regulation related to the subject of the Law (no obections or comments)

Provisions of Articles 4(Basic Principles of State Regulation in the Area of Electronic Trust Services and Electronic Identification) - sets principals of the State governance and regulation in Trusted Services and eID. (no obections or comment)

Conclusions: Provisions of CHAPTER I define terms relevant to Trust Services and eID, provide a good degree of legal certainty and correspond well with eIDAS 910 Regulation with the reservation on technological neutrality related to Public Key Infrastructure (PKI).

CHAPTER **II** comprises of eight Articles (5-13) with main objective is to define State Regulatory Bodies in the Area of Trust Services and eID.

Article 5. The System of Bodies Governing Electronic Trust Services and Electronic Identification
Article 6. Powers of the Cabinet of Ministers of Ukraine (CMU) in the areas of electronic trust services and electronic identification
Article 7. Powers of the main Central Certification Authority **(CCA)**, which ensures the formation and implementation of state policy in the field of electronic trust services
Article 8. Powers of State Special Communications Service of Ukraine (**SSCSU)** in the spheres of electronic trust services and electronic identification

Article 9. Powers of the National Bank of Ukraine **(NBU)** in the areas of electronic trust services and electronic identification
Article 10. Powers of the central executive authority, implementing the state policy in the field of informatization, e-governance, formation and use of national electronic information resources, development of the information society

Article 11. Subjects of relations in the field of electronic trust services
Article 12. Rights and Duties of Users of Electronic Trust Services
Article 13. Rights and Obligations of - Qualified Trust Service Providers(**QTSP)**
Summary

There are three bodies stipulated by the Law that are involved in and responsible for regulations and executions of Trusted Services and eID in Ukraine.

Central Certification Authority (CCA) report to Ministry of Justice of Ukraine (**MoJ) and thereafter** Cabinet of Ministers of Ukraine (CMU) this body is entrusted with powers and responsibilities to initiate legislations / set state policies / run and maintain Trusted List / liaison with Qualified Trust Service Providers and with Trust Service Providers / determine the standards / ensure the standards are met / deal on the matter of international collaboration an cooperation – in fewer works CCA hold nearly ALL responsibilities in the areas of Trusted Services and eID - related to Business, Citizens and Public Bodies (including Government and Civil servants')HOWEVER with exclusion of those related to banking those are governed and regulated separately by National Bank of Ukraine **(NBU)**

State Special Communications Service of Ukraine (**SSCSU) –** regulated by separate legislation № 411 **(from** 03.09.2014) report to Cabinet of Ministers of Ukraine (CMU) directly and given powers of oversight and control in a matters related to Trusted Services and eID.

In particular, SSCSU has powers to carry out inspections of Central Certification Authority **(CCA),** Qualified Trust Service Providers **(QTSP).** SSCSU approval needed in matter related to security and therefore linked to nearly ALL aspects of operation and governance of Trusted Services and eID, it also involved in international treaties, technical aspects of standardization of equipment used in Trusted Services and eID provisions, attestation and approval of conformity assessment laboratories. It makes the SSCSU the major stakeholder in the area of Trusted Services and eID of Ukraine. However, with exclusion of the aspects related to banking. Those are governed and regulated separately by the National Bank of Ukraine (NBU).

NB SSCSU prior 2014 was the structural unit of State Security Service of Ukraine (SBU) and still carries on strong links both organizational and procedural.

National Bank of Ukraine (NBU) – is country's Central Bank. The legal status of NBU and the principles of its organization and activities are determined by Law of Ukraine "On the National Bank of Ukraine" the main function of the country's central bank is to ensure stability of monetary unit – the Hryvnia. To carry out its main function, the National Bank ensures the stability of the banking system. In regards to Trusted Services and eID the Law 2155-VIII gives NBU powers to regulated and control ALL aspects linked and related to Trusted Services and eID provisions in banking as well as in area of fund transfers.

Conclusions: Provisions of CHAPTER II defines regulatory bodies in the area of Trust Services and eID good degree of legal certainty.

CHAPTER III comprises of two Articles (14-15) devoted to Area of electronic identification (eID) and sets assurance levels of electronic identification schemes

Article 14. Means of electronic identification
Article 15. Schemes of electronic identification

Summary

CHAPTER III Sets the requirements to international agreements on Trust Services and eID as such that should include correspondent with domestic assurance level for means of electronic identification**.** The assurance levels (for the perpouse of electronic identification scheme) are further defined in the way identically to Article 8 eIDAS 910 Regulation with t efollowing wording:
assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the **purpose of which** is to decrease the risk of misuse or alteration of the identity.
assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the **purpose of which** is to decrease substantially the risk of misuse or alteration of the identity.
assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterized with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

Usage of qualified means of identification such as: qualified electronic signature and qualified electronic seal acknowledged as means of identification with high level of assurance.
Usage of advanced electronic signature (AdES) acknowledged as means of identification with substantial level of assurance**.**

Conclusions: Overall on defining of the assurance levels for Trust Services and eID Ukrainian Law 2155-VIII provides good degree of legal certainty and corresponds well with eIDAS 910 Regulation.

CHAPTER IV comprises of fifteen Articles (16-31) devoted to Electronic Trust Services (Trust Services)

Article 16. Requirements in Trust Services
Article 17. Use of Trust services
Article 18. Qualified Electronic Trust Service (**QTS** - Qualified Trust Services) creation, verification and confirmation of a Qualified Electronic Signature and Electronic Seal
Article 19. Means of Qualified Electronic Signature and Electronic Seal
Article 20. Qualified electronic trust service used in verification and confirmation of the validity of a qualified certificate of electronic signature or seal

Article 21. Qualified electronic trust service for the creation, verification and validation of a qualified website authentication certificate
Article 22. Identification of a person during the formation and issuance of a qualified certificate of a public key (PKI)
Article 23. Qualified certificates of Open(Public) Keys
Article 24. Validity of Qualified Open (Public) Key Certificates
Article 25. Cancellation, blocking and renewal of qualified certificates of public (open) keys
Article 26. Qualified electronic trust service used in verification and confirmation of a qualified electronic time mark (timestamp)
Article 27. Qualified Trust Services of registered (signed for) electronic delivery
Article 28. Qualified Trust Services provisions in storage of qualified electronic signatures, seals and certificates related to these services
Article 29. Qualified Trust Services Provisions by the Central Certification Authority
Article 30. Acquiring the Status of Qualified Provider of Trust Services
Article 31. Termination of the activity of provision of qualified electronic trust services by the qualified provider of Trust Services

Summary

CHAPTER IV covers aspect related provisions and requirements and use of Trust Services with more aphesis on means of Qualified Electronic Signature and Electronic Seal, Qualified Electronic Time Mark (time stamp) and registered (singed for)electronic delivery. In regards to definitions given in national Law those are identical to definitions given in Sections 4 to Section 9 (Articles 25- 46) of eIDAS 910 regulation respectively. Ukrainian national Law 2155-VIII similarly to eIDAS 910 Regulation defines equivalent legal powers and legal effect of qualified electronic signature and handwritten signature.

Provisions of Article 21 in verification and validation of a qualified website authentication certificate corresponds well with ANNEX IV of eIDAS 910 - Regulation requirements for qualified certificates for website authentication whereas, Provisions of Article 18-20 on electronic Seal corresponds well with ANNEX III eIDAS 910 Regulation **-** Requirements For Qualified Certificates For Electronic Seals.
Attention is also devoted to procedural aspect of handling of Public Key Infrastructure (PKI)- describing the roles, and setting the procedures needed to create, manage, distribute, use, store & revoke digital certificates and related public\private –key pairs (later referred as Open and Private Keys).

References to PKI in Legislation (Law 2155-VIII) is vendor agnostic, however NOT technology natural.

Provisions of **Articles 29-31** define criteria and provisions of gaining status of Qualified Trust Services Provider, set timelines for Central Certification Authority to make decision. Also Article 31 set procedure and define responsibilities and timeframe of termination of the activity and provision of Qualified Trust Services Provider.

Conclusions: Overall with reservation to technological neutrality of PKI in section of Trust Services provisions Ukrainian Law 2155-VIII provides good degree of legal certainty and corresponds well with eIDAS 910 Regulation.

CHAPTER V REGULATORY ENFORCEMENT, INSPECTIONS and CONFORMITY ASSESMENT in TRUST SERVICES

Article 32. Conformity Assessment and Compliance in Trust Services
Article 33. State supervisions, enforcement and inspections to meet the requirements of the legislation Article 34. Powers of the officials and of the enforcement body in measures of supervision and compliance.

