UKRAINIAN CENTRE
FOR EUROPEAN
POLICY

Dr. Andrii Dresviannikov

Dr. Andrii Melashchenko

TRUST SERVICES IN UKRAINE

#research

www.ucep.org.ua

Review:

Dmytro Naumenko
Senior Analyst, Ukrainian Center for European Policy

Policy Research with relevance to EU-Ukraine Association Agreement Annex 17-3

TRUST SERVICES IN UKRAINE

Dr. Andrii Dresviannikov
Dr. Andrii Melashchenko

Literary correction: Kateryna Potapenko

Design and layout: Oleksandr Ivanov

This publication was produced with the support of the European Union and the International Renaissance Foundation within the framework of the EU4USociety project.

Its contents are the sole responsibility of of the authors and do not necessarily reflect the views of the European Union and the International Renaissance Foundation.

MOVING FORWARD TOGETHER
THIS PROJECT IS FUNDED BY THE EUROPEAN UNION

INTERNATIONAL
RENAISSANCE
FOUNDATION

UKRAINIAN CENTRE
FOR EUROPEAN
POLICY

CONTENT

SUMMARY

This document is the policy research on the Trust Services(TS) state-of-play and prospects of further development in Ukraine. It was initially planned as part of an independent assessment of EU-Ukraine Association Agreement (AA) Annex 17-3 (telecom, trust services, and e-commerce) regulatory approximation progress. Yet due to the announcement of the upcoming update on the EU eIDAS regulation with drafting proposal due June 2021[1] authors are extending the scope to provide analysis of Ukrainian TS, over four components, Legal Context, Supervision, Audit of Trust Service Providers, Best practices[2] also discussing: policy options, scenarios, identifying risk factors of Trust Services and eID in the Public Sector, exploring TS related implications in delivering public services that are more effective and create better value. The document targets an audience already accustomed to core concepts and regulations in the field of Trust Services and eID on both sides of the EU-Ukraine Association Agreement. In particular Ministry of Digital Transformation of Ukraine (MoDT), whom we see as the principal champion of the Ukrainian Euro-integration of Trust Services.

There is no guiding Policy document on Ukrainian Trust Services and eID in the form of a White Paper or the Program where a deliberate system of principles and statements of intent guiding decision-making is formulated. Nevertheless, the analysis revealed that the Ukrainian Trust Service development patterns closely resemble those of the EU, but also that there are several areas (Standards, Supervision and Control, Personal Data Protection) where practices can be improved. Work identifies the strategies that can support the Ukrainian Government in successfully addressing the issues and consequently better placing Ukraine in a position of further euro-integrational steps, namely singing Mutual Recognition Agreement (MRA) on Trust Services with the EU, gaining internal market regime and starting integration into Digital Single Market (DSM).

Summary of the major recommendations:

- Create set of White Papers/Program Documents on Digital Government, Trust Services, eID, Data Protection, e-Archiving, Accessibility / inclusivity of public services ICT systems, other related areas such as education (digital skills), telecom (5G network, IoT), scientific research and R&D, inclusivity.
- Develop Trust and Data Protection Models, incorporating those into the Policies.
- Initiate inclusion of Ukraine into international indexes, namely: a) Digital Economy and Society Index (I-DESI), b) Digital Trade Restrictiveness Index (DTRI), c)Global Acceptance of EU Trust Services (ETSI TR 103 684)
- Renew National Accreditation Agency of Ukraine (NAAU) Bilateral Agreement (BLA) signatory status. Provide guidelines, and change existing legislation on Conformity Assessment of Ukrainian QTSP to reduce risks of non-conformity, for instance, employing internationally recognised Conformity Assessment Bodies (EU CABs).
- Address standardization gaps within QTS, QTSP, RSS, QSCD, HSM and Conformity Assessment by reviewing and updating relevant standards.

[1] https://data.consilium.europa.eu/doc/document/ST-14351-2020-INIT/en/pdf

[2] https://esignature.ec.europa.eu/intl-comp/dss-demo/downloads/MRAinfo_Cookbook_v1.0.pdf

- Consider the introduction of Common Criteria Evaluation Assurance Level requirements for the hardware / equipment related to PKI infrastructure and trust service provisions.
- Update National Archive Strategy of Ukraine with the vision on e-documents long term preservation (LTP), studying and adopting the EU member states experience.
- Create / encourage e-signature e-seal validation service that can work with (validate) international e-signature (based on ECDSA, RSA) - provide more information on the ways domestic Ukrainian e-signatures are validated.
- Adopt and start to implement standard EN 301 549 - Accessibility requirements for ICT products and services. Update legislative base to incorporate European Web Accessibility Directive.

Major Risks are related to visionary, technological and standards related divergence from the EU policies on eID and Trust Services.

An ambiguity of the momentum is further highlighted by the fact that both the EU and Ukraine are planning the major update of legislation on Trust Services in the fashion that for now seems to be not quite aligned. Ukrainian Government is already prepared suggestion[3] to update 80+ domestic Laws that likely to trigger further changes in 150+ regulations, including significant changes to Law 2155-VII on Trust Services and eID. It is challenging to evaluate suggested legislative proposals unless some manifestation of the vision for the future is available in formats other than political statements and promotional materials. From the perspective of the EU-Ukraine integration, suggested changes may be seen as premature, as European eIDAS (Trust Services and eID regulation) is also updated with drafting due to be published June 2021.

3) https://bit.ly/3xw8X90

STATEMENT OF PURPOSE

Like many nations worldwide, Ukrainian society (people, governments, and businesses) is undergoing transformational changes due to digital technologies rapidly and disruptively entering everyday life. Changes are happening in nearly all segments, from education to agriculture. One of the essential requirements for new digital technologies is managing Trust in an often remote online and digital setting. Trust Services specifically deal with the subject of Trust and therefore applicable to many areas of Digital Transformation. For Ukraine, Digital Transformation drivers are twofold: domestic and those linked to EU-Ukraine cooperation.

Domestic factors of Trust Services development are driven mainly by the Government. There were public announcements of a "Digital State" and "All Public Services in the SmartPhone" by Ukrainian President Vladimir Zelenskiy in 2019. It followed by formation of the Ministry of Digital Transformation (MoDT), responsible for improving Trust Services adaptation and penetration. Upon formation, MoDT began a new cycle of public services digitisation. Yet strategy and desirable destination ware neither defined nor formulated in the form of publicly known White Parer or the Program.

The second driver of Trust Services development, linked to the EU-Ukraine Association Agreement (AA) and prospects for Ukraine to conclude Mutual Recognition Agreement (MRA) on Trust Services, Tel-Com and e-commerce, joining the EU Digital Single Market (DSM). On the Trust Services, Ukraine and the EU had drafted a joint plan[4] for cooperation with a view to a possible agreement based on an approximation to the EU legislation and standards.

Despite undoubtful progress (discussed further in details), there are also gaps in practicalities as well as in vision that, in authors view, may slow down both domestic and international efforts in Trust Services affecting e-commerce and conventional trade. This paper suggests that Digital Government and Trust Services development in Ukraine may benefit from:

1. Program documents that set Governmental long term vision on Trust Service and eID development.
2. Adaptation of European research on Data Protection Models (DPM) Trust Model (TM) as a solid base to Ukrainian eID efforts.
3. Ukraine inclusion to International Digital Economy and Society Index (I-DESI)[5], Global Acceptance of EU Trust Services (ETSI TR 103 684), Digital Trade Restrictiveness Index (DTRI)[6].
4. Conformity Assessment of Ukrainian Qualify Trust Services Providers (QTSP) and QTS based on international standards.
5. Improvements in Qualify Signature Creation Device (QSCD) Policy, that enhance sole control over e-signature/ e-seal, making those qualified QESig / QESeal in terms defined by eIDAS Regulation.
6. Adaptation and implementation of ITSE standards that guide Remote Signature Services (RSS) - QSCD TYPE 2

[4] https://bit.ly/3yXqlxZ

[5] https://digital-strategy.ec.europa.eu/en/library/i-desi-2020-how-digital-europe-compared-other-major-world-economies

[6] https://www.oecd-ilibrary.org/trade/the-oecd-digital-services-trade-restrictiveness-index_16ed2d78-en

7. E-signature e-seal validation service that can work with (validate) international e-signature (based on ECDSA, RSA).

8. Utilization of open-source solutions from the Building Block relevant to Trust Service Provisions (especially in state owned QTSP) e-Archiving etc, that may prevent vendor and developers lock-ups, and increase security and robustness of used ICT solutions.

9. Resolution of trade barriers resulted from the domestic cryptographic standards.

10. Adoptation of the European Web Accessibility Directive and ETSI 301 549 Standard to improve inclusivity of Ukrainian Public ICT systems web and mobile applications.

