DIGINNO CROSS-BORDER KYC UTILITY FEASIBILITY STUDY

September, 2019

Table of Content

Introduction

This document has been prepared jointly by the DIGINNO KYC showcase workgroup members[1] in Latvia, leaded by the Ministry of Environmental Protection and regional Development of the Republic of Latvia and in Estonia, leaded by the Ministry of Economic Affairs and Communication of the Republic of Estonia.

Information presented hereinafter is based on the DIGINNO KYC showcase workgroup members professional knowledge and experience, their presentations on thematic workshops, articles written by them and studies of the KYC subjects made by them.

Following documents gives overview about different aspects in a matter called Know Your Customer (or KYC), as well possible future vision of cross-border cooperation and data exchange in the subject of KYC, and more specifically about cross-border e-service example model called cross-border KYC utility.

DIGINNO (Digital Innovation Network) is a project funded by INTERREG Baltic Sea Region 2014-2020, the overall aim of which is to accelerate the movement of the Baltic Sea region towards a functioning digital single market. The DIGINNO project focuses on expanding the opportunities of the ICT sector in other sectors of the economy, cross-border innovation in public services, and organizing cooperation among policy makers involved in digitalization related issues. One of the focuses of the DIGINNO project is the digitization of cross-border e-services in the G2B direction. The goal is to increase the volume of cross-border e-services and also to raise awareness of G2B cross-border e-services among public authorities, businesses and organizations. Also it aims to promote transnational cooperation by building a digital network of G2B cross-border e-services and developing example models.

What is KYC

Know your customer, or simply KYC, is the process for oblidged legal entities to perform customer due diligence including verification of identity, beneficial owners, purpose and nature of business relationship and risk factors that warrant enhanced customer due diligence (politically exposed person (PEP), family member of PEP, person closely associated to PEP, business relationship with a customer from a High-risk Third Country, Shell Arrangements, etc.). The term is mostly used to refer to the bank regulations and anti-money laundering regulations which govern these activities. Know your customer processes are also used by non-oblidged entities in voluntary basis by the companies to reduce AML risk of their operations.

Terrorists and criminals have demonstrated their ability to transfer funds quickly between different banks, often in different countries, but lack of timely access to financial information means that many investigations come to a dead end. There is therefore a clear need to enhance cooperation between authorities responsible for combating terrorism and serious crime when financial information is a key part of an investigation.

According to anti-money laundering (AML) and contra-fighting with terrorism (CFT) laws and regulations, the obliged entities (e.g. banks, financial institutions, insurers, virtual money and

[1] Please look the list of persons who contribute for preparing this document in Annex 5.

digital payments institutions, notaries, attorneys etc.) are demanded by legislation, which is in place in every modern country of the world, to fulfill detailed KYC process to know their customers and their business better and therefor their customers are demanded to provide detailed due diligence information.

Aim of KYC is to find, eliminate and fight against of money-laundering, corruption and direct or indirect financing of terrorism or obstruct and limit cooperation with countries or organizations which are under international sanctions.

Before establishing and while upkeeping a business relation, every obliged entity within the meaning of the laws on the prevention of money laundering and terrorism financing (AML/CFT laws) must perform customer identification and assessment, by additionally also conducting transaction monitoring. KYC comprises all these measures for the identification of the customer, its operations and cooperation partners.

The legal framework for KYC

KYC policies have evolved into an important tool to combat illegal transactions in the international finance field. KYC is daily used by obliged entities, most visible among them are financial service providers such as banks, development finance institutions, credit companies, and insurance agencies, to ensure compliance with the AML/CFT regulations requiring to ensure that their customers are wetted and provide them with detailed information in order to ensure that they are not involved with corruption, bribery, or money laundering. KYC allows companies to protect themselves by ensuring that they are doing business legally and with legitimate entities, and it also protects the individuals who might otherwise be harmed by financial crime.

KYC regulations are local and differ from government or country to country, being jurisdiction also on a country to country basis.

On 24 July 2019, the European Commission adopted a Communication to the European Parliament and the Council towards better implementation of the European Union's anti-money laundering and countering the financing of terrorism framework. This was accompanied by four reports2:

- Supranational risk assessment of the money laundering and terrorist financing risks affecting the Union. The annex, in form of a Staff Working Document under the Supranational risk assessment, is also available on this page under the section 'Risk Assessment'.
- Report assessing the framework for Financial Intelligence Units' (FIUs) cooperation with third countries and obstacles and opportunities to enhance cooperation between Financial Intelligence Units within the EU
- Report assessing the conditions and the technical specifications and procedures for ensuring secure and efficient interconnection of central bank account registers and data retrieval system
- Report assessing recent alleged money-laundering cases involving EU credit institutions

[2] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en

The European Union (EU) adopted the first anti-money laundering Directive in 1990 in order to prevent the misuse of the financial system for the purpose of money laundering. It provided that obliged entities shall apply customer due diligence requirements when entering into a business relationship (i.e. identify and verify the identity of clients, monitor transactions and report suspicious transactions). This legislation has been constantly revised in order to mitigate risks relating to money laundering and terrorist financing.

One of the pillars of the European Union's legislation to combat money laundering and terrorist financing is Directive (EU) 2015/849. According to this Directive, banks and other obliged entities are required to apply enhanced vigilance in business relationships and transactions involving high-risk third countries. The types of enhanced vigilance requirements are basically extra checks and control measures which are defined in article 18a of the Directive.

Currently European Union has already adopted the 5th money laundering directive (5AMLD) (EU) 2018/843[3] was adopted regarding the prevention of money laundering or the financing of terrorism, which is amending the 4th directive (EU) 2015/849 which already amends Directives 2009/138/EC and 2013/36/EU. It is a directive aimed at the financial sector and aims to establish the measures that will allow banks to protect themselves against these threats.