Article 35. Trusted List
Article 36. Responsibilities in the field of Trust Services

Summary

In order to ensure compliance in Trust Services Provisions of Article 32 require conformity assessment of Qualified Trust Service Providers to be conducted in their own expense with regularity every 24 months and by the body that meets the requirement and has accreditation from Conformity Assessment Body (CAB).

eIDAS 910 Regulation Article 3 point (18) 'conformity assessment body' means a body defined in point (13) of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides.
Regulation (EC) No 765/2008 Article2 point (13) 'conformity assessment body' shall mean a body that performs conformity assessment activities including calibration, testing, certification and inspection;

List of EU 'conformity assessment body' available at **https://ec.europa.eu/futurium/en/content/list-conformity-assessment-bodies-cabs-accredited-against-requirements-eidas-regulation**

Provisions of Article 33 define detailed procedures of State supervisions, inspections and enforcement in Trust Services an eID by "controlling body". However there is no direct indication that "controlling body" is State Special Communications Service of Ukraine (**SSCSU)** the responsibilities of later define in Article 8, again with no reference to it as "controlling body", however Article 11 by exclusion leaves no other option, but to consider **SSCSU the** "controlling body" for purposes thereafter."controlling body" however given powers to inspect ALL parties involved in Trust Services provisions including (CAB, QTSP, TSP, CCA)

Provisions of Article 35 order supervisory body CCA verify whether the qualified trust service provider (QTSP) and the qualified trust services provided by it comply with the requirements, with obligation to include it into the National Trusted List. The inform about the decisions to grant\ withdrawals qualified status must be made publicly available. In this regards the norm corresponds well with eIDAS 910 Regulation Article 22 (Trusted lists) and Article 21(1-2) (Initiation of a qualified trust service) as well as with Implementing Decision (EU) 2015/1505 laying down technical specifications and formats relating to trusted lists.

Provisions of Article36 sets responsibilities in the field of Trust Services ranging from administrative to criminal

Conclusions: Overall this section of Ukrainian Trust Services Law 2155-VIII provides good degree of legal certainty and corresponds well with eIDAS 910 Regulation.

CHAPTER VI INTERNATIONAL COOPERATION

Article 37. Participation in international cooperation in the areas of electronic trust services and electronic identification
Article 38. Recognition of Foreign Electronic Trust Services

Summary

The norms on international agreement sign by Ukraine recognized as such that hold overruling power if oppose national legislations. Trusted Services provided by foreign QTSP recognized as valid in Ukraine if a)those QTSP are in Trusted List of their country in question AND b) mutual recognition bi/multi)–lateral agreement with such country/ies were signed by Ukraine.

In regards to EU mutual recognition of eID and trust Services Ukraine has to meet norms set in Article 14 International aspects - quote

1. Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU2. Agreements referred to in paragraph 1 shall ensure, in particular, that:

(a) the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide;

(b) the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or international organisation with which the agreement is concluded

Conclusions: Overall this section of Ukrainian Trust Services Law 2155-VIII holds no evident legal contradions with Article 14 eIDAS 910 Regulation (International aspects) and forms ground for EU - Ukraine mutual recognition of Trust Services.

CHAPTER VII FINAL AND TRANSITIONAL PROVISIONS

Summary & Conclusions Provisions of CHAPTER VII repeals one previous legislation and modifies four related legislations. It also stipulates timeline for the Law to entry into force and describes the transitional measures. There is no contradiction of CHAPTER VII with eIDAS 910 Regulation.

Risks related The Law 2155-VIII

- **Article 22 paragraph 4 -** there is limited information (with no reference to relevant legislation) as to the procedure to obtain Public Key by non-Ukrainian nationals **–** might be considered in conjunction with Chapter VII (International co-operation)of Ukrainian legislation on Trust Services
- **Article 30 paragraph 2 subparagraph 3)** - may exclude from domestic service provisions non-Ukrainian trust service providers (including those from EU member states)
- **Article 30 paragraph 2 subparagraph 4)** - may limit the usage of third-party cloud services for trusted services provisions

Analysis of implementing decisions related to (Law 2155-VIII – on Trust Services and eID)

Ukrainian Implementing decisions related to Trust Services and eID regulation ware worked through and crosschecked with eIDAS (910 Reg) with the finding as follows:

"Draft decree of the Cabinet of Ministers of Ukraine «On approval of the Course of the procedure of conformity assessment in the electronic trust services area"

What the regulation is about: It sets procedures of attestation / conformity assessment for Qualified Trust Service Providers (**QTSP)**, stipulated a form and the content of a certificate, sets requirement to the bodies (laboratories) that conduct the procedures of conformity assessment and/or attestation of **QTSP**. In conjunction with this legislation the following matter should be considered. It is suggested by draft legislation (Draft 1 in this study) that 17 existing **QTSP** shall automatically gain conformity assessment and thereafter be included into Trusted List, de facto this is already happen as otherwise QTSP would not be able to operate. Risk of irragularities and meeting conformity assessment criteria throughout the transition is subject in question as it has happened without legal backings. It also hould be noted that as for 2019 there is no publicly available information on Laboratory (either private or State-run) that can carry out the conformity assessment and/or attestation of **QTSP.**

Assessment

Regulation Identifier 1215-2018-п,

Status: passed- 18.12.2018 entered in to force from 28.02.2019

Regulation link to download: https://zakon.rada.gov.ua/laws/show/1215-2018-%D0%BF?lang=en

Draft proposal published at (https://czo.gov.ua/news-details?id=449)

Legal Certainty: Regulation provides a good degree of legal certainty
Technological neutrality: Yes
Use of Standards: ETSI standards are used (ETSI EN 319 403:2015, however regulation has overriding power
Non-discrimination: Yes
Interoperability: Yes
Cross-border recognition: Implied due to use of ETSI standards
Exclusions: Regulation is not applicable to provisions of trusted services in banking and in matters related to funds transfers. .

Conclusions: Positive

"Draft order of the Ministry of Justice of Ukraine «On approval of the Course of the trusty list maintenance"

What the regulation is about: Regulation sets: a) framework for National Trusted List of Electronic (Digital) Signatures and Infrastructures (ESI) Qualified Trust Service Providers (QTP) and b) sets framework as to the Article 35 of the Law (Trusted List) defining responsibilities/procedures /timelines / standards used / as well as describes the responsibilities and the duties of bodies and parties involved.

Assessment

Regulation Identifier № 3373/5
Status: entered in to force from 29.10.2018
Regulation link to download: https://czo.gov.ua/news-details?id=450
Legal Certainty: Regulation provides good degree of legal certainty and provides guidelines on management of Trusted List sets responsibilities of bodies and parties involved.
Technological neutrality: No (PKI and specific formats of document)
Use of Standards: refers to ETSI TS 119 612 V2.2.1 (2016-04) Trust List (ESI) standard when local Trusted List deals with foreign entities. On trust list itself regulation permits usage of ETSI TS 119 312:2015 and local standard ДСТУ 4145-2002.

Non-discrimination: Yes
Interoperability: Yes
Cross-border recognition: Implied due to use of ETSI standards
Exclusions: Regulation is not applicable to provisions of trusted services in banking and in matters related to funds transfers.

Conclusions: Positive with reservation regarding Technological neutrality **of PKI**

"Decree of the Cabinet of Ministers of Ukraine «On approval of the Requirements in the electronic trust services area and the Course of the verification of the requirements of legislation in the electronic trust services area»"

What the regulation is about: Regulation a) defines detailed requirements (136) for **QTSP** - b) sets detailed procedure regarding the measures of the control of all the parties involved in eID and Trust Service provision by State Special Communications Service SSCSU.

Assessment:

Regulation Identifier: - 992-2018-п
Status: passed- 07.11.2018, entered in to force from 01.01.2019
Regulation link to download: **https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF/sp:side:max20**

Legal Certainty: Regulation provides some degree of legal certainty. However one may suggest that it would be difficult for subjected parties to meet the requirements set in the regulation
Technological neutrality: Yes (with a reservation on PKI)
Use of Standards: Yes Used Local (domestic Ukrainian standards DSTU)
those believed to be identical and harmonized adaptation of CEN ETSI EN
102 778
119 xxx (000 001 100 124 101 124 134 144 400 401 403)
319 xxx (102 122 132 142 162 411 412 422 522 532 600 612)
419 211
and adaptation of ISO/IEC standards:
ISO/IEC 14888, 18045,15408, 27002, 9594-8,19790,
SR 003 186
In total there are 77 references to the above standards in the legislation the relevance some of the may be the sublect of stand alone study (namely: ISO/IEC and SR) mentioned in paragraphs 34,35,51,52,53 of Annex related to the standards

Non-discrimination: No (due to mandatory use of paper based documents with no electronic equivalent)
Interoperability: Yes
Cross-border recognition: subject is not covered or implied directly
Exclusions: Regulation is not applicable to provisions of trusted services in banking and in matters related to funds transfers.

Conclusions: Neutral (explained: Legislation comprise of two part and one annex legal certainty of the legislation late part 2 is open to interpretation and standards are applied only to some degree. In ragards to part 1 the structure of the legislation is such that reference to the standards are subject of separate Annex that is logically detached from the regulation norms and therefore norms can be deemed as such that open to interpretation at least on use of standards.
Adaptation of Guidelines on Supervision of Qualified Trust Services developed by European Union Agency for Network and Information Security (ENISA) can be cost effective way forward in achieving progress on the subject.