RELEVANT BACKGROUND

Ukrainian society journey to a better quality of the public services during the past two decades included numerous technological initiatives and created legacies, in the areas ranging from semantics/terminology, throughout legislative and organisational, to the sets of domestic standards. In 2014 significant milestone was reached when the EU and Ukraine signed Free Trade Agreement(DCFTA) and Association Agreement (AA)[7]. It solidified the Ukrainian development vector on Euro integration. It also set the road-map to the alignment with the EU regulations and technical standards. The regulatory approximations in three interconnected areas, TelCom, Trust Services and e-commerce, had been set out in Annex XVII – 3[8] of AA. Those approximations require changes in domestic standards and may conflict with existing legacies. In the Trust Services sphere, changes in domestic standards, in particular, touched upon business interests of hardware and software manufacturers (QSCD-Tokens, HSM - crypto modules, hash functions and crypto libraries). Business interests, legacies and standards are interconnected and may create tensions.

How did the problem arise?

For years, the area of public service provisions in Ukraine was perceived as least efficient and equally detached from citizen's needs and new technologies, creating widespread public frustration and corruption. Hurdles can be traced back to government and public bodies poor performance and ill service design. There were numerous modernization attempts linked to the particular ministries, departments and municipalities. Yet dysfunctional government procurement and fragmentation created a patchwork of localised ITC systems with issues ranging from conflicting data formats, connectivity, vendor lockups, IP rights, with overall little if any interoperability.

Meaningful reforms of public service started after the 2014 Revolution of Dignity and from a non-governmental initiative of civil society[9] that instigated and developed an open-source, public procurement system – later named ProZorro[10] (means Transparent). Launched in 2015, it quickly gained domestic popularity and international recognition[11] and enabled, among other things, the progress in ICT procurement for the public sector and emerging Trust Services.

Legal context: it seems that technology these days at least two steps ahead of legislative initiatives. To accommodate and support a transition to e-services and e-documents, Ukrainian Parliament in 2017 adopted Legislation on Trust Services - Law 2155-VIII[12]. The Law is reasonably aligned with EU eIDAS 910 Regulation[13] and follows technological neutrality principles. However, the network of the implementation decisions that guide information security and Trust Services may be seen as less technology agnostic and one that creates duality in applicable standards. The domestic Trust Service Provisions (TSP), Government and private ICT systems involved in TSP, are required by the implementation

[7] https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf

[8] https://eeas.europa.eu/archives/docs/ukraine/pdf/dcfta-annexes-xvii-xx_en.pdf - AA appendixes text can be (and one may argue should be) the subject of mutually agreed and beneficial renewals

[9] NGO - Transparent Public Procurement - https://www.facebook.com/transparentprocurement.UA

[10] https://prozorro.gov.ua/en

[11] https://openprocurement.io/en/cases/prozorro

[12] https://zakon.rada.gov.ua/laws/show/2155-19#Text

[13] https://bit.ly/3B0b9aQ

decisions (namely 991, 992)[14] [15] [16] to meet either (and in some cases both) ISO/ITSE and localised standards(DSTU), and obtaining by the operators the domestic information security validation clearance (КСЗІ)[17] on hardware and software. Later primarily guided by, and based on, domestic DSTU 4145 standard (discussed further in details). Thereafter Ukrainian Qualify Trust Service Providers (QTSP) and their services only selectively follow international standards with no conformity assessment that can be independently and internationally validated.

What original assumptions are no longer valid or about to change?

1. The Trust Service legislations have a dynamic in Ukraine as well as in the EU. Therefore harmonisation required by AA Annex 17-3 back in 2014 is subject of changing substance and requirements in particulars due to the planned 2021 update in EU eIDAS regulation and development in eID and telecom.

2. In the beginning of 2021 the EU has issued detailed guidelines of Mutual Recognition of Trust Services (MRA cookbook)[18] with the 3-rd countries, those include, in addition to legal approximations, specified in AA Annex 17-3, Supervision and Auditing, Best Practice and Trust Representation alignment.

3. Digital Single Market Strategy for Europe (DSM)[19] had been formulated year after EU - Ukraine AA and had significantly evolved and developed ever since.

4. Changes in TelCom (5G) may, and likely will, alter the ways and possibly even the nature of Public and Trust Services Provisions.

5. Technological advances and corresponding development in International Standardisation (for instance: number of consecutive updates to Cryptographic Suites standard ETSI TS 119 312, 2021 due update of FIPS 140-2 to FIPS 140-3 = ISO/IEC 19790).

6. Ukraine has range of new and ambitious digitisation initiatives that yet to create a coherent picture formulated in specific policies, nevetheless on the ground, technological development is fast and evolving.

[14] https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF#n458

[15] https://zakon.rada.gov.ua/laws/show/z0728-18#Text НАКАЗ № 222 від 31.05.2018

[16] https://zakon.rada.gov.ua/laws/show/z1039-20#n21 НАКАЗ № 140/614 30.09.2020

[17] Complex System of Information Protection – applicable to hardware and software used by QTSP and public ICT systems - https://data.gov.ua/dataset/eab73672-181f-4b20-8819-56d47723ff11

[18] https://data.gov.ua/dataset/eab73672-181f-4b20-8819-56d47723ff11

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

REVIEW THE CURRENT POLICIES

As already discussed, policies in the area of eID and Trust Services in Ukraine based on Law 2155-VIII and a network of implementation decisions as well as a set of domestic standards. Since 2016 Ukraine Digital Agenda - 2020 Program[20] where Trust Services and eID had been mentioned three times in general terms, there were no extended Policies or vision document / White Paper. We therefore shall try to reconstruct those based on available implementation decisions, standards, regulations, matching those against political statements and promotional materials of MoDT available from a public sources.

The Trust Services in Ukraine comprises of:

i.) the provision of qualified certificates for electronic signatures, ii.) the provision of qualified certificates for electronic seals, iii.) the provision of qualified certificates for website authentication, iv.) the qualified validation service for qualified electronic signatures, v.) the qualified validation service for qualified electronic seals, vi.) the qualified preservation service for qualified electronic signatures, vii.) the qualified preservation service for qualified electronic seals, viii.) the provision of qualified time stamps, and ix.) qualified electronic delivery services.

Policy on cryptographic standards

Domestic Ukrainian Cryptographic Standards guided by 124-VII[21], 991[22], 992[23]) Why is it important?

Cryptographic suites that secure e-signature and eID and serve as an underlying element of Public Key Infrastructure (PKI) and Trust infrastructure. In theory, Trust Services can and should be technology agnostic, yet in practice, some standards may be formed based on particulars cryptographic suits, and those are not easily interchangeable. From 2001 Law on Standardisation in Ukraine initiated the development of a domestic custom cryptography suite based on ECC (elliptic curve cryptography)[24]. From 2002 the standards GOST/DSTU 34.311-95[25], DSTU 4145 and GOST/DSTU 28147[26] formed the core requirements and technological stack of nationwide PKI and Root Certification Authority (Root CA). Besides classified and militarily use, those were the major applications of cryptography at the time. De facto, it was done in line with former USSR and Russian Federation standards, deepening the divergence of Ukrainian domestic standards from standards used in Europe and worldwide at the time (RSA, ECDSA). Yet mathematically, DSTU 4145 is similar to ECDSA.[27] as both are based on CCE. With the reintroduction of international ISO and ETSI standards, Ukraine formed a duality in standardisation of information security and Trust Services that remains in 2021[28]. All Government and public administration ICT systems in Ukraine are required by the implementation decision[29] to meet domestic

20) https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf - Цифрова адженда України – 2020 (Draft 2016)

21) https://zakon.rada.gov.ua/laws/show/124-19#n71 -ЗАКОН УКРАЇНИ Про технічні регламенти та оцінку відповідності

22) https://www.kmu.gov.ua/npas/pro-zatverdzhennya-tehnichnogo-reg-a991 - Про затвердження Технічного регламенту засобів криптографічного захисту інформації

23) https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF#Text - Про затвердження вимог у сфері електронних довірчих

24) Elliptic Curve Cryptography (ECC) -Technical Guideline BSI TR-03111 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf

25) https://en.wikipedia.org/wiki/GOST_(hash_function)

26) https://uk.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_28147-89

27) Elliptic Curve Digital Signature Algorithm

28) https://zakon.rada.gov.ua/laws/show/z1039-20#n21 —30.09.2020 № 140/614 regulation guides the use of the dual standards system in cryptography for domestic and cross-border use.

29) https://zakon.rada.gov.ua/laws/show/z0728-18#Text НАКАЗ № 222 від 31.05.2018

information security validation procedure (КСЗІ) based on, and guided by, a set of domestic standards (including DSTU 4145 and DSTU 7564-2014 GOST/DSTU 34.311-95 GOST/ DSTU 28147). DSTU 7564-2014[30] is relatively new domestic standard on hash functions used in e-signatures validation.

The SOG-IS Crypto Evaluation Scheme[31] that helps the EU and worldwide regulators and developers of cryptographic systems with an evaluation of expected lifetimes of secure (recommended) and outdated (legacy) cryptography predicts that crypto algorithms may become vulnerable with progress in quantum computing and new approaches to decryption[32]. A stable and resilient nationwide Trust Services system should account for need of rapid migration to more recent cryptography algorithms. Yet, security is not the only issue that can be addressed with a better adaptation of international standards. Cross-border and even domestic Interoperability of Trust Services is more pressing in the short term.