The 5th money laundering directive (5AMLD)[4]

- extends the scope to virtual currency platforms and wallet providers, tax related services and traders of art
- grants access to the general public to beneficial ownership information of EU based companies
- makes it an obligation to consult the beneficial ownership register when performing AML due diligence
- obliges member states to create a list of national public offices and functions that qualify as politically exposed (PEP)
- introduces strict enhanced due diligence measures for financial flows from high-risk third countries
- ends the anonymity of bank and savings accounts, as well as safe deposit boxes and creates central access mechanisms to bank account and safe deposit boxes holder information throughout the EU
- makes information on real estate holders centrally available to public authorities
- lowers thresholds for identifying purchasers of prepaid cards and for the use of e-money
- further enhances the powers of the FIUs (Financial Intelligence Unit) and facilitates cooperation and information exchange among authorities

The EU Directive (EU) 2019/1153 enhances the use of financial information by giving law-enforcement authorities direct access to information about the identity of bank-account holders contained in national centralized registries. In addition, it gives law enforcement the possibility to access certain information from national Financial Intelligence Units (FIUs), including data on financial transactions, and also improves the information exchange between FIUs as well as their access to law enforcement information necessary for the performance of their tasks. These

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843
[4] https://globalcompliancenews.com/eu-5th-anti-money-laundering-directive-published-20180716/

measures will speed up criminal investigations and enable authorities to combat cross-border crime more effectively.

Despite the EU directives countries have regulated the AML/CFT in national level, et[5]:

- Local AML/CFT legislation
- Regulations and guidelines issued by the local FSA (Financial Supervision Authority)
- Regulations and guidelines issued by the local FIU (Financial Intelligence Unit)

As well institutions and obliged entities are following the The Financial Action Task Force (FATF) guidelines in relevant extend.

The objectives of the FATF[6] are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF has developed a series of recommendations that are recognized as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. All the Nordic countries are members of FATF, but at the same time none of the Baltic countries are not members of the FATF, but all the Baltic countries are members of the organizations which are members of the FATF (for example Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL), which is a a permanent monitoring mechanism of the Council of Europe, a pan-European organization with 47 member states, reporting directly to its principal organ, the Committee of Ministers).

What is also important to know, that AML/CFT regulations stand above the General Data Protection Regulations (GDPRS) of the European Union and therefor for a obligated persons to conduct KYC the GDPRS does not apply. Still, in a case of voluntary KYC, the rules and provision set by the GDPRS must be followed.

KYC as it is

In all the EU members Baltic countries (Estonia, Latvia, Lithuania) and Nordic countries (Finland, Sweden, Denmark), just like in the rest of the world, the obliged entities[7] are required to apply the principle "Know your customer". The purpose of this principle is to ensure a secure environment and prevent any potential money laundering and terrorist financing risks.

Although the AML/CFT regulatory framework country by country differs, in large scale the AML/CFT legislation and principles are rather similar.

And at the same time, although the legislation has been in place, during recent years all Baltic and Nordic countries have been suffering with several world-shaking money-laundering scandals (i.e. Ukio Bankas, ABLV Banks, Danskebank, Swedbank, Nordea). As a result many countries are amending their AML/CFT legislation to increase efficiency and effectiveness of AML processes.

[5] Please look for more precise Baltic countries based information in the „KYC as-is" description document (Annex 2)
[6] https://www.fatf-gafi.org/about/whoweare/
[7] For detailed list of the "obliged entities" or "obligated person" within Baltic countries please look for more country based information in the „KYC as-is" description document (Annex 2)

However, countries have taken different approach to fight with money laundering issues. While Estonia took the path for extreme raising the penalties for obligated entities who will not follow the KYC procedures and has tighten the rules for financial institutions, the Latvia at the same time named KYC as a state priority to dealt with, and has passed series of reforms to modernize the current ineffective approach to KYC customer due diligence processes. Nordic countries private sector (banks) have been take an initiative to build up their Nordic shared KYC utility.

On September 25, 2018, the Cabinet of Ministers of Latvia has approved a plan on AML/CFT activities for implementation by the end of 2019. Ultimate goal – zero tolerance to financial crime. By the current vision of Latvian politicians, the shared KYC Utility might be one of the solutions to improve information sharing and deliver on prevention of financial crime.

Still, at this particular moment the KYC is applied rather similarly, in all the Baltic and Nordic countries. If to compare the Money Laundering and Terrorist Financing Prevention Acts of the Baltic and Nordic countries, the obliged entities, in order to apply the KYC principles in practice, are required to obtain information about their customers and origin of the funds. Laws in detail regulate what information is needed (must to) obtain and what circumstances needed to be checked and verified by obtaining relevant proofs.

For example, in all the Baltic countries, very similar to Nordic countries, the banks are requesting their customers to submit to banks the information and documents necessary for carrying out customer due diligence measures (KYC), including information about the true beneficiaries thereof, about transactions carried out by customers, the business and individual activities of the customers and the true beneficiaries thereof, as well as about their financial position and the origin of cash or other assets. In some cases, banks may also request other additional information. What is at the same time surprising, a lot of information asked from the customers already exist in the state institutions (state/governmental) databases, but access to such information for the KYC purpose in not granted. Therefore relevant information shall be collected again and again and mostly hand-processed by obliged entities.

Taking into account that there are 40 000 - 70 000[8] obliged entities within Baltic countries, and many times more in the Nordic countries, conducting KYC is increasingly time and money consuming process for obliged entities. There are several KYC info-technology tools existing, which provide some analytics and some from the needful data, but mainly are aimed for identifying the client (e.g. Veriff, ID.credit, SISUID, KYC.pass etc). Most of the information needed to conduct KYC is still gathered in paper, then scanned and archived (i.e copies of ID documents, utility bills etc). Even the registry cards of legal entities, which are public accessible via online means of communication, are printed out in paper and then archived by obliged entities.

For example, onboarding a new client to a bank, who is a private person and a resident, could take just 4 minutes, while with non-resident minimum as 40 minutes to several weeks[9] shall be spend. Currently it is very hard and time consuming an impossible for a non-resident to open bank account in any of the banks within Baltic States. Even for a resident legal entity, who has non-resident as a member of the board or non-resident as a beneficial owner, has severe difficulties to open or to maintain open its banking account in the banks within Estonia.

[8] The number may vary since legal person can turn into obliged entity in one situation and loose that obligation in other.

[9] Based on the survey information received from the bank in Estonia.

Additional to information already available in the databases of the state/governmental institutions, there will always remain information what obliged entities, based on their specific needs and tasks, will and shall be asking and need to ask from their customers. And even thought, if the state/governmental databases will be made available for use in a purpose for conducting KYC procedure, still such information is usable intra country and not cross-border, because of the absence of such international and intro- and intra-EU regulations. And not only the legislative provision or bi- or multilateral agreements are needed to make cross-border exchange of such information to become real, but also the information itself needs to be standardized. Currently the quality of information and content of it varies not only in between different countries but also within a country, as well the information is stored by using different data exchange standards (i.e XML, UBL, JASON etc.) which complicates the usage of data from different sources simultaneously.