“Decree of the Cabinet of Ministers of Ukraine «On approval of the Course of use of the electronic trust services in the government authorities, local self-government bodies and state-owned enterprises, institutions and organizations»”

What the regulation is about: regulation names the Trust Services used in public institutions (government municipal, state owned companies), and sets requirements of managing Public Key Infrastructure (PKI) for civil servants.

Assessment:

Regulation Identifier 749-2018-п
Status: passed- 19.09. 2018, entered in to force from 07.11.2018
Regulation link to download **https://zakon.rada.gov.ua/laws/show/749-2018-%D0%BF**

Legal Certainty: low degree of legal certainty
Technological neutrality: Yes (with a reservation on PKI)
Use of Standards: Not used / or referred to
Non-discrimination: Yes
Interoperability: Yes
Cross-border recognition: the subject is not covered or implied
Exclusions: the subject is not covered or implied

Conclusions: Positive with a reservation on PKI

Note: There are extensive guidelines on the use of Trust Services and eID in public bodies in the EU Member States. The following use cases may be considered as relevant to develop similar guidelines in Ukraine

- Person-to-Government interaction (and visa versa) domestic
- Business-to- Government interaction (and visa versa) domestic
- Government -to- Government interaction domestic
- Government -to- Government interaction cross-border
- Business-to-Business interaction domestic
- Business-to-Business interaction cross-border
- Person-to-Business interaction (and visa versa domestic
- Person-to-Business interaction cross-border

Due to the legal requirements most of interaction with the government and/or the municipal authorities occurred throughout trust services requires qualified services with level of confidence “substantial “ or “high” therefore use cases of Person-to-Gov interaction (and visa versa), Business-to-Gov interaction (and visa versa) , Gov-to-Gov interaction domestic and cross-border are most relevant and shall be considered first.

"Draft decree of the Cabinet of Ministers of Ukraine «On approval of the Course of the mutual recognition Ukrainian and foreign certificates of a public keys, electronic signatures and use of the information and telecommunication system of central authentication authority for ensuring recognition in Ukraine of the electronic trust services, foreign certificates of a public keys, what are using during the provision of legally significant electronic services in the process of interaction between subjects from different countries»"

What the regulation is about: regulation address the issues related to cross boarder mutual recognition of eID and trust services of Ukraine with other countries - it does so by acknowledging need for bi-lateral mutual recognition agreements with other countries, and sets bodies responsible to sign up such agreements, it also stipulates the procedural technicalities. Bi-lateral agreements ought to be signed separately in accordance with "Law on Interfacial Agreements" 1906-IV from 2004 with amendments from 20.07.2014

Assessment:

Regulation Identifier 60-2019-п
Status: passed- 23.01.2019, entered in to force from 08.02.2019
Regulation link to download:
https://zakon.rada.gov.ua/laws/show/60-2019-%D0%BF
Drafts MoJ website https://czo.gov.ua/news-details?id=443
Legal Certainty: Regulation provides good degree of legal certainty
Technological neutrality: Yes (with a reservation on PKI)
Use of Standards: Not used / or referred to
Non-discrimination: Yes
Interoperability: the subject is not covered or implied
Cross-border recognition: Core subject of this regulation – it set general rule and determines that details and particulars are set by additional bi-lateral agreements
Exclusions: ambiguous interpretation either the Regulation is not applicable to providers of trust services certified by CCA in banking in matters related to funds transfers, **or** Regulation is not applicable to all Providers from Trusted List AND technical means used by Certified Trust Service Providers used in banking and in matters related to funds transfers.

Conclusions: Positive (with a reservation on PKI and Exclusions)
Notes: Regulation should be considered as a starting point of cross-border cooperation with particular details set out in bi-lateral agreements with each country / international bodies)
In regards to the EU co-operation in Trust Services and eID its down to Article 14 of eIDAS Regulation that stipulates quote "Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU" and quote "the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country or international organisations with which the agreement is concluded, and by the trust services they provide"
In conjunction with Article 37 and Article 38 of Ukrainian legislations "Law on Trust Services and eID" 2155-VIII stipulates that Ukraine has to sign Mutual recognition agreement in order to fulfill norms of this regulation.

for instance on Common Criteria CCRA (https://www.commoncriteriaportal.org/)

"Draft Order of the Administration of the State Service of Special Communications and Information Protection of Ukraine «On establishment of the requirements for information security and protection for the qualified provider of the electronic trust services and their individual registration points»"

What the draft regulation is about: draft regulation sets the requirements of information security for Qualified Trust Services providers (QTSP). Those requirements in first instance thereafter applicable to 17 "Key Certificate Centres" that are already in operation it is also understood that de facto those QTSPs the **only** providers of Trusted Services in Ukraine. Draft regulation sets criteria and regulates: 1) risks management procedures 2)TSP staff management 3)Hardware Assents Management 4)Access management 5)Cryptographic means 6) PKI infrastructure 7) Networks management - 8)service continuity management 9) service troubleshooting management 10) service termination management and some other aspects.

Assessment:

Regulation Identifier Draft 1
Status: Draft published at SSCSU website
Regulation links to download:

http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=297434&cat_id=38837
http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=297421&cat_id=38837&ctime=1537345074833
http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=297416&cat_id=38837&ctime=1537344950454

Legal Certainty: pore degree of legal certainty
Technological neutrality: No (due to introduction of local standards in data security (KZI) and PKI)
Use of Standards: No
Note and Reservations as follows:
Outdated domestic standards are used as the ground for formation of digital security (НД ТЗІ 3.7-003-05)
Risk management standard ISO 3100 is not used in maters related in risk assessment
Use of domestic standards (DSTU) those believed to be identical and harmonized adaptation of CEN ETSI EN (ETSI EN 319 401, ETSI EN 319 411, ETSI EN 319 421, as well as ISO/IEC 27001 ISO/IEC 27002 27001 ISO/IEC 27005)
Non-discrimination: No (in some cases paper document are required with no digital (e-document)alternative suggested)
Interoperability: Not used / or referred to
Cross-border recognition: Not used / or referred to
Exclusions: it is understood that regulation is applicable to Trust Services providers (TSP) only

Conclusions: Negative

Major reservations:
Suggested draft legislation introduces the requirement for information systems security used in Qualified Trust Services providers (QTSP) as well as in Central Certification Authority and presumably in all public bodies.
Drafted legislation on number of occasion refers to the separate legislation, which introduces aditional separate sets of technical, organizational and security requirements (those regulations are not the subject of this review however it should be noted that it are 10+ years old and "long reads")
Highlights : 1) Chapter 1 (Organizational Matters) Paragraph 1.1 refers to separate regulation (№ 373 from 29.03.2006) https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF issued in 2006 and last updated in 2011.

2) Chapter 1 (Organizational Matters) Paragraph 1.3 Refers to the instruction (НД ТЗІ 3.7-003-05)– it was not possible to obtain official up-to=date version of this document, however from review of version available from SSCSU website (http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074)it becomes evident that it sets separate requirement as to the licensing of service providers who entitled to carry out mandatory works on digital security, this regulation also retains set of domestic standards on the matters.

3) Lake of alignment with EU implementing decisions 2015/1506 (advanced e- signature) Alignment with EU implementing decisions 2016/650 (3/4/7/8)

"Decree of the Cabinet of Ministers of Ukraine «On approval of the criteria, on which they assess the degree of risk from doing business in the provision of electronic trust services and the frequency of planned state supervision (control) activities is determined of the Administration of the State Service of Special Communications and Information Protection of Ukraine»"

What the regulation is about: regulation sets criteria for risk assessment of various types of Trust Service Providers and gives instruction as regularity of conformity checks.

Assessment:

Regulation Identifier 914-2018-п
Status: passed- 31.10.2018, entered in to force from 14.11.2018
Regulation link to download **https://zakon.rada.gov.ua/laws/show/914-2018-%D0%BF**

Legal Certainty: good degree of legal certainty
Technological neutrality: Not applicable
Use of Standards: No (use of ISO 31000 standard on risk management may be appropriate)
Non-discrimination: Not applicable
Interoperability: Difficult to assess
Cross-border recognition: the subject is not covered or implied
Exclusions: it is understood that regulation is applicable to Trust Services providers (TSP) only

Conclusions: positive (with reservation on not use of standards)

Draft decree of the Cabinet of Ministers of Ukraine «On approval of the Technical regulation means of cryptographic protection of information»

What the regulation is about: It aims to regulate all the aspects of hardware security devices (such as: eID hardware, QSCD - Qualified Signature and Seal Creation devices, other cryptography hardware and software) and means of cryptography used by government and TSPs in Ukraine. Suggested draft document substitutes globally recognized (and widely adopted in the EU member states) Common Criteria Approach / Framework that combined best practices tandards and instruction. The Draft has over 100 pages of technical information with 10 Annexes.