Policy on e-signature

The concepts e-signature and e-document have a strong analogy with paper-based documents, handwritten signature and wet seal. It took centenaries for paper-based documents to form the widespread conventions. E-signature and e-document have their concepts, technologies, and rules that yet not that well agreed upon and may vary from country to country. Therefore, defying terms, processes, and standards involved in creating, applying, validating, and preserving legally binding e-signature and e-documents is essential.

Types / Formats /strength / packaging=envelops/and other characteristics of e-signature

European Directive on Electronic Signatures (1999) defines an electronic signature as: "data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication". Ukrainian Trust Services Law 2155-VII (2017), as well as eIDAS Regulation (2014), define three types of e-signature a) basic (SES), b) advanced (AdES) and qualified (QES). AdES and QES e-signatures to be legally meaningful required to meet the following criteria. 1) be uniquely linked to the signatory; 2) be capable of identifying the signatory; 3) created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; 4) be linked to the data signed in such a way that any subsequent change in the data is detectable. A further distinction between AdES and QES is defined by the technical specification and legal requirement to the e-signature issuer, and way e-signature is stored, conformity assessment of the e-signature issuer. The critical distinction between AdES and QES is the requirement to store QES at QSCD (Qualify Signature Creation Device) that also entails the use of Cryptographic Token Interface (PKCS#11) with QcStatement (in EU eIDAS requirements standardised by ETSI EN 319 412-5). It should be noted that definitions of AdES by eIDAS leave enough room for an implementation perspective. Therefore, there are range of AdES e-signature formats CAdES, XAdES, PAdES that can be understood as different technical implementations of AdES. The CAdES is based on and works with CMS binary files, XAdES respectively on XML file type and PAdES on PDF file type. Furthermore, there are sub-formats for each, that accounts for presents of times-temp and strength of encryption, respectively: B-B level - no time stems B-T level - with a trusted timestamp, B-LT level - long term, and B-LTA e-Archiving level.

[30] https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-7564-2014.pdf

[31] https://www.sogis.eu/documents/cc/crypto/obsolete/SOGIS-Agreed-Cryptographic-Mechanisms-1.0.pdf

[32] novel technique to modify the SHOR'S algorithm https://ieeexplore.ieee.org/document/8117822

Ukrainian e-signatures main characteristics[33]

Number of Qualify Trust Service Providers issuing e-Signatures	21 (2021)
Format of e-signature in Ukraine	CAdES (by DSTU 4145) -99.9% ECDSA -0.05% RSA - few
number of e-signatures issued	2019 – 4 283 000 2020- 7 274 000
E-signatures on QSCD (Tokenised secure QES)[34]	>11% of e-signatures (2020)
Remote Signature Services (RSS) using TYPE 2 QSCD	Yes (introduced 2021 by PrivatBank QTSP) and about to be provided via DiiyApp from 17May2021
Hash functions used	GOST/DSTU 34.311-95 - somewhat similar to FIPS140-2[35] if look at the technicalities
Duration of e-signature validity	Two years
Archiving of e-document	N/A
Guiding standard	up to 75 domestic standards[36] - including DSTU 4145, DSTU 34.311-95, DSTU 28147, DSTU 7564-2014 / international QES - ETSI TS 119 312

NB best aligned with EU e- signature format would be XadES - ASiC with the long-time (B-LT and B-LTA) Such technical implementation is theoretically allowed by Ukrainian regulations[37] but not available from any of the QTSP as of q12021.

[33] https://czo.gov.ua/development?tab=1

[34] Qualified Signature Generation Device based on DSTU 41 45 with - Cryptographic Token Interface PKCS#11

[35] Federal Information Processing Standard Publication 140-2

[36] https://www.kmu.gov.ua/npas/pro-zatverdzhennya-tehnichnogo-reg-a991

[37] https://zakon.rada.gov.ua/laws/show/z1039-20#n21

There are also different ways to package and store e-signed e-document. The Envelop of the electronically signed document contains: 1) digital data to be signed (text, etc), + 2) e-signature, + 3) timestamp, + 4) the result of the validation of certificated of e-signature at the time of signing (either Certificate Revocation List (CRL) archive, or Online Certificate Status Protocol (OCSP) stapling). Different ways of enveloping and archiving e-signed e-document create rangeof file extensions - p7s, ASIC (zip) etc. All these criteria set and guided by ETSI[38] or other standards, in case of Ukraine 76 of them (annex 2 table 3 regulation 991[39].

Policy on e-seals

E-seal — b2b and b2g documents exchange represents 95%+ of transacted e-documents in Ukraine. These e-documents required not only e-signature but e-seal of legal entity too. There is, however, downward trends in the issuance of e-seals in 2019 2020 that in our view resulted from the change to non-compulsory nature of business seal (and e-seal respectively) in dealings with tax returns from 2017 (more info see Order 557)[40]. New e-seal issuance in Ukraine is down 48% in 2020 compare to 2019 (558 864 fewer e-seals were issued year-on-year)[41]. E-seal in Ukraine is baring same technical and standartization characteristics and issues as e-signature does. Descending dynamics of e-seals also linked to the changes in the way e-seal is handled by QTSP of Tax Office and QTSP of State-owned banks (Privat Bank) that may effect the ways statistical data are collected. From 2020 e-seal is issued in conjunction with e-signature (technically one file) containing two certificates

[38] ETSI Electronic Signatures and Infrastructures (ESI) — set of 200+ standards - https://www.etsi.org/committee/esi

[39] https://www.kmu.gov.ua/npas/pro-zatverdzhennya-tehnichnogo-reg-a991

[40] https://zakon.rada.gov.ua/laws/show/z0959-17#Text

[41] https://czo.gov.ua/development?cat=4&fromyear=2019&toyear=2020

e-signature of company director and e-seal of the legal entity. Such an approach may have justification (subject of standalone study), but it also changes the business logic of an e-seal application. Validity of such approach cannot be verified for now due to the lack of the policy that includes e-seal.

Policy on Qualify Signature Creation Devices

Tokens (QSCD) - Secure e-signature e-seal token is a portable Qualified Signature Creation Device (QSCD in eIDAS terms) that protects e-signature / e-seal under the standards and allows sole control of user over the e-signature / e-seal. QSCD is required by Ukrainian Trust Services Law 2155-VII and had transition period till 07.11. 2020. Yet as discussed, Ukraine still has 88% of e-signatures that are AdES, albeit being called QES (КЕП in Ukrainian) that are not meeting criteria of sole control. The under-usage of tokens or other means to increase solo control is understood as a temperamental trade-off that aims to increase e-signatures penetration and usage. It was legitimised by introduction of experiment conditions[42]. The tokens (QSCD), that can be used in Ukraine are subject to: a) Special Service of (SSSCIPU) approval b)subject of local (КСЗІ) expertise and meeting local standards listed in table 3 of annex 2 of implementation decision 991[43]. Effectively, it imposes a non-tariff barrier and protects the market to predefined QSCD tokens' manufacturers until 2027. There are four domestic business suppliers of QSCD and other security hardware and software.

Remote Signature Services (RSS) = TYPE2 QSCD – the technological solution that stores QESig and QESeals at the server-side of Trust Service Provider (QTSP). It is gaining popularity in the EU and represents an alternative token (QSCD) physically owned by the user as well as to MobileID. This technical implementation is called TYPE2 QSCD or RSS. However, certification of TYPE2 QSCD, where the QSCD is managed on behalf of the signer, goes beyond the certification of the crypto module, handling the e-signature creation data, and also covers the operational environment of QTSP. The ETSI standards guiding RSS are in the final stages of development. Ukraine already has RSS (Smart-Id[44] by PrivatBank launched 2021 and DiiyID lunched May 2021) yet technical aspects of it are not known. Concerns can be related to the type and standards of e-signature(QES), Hardware Security Module (HSM) that store QES, as Ukraine has its own set of standards for the crypto hardware that is not certified under Common Criteria[45] therefore RSS operators presumably limited in hardware options and in technology behind e-signature incription.

MobileID – QSCD can be embedded into a mobile SIM card, and after that, it creates QESig linked to a mobile phone. In Ukraine, Mobile ID was offered by three network providers KyivStar, Vodafone and LifeCell. KyivStar uses RSA and ECDSA algorithm and partially implemented international standards; Vodafone and LifeCell solutions are based on local DSTU 4145 based on ECC but is not internationally comparable. E-signature format is CadES. Besides daunting technical difficulties, the major issue with Ukrainian mobile ID, regardless of the technology used, is boycotting its use in the Ukrainian Tax Office (QESP itself) and other public online services. As a result, RSA and ECDSA halted broader adaptation by the general public. All MobileID services in Ukraine are due to be closed in mid 2021.