Today the most of information needed for KYC is collected using questionnaires. For example, for banks such questionnaires form an integral part of the information (including contact information) provided by the customer. It is therefore necessary to update the data in the questionnaire whenever any major changes occur, such as the change in the country of residence or in the status of a politically exposed person.

In accordance with the above mentioned AML/CFT laws and regulations, for example the banks must keep and regularly update the documents, data and information obtained in the course of the customer's due diligence. The failure to complete the questionnaire may therefore lead for a client to limited availability of online banking services until the relevant data is updated. Taking into account the requirements of the laws and regulations to identify the customers and obtain the information and documents necessary for the customer's due diligence, the bank will regularly remind its customers about the need to update the questionnaire, i.e., the relevant notification will appear in the internet bank at specified times. If a customer does not wish or refuses to provide the requested information and documents to enable carrying out the customer's due diligence in substance, the bank has the right to terminate the business relationship with the customer. as well to require early performance of the customer's obligations. Therefore, to continue the business relationship successfully, timely submitting of the required information and documents is key for the client. Still, taking account the long questionnaires and time needed to check, amend and re-enter data to the questionnaires, has raised customer dissatisfaction in all Baltic countries. But banks also have their hands tied, since inability to properly conduct KYC may and will lead to harsh penalties, even up to the bank's moratorium, levied by the supervision authorities (e.g. FIU, FSA, National Banks).

Cross border remote Know-Your-Customer processes with eIDAS application

eIDAS (electronic Identification, Authentication and trust Services) is an EU regulation on, a set of standards, for electronic identification and trust services for electronic transactions in the European Single Market. It regulates electronic signatures, electronic transactions, involved bodies, and their embedding processes to provide a safe way for users to conduct business online like electronic funds transfer or transactions with public services. It was

established in EU Regulation 910/2014[10] of 23 July 2014 on electronic identification and repeals directive 1999/93/EC from 13 December 1999.

It entered into force on 17 September 2014 and applies from 1 July 2016 except for certain articles, which are listed in its Article 52 All organizations delivering public digital services in an EU member state must recognize electronic identification from all EU member states from September 29, 2018.

eIDAS has created standards for which electronic signatures, qualified digital certificates, electronic seals, timestamps, and other proof for authentication mechanisms enable electronic transactions, with the same legal standing as transactions that are performed on paper.

In a sense for KYC, it to allows in practice the remote identification of customers for example by financial service providers, digital payment providers etc. across the member states for the purpose of digital on-boarding, i.e. opening a bank account, to provide easy to use service for small and medium size enterprises (SME) working cross borders, especially in the area of financial technology (Fintech), to identify and verify business partners.

The DIGINNO KYC showcase responds the need to facilitate the uptake of digital tools to identify customers remotely across entire World. KYC portability will be based on capabilities enabled by identification and authentication tools under eIDAS and enable financial institutions to identify customers digitally for onboarding purposes.

- The technology behind the set up: EU Building Blocks, primarily, eIDAS, covering electronic identification and authentication. The G2B component: institutions have to provide information/data about customers/clients. Legislation have to be in place in order to allow KYC information portability. The automatized information exchange among national authorities and financial services providers, including carrying out the once only principle and to possible extent using common technical solutions will reduce barriers to information-sharing among financial market participants.
- Public service provision: facilitating once only principle in the data exchange among national authorities and financial services providers, where taking reliable data based decisions, ensuring protection of personal data, if applicable ensuring the permit for the transfer of the personal data.
- Effective and trusted functions provision: use of the state/government information systems integrator (aggregator) for the data exchange purpose among state/government information systems and services providers.

Currently all Baltic and Nordic countries have state guaranteed electronic ID (and ID cards) and electronical signature solutions, in some countries also mobile ID is available. For example in Estonia is mandatory for every citizen and resident to have electronic ID card with electronic signature, but it is not mandator to have a passport. Also from private sector has been developed national wide eID solution (i.e SMART-id). But we should not forget, that according to the World Bank, there are at least 1,6bn people, who are unable to prove their identity.

Although eIDAS is implemented and in use in all of the Baltic and Nordic countries, the Latvia has been taking currently step further.

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

At the end of 2018 year Ministry of Environmental Protection and regional Development of the Republic of Latvia submitted to the Cabinet of Ministers of Latvia the Conceptual Report that determines mandatory use of the State information systems' integrator (Law On State Information Systems, Article 17), thereby decreasing the number of agreements on data exchange and number of data exchange channels and in long term make one information exchange point for all public institutions. To formulate the tasks of the Cabinet of Ministers concerned to the mentioned draft Conceptual Report as well the coordination of the recently initiated draft State ICT Governance Law[11] in the Saeima, the involvement of the Finance Latvia Association may be required. One exchange point is better in context in interoperability between different formats and protocols, capacity sharing. The report includes the establishment of a principle - ensuring the circulation of centralized information through the use of the National Information Systems intermediary. This principle will ensure that each institution will have all the information necessary for its work, created and maintained by the public administration authorities, electronically. This will actually put into practice the principle that public authorities obtain information from the resident or company rather than from the authority holding the information resource in question.

The Ministry of Finance of the Republic of Latvia assumes that the access to public registries should be open not only to the credit institutions and insurance companies (as currently stipulated in Article 41 of the Law) but to all subjects of the law (as in Article 5.1).

Finance Latvia Association has indicated the multiple aspects of the data exchange. First point is the volume of data, costs and method of the calculation (scans, hits, channel fees etc). Second point is the data exchange technological solution, where prevails the development of the information systems integrator. By certification as Qualified or Qualified Increased Security Electronic Identification Service Provider for example banks obtain the access to their services in an EU scale. EU Self Sovereign blockchain based Identity Framework Concept. Distributed Ledger Technology makes possible to conceive a Digital Identity system where identity of an entity is managed autonomously by itself, in a system where it is possible to manage a root-of-trust without a central authority or a single point-of-failure. The proposal is to create an European-wide public blockchain infrastructure hosting legally binding digital identities for the public sector. Existing electronic signatures should made interoperable with the self-sovereign identity model by using DIDs. The identity infrastructure to be developed is best understood as a decentralized register infrastructure operated jointly by all 28 member states of the European Union.