Assessment:

Regulation Identifier: Draft 2
Status: Draft published at - 20.04.2018 at SSCSU website
Regulation link to download
http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=1599066DEE1A959B97E635D22C76B55A.app2?art_id=288496&cat_id=38837

Legal Certainty: None
Technological neutrality: No
Note: Due to lake of adaptation of either Common Criteria Framework or any other globally recognized alternative as for Cryptographic products CESG Assisted Products Scheme (CAPS))
Use of Standards: Yes
Note: Albaite formally standards are reffered to, its done with negative connotation for the following reasons:- Used Local (domestic Ukrainian standards DSTU) those are believed to be identical and harmonized adaptation of CEN ETSI EN 119 6xx, x19 4xx, x19 5xx, x19 1xx , 1193 xx , 419 2xx, 119 0xx standards, however those mentioned and referred to with NO framework and no Globally recognized Security Assurance Requirements (SARs)
Non-discrimination: Difficult to assess
Interoperability: No
Cross-border recognition: No
Exclusions: the subject is not covered or implied

Conclusions: Negative

Notes: Major reservation is related to not use of Common Criteria (CC) in security conformity assessment of hardware equipment. Common Criteria or **(**Common Criteria for Information Technology Security Evaluation**)** - is a framework based on good practices in security standards in which computer system users can specify their security functional and assurance requirements. Vendors can then implement or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment**.** CC is an internationally recognized framework with set of Assurance Level / category ranking (EAL1 through to EAL7) that is assigned to IT product and\or system after a Common Criteria security evaluation. The EAL indicates to what extent the product or system was tested. A product or system must meet specific assurance requirements on Target of Evaluation (TOE) to achieve a particular EAL level.

EALs are interpreted in the following way:
EAL1 – TOE was functionally tested,
EAL2 – TOE was structurally tested,
EAL3 – TOE was methodically tested and checked,
EAL4 – TOE was methodically designed, tested and reviewed,
EAL5 – TOE was semiformally designed and tested,
EAL6 – TOE was semiformally verified design and tested,
EAL7 – TOE was formally verified design and tested.
EALs declared by developers for given IT products are described by especially composed sets of assurance components, called assurance packages. Regulation can use an approach that set the requirement of security hardware/equipment ranking in accordance with Common Criteria Recognition Arrangement. Such approach likely to meet constantly updating security requirements, ensure that government communication security is constantly up-to-date, use latest yet trustworthy state-of-art hardware and do not create obstacles on the way of cross-border mutual recognition of national trust services with other countries. Adaptation of CC approach is likely to facilitate cross-border integration in military and defence. Use of globally recognized modern technology provides confidence of individuals, legal entities, and other governments in Ukrainian trust services, and security of information.

"Draft order of the State Agency for e-Governance of Ukraine «On approval of the requirements for formats of electronic documents workflow data in the government authorities»"

What the regulation is about: Regulation issued by The State Agency for E-Governance of Ukraine and sets: a) formats requirements for electronic document (e-document) ought to be used in Ukrainian public institutions including but not limited to government b) sets general rules for government e-document structure / amendatory fields / requirements for archiving

Assessment

Regulation Identifier z1309-18 № 1309/32761
Status: passed 07.09.2018 entered in to force from 29.10.2018
Regulation link to download **https://zakon.rada.gov.ua/laws/show/z1309-18**

Legal Certainty: Regulation provides reasonable degree of legal certainty
Technological neutrality: Yes
Use of Standards: Some but not sufficient – refers ISO/IEC 21320-1:2015, and local adaptation of ETSI EN 319 162-x:2016 / Reservation on standards Usage of other - ETSI EN x19 1xx on formants (XML CMS PDF ASiC) ETSI EN 119 3 xx Cryptographic Suites used , ETSI EN x19 5xx – Long term preservation , ETSI EN 119 0xx (General Framework)
Non-discrimination: Yes
Interoperability: Yes
Cross-border recognition: Implied due to some use of ETSI standards
Exclusions: the subject is not covered or implied
Conclusions: Positive with reservations regarding the use of standards

---

Package of implementation decisions/orders and instruction that was the subject of this review is mandatory legal requirement that ought to be completed and taken in to force within one year transition period (by 7th November 2018)determine by the Law 2155-VIII. The Law alters four and repeal one other Legislations as stipulated in Chapter VII (Final and Transitional Provisions) it also made the Government responsible for package of implementation decisions/orders. Within the government of Ukraine there are two bodies that meant to share responsibilities on legislations and further work together on service provisions implementations and oversight. Ministry of Justice of Ukraine (**MoJ)** and State Special Communications Service of Ukraine (**SSCSU**). Outside of the Government responsibility is the corpus of implementation decisions/orders related to Trust Services provisions and eID in banks those are responsibility of Central Bank of Ukraine and not the subject of this report.

Legislations that had been passed and acting (as to 1 April 2019):

1. 1215-2018-п
2. № 3373/5
3. 992-2018-п
4. 749-2018-п
5. 60-2019-п
6. 914-2018-п
7. z1309-18

Two other suggested for the review implementation decisions are still at the draft stage

8. **Draft 1**
9. **Draft 2**

Later two got negative overall assessment due to non-passing 'interoperability checks' in regards to Legal Certainty, Technological neutrality, Non-discrimination, Overall Interoperability and Cross-border recognition. There are also concerns regarding **992-2018-п** implementation decisions that is entered into legal force but has questions in regards to Legal Certainty and may pose issue on Cross-border recognition

Draft 1 Major reservations: Suggested draft legislation introduce requirement for information systems security used in Qualified Trust Services providers (QTSP) as well as in Central Certification Authority and presumably in all other public bodies this contradicts with EU implementing decisions 2015/1506 (advanced e- signature) and with EU implementing decisions 2016/650 (3/4/7/8) and may create obstacles in signing Mutual recognition on eID and Trust Services between EU and Ukraine

Drafted legislation on a number of occasions refers to the stand alone legislations, those introduce separate sets of technical, organizational and security requirement (the regulations in question are not the subject of this review however it should be noted that those can be considered as outdated)

Examples 1) Chapter 1 (Organizational Matters) Paragraph 1.1 refers to separate regulation (№ 373 from 29.03.2006) https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF issued in 2006 and last updated in 2011.

2) Chapter 1 (Organizational Matters) Paragraph 1.3 Refers to the instruction(НД ТЗІ 3.7-003-05)– it was not possible to obtain official up to date version of this document, however from review of version available from SSCSU website (http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074)it become evident that it sets separate requirement as to the licencing of service providers who entitled to carry out mandatory security works , this regulation also retains set of domestic standards on the matters ("long read").

Draft 2 - Major reservation is related to not Use of Common Criteria (CC) in security conformity assessment of hardware equipment.) Common Criteria or **(**Common Criteria for Information Technology Security Evaluation**)** - is a framework based on good practices in security standards in which computer system users can specify their security functional and assurance requirements. Vendors can then implement or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment**.** It is internationally recognized framework with set of Assurance Level / category ranking (EAL1 through to EAL7) that is assigned to IT product or system after a Common Criteria security evaluation. The level indicates to what extent the product or system was tested. A product or system must meet specific assurance requirements on Target of Evaluation (TOE) to achieve a particular EAL.

EALs are interpreted in the following way:
EAL1 – TOE was functionally tested,
EAL2 – TOE was structurally tested,
EAL3 – TOE was methodically tested and checked,
EAL4 – TOE was methodically designed, tested and reviewed,
EAL5 – TOE was semiformally designed and tested,
EAL6 – TOE was semiformally verified design and tested,
EAL7 – TOE was formally verified design and tested.
EALs declared by developers for given IT products are described by specially composed sets of assurance components, called assurance packages. Regulation can use approaches that sets the requirement of security hardware/equipment ranking in accordance with Common Criteria *Recognition Arrangement*. Such approach likely to meet constantly updating security requirements, insure that government communication security is constantly up-to-date, use latest yet trustworthy state-of-art hardware and do not create obstacles on the way of cross boarder mutual recognition of national trust services with other countries. Adaptation of CC approach is likely to facilitate cross-boarder integration in military and defence. Use of globally recognized modern technology provides confidence of individuals, legal entities, and other governments in Ukrainian trust services, and security of information.

Risks related to Implementation decisions

- Risk related to international legal recognition of electronic signatures, seals and time stamps on Ukrainian e-Documents ;
- Risk of developing partial (fragmented)rather than end-to-end digital services frameworks
- Risk that existing legislation can compromise ongoing and future interoperability efforts
- Risk to create in Ukraine isolated digital environments and consequently electronic barriers that may prevent Ukrainian business and public administrations from connecting with each other and in future to EU member states established digital frameworks and tools.
- Risk to Ukrainian business and citizens to experience hurdles' in identification and usages of available digital public services in EU member states countries
- Risks related to archival norms and legal frameworks for archiving documents and files used by public administrations.
- Risks related to personal data protection, which set the conditions and liabilities for the processing of personal data;
- Risks related to fragmented adaptation and limited usage of e-Documents in administrative procedures when interacting with public administrations;
- Risk related to shortage of in-house skillsets staff (in QTSP CCA and in particular in **SSCSU)** with understanding of EU norms and principals in mattera related to Trusted Serices. In edishin desire to develop domestic standards may be yet another barrier to implementing EU interoperability policies.