Policies on Interoperability in Governmental and Public Services ITC

Trembita system - Ukrainian Gov Interoperability Framework. The milestone in digitisation of public services was the Trembita system - centrally managed distributed data exchange layer (via API) between existing ministerial information systems providing Government and municipalities with electronic data interchange (EDI) capabilities. The project was initiated in 2016, and due to the digression to utilize box solution (x-road) system became operational in 2017. The Trembita system roll-out was linked to the implementation of an anti-corruption strategy, which created an online

[42] https://zakon.rada.gov.ua/laws/show/193-2020-%D0%BF#Text - ПОСТАНОВА 193

[43] https://www.kmu.gov.ua/npas/pro-zatverdzhennya-tehnichnogo-reg-a991

[44] https://privatbank.ua/ru/smart-id

[45] https://www.commoncriteriaportal.org/products/

and open registry of civil servants declaration. The Trembita System interconnects and opens thousands of databases and data sets, therefore, fulfilling one of 6 main principles of Digital Government openness[46]. It works with another system of Government e-documents exchange CEB OBB (see more in e-delivery) and lately positioned as an Interoperability Framework. Despite the success of Trembita, more can to be done to facilitate its uptake by some governmental bodies and municipalities, further integration into Unified State Registries[47], and applying once-only principals[48] risk management and further development of open data strategy.

E-delivery - there is no qualified service of e-delivery in Ukraine as of 2021 q2. However, there are business and government application that do e-delivery. System of Electronic Interaction for Governmental and Municipal Institutions (abbreviation in Ukrainian CEB OBB)[49]. The CEB OBB has over 2600 legal entities and serves as Governmental EDI and e-documents exchange. It pioneered by adopting an e-document format (ASiC) and, for the first time, created legally binding e-document flow within the Government. E-delivery of e-invoices - There was a pilot project on Ukraine-Poland e-trade facilitation in 2020 (EU4Digital Eastern-partnership Program[50]) that used e-delivery for e-invoices exchange via PEPPOL network. Whether Ukraine now has a permanent PEPPOL[51] Accesses Point for e-invoices exchange with the EU counterparts, as the result of the pilot is unclear.

Diiy App, another governmental digital undertaking, was launched in early 2020 and comprise of a)Diiy web portal, b) Diiy Android Application c) Diiy iOS Application d) Diiy API. The DiiyApp is connected to Unified State Registers of Ukraine and initially was introduced as a means of centralized digital communication between the Government and the citizens. DiiyApp contains a digital representation of the ID documents (passport, driving lenience) that increasingly can be used as a substitute for conventional paper based ID. The DiiyApp pipeline[52] has 94 administrative procedures and municipal and central government services (work in progress). State owned administrating legal entity of Diiy is also registered as Qualify Trust Services Provider and have become Remote Signature Service (RSS) for QESig and eID/e-passport in May 2021. The e-passport concept was introduced by Law 4355 "On the Unified State Demographic Register and documents in March 2021[53]. The new Law stipulates that from 23rd August 2021, all Ukrainian companies and government agencies will accept e-passports via DiiyApp application. Being QTSP MoDT subsidiary that runs DiiyApp also likely to become qualify e-delivery service provider conducting legally meaningful g2c g2b notifications and enhancing paperless in public servcies There is ongoing work to improve security[54], usability and extend the list of public services, documents and connectivities available in and via DiiyApp.

Policy on Trust Service Providers and Trust Representation

Trust Service Providers (TSP QTSP) As mentioned before, Ukraine has a mixed model of trust services, whereas QTS can be provided by private and state-owned QTSP. The number of QTSP as of 2021 is 21[55] Six (6) are privately owned, three(3) owned by State banks, and the rest are either government bodies or state-owned enterprises (See Annex 1 for statistical data and quantitative analyses). For Private QTSP Trust Services Business model is challenging as a majority (90%+) of the e-signatures in 2020 was issued free of change by State Banks, Tax Office and other Governmental QTSP. Share of the e-signature issuance by commercial QTSP is down from 18%

[46] https://eur-lex.europa.eu/resource.html?uri=cellar:2c2f2554-0faf-11e7-8a35-01aa75ed71a1.0017.02/DOC_3&format=P

[47] https://nais.gov.ua/

[48] https://en.wikipedia.org/wiki/Once-only_principle

[49] https://dir.gov.ua/projects/sev-ovv - Система електронної взаємодії органів виконавчої влади

[50] https://eufordigital.eu/eu4digital-and-edelivery-what-do-they-mean-for-digitalisation-in-ukraine/

[51] https://peppol.eu/

[52] https://plan2.diiy.gov.ua/projects

[53] https://www.kmu.gov.ua/en/news/mihajlo-fedorov-ukrayina-persha-derzhava-svitu-v-yakij-cifrovi-pasporti-u-smartfoni-stali-povnimi-yuridichnimi-analogami-zvichajnih-dokumentiv

[54] Diiy Bug Bounty Program – report - https://thedigital.gov.ua/storage/uploads/files/news_post/2020/12/diya-proyshla-perevirku-bagbaunti-ta-pidtverdila-bezpechnist-zastosunku/Bounty_17-DEC-2020_Diiy.pdf

[55] https://czo.gov.ua/ca-registry

to 9.5% 2020/19. The largest Ukrainian QTSP is Privat Bank with 72% of e-signatures issued

Trust List (TL) is an essential element of the EU System of Trust and technology that replaces Root CA while creating a more distributed trust PKI ecosystem. Ukrainian Law 2155-VII on Trust Services (in line with eIDAS Regulation) introduced the first national Trusted List (TL)[56]. Technicalities of TL is governed by implementation decision 775[57] with specifications and formats build upon ETSI TS 119 612 Trusted List Standards. Ukrainian TL is available in XML machine-processable format and compliant to the specifications established by CID (EU) 2015/15053 and Article 22(5) of eIDAS. TL as specified by TS 119 612, enables any interested party to determine whether a trust service is or was operating in compliance with the requirements at present or at a given time in the past (e.g. at the time the service was provided, or at the time at which a transaction reliant on that service took place). It is believed that Ukrainian TL contains machine-readable information from which the present and past status of TSP's and their QT services can be established. Trusted List Scheme Operator (TLSO) – is CCA[58] subordinate to the Ministry of Digital Transformation (MoDT). The Trust List set up and maintenance is an excellent example of practical steps Ukraine is taking in creating an equivalent Trust Representation Model and the progress towards MRA as set in eIDAS Art.14. Under MRA, Ukraine will be required to establish, publish and maintain a Trust List providing constitutive information on those TSP/TS that can be recognised as legally equivalent to EU QTSP/QTS. Despite the success of the Ukrainian Trust List and its importance to the EU integration issues remains on a) qualify services (in particular e-signature) validation mechanisms, b) acceptance of e-signatures based on international standards (ECDSA, RSA) in domestic services, including state operating tax office online tax returns submissions, c) other matters directly linked to the usage/not usage of the Trust List that for now seems to be underused and little known to Ukrainian domestic users.

> NB! Trust Representation by TL is an information supplying element that aims to make the equivalence mapping between key URIs or statements used in the EU Member States TL and the 3rd country (potentially Ukraine) TL, respectively. ETSI TS 119 615 offers a standardised process for validating a non-EU QTS output equivalent to an EU QTS output.

Control and Supervision of Trust Services / QTS / QTSP /QSCD

It is complicated in Ukraine. Trust Services supervision defined by Trust Services Law 2155-VII singles out all banking related Trust Services into the jurisdiction of National Bank of Ukraine (NBU) supervisory body[59]. The rest of TS / QTSP /QSCD / PKI / hardware and software is regulated by the Ministry of Digital Transformation (MoDT)[60] and State Service of Special Communications and Information Protection of Ukraine (SSSCIPU)[61]. National Accreditation Agency of Ukraine (NAAU)[62] also involved at the level of Conformity Assessment Body (CAB) accreditation. Matters related to telecom, data protection, cybersecurity or identification are referring to other governmental bodies.

Let's try to work it out based on examples, How to become Qualify Trust Services Provider (QTSP) in Ukraine – upon request from the interested party and meeting Law 2155-VII requirements, MoDT includes a new entity into Trust List and issue Certificate by Root CA (MoDT). Yet in practice interested party also requires a) QTSP "reglament" approvals by the SSSCIPU b) localized technical implementation (hardware+ software+) that meets domestic information security validation procedure with (КСЗІ) and approved by the SSSCIPU c) QTSP Key issuing and crypto equipment approval by the SSSCIPU - complete set of licensing document required for QTSP can be examined at the website of QTSP of State Broader Control Services of Ukraine[63].

[56] https://czo.gov.ua/trustedlist

[57] https://zakon.rada.gov.ua/laws/show/1068-2019-%D0%BF#n40

[58] https://czo.gov.ua/

[59] https://zc.bank.gov.ua/

[60] https://czo.gov.ua/

[61] https://cip.gov.ua/en

[62] https://naau.org.ua/?lang=en

[63] https://acsk.dpsu.gov.ua/registration-examples

Policy on Public Key Infrastructure (PKI)

A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. There are various architectures of PKI that insure validity and failure-resistance of public-key encryption, whereas X.509[64] standard defines the most commonly used format for PKI. In addition to Trust List, Ukrainian authority (MoDT) also runs Central Certificate Authority (CCA). CCA is a legacy policy that provides an extra measure of oversight. Hierarchical PKI structure helps accomplish the following security services in online and otherwise digital communications: a) be the point of initial Trust - registration authority (RA) behind "self-signing" root certificated of Ukrainian QTSP, b) provide certificate revocation list (CRL) or otherwise insure validity of certificated for instance via Online Certificate Status Protocol (OCSP), c) may play future role in websites authentication (not applicable yet as most of internet users in Ukraine as elsewhere use SSL/TLS and relay upon root CAs of operational systems or a browsers (Microsoft, Apple, Google, Mozilla etc) that for now don't contain by default national root certificates.