Global solutions for KYC utility

At international scale there is a regional and overall urgency for setting up a high quality shared or cross-border KYC utility. Multiple recent developments speak for that: five largest North European banks are currently developing a joint KYC tool; HSBC bank recently agreed to sell its compliance system that is intended for customer due diligence as this solution covers cooperative and also institutional clients and to offer it as a service that is accessible also by other financial institutions.

11 http://titania.saeima.lv/LIVS12/saeimalivs12.nsf/0/DF88BF91A58612C2C2258226002B3762?OpenDocument

The already existing cross-border KYC utilities operate as full-service providers and comprise check-ups and entry monitoring or operate without setting up or attraction of any tools for information sharing among stakeholders, however this approach is associated with a high level of information duplication.

Different forms of the KYC utility platforms operate globally for around 5 years.

There are several KYC utilities operating models, entailing different advantages and drawbacks:

- Public model – the KYC utility that is maintained and belonging to the state, involving the necessity to address the issue as to how it will be administered and what does it mean in terms of liability
- Public-private model –belongs jointly to the state and private entities. Thus, it is necessary to determine the form of operation of this model in terms of contributions and potential profit sharing, possibly it should be set up as a non-profit entity
- Private model – the utility would either belong to one financial institution or a special-purpose vehicle (SPV) which would administer the platform and offer it as a service. In case the platform would be owned by a single financial institution it would be impossible to use it on a wider scope and ensure complete independence

In Singapore it has been recognized that the setting up of a separate entity would be the most appropriate solution.[12]

In all, the most suitable form of operation would be a public - private partnership (PPP) as it would neither belongs to any industry or the state and would therewith ensure independence and higher level of safety as the utility would be overseen at national level (functional supervision, a licensable subject).

To set up a PPP model, the state should initially invite stakeholders to join in and test the utility.[13] However, it should be recognized that at a global scale more widespread are models which do not involve the state, namely financial institutions agree on the establishment of a joint venture for collecting their KYC information, therewith facilitating customer check-ups.

The leading Nordic banks DNB Bank, Danske Bank, Nordea Bank, Svenska Handelsbanken, and Skandinaviska Enskilda Banken (SEB*)* have announced their plans to set up a KYC utility as a joint venture. The joint venture will be owned and controlled by the founding banks, with a focus on developing an efficient, common, secure and cost-effective utility for sharing confidential customer credentials. After commencing its operations Nordic KYC utility plans to service large and midsize Nordic corporates.[14] As per the accessible information, it may be concluded that the solution does not foresee that the state will feed into the utility the information at its disposal. This KYC utility will be active in the Nordic region offering KYC services consisting in gathering, validating, and providing to customers the information required under the applicable AML/CFT regulations, to facilitate compliance with these regulations.[15]

---

[12]: https://abs.org.sg/docs/library/kyc-aar_15-nov-2018.pdf

[13] https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-services/deloitte-uk-thecityuk-splitting-the-bill-the-role-for-shared-utility s-in-financial-services-regulation.pdf

[14]: https://www.finextra.com/newsarticle/32178/nordic-banks-explore-shared-kyc-utility?utm_medium=dailynewsletter&utm_source=2018-6-1&member=63850

[15] http://europa.eu/rapid/press-release_MEX-19-3011_en.htm

The South African shared KYC service is a result of a partnership amongst the largest financial institutions of South Africa and Refinitiv (former name - Thomson Reuters). The South African shared KYC service makes collection and distribution of information easier. Large corporations, hedge funds, asset managers, and others use the South African shared KYC service as an efficient, centralised solution for sharing KYC documents and information among several financial institutions through a secure and free-of-charge web-based portal. The main reason for the efficiency of the South African KYC service is a KYC information collection policy that has been standardised across all participating financial institutions.[16]

In 2014 the South African Reserve Bank fined the country's four largest banks a collective fine of 8 million EUR for failing to implement adequate anti-money laundering controls and risk measures. 2016 marked the launch of a KYC utility partnered with Thomson Reuters (current name – Refinitiv) to efficiently combat AML/CFT risks and to reduce the costs of customer assessment.[17] Also in case of South Africa, the state does not supplement the KYC system with information at its disposal.

It must be noted that the African Afrexim bank has set up its own KYC tool – MANSA. MANSA was intended to serve the purpose of a repository that would cooperate with the leading African banks and regulatory authorities to ensure the most comprehensive KYC tool in Africa. Information about MANSA emerged only in July 2018 and no detailed information on its performance in reaching the set goals is available so far.[18]

In 2017 the Monetary Authority of Singapore (MAS) announced that it is piloting a national shared know-your-customer (KYC) utility for financial services, based on the MyInfo digital identity service, developed by the Ministry of Finance.[19] Singapore intended the KYC utility to enhance customer on-boarding and verification through the MyInfo system.[20] It was planned to put the KYC utility in place by the end on 2018, however due to the costs and also because of insufficient activity of financial institutions in feeding information into the system as it is a complicated process and requires significant investments, the implementation of the KYC utility has hit a snag and the date of launching and putting the utility in operation remains unclear. The managing director of the Monetary Authority of Singapore Ravi Menon notes that, greater complications arose from streamlining KYC processes for corporates than individuals. Financial institutions would among other things, have to figure out the beneficial owners of entities such as shell companies, which creates complications in establishing credentials.[21] Later was added by him, that project has been put to shelve because due the high cost of SME innovation platform.[22] In case of Singapore, the assignment of setting up the utility was taken by the state, provided that private financial institutions will furnish information.

In terms of information accessible, the Singaporean model, although not operational yet, should be considered the most rational one, although it must be noted that the planed cooperation

[16] https://africa.thomsonreuters.com/en/products-services/risk-management-solutions/kyc-as-a-service.html
[17]: https://blogs.thomsonreuters.com/answerson/south-africa-leads-way-know-customer-kyc-compliance/
[18] https://ej.uz/e4p1
[19] https://www.finextra.com/newsarticle/30332/mas-to-roll-out-national-kyc-utility-for-singapore
[20] https://www.opengovasia.com/mas-working-closely-with-local-and-foreign-banks-to-explore-a-banking-kyc-shared-services-utility/
[21]: https://www.businesstimes.com.sg/government-economy/singapores-know-your-customer-utility-experiment-hits-snag-mas
[22] https://www.straitstimes.com/business/banking/mas-to-shelve-know-your-customer-utility-project-due-to-unexpected-high-costs-ravi

model (single customer profile accessible on a common platform by several obliged entities) is an expensive and ambitious solution and from this perspective it should not be used as the best example. If the existing South African and the planned North European models foresee that financial institutions share information at their disposal, the Singaporean utility would receive customer information at the disposal of financial institutions and state registers what could reduce one of the major problems faced by KYC utilities, namely, information credibility. The information that is found in state registers has a higher degree of credibility than that at the disposal of financial institutions.