Recommendations

1. Develop and adopt EU aligned strategy of usage of e-Documents in Government base it on Solution Building Blocks(SBB) and account for case studies of implementation in EU member states.
2. Adopt recommendation of EU ISA² Programme in particular in regards to building Interoperability Reference Architecture (EIRA©)
3. Adopt recommendation of EU Electronic Signatures and Infrastructures (ESI)
4. Adaptation of Guidelines on Supervision of Qualified Trust Services developed by European Union Agency for Network and Information Security (ENISA) can be cost effective way forward in achieving progress on the subject.
5. Relationship between Trust service providers and service consumers must be clearly defined – for now there is now evident guidelines on the matter
6. Interoperability in Trust services between public administrations at different administrative levels and with other stakeholders (businesses citizens other States and international bodies)can only be successful if governments give sufficient priority and assign resources to their respective interoperability efforts to achieve it the following recommendation can be considered:
7. Ensure that Ukrainian interoperability frameworks and interoperability strategies are aligned with the EIF[i] guidelines and, if needed, tailor and extend them to address the local context and needs.
8. Publish government data as an open data unless certain restrictions apply. On top if it the concept of openness related not only to the data and specifications but to the software. Open government data (here simply referred 'open data') refers to the idea that all public data should be freely available for use and reuse by others, unless restrictions apply e.g. for protection of personal data, confidentiality, or intellectual property rights. Public administrations collect and generate huge amounts of data. EU good practices suggest sharing of datasets and services between public authorities with no restrictions or practical obstacles to its reuse. This data should be published with as few restrictions as possible and clear licenses for its use to allow better scrutiny of administrations' decision-making processes and realise transparency in practice.
9. Reusability of ITC solutions and Data itself as a major driver for interoperability. Public administrations should use open source software technologies and products when it comes to implementation of Trust services and beyond. It can help save development cost, avoid a lock-in effect and allow fast adaptation to specific business needs because the developer communities that support them are constantly adapting them. Public administrations should not only use open source software but whenever possible contribute to the pertinent developer communities.
10. Public administrations should not only aim to use open source software (ITC solutions related to Trust service) but also ensure a level playing field for different vendors of open source software and demonstrate active and fair consideration of using open source software, taking into account the total cost of ownership of the solution.
11. Intellectual property rights of ITC products deployed by public administrations best to be licensed on FRAND[ii] terms, in a way that allows implementation in both proprietary and open source software, and preferably on a royalty-free basis. On practical side it may include become part of free and reusable EU ITC tools for public e-services (JOINUP) -https://joinup.ec.europa.eu. Catalogue of reusable domestic ITC solutions used in public sector already implemented in 2019 – NBIT https://cid.center/projects/nbit/)
12. Public administrations in ITC procurement and development should give preference to open specifications, taking due account of the coverage of functional needs, maturity and market support and innovation. However, public administrations may decide to use less open specifications if open ones do not exist or do not meet functional needs. In all cases, specifications should be mature and sufficiently supported by the market, unless they are being used to create innovative solutions.

13. Public administrations should create inclusive environment that empowers citizens and businesses to get involved in the design of new Digital Trust Services, to contribute to service improvement and to give feedback about the quality of the existing public services.
14. Ensure internal visibility and provide external interfaces for trust related public services. This is about allowing other public administrations, citizens and businesses to view and understand administrative rules, processes, data, services and decision-making. Ensuring availability of interfaces with internal information systems. Public administrations operate a large number of what are often heterogeneous information systems in support of their internal processes. Interoperability depends on ensuring the availability of interfaces to these systems and the data they handle. In turn, interoperability facilitates reuse of systems and data, and enables these to be integrated into larger systems.
15. Reuse and share solutions information and data, and cooperate in the development of joint solutions when implementing European public service unless certain privacy or confidentiality restrictions apply.
16. Albeit in Ukraine in might be politically sensitive issue still multilingualism needs to be carefully considered in design of Trusted services information systems and technical architectures especially in regards to public services. Guided EU rule can be that public services available in the languages of the expected end-users.
17. Administrative simplification via digital-by-default services, whenever appropriate, so that there is at least one digital channel available, and digital-first which means that priority is given to using public services via digital channels while applying the multi-channel delivery concept. Simplify processes and use digital channels whenever appropriate for the delivery of public services, shall help to respond promptly and with high quality to users' requests and reduce the administrative burden on public administrations, businesses and citizens.
18. Formulate a long-term preservation policy for information related to public service records. Information in electronic form must be preserved and be converted, where necessary, to new ITC solutions when old media become obsolete. The goal is to ensure that records and other forms of information keep their legibility, reliability and integrity and can be accessed as long as needed subject to security and privacy provisions. Ensure long-term accessibility, including preservation of associated electronic signatures or seals. In this regard, the use of qualified preservation services, in line with Regulation (EU) 910/2014, can ensure the long-term preservation of information
19. Standards and specifications are fundamental to interoperability. Therefore Government should consider to put in place processes to select relevant standards and specifications, evaluate them, monitor their implementation, check compliance and test their interoperability. In some areas of information security there are several different groups of standards that are defined. Standards are competing with each other for adoption and it is often difficult for the end user to judge which standards are the best choice for their particular requirements. Occasionally, it is necessary to mix and match standards from different families in order to achieve the goal. When implementing Public key Infrastructure (PKI) for instance, it is not unusual to see organisations adopt such a combination of standards (for example X.509 (ITU) for the certificate format, PKIX (IETF) standards for core PKI and PKCS (RSA) standards for interfacing to secure devices. In some other (rare cases), public administrations may find that no suitable standards/specifications are available for a specific need in a specific domain. Active participation in the standardisation process mitigates concerns about delays, improves the alignment of standards and specifications with public sector needs and can help governments keep pace with technological innovation.
20. When multiple organizations/stackeholders are involved there is a need for coordination and governance by the authorities with a mandate for planning, implementing and operating European public services. Ensure interoperability and coordination over time when operating and delivering integrated public services by putting in place the necessary governance structure.

21. Organizations involved in domestic public service provision as well as as those involved in international collaborations should make formal arrangements via interoperability agreements. Establish interoperability agreements in all layers, complemented by operational agreements and change management procedures.
22. Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved. An information management strategy should be drafted and coordinated at the highest possible level (corporate or enterprise) to avoid fragmentation and set priorities.
23. Communicate clearly the right to access and reuse open data. The legal regimes for facilitating access and reuse, such as licenses, should be standardized as much as possible
24. Country-wide expedient implementation of the eID and Trust Services is an effective measure for achieving cross-border use of electronic state services with EU member states and beyond
25. Creation of National Ukrainian Security Products Compliance List (analogue of USA - National Information Assurance Product Compliant List (NIAP PCL) or other Countries that adopted CC
26. Create PEPPOL assess point – this is in fact mandatory requirement from 2018 for participation in of overseas vendors in EU member state public procurement procedures and contracts. It can enable cross-boarder exchange with e-Orders, e-Advance Shipping Notes, e-Invoices, e-Catalogues.
27. National Standards and accreditation bodies envisaged to contribute to the assurance process of accrediting conformity assessment Laborotories who will audit QTSP conformity with the Law and Standards. Openig th file to EU \ international conformity assessment Laborotories should be considered .

Annex 1

Comparison table of main terms used in Ukrainian Trust Service Law vs. EU Reg. 910

UA term reference (order as defined in Ukr Law)	UA term reference (as defined in Ukrainian Law) Chapter1 Article1 or elswhere in the Law	ref term in 910 (Ukrainian translation of reg910) Article 3 L 257/83- L 257/86	ref term in 910 (English) Article 3 L 257/83- L 257/86	Conclusion on how terms and legal wording of the terms corresponds (IDENTICAL \ SOMEWHAT IDENTICAL \ POORLY CORRESPONDS \ NO EQUIVALENT#NOT DEFINED)
1) автентифікація	електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно телекомунікаційної системи та/або походження та цілісність електронних даних;	електронний процес, що дозволяє підтвердити електронну ідентифікацію фізичної або юридичної особи; або походження та цілісність даних в електронній формі;	means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;	IDENTICAL
2) блокування сертифіката відкритого ключа	тимчасове зупинення чинності сертифіката відкритого ключа;			NO EQUIVALENT
3) вебсайт	сукупність програмних засобів, розміщених за унікальною адресою в обчислювальній мережі, у тому числі в мережі Інтернет, разом з інформаційними ресурсами, що перебувають у розпорядженні певних суб'єктів і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інших інформаційних послуг через обчислювальну мережу;			NOT DEFINED
4) відкритий ключ	параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;	"дані для перевірки достовірності" - дані, які використовуються для перевірки достовірності електронного підпису або електронної печатки;	'validation data' means data that is used to validate an electronic signature or an electronic seal;	SOMEWHAT IDENTICAL