Central Certificate Authority CCA = Root CA)[65] run by Ministry of Digital Transformation (MoDT) issuing "self-signing" certificates to QTSP and maintains joint certificate revocation list (CRL)[66].

Certification Practice Statement (CPS) = Certificate PS Do those exist in Ukraine? – Yes - in formats of orders issued by the Government via SSSCIPU or MoDT(available only in Ukrainian).

Policy on eID - Ukraine eID

The relationship between personal data and authentication mechanisms is increasingly important globally and actualized by the covid-19 pandemic. In the EU countries there are over 50 eID schemes[67] [68] with 14 Member States have notified at least one national eID scheme and four Member States have already notified multiple schemes. In total, there are 19 eIDAS compliment eID schemes in the EU[69]. Capable agents can exercise their rights duties online and people who can authenticate themselves are electronically active in a more responsible way. On the contrary, inability or fear to identify online creates room for abuses and fraud, identity theft etc. Fears of online surveillance and compromised privacy are among known reasons for citizens' sabotage a governmental eID efforts. Ukraine eID landscape has strongly developed during the last decade. Ukraine has 21 QTSP that can issue e-signature with over 7 million e-signatures issues Besides e-signature (AdES+QESig), Ukrainian also have an alternative way of electronic identification – BankID[70]. BankID is supported by 35 banks and used to secure online logins to the bank accounts and confirm online actions. The BankID cannot be used to sign e-documents.

Ukraine is by no means the first country where the Government is seeking to rollout the large-scale program to supply citizens with digital eID to use in online e-government services. Trust Models(TM) and Digital Identity Management (DIM) good practices are used to form an eID Policy that duly addresses and deals with authentication, access control, confidentiality, and unlinkability of eIDs. None of the eID Policy, TM, DIM or related research or modeling was identified in conjunction with Ukrainian national eID, yet Ukraine has new Law on e-passport/eID. New reading of Law

[64] X.509 2019 - https://www.itu.int/rec/T-REC-X.509-201910-I/en - originally (1988) X.509 was composed of three entities: the certification authority (CA),the certificate holder (or subject), and the Relying Party (RP). The CA plays the role of a trusted third party between the certificate holder and the RP. In many use cases, this trust model has worked successfully.

[65] https://czo.gov.ua/about -Central Certificate Authority CCA

[66] https://czo.gov.ua/crls

[67] E-Identity Initiatives – The European Way A brief market overview 2018 by Andrea Müller & Andreas Windisch

[68] Study on the use of Electronic Identification (eID) for the European Citizens' Initiative 2017

[69] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

[70] https://bank.gov.ua/en/bank-id-nbu Bank ID

5492-VI "On the Unified State Demographic Register and documents[71]" stipulates that from 23rd August 2021, all Ukrainian companies and government agencies will accept e-passports via the Ministry of Digital Transformation (MoDT) Diiy application. The regulation and the current eID scheme implementation does not account for the principles of data minimisation and privacy by default with user control over which data to share and with whom. It would be interesting to learn how new e-passport/eID capabilities be received, and if Law 5492-VI will follow the EU GDPR logic on Personal Data Protection while providing seamless and friction-less digital public services via DiiyApp. From the technological prospective and for the alternatives see more in Available Options › Alternatives in eID.

Policy on archiving of e-document (long-term data preservation)

Overall Archives in Ukraine are regulated by 1993 Law on Archives 3814-XII[72]. The requirements for business, banking, governmental, administrative and other e-documents creation, processing and archiving set in two MoJ Regulations a) #578/5[73] as of 12.04.2012 and b) #1886/51ц[74] as of 11.11.2014, those appear to be quite comprehensive and detailed sets of instructions on unifying and transferring information in electronic format. Further development in e-Archiving was regulation #60[75] from 07.09.2018 setting ASiC[76] as format for e-documents. It was further reinforced by suggested Strategy of Ukrainian Archives development till 2025[77] – percents of White Paper is in itself exceptional and should be regarded as outstanding progress. The substance of drafted White Paper on technicalities of e-documents archiving can be improved. The e-Archiving development is complicated by inadequate technical resourcing of the National Archive of Ukraine and municipal archives. Positive example of due e-archiving exists too. The Banking Archive run by the National Bank of Ukraine (NBU). It is understood that since 2016 NBU is running e-archiving procedures, including those of e-documents with QES and Long-Term Validation (LTV).

Trust Services penetration (+Annex1)

Different Trust Services in Ukraine exhibit varied levels of maturity and penetration into public service provisions, internal government procedures, and business environment. Those are complex multi-parametric measurements best assessed by stand alone study (not available for Ukraine) summarised by international indexes such as a) International Digital Economy and Society Index (I-DESI is not available for Ukraine), b) United Nations E-Government Development Index (EGDI – 0.7119 as for 2020[78]), c) Global Acceptance of EU Trust Services (ETSI TR 103 684-not available for Ukraine) in combination with analysing of domestic statistical data dynamics. Later reveal that there were 7.2 million (4.5 million of unique) valid e-signatures (AdES+ QESig) as of 2020[79] this is 69% more than in 2019 (4.3 million) see Annex 1. Ukrainians are steadily switching to e-signatures in c2g, g2b, b2g, and b2b interactions. A number of timestamps on the rise too, which indirectly points to the number of electronically signed e-documents (3 922 809 328 timestamps in 2020 compared to 1 670 258 087 in 2019); see Annex 1. It gives a 39% year-on-year increase in e-signature usage. Those are outstanding numbers indicating that uptake of digital services by citizens and businesses in Ukraine is going through a period of rapid growth.

[71] https://www.kmu.gov.ua/en/news/mihajlo-fedorov-ukrayina-persha-derzhava-svitu-v-yakij-cifrovi-pasporti-u-smartfoni-stali-povnimi-yuridichnimi-analogami-zvichajnih-dokumentiv

[72] https://zakon.rada.gov.ua/laws/show/3814-12#Text

[73] https://zakon.rada.gov.ua/laws/show/z0571-12#Text

[74] https://zakon.rada.gov.ua/laws/show/z1421-14#Text

[75] https://zakon.rada.gov.ua/laws/show/z1309-18#n17

[76] Associated Signature Containers

[77] https://bit.ly/3hE32Ju

[78] https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine

[79] https://czo.gov.ua/development?cat=1&fromyear=2019&toyear=2020

What circumstances have changed that make a new approach advisable?

- The Ukrainian Government is seeking mutual recognition of Trust Services with the EU. When such a request was made (2019), no clear guidelines on how to achieve it were available. The guidelines on Mutual Recognition Agreement (MRA) Cookbook were published in early 2021, it makes new policy advisable.

- Domestic Ukrainian changes, namely digital public service development, made a case for Ukrainian Trust Services and eID Law amendments. Yet it should be noted that EU -Ukraine MRA on Trust Services, besides legal approximation requirements set in 17-3, will likely include three other areas of alignment: supervision and auditing, best practice, trust representation.

- The Law requirement on certification schemes and Conformity Assessment Bodies (CAB) in the area of Information Security are overdue (expiration of transition period set in the Law)

- Changes in technical standards involved in remote identification, issuance of QES by QTSP QSCD etc

- Global and the EU development in a) Personal Data handling, b) compliance, c) Digital Identity Management.

- New use cases on how the governments are addressing the privacy challenges inherent in the use of digital identity technologies (eID)

- Implementation of new standards on Accessibility of ICT systems of public services for persons with disabilities (in the EU standard EN 301 549

AVAILABLE OPTIONS

What are the alternative ways of meeting the need?

Modern digital information and communication technologies, the Internet, in particular, are based on its ability to link data, resources and people together in a way, it was never possible before; this can be both valuable and harmful. For over four decades, governments and business around the world have been designing and building digital infrastructure, developed and implemented a range of concepts on Electronic Data Interchange (EDI), Digital Identity and lately on Trust Services (TS) to enable customers and/or citizens to login and use online/remote services with trustworthy credentials. Let's investigate available options.

Alternatives in Business models for Trust Services

- Centralized with a leading role of the Public Sector/ the Government
- Federal with a leading role of the Commercial Sector
- Mixed (both public and commercial sector)

Ukraine used mixed model of Trust Services yet with dominance of Government and public sector QTSPs (the largest domestic provider of Trust Services is State owned Private Bank QTSP with 70%+ of market share in 2020 – see Annex 1). In the segment of hardware and software equipment used in for Trust Services Provisions, there are four private suppliers yet overall segment can be seen as protected from competition form international and EU suppliers via means of domestic standards.

Alternatives in Hardware security equipment and QSCD standardisation.