Thus, there is room for the conclusion that globally there are different shared KYC utility models – North European banks are looking forward to set up a private utility, the South African utility is private, though partnered with the international media and information company Refinitiv, the Singaporean utility is set up by the state in partnership with financial institutions.

The idea behind the shared KYC utility is to serve as a tool assisting financial institutions in performing customer assessment and for curtailing and preventing AML/CFT risks. However, the liability for customer due diligence would still lie with the financial institution. It is expected to streamline the shared KYC utility in the future allowing a liability shift, i.e. the shared KYC utility would be improved and contain sufficient information to undergo customer assessment and financial institutions will no longer have to perform assessment and assume liability as it would be taken over by the shared KYC utility. This is the ultimate (supreme) and potential future objective of the utility.

KYC as a cross-border utility

Resource sharing and widespread usage of innovation in combating financial crime has become the spotlight of today's world. Special attention is drawn to the continuous improvement of customer due diligence and development of platforms for information sharing. The goal is clear and unequivocal: strengthen the ability to reduce the risks associated with money laundering and terrorism financing (AML/CTF).

Bases on a discussion within DIGINNO KYC showcase national workgroups[23] and reached common understanding, that cross-border KYC will be possible[24] only, if there has been harmonized a minimum list of questions, documents and collectable data that are needed to conclude KYC (i.e. shall be listed which data will be collected from business register, population register, PEP register, beneficial owners register, state revenue register, land book, vehicle register, criminal records database, document register, credit bureaus data etc.). Currently in national level differs the understanding what shall be collected and what is needed to collect. As well often are collected information that really is not needed or relevant to collect, having no real value for KYC (e.g. collected for just in case purpose). There are currently two solutions, either some of the countries will take an initiative and will draft the standard set of questions and then will agree about them at first bi-laterally with other country, which makes possible to have 1st over the border flow of KYC comparable, or alternative solution, that countries together will establish joint workgroup which will start the process of harmonization. Most probably it would take many years to achieve the result with the latter solution.

[23] Please look at Annex 1 „DIGINNO KYC showcase Workgroups activities "
[24] Please loot at Annex 3 „Baltic KYC to-be vision"

Also have been reached to common understanding, that it is essential to agreed normative, substantive, and best practice for data transmission framework (i.e. possible data exchange standards XML, XBRL, JSON or other) under which the future KYC service providers can create their services.

Above mention could be taken as a pre-condition to make at all possible to use and re-use the data cross-border. But at the same time there is an inevitable need to adopt cross-border (or transnational) acts/regulations to guarantee cross-border usage/applicability of such services. Other states shall accept the KYC data that is recognized by the first state. As well state confirmation of the data it has/owns is needed (i.e. state symbolically confirms accuracy of data which is taken from national registers).

The core of the cross-border KYC is an ability to create a KYC profile, which consists of both automatically collected (query-based) and self-contained data (e.g. documents that cannot be obtained from national databases based on inquiries). Profile can be created by person itself or by obliged entities and/or licensed entities (e.g. credit institutions, audit firms, credit bureau, service provider etc.). This Profile (i.e AML passport), which has already created, is interoperable in all cases where obliged entities want or need to carry out KYC. Profile shall be created on once-only principle and updated (incl. automatic updates) every time the profile is used again. On the basis of existing and entered data, visual display is created of inter-dependency links between the person(s) and the company(s).

For storing the profile and collecting and distributing the data, there is a need to licenses the KYC service providers (e.g. credit institutions, audit firms, credit bureau, service provider etc.). Licensing shall grant, that these service providers have in place all measures to secure and maintain the data and the risk of data leaking or manipulations with such data at the service provider, are totally eliminated.

As shown above, the workgroups have mainly found, that as soon as there is in place the harmonization, standardization and licensing, the market itself will further develop the service. There is no need for a state to build or develop such cross-border KYC utility, but just to enable it existence. There are currently in the market dozens and dozens KYC service providers and there are thousands and thousands obliged entities who are obliged to conduct KYC and are in a need for proper cross-border KYC service. Since there is a strong demand for such a service from obliged entities side, there will be also offer from possible service providers side.

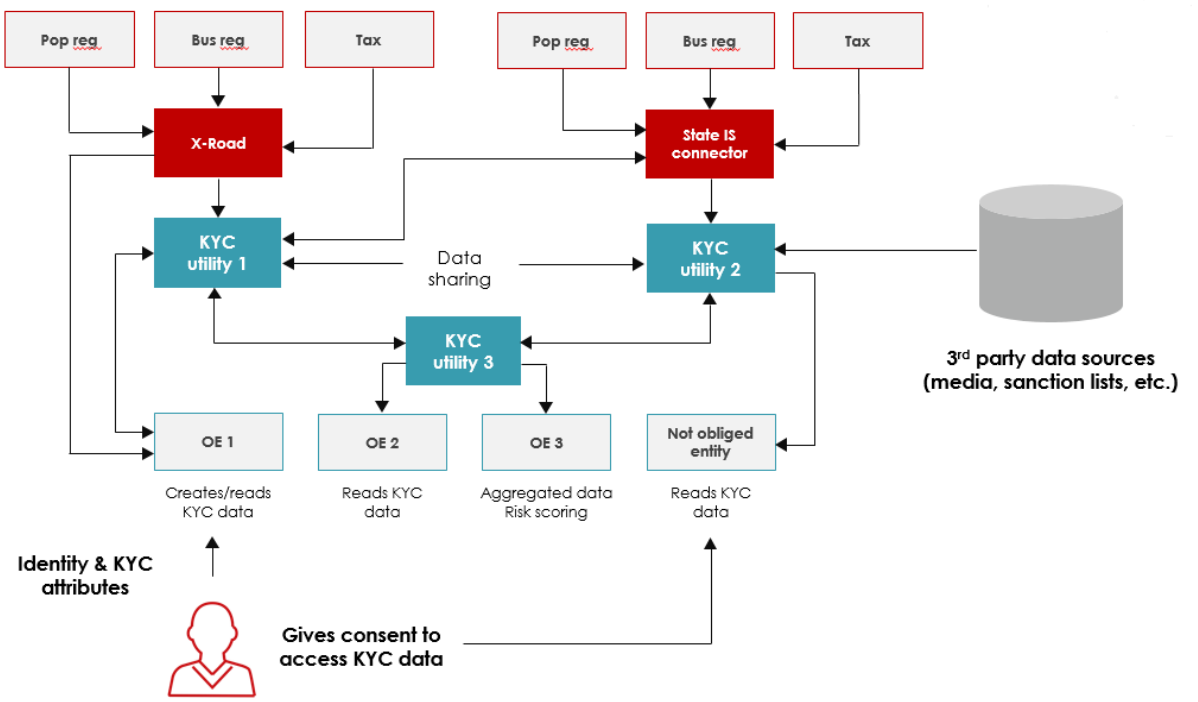
Taking into account the legal complexity of such cross-border utility, the state itself must be the owner of the process of cross-border KYC (i.e. different ministries in different countries which have core interest in the AML/CFT area): Ministry of Finance, Ministry of Internal Affairs, FIU etc. But such cross-border services will be provided (built) by private sector (licensed) under standards and regulations made by public sector (state).