5) відокремлений пункт реєстрації	представництво (філія, підрозділ, територіальний орган) надавача електронних довірчих послуг або юридична чи фізична особа, яка на підставі наказу надавача електронних довірчих послуг (його керівника) або договору, укладеного з ним, здійснює реєстрацію підписувачів з дотриманням вимог цього Закону та законодавства у сфері захисту інформації;			NO EQUIVALENT
6) Довірчий список	перелік кваліфікованих надавачів електронних довірчих послуг та інформації про послуги, що ними надаються;	ст. 22 Кожна держава-член розробляє, веде та опубліковує довірчі списки, враховуючи інформацію про кваліфікованих провайдерів довірчих послуг, за яких вона несе відповідальність, а також інформацію про кваліфіковані довірчі послуги, що ними надаються.	22. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.	IDENTICAL
7) електронна довірча послуга	послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги;	"довірча послуга" - електронна послуга, що зазвичай надається за винагороду і яка полягає у: (a) створенні, перевірці та підтвердження електронних підписів, електронних печаток або електронних позначок часу, послугах рекомендованих електронних відправлень та використанні сертифікатів, що пов'язані з цими послугами; або (b) створенні, перевірці та підтвердженні сертифікатів для автентифікації веб-сайту; або збереженні електронних підписів, електронних печаток або сертифікатів, пов'язаних з цими послугами;	'trust service' means an electronic service normally provided for remuneration which consists of: the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or the creation, verification and validation of certificates for website authentication; or the preservation of electronic signatures, seals or certificates related to those services	SOMEWHAT IDENTICAL

8) електронна ідентифікація	процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;	"електронна ідентифікація" - процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну або юридичну особу або фізичну особу, що представляє юридичну особу;	'electronic identification' means the process of using person identification data in electronic form uniquely repre senting either a natural or legal person, or a natural person representing a legal person;	IDENTICAL
9) електронна печатка	електронні дані, які додаються створювачем електронної печатки до інших електронних даних або логічно з ними пов'язуються і використовуються для визначення походження та перевірки цілісності пов'язаних електронних даних;	"електронна печатка" - дані в електронній формі, які додаються або логічно пов'язані з іншими електронними даними для підтвердження походження та цілісності останніх;	'electronic seal' means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;	IDENTICAL
12) електронний підпис	електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис;	дані в електронній формі, які приєднуються або логічно пов'язуються з іншими електронними даними, і використовуються підписувачем в якості підпису (13) "дані для створення електронного підпису" - унікальні дані, які використовуються підписувачем для створення електронного підпису;	data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign; unique data which is used by the signatory to create an electronic signature;	IDENTICAL
13) електронні дані	будь яка інформація в електронній формі;			NOT DEFINED
14) засвідчення чинності відкритого ключа	процедура формування сертифіката відкритого ключа;			NO EQUIVALENT
15) засіб електронного підпису чи печатки	апаратно-програмний або апаратний пристрій чи програмне забезпечення, які використовуються для створення та/або перевірки електронного підпису чи печатки; + (31)"засіб для створення електронної печатки" - налаштоване програмне або апаратне забезпечення, яке використовується для створення електронних печаток;	"засіб для створення електронного підпису" - налаштоване програмне або апаратне забезпечення, яке використовується для створення електронного підпису; (31) "засіб для створення електронної печатки" - налаштоване програмне або апаратне забезпечення, яке	'electronic signature creation device' means configured software or hardware used to create an electronic signature. electronic seal creation device' means configured software or hardware used to create an electronic seal; + (31)	IDENTICAL

		використовується для створення електронних печаток;	‘electronic seal creation device’ means configured software or hardware used to create an electronic seal;	
16) засіб електронної ідентифікації	носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг;	засоби електронної ідентифікації видаються за схемою електронної ідентифікації, що міститься в переліку, опублікованому Комісією відповідно до статті 9. Комісія повинна опублікувати в Офіційному віснику Європейського Союзу перелік схем електронної ідентифікації, що були нотифіковані на підставі частини 1, та основну пов’язану з цим інформацію.	the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9; Commission shall publish in the Official Journal of the European Union a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.	IDENTICAL
17) засіб кваліфікованого електронного підпису чи печатки	апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки, який відповідає вимогам цього Закону;	"засіб для створення кваліфікованого електронного підпису" - засіб для створення електронного підпису, що відповідає вимогам, викладеним у Додатку II; (32) "засіб для створення кваліфікованої електронної печатки" - засіб для створення електронної печатки, який відповідає вимогам, викладеним в Додатку II;1. Засоби для створення кваліфікованого електронного підпису забезпечують за допомогою належних технічних засобів та процедур,	‘qualified electronic signature creation device’ means an electronic signature creation device that meets the requirements laid down in Annex II;‘qualified electronic seal creation device’ means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II; Qualified electronic signature creation devices shall	IDENTICAL

			ensure, by appropriate technical and procedural means,	
18) засіб удосконаленого електронного підпису чи печатки	апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення удосконаленого електронного підпису чи печатки, та/або перевірки удосконаленого електронного підпису чи печатки, та/або зберігання особистого ключа удосконаленого електронного підпису чи печатки;	(22) "засіб для створення електронного підпису" - налаштоване програмне або апаратне забезпечення, яке використовується для створення електронного підпису; + (32) "засіб для створення кваліфікованої електронної печатки" - засіб для створення електронної печатки, який відповідає вимогам, викладеним в Додатку II	(22) ‘electronic signature creation device’ means configured software or hardware used to create an electronic signature +(32) ‘qualified electronic seal creation device’ means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II	IDENTICAL
19) ідентифікаційні дані особи	унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи;	(3) "дані персональної ідентифікації" – сукупність даних, яка дозволяє встановити відомості про особу для фізичних або юридичних осіб або для фізичної особи, що представляє юридичну особу;	(3) person identification data’ means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;	IDENTICAL
20) ідентифікація особи	процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи;	1) "електронна ідентифікація" - процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну або юридичну особу або фізичну особу, що представляє юридичну особу; + (2) "засоби електронної ідентифікації"- матеріальна та/або нематеріальна складова, яка містить дані персональної	(1) ‘electronic identification’ means the process of using person identification data in electronic form uniquely repre senting either a natural or legal person, or a natural person representing a legal person; +(2) ‘electronic identification means’ means a material and/or	IDENTICAL

		ідентифікації і використовується для автентифікації в он-лайн послугах;	immaterial unit containing person identification data and which is used for authentication for an online service;	
21) інтероперабельність	технологічна сумісність технічних рішень, що використовуються під час надання електронних послуг, та їх здатність взаємодіяти між собою;	(54) Транскордонна сумісність і визнання кваліфікованих сертифікатів є попередньою умовою для транскордонного визнання кваліфікованих електронних підписів. Отже до кваліфікованих сертифікатів не повинно висуватись жодних обов'язкових вимог, що перевищують вимоги, викладені в цьому Регламенті. Проте, на національному рівні має бути дозволено включення до кваліфікованих сертифікатів спеціальних характеристик, таких як унікальні ідентифікатори, але за умови, що такі спеціальні характеристики не перешкоджають транскордонній сумісності та визнанню кваліфікованих сертифікатів та електронних підписів	(54) Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in qualified certificates should be allowed, provided that such specific attributes do not hamper cross-border interoperability and recognition of qualified certificates and electronic signatures.	IDENTICAL

22) кваліфікована електронна печатка	удосконалена електронна печатка, яка створюється з використанням засобу кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки;	"кваліфікована електронна печатка" - удосконалена електронна печатка, яка створюється засобом для створення кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки;	'qualified electronic seal' means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;	IDENTICAL
23) кваліфікований електронний підпис	удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;	удосконалений електронний підпис, який створюється засобом для створення кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті для електронних підписів;	an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;	IDENTICAL
24) кваліфікований надавач електронних довірчих послуг	юридична особа незалежно від організаційно правової форми та форми власності, фізична особа підприємець, яка надає одну або більше електронних довірчих послуг, діяльність якої відповідає вимогам цього Закону та відомості про яку внесені до Довірчого списку;	"кваліфікований провайдер довірчих послуг" - провайдер довірчих послуг, який надає одну або декілька кваліфікованих довірчих послуг та має статус кваліфікованого, наданий йому наглядовим органом;	'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;	IDENTICAL
26) компрометація особистого ключа	будь яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа;	Стаття 10 Порушення безпеки	Article 10 Security breach	NOT DEFINED
27) користувачі електронних довірчих послуг	підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог цього Закону;	"сторона-користувач" - фізична або юридична особа, яка покладається на електронну ідентифікацію або довірчу послугу;	'relying party' means a natural or legal person that relies upon an electronic identification or a trust service;	IDENTICAL
28) надавач електронних довірчих послуг	юридична особа незалежно від організаційно правової форми та форми власності, фізична особа підприємець, яка надає одну або більше електронних довірчих послуг;	"провайдер довірчих послуг" - фізична або юридична особа, яка надає одну або декілька довірчих послуг. Існують кваліфіковані та некваліфіковані провайдери довірчих послуг;	'trust service provider' means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;	IDENTICAL