There are viewer options and alternatives worldwide in this field, and even large global economies (US, Europe and Japan) are unifying approaches to security hardware standardisation. Ukraine on the contrary favour domestic standardisation only selectively implement international / EU standards.
An absents of Common Criteria Evaluation Assurance Level (EAL) applicable to the domestic security equipment creates risks (including those to National Security and military applications). It likely to be challenging and not secure to maintain an autonomous and isolated security hardware/software/ cryptography ecosystem in Ukraine, it also can be considered as non-sustainable in the long run, and detrimental to Ukraine-EU integration. Remote Signature Services(RSS) can be seen as an alternative to token based QSCD for e-signature(QES) providing QTSP, their environment and hardware are meeting security requirements.

Alternatives in Conformity Assessment of Qualify Trust Services Providers QTSP

Conformity Assessment of Ukrainian QTSP and QTS by duly appointed Conformity Assessment Body (CAB) in Trust Services and information security – approach has several obstacles (see recommendations), but can be implemented in the long run.

Quick fix and viable alternative can be to allow Conformity Assessment of Ukrainian QTSP by the EU based CABs, at least for cross-border trust services and until domestic Ukrainian CAB is formed and gained sufficient expertise.

Build open model whereas EU CABs are treated equally to Ukrainian CABs on the permanent bases.

Alternatives in eID

Electronic identification (eID) is the process of using person identification data in the electronic form to uniquely represent either a natural/legal person, legal entity, or even a devise. Currently, Ukraine has two major eID scheme e-signature (AdES+QESig) and BankID. However, with no policy on eID we refrain from validation and just list some known global options:

- Federated eID schemes
- SelfServing eID schemes
- Polymorphic eID schemes
- Attribute-based eID schemes
- Centralized eID schemes
- Biomentry based eID schemes

The field of eID and Digital Identity Management is large and dynamic. Each of mentioned above eID Schemes options can be used in combination and have varied technical details that are out of the scope of this paper. 14 EU Member States have notified at least one eID scheme and four Member States have already notified multiple schemes. In total, 19 eID schemes are evident in the EU[80].

[80] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

SCENARIOS

Three core scenarios would be Default, Progressive, and Downbeat in two dimensions: domestic and in the context of eurointegration. Since Ukraine at the constitutional level stated its eurointegrational direction of development, we will paying less attention to catastrophic black-swan-type possibilities.

Default -

Ukraine retains the existing dynamic of eurointegration, selectively adopting EU regulations, standards and good practices with 3 5 years lag and modifications. Domestic Public Key Infrastructure (PKI) and Trust Services retain reliance on the local standards, and new cutting-edge international technologies will require compliance with those standards. The Government carries out policies of digitisation of public services, transferring those online and via the deployment of centralized gov. mobile application (Diiy), later plays a prime role in public e-services design, ways of delivery, and means of Digital Identity Management with less emphasis on personal data protection and unlinkability. The eID program after initial gains may receive increasing resistance due to privacy concerns. Mutual Recognition Agreement (MRA) of Trust Services between the EU and Ukraine likely to be concluded within 4-6 years contingent on maturity of Ukrainian Trust Service Infrastructure and Supervision and convergence of relevant standards. Trade benefits resulting from MRA and DSM to be realized gradually, subject of technological and operational interoperability and business need that drives it.

Progressive -

Ukraine and EU coherently accelerate integration while the Ukrainian Government, civil society, and business interactively develop and actively participate in the digital transformation of domestic institutions. Ukraine develops international expertise in Conformity Assessment of Trust Services, domestic CAB is credible and operational. The Trust and Data Protection models are agreed and implemented. Ukrainian security hardware and cryptography software applications do gain Evaluation Assurance Level (EAL) by Common Criteria. Domestic Trust Services (TS) are converging with updated eIDAS Regulation and EU TS infrastructure at semantic, legal, administer and technological levels. The Ukrainian Digital Government adopts the following principles a) digital-by-design, b) data-driven, c) open to revisions and scrutiny, d) proactive and user-driven. The eID program developed with robust privacy and unlinkability that foster widespread acceptance. Mutual Recognition of Trust Services between the EU and Ukraine happens within 1-3 years, possibly predated by Mutual Recognition (MRA) of Trust Services with one of the Eastern Partnership countries(Moldova, Georgia). The EU-Ukraine MRA and DSM process supported by the pilots and facilitation schemes, results in dynamic trade and investments, creating the case for mutually desirable further integration.

Downbeat -

Ukraine and the EU slows down cooperation. Ukrainian Government, despite declared intentions, to achieve digital transformation and build Digital Government (as defined by OECD[81]) fails or under-deliver. Failure may be defined as systematic ignorance/inability to implement, maintain and develop international/ EU standards in ICT, eID, telecom and Trust Services. Repetitive and gross issues with Trust and Data Protection. If systematic abuses of data protection prevail, it leads to the debasement of public Trust in digital tools and e-services paper-based document exchange remains significant, even if supplemented by available yet underused e-services. The Government introduced digital tools (Diiy app, eID possibly others), and e-services are not trusted by the citizens; business and personal data are centrally collected and occasionally mishandled. Trust Services adherence to international standards remains low, local non-international standards prevail. All above forms wide sped domestic concerns and contradicted international and EU practices. Mutual Recognition of Trust Services between EU and Ukraine unlikely to occur as potential economic gains of MRA cannot be realized or outweighed by the risks for the EU.

[81] https://www.oecd-ilibrary.org/governance/the-oecd-digital-government-policy-framework_f64fed2a-en 'The OECD Digital Government Policy Framework'.

WHAT POINT OF VIEW WE ARE ARGUING FROM

The desire to achieve quick progress in Trust Service and eID by the Ukrainian Government should be reinforced by systemic approaches in strategic planning, standardisation, conformity assessment, data and privacy protection, in the fashion aligned with the EU Policies and based on international standards. Reinforcement is needed to mitigate risks of technological fallout and public trust erosion in Trust Services and eID.

Explained:

The Ukrainian progress in "digitisation" is little know internationally and in the EU, EU run International Digital Economy and Society Index (I-DESI)[82] not includes Ukraine, whereas EU Digital Government Fact-sheets[83] included Ukraine for the first time in 2019 but only in informative non-evaluatory format. Never-the-less Ukraine is developing digitally, let's illustrate the progress that already had been achieved in Trust Services: a) Ukrainian Trust Services semantics and architecture already resemble that of the EU; b) Business model of Trust Service Provisions (TSP) is mixed, implies that both the Government and private sector are involved; c) Government is aware of main principles of Digital Transformation and understands the pivotal role of Telecom and Trust Services in new paradigm; d) Ukraine already have reasonably aligned Law on Trust Services with the EU eIDAS Regulation; e) Ukraine has domestic system of Supervision and control of Qualify Trust Service Provisions that can be good starting point to develop domestic CABs; f) There is the Trust List that meets eIDAS Article 14 and ETSI standards requirements on trust representation; g) There is a rapid rise in e-signatures and e-documents usage in b2g and c2g in 2019 and 2020 (see Annex1 for statistics); h) There were several successful roll-outs of country-wide ITC systems and apps (Trembita, CEB OBB, Diiy App); i) active development is continuing with more digital transformation initiates are in the pipelines (e-passport /eID, Unified State Registry / Remote Signature Services RSS, paperless public services etc.)

To safe-guard the achievements, insure further euroentegrational development and mitigate risks, the following shortcomings should be addressed: a) EU-Ukraine misalignment at the level of standards in cryptography and hardware used for Trust Service Provisions, b) shortcomings in audit and supervision of trust services, missing Conformity Assessment of Qualify Trust Service Providers (QTSP) by internationally recognised Conformity Assessment Bodies (CAB)s; c) existing supervision of Ukrainian QTSP and QTS only selectively follow international standards; d) domestic security equipment (Tokens/ QSCD, HSM) are not evaluated by independent licensed laboratories to determine the fulfillment of particular security properties, or/ and instances of granted assurance against already introduced adaptations of international standards namely DSTU/ISO 15408, DSTU ISO 18045, DSTU EN 419 211, DSTU ISO/IEC 19790, DSTU ISO/IEC 19896-2; e) extensive usage of the security products (hardware and software) without internationally recognised Evaluation Assurance Levels(EAL) under Common Criteria for Information Technologies security evaluation.

Shortage of resources combined with desire of quick wins and/or protectionism may lead to over-reliance on high-risk strategies. It increases the likelihood of a downbeat scenario summarized in the previous section.

[82] https://digital-strategy.ec.europa.eu/en/library/i-desi-2020-how-digital-europe-compared-other-major-world-economies

[83] https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Ukraine_2019_0.pdf

DESIRED OUTCOME

1. Strategies/White Papers with Data Protection Model and Trust Models are created, disseminated and followed.
2. Conformity Assessment of Ukrainian QTSP is performed in accordance with the international standards by domestic and other European CABs.
3. Ukrainian security and crypto hardware used by QTSP gains Evaluation Assurance Level (EAL) under Common Criteria.
4. Domestic and cross-border e-signature e-seal validation is performed in compliance with ETSI standards.
5. Ukrainian trust service community makes better use of Digital Signature Services (DSS) open-source libraries.
6. Ukrainian Trust Infrastructure, QTSPs, QSCD, RSS are made compliant and trusted in the EU.
7. Mutual Recognition Agreement (MRA) on Trust Service Tel-Com and e-commerce with the EU is concluded within 2 years (till 2023) and the EU has sufficient grounds to initiate a sectoral inclusion of Ukraine in DSM.
8. Archiving of e-document is better sourced and conducted countrywide following the strategy and the standards.
9. Publicly used ICT system and applications in Ukraine are compliant with the European Web Accessibility Directive and ETSI 301 549 Standard.