As an example - the cross-border KYC for Latvian resident, who desires to open the banking account in Finland, shall work as following:

- He logs in into local (Latvian) KYC utility or goes to the bank office in Estonia and the bank opens the KYC profile in the local (Finnish) KYC utility
- Client/bank selects the KYC package suitable for such transaction

- The KYC utility collects in accordance to the package the available and needful data from public registers (directly or via other KYC utility tools in other countries) and will reply also which data is missing or where are mismatches
- The bank informs the client which additional data (documents) is needed
- The bank opens the banking account at the spot if all relevant information is received

Scheme 1. Main working principle of cross-border KYC utility



Benefits from the cross-border KYC utility

Cross-border KYC utility will allow easier and cheaper identification of AML/CFT risks, considering that in case there one obliged entity has performed assessment and identified high AML/CFT risk for a certain customer and its transactions, the obliged entity will feed the given data into the KYC utility and together with the query based collected data from state/government registers shall be visible to other obliged entities, who will have the chance to make use of these data for their operations based on their data access needs (obliged entities will see only data what is assigned them in accordance to the standard i.e. banks will see much wider range of data than notaries etc). The data collected is machine-readable and usable for risk-assessments modules/analyses. The obliged entities will not have to start the assessment again and again from zero, therewith bringing to a half the use of proceeds from crime considerably faster.

Everybody benefits from such cross-border KYC utility, citizens because they are living in country with less AML/CFT risks, society by lower AML/CFT risk, the business is more transparent and gray economy is lower, leading to higher GDP and government by having lower risk level for the state and better state reputation. Such utility will reduce the resource for collecting and analyzing data and for transmitting data (time and money), allows automated data management and analysis (e.g. XBLR) which leads to a better and more accurate risk

prevention/detection and fights against grey economy. Beside ANF/CFT regulations obligatory KYC conducted by the obliged entities (i.e. banks, financial institutions, notaries, attorney offices/attorneys, auditors, debt collection companies, accountant companies etc), the same service could be also used in voluntary bases between business partners.

Institutional benefits from cross-border KYC utility:

- Consolidates information from multiple local, foreign, global sources
- Increase efficiency and quality of AML/CFT compliance for obliged entities who use cross-border KYC utility
- Decrease AML/CFT risks on the country and regional level
- Allows machine to machine data analyze for better risk prevention and detection
- Monitors online (push notifications) of changes in customer KYC profile
- Distributes customers KYC data changes to all obliged entities who use cross-border KYC utility
- Makes KYC process faster and therefor cheaper, allowing to use artificial intelligence possibilities

Customer personal benefits from cross-border KYC utility:

- One button solution to create his/her KYC profile
- One source for updating and sharing his/her KYC data and give or restrict access to his/her data
- One source for updating and sharing KYC data within all obliged entities
- No need to fill again and again the KYC checklists and gather additional documents

Practical solutions for DIGINNO cross-border KYC utility

In order to be able to complete this task more effectively, information technology tools are developed, which import data from several sources into a single platform, both publicly available and unavailable, both publicly maintained, private and customer.

The cross-border KYC utility can work exclusively with customer transactions within a single legal entity or group of commercial companies, as well as as a data aggregation that provides data exchange and comparison without their accrual. However, only an individual solution at the level of one subject of the law, although it may exist, does not make the most significant contribution to society as a whole. Both models, whether centralized data storage or decentralised data processing tools, are possible, assessing the solution of the specific developer, regulatory requirements and personal data protection rules. Both of these models can be combined. For example, in credit information offices, some information is in a single database, but some information is obtained only for immediate delivery and/or rating.

Regardless of the operating model of the data-processing tool, it is clear that this will require the establishment of secure data exchange channels, a machine-readable data structure, as well as the establishment of uniform technical standards in both the national and private sectors (including the API). It would therefore be advisable to introduce a single channel (aggregating) for the transmission of national register data.

Currently, each country and financial institution chooses solutions that are most convenient for itself, resulting in multiple individual solutions. However, in order to achieve the highest standards of compliance, it is essential that each country, in collaboration with its financial

sector and the largest actors of the real economy, decides on the single best way for the development of the shared KYC utility. Such cooperation would bring remarkable benefits since a country which achieves and maintains the highest standards of compliance improves its reputation and credibility in the international setting, reduces the overall administrative burden, and decreases the costs of business partner and customer due diligence. Still, because of the open market and freedom of flow of assets and people, its is common that resident of one country has a business in other or has because of globalization, place of domicile in several countries. The shared KYC will soon limit its possibility of usage (limited only with the residents), if cross-border data collection, exchange and usage, is not made possible.

Continuing its endeavor of ensuring compliance with the best World practice in the field of compliance in Latvia, the Finance Latvia Association has prepared a report on options for introducing a Shared KYC Utility in Latvia[25]. Finance Latvia Association being an active member of Latvian DIGINNO KYC showcase national workgroup and attending the Estonian-Latvian workgroups and joint events, has already in their Shared KYC Utility proposal taken account the DIGINNO KYC to-be vision aspects, and therefore Shared KYC Utility model could be taken as possible example model for DIGINNO cross-border KYC utility .