29) особистий ключ	параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів;			NOT DEFINED
30) пара ключів	особистий та відповідний йому відкритий ключі, що є взаємопов'язаними параметрами алгоритму асиметричного криптографічного перетворення;			NOT DEFINED
31) перевірка	процес засвідчення справжності і підтвердження того, що електронний підпис чи печатка є дійсними;	"перевірка достовірності" - процес перевірки та підтвердження достовірності електронного підпису або електронної печатки.	'validation' means the process of verifying and confirming that an electronic signature or a seal is valid.	IDENTICAL
32) підписувач	фізична особа, яка створює електронний підпис;	це фізична особа, яка створює електронний підпис;	means a natural person who creates an electronic signature;	IDENTICAL
33) поновлення сертифіката відкритого ключа	відновлення чинності попередньо заблокованого сертифіката відкритого ключа;			NOT DEFINED
34) програмно-технічний комплекс	технічний комплекс, що використовується під час надання електронних довірчих послуг (далі програмно технічний комплекс), апаратні, апаратнопрограмні та програмні засоби, що забезпечують виконання функцій, пов'язаних з наданням електронних довірчих послуг;	"засоби електронної ідентифікації"- матеріальна та/або нематеріальна складова, яка містить дані персональної ідентифікації і використовується для автентифікації в он-лайн послугах;	electronic identification means' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;	IDENTICAL
35) реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів	електронна база даних, в якій містяться відомості про сертифікати відкритих ключів, сформовані надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом, їх статус та списки відкликаних сертифікатів відкритих ключів;			NO EQUIVALENT

36) реєстрована електронна доставка	послуга, яка дає змогу передавати електронні дані між третіми сторонами за допомогою електронних засобів, засвідчувати обробку переданих електронних даних, у тому числі підтверджувати відправлення та отримання електронних даних, та захистити відправлені електронні дані від втрати, крадіжки, пошкодження або несанкціонованих змін;	"послуга рекомендованого електронного відправлення" - послуга, яка дозволяє передавати дані між третіми сторонами за допомогою електронних засобів та надає докази стосовно обробки переданих даних, в тому числі підтвердження передачі та прийому даних, і яка захищає передані дані від ризику втрати, крадіжки, пошкодження або самовільних змін;	'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;	IDENTICAL
37) самопідписаний сертифікат відкритого ключа	сертифікат відкритого ключа, який формується центральним засвідчувальним органом або засвідчувальним центром з використанням особистого ключа центрального засвідчувального органу або засвідчувального центру;			NO EQUIVALENT
38) сертифікат відкритого ключа	електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію веб-сайту;	"сертифікат для автентифікації веб-сайту" - свідоцтво, що надає можливість автентифікації веб-сайту та пов'язує веб-сайт з фізичною або юридичною особою, якою було отримано сертифікат;	'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;	SOMEWHAT IDENTICAL
39) скасування сертифіката відкритого ключа	зупинення чинності сертифіката відкритого ключа;			NO EQUIVALENT
40) створювач електронної печатки	юридична особа, яка створює електронну печатку;	розробник печатки" - юридична особа, яка створює електронну печатку;	'creator of a seal' means a legal person who creates an electronic seal	IDENTICAL
41) схема електронної ідентифікації	система електронної ідентифікації, в якій засоби електронної ідентифікації видаються фізичним, юридичним особам та представникам юридичних осіб;	(1) система електронної ідентифікації, на підставі якої засоби електронної ідентифікації видаються фізичним або юридичним особам або фізичним особам, що представляють	means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural	IDENTICAL

		юридичних осіб;	persons representing legal persons	
42) технологічна нейтральність національних технічних рішень	невтручання органів, що здійснюють державне регулювання у сфері електронних довірчих послуг, у процес розроблення програмно-технічних комплексів, засобів електронного підпису чи печатки та засобів криптографічного захисту інформації, який не перешкоджатиме досягненню інтероперабельності між ними;			NOT DEFINED
43) удосконалена електронна печатка	електронна печатка, створена за результатом криптографічного перетворення електронних даних, з якими пов’язана ця електронна печатка, з використанням засобу удосконаленої електронної печатки та особистого ключа, однозначно пов’язаного із створювачем електронної печатки, і який дає змогу здійснити електронну ідентифікацію створювача електронної печатки та виявити порушення цілісності електронних даних, з якими пов’язана ця електронна печатка;	"удосконалена електронна печатка" - електронна печатка, яка відповідає вимогам, зазначеним у статті 36 Удосконалена електронна печатка повинна відповідати таким вимогам: (a) бути однозначно пов'язаною із розробником печатки; (b) надавати можливість ідентифікувати розробника печатки; (c) створюватись з використанням даних для створення електронної печатки, які розробник печатки може, з високим ступенем впевненості контролювати та використовувати для створення електронної печатки і (d) бути пов’язаною з даними, до яких вона відноситься, таким чином, що будь-яка наступна зміна даних може бути виявлена.	advanced electronic seal’ means an electronic seal, which meets the requirements set out in Article 36. An advanced electronic seal shall meet the following requirements: (a) it is uniquely linked to the creator of the seal; (b) it is capable of identifying the creator of the seal; (c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and (d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.	IDENTICAL

44) удосконалений електронний підпис	електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов’язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов’язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов’язаний цей електронний підпис.	електронний підпис, який відповідає вимогам, викладеним у статті 26; Удосконалений електронний підпис повинен відповідати таким вимогам: (a) бути однозначно пов'язаним з підписувачем; (b) надавати можливість ідентифікувати підписувача; (c) створюватись з використанням даних для створення електронного підпису, які підписувач може, з високим ступенем впевненості, одноосібно контролювати; (d) бути пов’язаним з підписаними даними таким чином, що будь-яка наступна зміна даних може бути виявлена.	electronic signature’ means an electronic signature which meets the requirements set out in Article 26 An advanced electronic signature shall meet the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.	IDENTICAL
		"орган державного сектору" – Держава, регіональні або місцеві органи влади, установи публічного права та об’єднання, утворені одним або декількома органами влади, однією або декількома установами публічного права або приватні особи, уповноважені, принаймні одним або однією з таких органів влади, установ або об'єднань, надавати державні послуги, якщо останні діють на підставі цих повноважень;	‘public sector body’ means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;	NO EQUIVALENT

		"установа публічного права" – установа відповідно до визначення в пункті 4 частини 1 статті 2 Директиви 2014/24/ЄС Європейського Парламенту та Ради	'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council	NO EQUIVALENT
	орган оцінки відповідності	"орган оцінки відповідності" - орган, визначений у пункті 13 статті 2 Регламенту (ЄС) № 765/2008, акредитований відповідно до зазначеного Регламенту як компетентний у здійсненні оцінки відповідності кваліфікованого провайдера довірчих послуг та кваліфікованих довірчих послуг, які надаються зазначеним провайдером;	'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;	NOT DEFINED
		"продукт" – це апаратне або програмне забезпечення, або їх відповідні складові, які призначені для використання під час надання довірчих послуг;	'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;	NO EQUIVALENT

	кваліфікована електронна позначка часу	"кваліфікована електронна позначка часу" - електронна позначка часу, яка відповідає вимогам, викладеним у статті 42; 1. Кваліфікована позначка часу повинна відповідати таким вимогам: (a) пов'язувати дату і час з даними в такий спосіб, що цілком виключає можливість непомітної зміни даних; (b) базуватися на точному джерелі часу, пов'язаному з універсальним координованим часом (UTC); (c) бути підписаною за допомогою удосконаленого електронного підпису або містити проставлену удосконалену електронну печатку кваліфікованого провайдера довірчих послуг, або іншим еквівалентним методом. 2. Комісія, шляхом прийняття виконавчих актів, може встановлювати перелік стандартів щодо пов'язання дати та часу із даними та щодо точності джерела часу. Дотримання вимог, викладених в частині 1, вважається досягнутим, якщо прив'язка дати та часу до даних та точність джерела часу відповідають цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.	'qualified electronic time stamp' means an electronic time stamp which meets the requirements laid down in Article 42;A qualified electronic time stamp shall meet the following requirements: (a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably; (b) it is based on an accurate time source linked to Coordinated Universal Time; and (c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method. 2. The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accurate time source meets those standards. Those	NOT DEFINED

			implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	
		"електронний документ" - будь-який контент, який зберігається в електронній формі, зокрема текст або звук, візуальний або аудіовізуальний запис;	'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;	NOT DEFINED