RECOMMENDATIONS

1. Create the Program document (White Papers) that formulates the Vision and forms the Policies on each aspect of Digital Government transformation and in particular on Trust Services and eID

Explained:

The Ukrainian progress in "digitisation" is little know internationally, EU run International Digital Economy and Society Index (I-DESI)[84], Global Acceptance of EU Trust Services (ETSI TR 103 684) – not include Ukraine, whereas EU Digital Government Factsheets[85] did it for the first time in 2019. To the degree it related to the shortage of a)Program Documents; b) trusted statistics data; c) quality, peer reviewed, internationally published research on the subject; d) think tanks or non-of-profit reputable scientific institutions with relevant expertise. Absents of well-formulated policies also create leeway that may lead substandard quality of public services, and to the debasement of standards, higher risks, and limited stakeholders' engagement. Constitutionally defined Euro integration vector of Ukraine development makes it easier to accomplish such Vision and Policy documents using EU research argumentation and already conducted research and "lesson learned" studies. In absents of such formulated vision it appears that Ukraine, at best, is moving towards e-government, not Digital Government, with undefined Trust and Data Protection Models. The e-government implies the use of ICTs, and particularly the Internet,(OECD)[86] putting public services online; however, it has little impact on service workflows and back-office processes, nor has it made services and operations digital-by-design. On the contrary, Digital Government is understood as "the use of digital technologies, as an integrated part of governments' modernisation strategies, to create public value" (definition from OECD 2020 policy paper), adhering to six dimensions of Digital Government Policy Framework: 1) digital by design, 2) data-driven, 3) Government as a platform (in the IT sense), 4) open by default, 5) user-driven, 6) proactive.

In the context of Trust Services, it may mean that government works as a services provider that operates in a competitive business environment. Some degree of competition is a key to Trust Services fine-tuning and development. It's applicable to e-signature, QSCD / token, Mobile ID, and RSS (Remote Signature Services), eID, where competitive environment helps to improve quality while containing the cost.

Action:

Create White Papers / Program Documents on Digital Government, Trust Services, eID, Data Protection, e-Archiving, Accessibility / inclusivity of public services ICT systems, other related areas education (digital skills), telecom (5G network, IoT), scientific research and R&D. Increase international visibility of domestic efforts in digital transformation, for instance to be included in International Digital Economy and Society Index (I-DESI) other Indexes.

2. Develop domestic Trust Models + Data Protection Model + Digital Identity Management Models

Explained:

The products (public services, eID, Trust Services) are a results of certain processes, product and process require vision, policies,

[84] https://digital-strategy.ec.europa.eu/en/library/i-desi-2020-how-digital-europe-compared-other-major-world-economies

[85] https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Ukraine_2019_0.pdf

[86] https://bit.ly/3kgZdeL

resources, standards and stakeholders participation. Modeling helps to realize how its parameters correspond and affect outcomes. The interaction with expert and scientific community further supports government official in digital skills and forms knowledge base that may help in the development of the Policies. In the context of Trust and Data protection, one may wish to explore concepts of unlinkability, SelfServing (SSI) vs Federated Identity (FI), various ways to achieve pseudonymity, Enhanced Role Authentication (ERA), mutual authentication with services providers, etc.

Action:

Develop Trust and Data Protection Models, incorporating those into the Policies.

3. Conformity Assessment of Ukrainian QTSP to internationally recognised standards

Explained:

It is understood that currently, ALL Ukrainian Qualified Trust Service Providers (QTSP) are operating without internationally recognised Conformity Assessment. Furthermore Ukrainian Accreditation Agency (NAAU) failed latest peer review; thereafter, NAAU BLA signatory status for Product Certification was suspended from 24th March 2021[87].It affects, among other things, the capacity to establish domestic CAB in Trust Services, later is the requirements of the EU MRA. Absents of due Conformity Assessment poses the risks for the quality of QTS and short of meeting Mutual Recognition Agreement good practices. There are several ways to resolve this issue. The most cost-effective would be to allow Conformity Assessment of Ukrainian domestic QTSP by the Conformity Assessment Bodies (CAB) from the EU countries. In a longer run, Ukraine should create a domestic Conformity Assessment Body that is subject to ISO/IEC 1701 ISO/IEC 17065 EN 319 403 standards and peers review by the European cooperation for accreditation and IAF. Desirable outcome would be ecosystem where domestic CAB and other European CABs can conduct the conformity assessment of Ukrainian QTSP and QTS.

Action:

Renew NAAU BLA signatory status. Provide guidelines and allow Conformity Assessment of Ukrainian QTSP by EU Conformity Assessment Bodies (CABs.

4. Standardisation gaps within QTS, QTSP, RSS, and Conformity Assessment (CAB)

explained Ukraine is following footsteps of the EU Member States in Trust Services roll-outs and therefore can gain full advantage of already created best practices, research and surveys[88] conducted upon the "first wave" of EU eIDAS implementation. The main barriers for further developing the Trust Services market in the EU 2017 Survey were identified as the gaps in standardisation, highlighted by both Supervisory Bodies and Conformity Assessment Bodies, 80% and 86% respectively acknowledged as the main issue. Ever since European Commission and country-specific Trust Services Supervisory Bodies took notice of it and responded as follows: a) reviewed the standards[89], b) extended M-460 standardisation mandate and allocated resources, c) issued ROLLING PLAN FOR ICT STANDARDISATION 2020[90], d) initiated updates to eIDAS 910 regulation that likely will introduce more and better standards for AdTS, QTS, QTSP, as well as to Conformity Assessment by CAB, and hardware used for QTS.

On the contrary to the EU, Ukraine pays less attention and commits fewer resources to improve standardization aligned with the European Standardisation Organisations; furthermore, the level of international recognition of NAAU was debased due to failed peers audit. That leaves Ukraine with fewer options and hamper eurointegration efforts. Whereas meeting the requirement of the MRA cookbook in a forward-looking manner can also be beneficial for strengthening the reliability of domestic Ukrainian Trust Services as well as for opening new markets. Relevant Standards in need of attention are : ETSI TR 103 684, ETSI TS 119 101, ETSI TS 119 102-1, ETSI TS 119 102-2,

[87] https://ilac.org/latest_ilac_news/signatory-status-of-naau-ukraine-suspended/

[88] https://op.europa.eu/s/oTON

[89] https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas-i

[90] https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2020

ETSI EN 319 132, ETSI EN 319 142, ETSI EN 319 162, and for the Conformity Assessment and CAB ISO/IEC 1701 ISO/IEC 17065 EN 319 403. The following standards in development also should be taken notice of: ETSI EN 319 411-2, ETSI TS 119 432, ETSI 419 241-2, ETSI TR 103 684, ETSI TR 119 460. Modification of domestic standards on domestic security equipment/hardware (QSCD HSM) and software namely: DSTU/ISO 15408, DSTU ISO 18045, DSTU EN 419 211, DSTU ISO/IEC 19790, DSTU ISO/IEC 19896-2 result in Ukrainian security products NOT gaining internationally recognized Evaluation Assurance Levels under Common Criteria for information technologies security evaluation.

Action:

Address standardisation gaps within QTS, QTSP, RSS, QSCD, HSM and Conformity Assessment (CAB) by review and updating mentioned above standards with view alterations. Providing better resourcing to the National Standardization Body (NAAU), encouraging more of international peers reviews and audits of domestic CABs, possibly allowing EU CABs to take part on Conformity Assessment of Ukrainian QTSP (at least of those who are seeking international recognition of their trust services). Consider the introduction of Common Criteria Evaluation Assurance Level (EAL)[91] for the hardware equipment related to PKI infrastructure and Trust Services Provisions – matters for military applications.

5. Archiving of e-documents (long-term data preservation)

Explained:

Paper based document are likely to be obsolete in 10-15 years worldwide. Forward looking countries archiving system must be ready for such changes. Working on both: old body of paper based documents that should be transferred into e-formats and with new stream of e-documents that contains a new (possibly changing) technological concepts and increased throughput as well as capacities. Reconciling those two distinct workflows isn't easy and will require from the archives a dexterity, technological savvy, co-operation and extra resources to: a) keep the e-document and other formats of archived data- most obvious function that is required of archiving; b) access to the those data - means one can find the document and data on the storage media and open the files; c) preserve the intelligibility of the data and the documents - to ensure that the document retain integrity and is understandable to potential users through time. Later is the core of an archivist job that distinguish it from secure backup which only takes into account the a) and b) goals listed above and only in the short and medium terms. The EU member state countries are facing and solving similar problems as Ukraine is facing.