Key options of KYC utilities as described in the Finance Latvia report are:

- An obliged entities can outsource KYC services, inter alia by creating a joint venture for all or a particular part of the due diligence process; such model is currently envisaged by the European Commission in the recently approved Nordic KYC utility project;
- the shared KYC Utility that works similarly as credit information bureaus; allowing obliged entities to exchange information for the purpose of AML/CFT risk management in a standardized way;
- an individual stores his/her identification data and relevant (necessary to carry out a KYC analysis) data from public registries (including tax payments) in a specified way, and is able to transfer that data to a merchant or an obliged entity without having to fill out detailed questionnaires each time on the data that is at the disposal of the state; the model is currently being discussed in the Baltics within the framework of a project financed by the European Commission (DIGINNO). (Such model is currently applied in Singapore)

Share KYC utility or cross-border KYC utility is not intended as a "supersystem" that would cover all KYC processes, redistribute responsibility or create a valid solution/model for all. The legal entities may create their own KYC solutions or outsource KYC processes (service providers for parts of KYC process already exist in the market). Such a model could be described as a private KYC utility.

The shared or cross-border KYC utility, or part of it, can be formed as a channel through which to obtain information from public registers (usually at the customer's request). Such KYC utility model would require access to public registers and would be appropriate for individuals to identify and obtain basic information.

The shared or cross-border KYC utility would be primarily intended for a number of unrelated legal entities to share the information obtained during the exploration of significant customers. Such shared or cross-border KYC utility offer its customers information as a service. For

[25] https://www.financelatvia.eu/wp-content/uploads/2019/07/KYC-utility-report-June-2019.pdf

example, give access to a substantial part of the KYC questionnaire, provide information on whether a person is not included in any list (e.g. sanctions list), indicate whether the person is politically exposed person (PEP)_requiring additional due diligence .

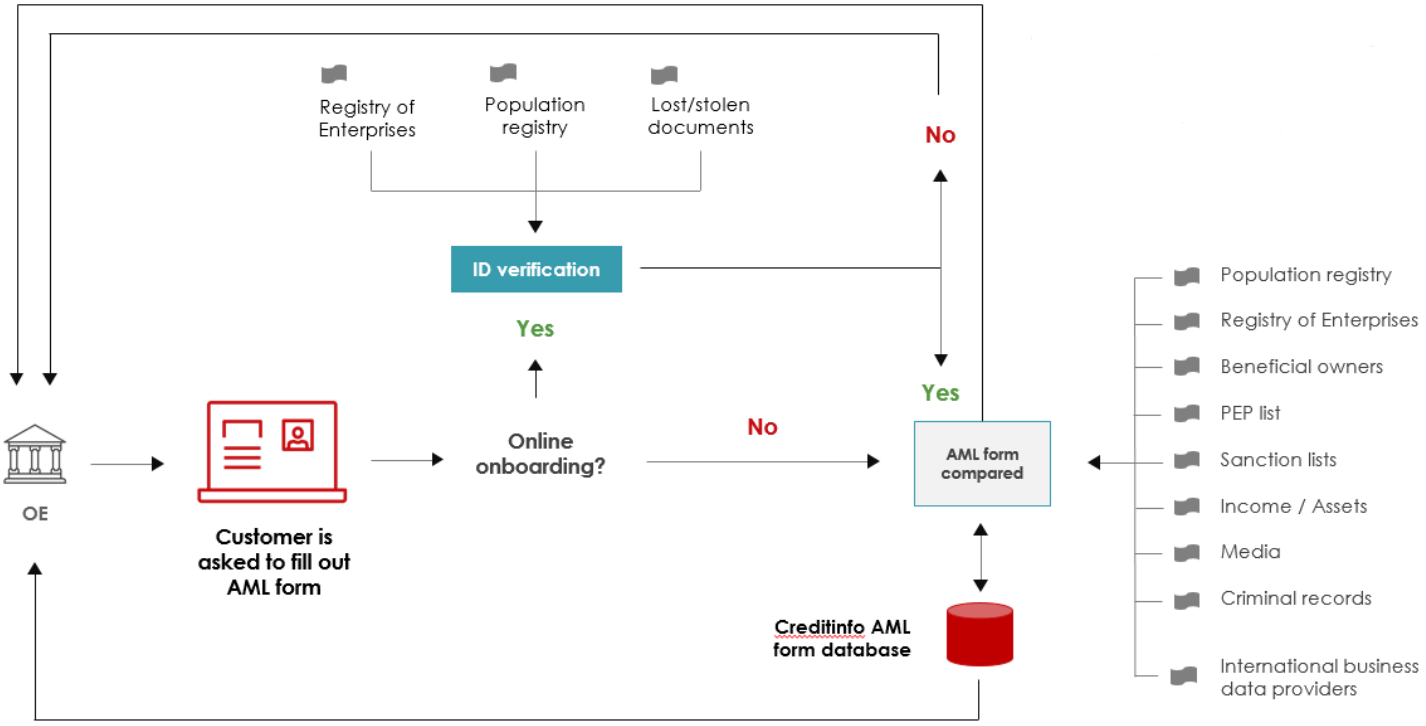
The shared or cross-border KYC utility:
Several or many obliged entities

- Share data gathered from/about their clients like credit bureaus do
- Get data from public registries
- Cross-referencing data to find predefined irregularities