		"кваліфікована послуга рекомендованого електронного відправлення" - послуга рекомендованого електронного відправлення, яка відповідає вимогам, викладеним у статті 44; Вимоги до кваліфікованої послуги рекомендованого електронного відправлення 1. Кваліфіковані послуги рекомендованих електронних відправлень повинні відповідати таким вимогам: (a) вони повинні надаватися одним чи кількома кваліфікованими провайдерами довірчих послуг; (b) вони повинні забезпечувати ідентифікацію відправника з високим рівнем довіри; (c) перед доставкою даних, повинна бути забезпечена ідентифікація отримувача; (d) відправка та отримання даних повинні бути захищеними з використанням вдосконаленого електронного підпису або удосконаленої електронної печатки кваліфікованого провайдера довірчих послуг у спосіб, який виключає можливість непоміченої зміни даних; (e) відправник і отримувач даних повинні бути чітко повідомлені про будь-яку зміну даних, необхідну для відправки або отримання даних; (f) дата і час відправки, отримання та будь-яка зміна даних повинні бути позначені за	'qualified electronic registered delivery service' means an electronic registered delivery service which meets the requirements laid down in Article 44;Qualified electronic registered delivery services shall meet the following requirements: (a) they are provided by one or more qualified trust service provider(s); (b) they ensure with a high level of confidence the identification of the sender; (c) they ensure the identification of the addressee before the delivery of the data; (d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably; (e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data; (f) the date and time of sending, receiving and any	NO EQUIVALENT

		допомогою кваліфікованої електронної позначки часу; У разі відправки даних між двома або більше кваліфікованими провайдерами довірчих послуг, вимоги пунктів (a) - (f) повинні застосовуватися до всіх кваліфікованих провайдерів довірчих послуг. 2. Комісія, шляхом прийняття виконавчих актів, може встановлювати перелік стандартів щодо процесів відправки та отримання даних. Дотримання вимог, викладених в частині 1, вважається досягнутим, якщо процеси відправки та отримання даних відповідають цим стандартам. Ці виконавчі акти повинні бути прийняті відповідно до процедури експертизи, зазначеної в частині 2 статті 48.	change of data are indicated by a qualified electronic time stamp. In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers. 2. The Commission may, by means of implementing acts, establish reference numbers of standards for processes for sending and receiving data. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).	

“by Article” comparison of Law of Ukraine "On electronic trust services" according to the Regulation (EU) No 910/2014.

ЗАКОН УКРАЇНИ Про електронні довірчі послуги	Corresponds in Reg 910 to:
Розділ I ЗАГАЛЬНІ ПОЛОЖЕННЯ	
Стаття 1. Визначення термінів	CHAPTER I Article 3 Definitions L 257/83 L 257/86
Стаття 2. Сфера дії Закону	CHAPTER I Article 2 Scope
Стаття 3. Законодавство у сферах електронних довірчих послуг та електронної ідентифікації	No refference found
Стаття 4. Основні принципи державного регулювання у сферах електронних довірчих послуг та електронної ідентифікації	CHAPTER I Article 4 Internal market principle, Article 5 Data processing and protection
Розділ II СУБ’ЄКТИ ВІДНОСИН У СФЕРІ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ТА ОРГАНИ, ЩО ЗДІЙСНЮЮТЬ ДЕРЖАВНЕ РЕГУЛЮВАННЯ У СФЕРАХ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ ТА ЕЛЕКТРО...	perambula 70-71; Article 17 Supervisory body
Стаття 5. Система органів, що здійснюють державне регулювання у сферах електронних довірчих послуг та електронної ідентифікації	Article 17 Supervisory body Article 47 Exercise of the delegation Article 48 Committee procedure
Стаття 6. Повноваження Кабінету Міністрів України у сферах електронних довірчих послуг та електронної ідентифікації	No refference found
Стаття 7. Повноваження головного органу у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері електр...	No refference found
Стаття 8. Повноваження спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв’язку та захисту інформації у сфера...	No refference found
Стаття 9. Повноваження Національного банку України у сферах електронних довірчих послуг та електронної ідентифікації	No refference found

Стаття 10. Повноваження центрального органу виконавчої влади, що реалізує державну політику у сфері інформатизації, електронного урядування, формування і вик...	No refferce found
Стаття 11. Суб’єкти відносин у сфері електронних довірчих послуг	No refferce found
Стаття 12. Права та обов’язки користувачів електронних довірчих послуг	CHAPTER III Article 15 Accessibility for persons with disabilities
Стаття 13. Права та обов’язки кваліфікованих надавачів електронних довірчих послуг	No refferce found
Розділ III ЕЛЕКТРОННА ІДЕНТИФІКАЦІЯ	CHAPTER II ELECTRONIC IDENTIFICATION
Стаття 14. Засоби електронної ідентифікації	CHAPTER II Article 9 Notification
Стаття 15. Схеми електронної ідентифікації	CHAPTER II Article 7 Eligibility for notification of electronic identification schemes Article 8 Assurance levels of electronic identification schemes
Розділ IV ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ	No refferce found
Стаття 16. Вимоги до електронних довірчих послуг	Article 19 Security requirements applicable to trust service providers Article 36 Requirements for advanced electronic seals
Стаття 17. Використання електронних довірчих послуг	Article 27 Electronic signatures in public services Article 37 Electronic seals in public services
Стаття 18. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки	Article 21 Initiation of a qualified trust service Article 26 Legal effects of electronic signatures Article 29 Requirements for qualified electronic signature creation devices Article 35 Legal effects of electronic seals

Стаття 19. Засоби кваліфікованого електронного підпису чи печатки	SECTION 4 Electronic signatures Article 25 Legal effects of electronic signatures Article 29 Requirements for qualified electronic signature creation devices Article 30 Certification of qualified electronic signature creation devices Article 39 Qualified electronic seal creation devices
Стаття 20. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки	Article 32 Requirements for the validation of qualified electronic signatures Article 33 Qualified validation service for qualified electronic signatures Article 38 Qualified certificates for electronic seals
Стаття 21. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката автентифікації веб	SECTION 8 Website authentication Article 45 Requirements for qualified certificates for website authentication
Стаття 22. Ідентифікація особи під час формування та видачі кваліфікованого сертифіката відкритого ключа	
Стаття 23. Кваліфіковані сертифікати відкритих ключів	Article 28 Qualified certificates for electronic signatures
Стаття 24. Чинність кваліфікованих сертифікатів відкритих ключів	
Стаття 25. Скасування, блокування та поновлення кваліфікованих сертифікатів відкритих ключів	
Стаття 26. Кваліфікована електронна довірча послуга формування, перевірки та підтвердження кваліфікованої електронної позначки часу	Article 41 Legal effect of electronic time stamps Article 42 Requirements for qualified electronic time stamps
Стаття 27. Кваліфікована електронна довірча послуга реєстрованої електронної доставки	SECTION 7 Article 43 Legal effect of an electronic registered delivery service Article 44 Requirements for qualified electronic registered delivery services
Стаття 28. Кваліфікована електронна довірча послуга зберігання кваліфікованих електронних підписів, печаток та сертифікатів, пов’язаних з цими послугами	Article 34 Qualified preservation service for qualified electronic signatures Article 40 Validation and preservation of qualified electronic seals

Стаття 29. Особливості надання кваліфікованих електронних довірчих послуг центральним засвідчувальним органом	No refference found
Стаття 30. Набуття статусу кваліфікованого надавача електронних довірчих послуг	Article 24 Requirements for qualified trust service providers
Стаття 31. Припинення діяльності з надання кваліфікованих електронних довірчих послуг кваліфікованим надавачем електронних довірчих послуг	No refference found
Розділ V НАГЛЯД (КОНТРОЛЬ) У СФЕРІ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ	No refference found
Стаття 32. Оцінка відповідності у сфері електронних довірчих послуг	Article 22 Trusted lists Article 46 Legal effects of electronic documents
Стаття 33. Державний нагляд (контроль) за дотриманням вимог законодавства у сфері електронних довірчих послуг	Article 20 Supervision of qualified trust service providers
Стаття 34. Повноваження посадових осіб контролюючого органу під час здійснення заходів державного нагляду (контролю) за дотриманням вимог законодавства у сфе...	No refference found
Стаття 35. Довірчий список	Article 31 Publication of a list of certified qualified electronic signature creation devices
Стаття 36. Відповідальність у сфері електронних довірчих послуг	CHAPTER I Art 10-11 Security breach, Liability CHAPTER III TRUST SERVICES SECTION 1 Article 13 General provisions Liability and burden of proof Article 16 Penalties
Розділ VI МІЖНАРОДНЕ СПІВРОБІТНИЦТВО	No refference found
Стаття 37. Участь у міжнародному співробітництві у сферах електронних довірчих послуг та електронної ідентифікації	CHAPTER II Article 12 Cooperation and interoperability Article 14 International aspects Article 18 Mutual assistance
Стаття 38. Визнання іноземних електронних довірчих послуг	CHAPTER II Article 6 Mutual recognition Article 23 EU trust mark for qualified trust services
Розділ VII ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ	CHAPTER VI FINAL PROVISIONS Article 49 -52