Action:

Reinforce drafted National Archive Strategy of Ukraine with the vision on e-documents long term preservation (LTP), studying and adopting the EU member states experience. Provide/ improve technical assistance and continuous education to the relevant archive staff in new e-documents and trusted services.

6. Accessibility of ICT systems of public services for persons with disabilities (including but not limited to Trust Services)

Explained:

No doubt this point is already understood in Ukraine. Lets just remind that the standards on accessibility requirements[92] applicable to ICT products and services too and such products in public use should meet the minimum requirements of web accessibility for example as set out in the European Web Accessibility Directive (Directive 2016/2102). It is understood that for now Ukraine has NOT have comparable with the EU standards and requirements in this area.

Action:

Adopt and start to implement standard EN 301 549 - Accessibility requirements for ICT products and services. Update legislative base to incorporate European Web Accessibility Directiv.

[91] https://www.commoncriteriaportal.org/ccra/index.cfm

[92] https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.01.01_60/en_301549v030101p.pdf -EN 301 549 -Accessibility requirements for ICT products and services

LONG TERM IMPACT

Desired long-term impact if suggested changes are implemented :

1. The Ukrainian Government, citizens, and business, actively participate in digital transformation projects (better Trust Services, better Digital Transformation, better EU alignment).
2. eID, e-signature and e-documents are gaining wide adaptation within the next five years and are becoming mainstream(90%+) by 2030 (better Trust Services, better Digital Transformation).
3. Lower risks and better chances of successful Digital Transformation when public services are becoming digital-by-design, data-driven, open to revisions and scrutiny, changes are user-driven. (better Trust Services, better Digital Transformation).
4. Conformity Assessment of Ukrainian QTSP and QSCD is performed in concordance with the international standards by domestic and other European CABs (better Trust Services + better EU alignment).
5. Mutual Recognition of Trust Services between the EU and Ukraine happens within 1-3 years; MRA rests on the solid background of legal technical and organisational interoperabilities, best practices implementation and sharing, transparent supervision and international audit concluded by solid mutually recognised trust representation. (better Trust Services + better EU alignment).
6. Ukraine is gaining the EU internal market regime in Trust Services, Tel-Com and e-commerce. It creates mutual economic benefits and adds up to 12%[93] of Ukrainian GDP (better Trust Services, better EU alignment).
7. Digital Transformation of the Government and Public Services works as a driver of Industry 4.0[94] and Society 5.0[95] concepts implementation. Digital Ecosystems in Ukraine is serving as the model and positive case for others to follow (better Trust Services, better Digital Transformation, better EU alignment).

[93] http://ucep.org.ua/wp-content/uploads/2021/02/dig_ukraine_eu_ENG-_2_WEB.pdf

[94] https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/568337/EPRS_BRI(2015)568337_EN.pdf

[95] https://www.jica.go.jp/activities/issues/ict/ku57pq00002ma0c1-att/Keidanren_JICA_Co-Creation_en.pdf

ANNEX 1

Statistical Data on e-signature issuance (source Ukrainian MoDT https://czo.gov.ua/development?tab=1)

Number of all generated electronic signature certificates (excluding encryption certificates) 2020

QTSP / Кваліфіковані Надавачі	Type of QTSP	Sector QTSP	E-signatures issued (AdES+ QESig) 2020	E-signature algorithm used		
				DSTU 4145	RSA	ECDSA
АТ "ПРИВАТБАНК"	State owned	banking	5,284,751	5,284,744	6	1
АТ "Українська залізниця"	State owned		29,677	29,669	7	1
АТ "УкрСиббанк"	State owned	banking	92,684	92,684	0	0
АЦСК Нацбанку	State owned	banking	1,279	1,279	0	0
Військова частина 2428	State owned		6,911	6,911	0	0
Генеральний штаб Збройних Сил України	State owned		8,394	8,296	97	1
Державна казначейська служба України	State owned		85,281	85,281	0	0
ДП "Оператор ринку"	State owned		248	248	0	0
ДП "Українські спеціальні системи"	State owned		285,805	285,805	0	0
ДП ДІЯ ("НАІС")	State owned		82,305	78,424	27	3,854
ЗЦ Нацбанку	State owned	banking	10	6	2	2
ІДД ДПС	State owned		534,089	534,089	0	0
Міністерство внутрішніх справ України	State owned		19,822	19,822	0	0
Офіс Генерального прокурора	State owned		28,930	28,928	1	1
ПАТ "Державний ощадний банк України"	State owned	banking	92,586	92,586	0	0
ПАТ "Національний депозитарій України"	State owned		0	0	0	0
ТОВ "Арт-мастер"(MasterKey)	Business		74,306	74,306	0	0
ТОВ "ДЕПОЗИТ САЙН"	Business		8,547	8,541	4	2
ТОВ "Інтер-Метл"	Business		28	28	0	0
ТОВ "КЛЮЧОВІ СИСТЕМИ"	Business			0	0	0
ТОВ "Центр сертифікації ключів "Україна"	Business		608,313	608,313	0	0
Total			**7,243,966**	**7,239,960**	**144**	**3,862**
including physical persons			5,832,267	5,829,296	15	2,956
including physical persons representitives of legal entities			1,339,259	1,338,236	121	902

Number of generated qualified electronic signature certificates (for the relevant period, excluding encryption certificates) with QSCD -2020

QTSP / Кваліфіковані Надавачі	—	—	QESig 2020	E-signature algorithm used		
	—	—		DSTU4145	RSA	ECDSA
АТ "ПРИВАТБАНК"	—	—	412,253	412,253	0	0
АТ "Українська залізниця"	—	—	521	521	0	0
АТ "УкрСиббанк"	—	—	72,852	72,852	0	0
АЦСК Нацбанку	—	—	756	756	0	0
Військова частина 2428	—	—	1,601	1,601	0	0
Генеральний штаб Збройних Сил України	—	—	1,423	1,423	0	0
Державна казначейська служба України	—	—	85,281	85,281	0	0
ДП "Оператор ринку"	—	—	38	38	0	0
ДП "Українські спеціальні системи"	—	—	369	369	0	0
ДП ДІЯ ("НАІС")	—	—	32,194	28,340	8	3,846
ЗЦ Нацбанку	—	—	10	6	2	2
ІДД ДПС	—	—	37,155	37,155	0	0
Міністерство внутрішніх справ України	—	—	19,817	19,817	0	0
Офіс Генерального прокурора	—	—	48	46	1	1
ПАТ "Державний ощадний банк України"	—	—	92,586	92,586	0	0
ПАТ "Національний депозитарій України"	—	—	0	0	0	0
ТОВ "Арт-мастер"(MasterKey)	—	—	3,245	3,245	0	0
ТОВ "ДЕПОЗИТ САЙН"	—	—	7,679	7,679	0	0
ТОВ "КЛЮЧОВІ СИСТЕМИ"	—	—	0	0	0	0
ТОВ "Центр сертифікації ключів "Україна"	—	—	54,936	54,936	0	0
Total	—	—	**822,764**	**818,904**	**11**	**3,849**
including physical persons	—	—	570,431	567,474	6	2,951
including physical persons representitives of legal entities	—	—	228,543	227,646	2	895
including physical persons representitives of legal entities	—	—	1,339,259	1,338,236	121	902

RESEARCH

ON THE WAY TO THE EU DIGITAL SINGLE MARKET

1/3

Інна Таптунова
Маріанна Казацька

НА ШЛЯХУ ДО ЄДИНОГО ЦИФРОВОГО РИНКУ ЄС: ЕЛЕКТРОННА КОМЕРЦІЯ

#дослідження www.ucep.org.ua

2/3

Лілія Мальон

НА ШЛЯХУ ДО ЄДИНОГО ЦИФРОВОГО РИНКУ ЄС: ТЕЛЕКОМУНІКАЦІЇ

#дослідження www.ucep.org.ua

3/3

Андрій Дресвянніков

НА ШЛЯХУ ДО ЄДИНОГО ЦИФРОВОГО РИНКУ ЄС: ДОВІРЧІ ПОСЛУГИ

#дослідження www.ucep.org.ua

E-commerce

Telecommunications

Trust services

The Ukrainian Center for European Policy (UCEP) is an independent analytical center for policy analysis and development, established in 2015.

Our mission is to promote reforms in Ukraine for sustainable economic growth and the building of an open society in partnership with institutions at all levels.

Priority areas of activity:

- preparation and dissemination of expert-analytical materials to promote European integration reforms in Ukraine;
- popularization of European values in Ukrainian society;
- informing the public about the opportunities and benefits of close cooperation with the EU;
- promoting enhanced economic, political and trade cooperation between Ukraine and the European Union;
- informing the international community about the challenges and achievements in the implementation of Ukraine’s reforms under the Association Agreement between Ukraine and the EU.

01001, Kyiv, Ukraine
9B Glushkova Avenue,
office 294

www.ucep.org.ua
press@ucep.org.ua
facebook.com/UCEP.org.ua

Kyiv, 2021

MOVING FORWARD TOGETHER
THIS PROJECT IS FUNDED BY THE EUROPEAN UNION

INTERNATIONAL
RENAISSANCE
FOUNDATION

UKRAINIAN CENTRE
FOR EUROPEAN
POLICY