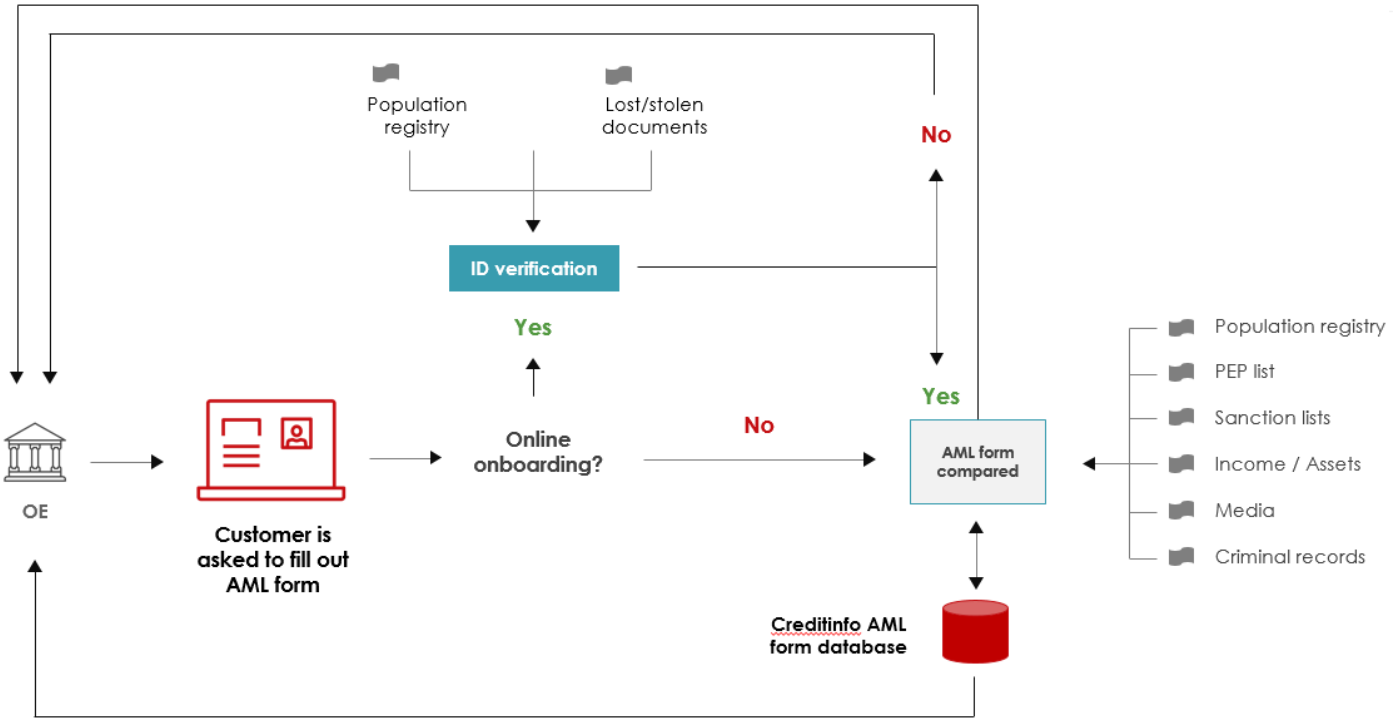
Relies on everyone's participation

- Not necessarily banking only
- Obligation vs free participation
- Bigger help smaller but all must commit
- Full vs. limited access

Scheme 2. Onboarding of a company.



Scheme 3. Onboarding of an individual.



Implementation of DIGINNO cross-border KYC utility

Implementation of cross-border KYC involves almost uncountable number of different stakeholders as countries define differently and by different criteria who fell under term of obliged entity from one side and countries have differently divided their governmental structures responsibilities at the area of AML/CFT.

But in large scale there are 4 types of stakeholders:

- State/government and its different institutions - Ministry of Finance, Ministry of Justice, Ministry of Internal Affairs (eIDAS), Financial Supervisory Authority (FSA), Financial Intelligence Unit (FIU). Data Protection Agency, Accountants' Assembly, Tax and clusters, professional associations (eg ITL), trade unions (Banking Association, Notaries Chamber, Bar Association, Board of Auditors), National banks etc.
- Obliged entities - Credit institutions; financial institutions; gambling operators; auditors and providers of accounting services; providers of accounting or tax advice services; providers of a service of exchanging a virtual currency against a fiat currency; providers of a virtual currency wallet service; undertakings providing a cross-border cash and securities transportation service; pawnbrokers; notaries, attorneys; enforcement officers; bankruptcy trustees; interim trustees etc.
- Private and legal entities about whom KYCs are made and from whom the information, data, proofs and documents are demanded.
- Licenses KYC service provider – legal entity who develops and maintains the cross-border KYC utility (will be different in each country, also can be multiple service provides in one country) in accordance to rules, requirements and standards.

In general all Baltic and Nordic countries have now declared, after numerous money laundering and terrorism financing cases in all three countries, the business interests should not prevail, instead, effective combatting of financial crimes should take the primary role. But it cannot name balanced a solution, where the governments impose significant requirements and harsh penalties to the private sector, making it invest millions in the implementation of the compliance function, without providing any assistance in effective implementation of that function. Therefore the cross-border KYC utility would be a valuable aid not only for large corporations and authorities combating crime, but also to small businesses in preventing financial crimes.

For upkeeping a business relation with its client, every obliged entity must perform customer identification and assessment, by additionally also conducting transaction monitoring. In order to ensure a comprehensive accomplishment of this task, it is worked upon development of technological tools (hereinafter – IT) for importing data from several sources to a single platform – comprising publicly accessible and restricted, state-maintained, as well as private information provided by the customer of the cross-border KYC utility. The tool share transactions when operating within a single obliged entity or a group of companies, however it may also operate as a data aggregation which ensures data sharing and comparison without accumulating such data. An individualized solution at the level of a single obliged entity may though exist, however, such a solution will not account for significant overall contribution.

A centralized data repository or a decentralized data processing tool are both possible by considering the solution of a specific developer, the applicable legislative requirements and personal data protection requirements. It is also possible to combine both these models, e.g. licensed KYC service providers part of information is kept within a single database, whereas part of information is obtained for immediate sales purposes and/or rating purposes.

Irrespective of the model of the data processing tool, it requires setting up a safe information sharing medium, a machine-readable data structure and a single/open standard for technical solutions available to the public as well as private sector (including API). Thus, it would be recommendable to introduce a single channel (aggregator) for the transfer of data of public registries.

Effective management of AML/CFT risks requires cooperation of a number of obliged entities and public institutions, including information sharing, which can be described as private-private or public-private information sharing, also cross-border private-private and public-private data sharing. The current wording of the AML/CFT laws foresees information sharing or acquisition limitations, for the most part focusing on sharing information. All obliged entities have the right to engage in mutual exchange of information, likewise, exchange information with state authorities within the framework of the FIU's.

Thus, currently the possibilities of all obliged entities to acquire and exchange information are limited. Nevertheless, it is rather complicated to set up infrastructure that would enable participation in the acquisition, analysis and information sharing of all the entities due to considerations of data safety, limited resources and differing interests in the acquisition and further use of certain data. Thus, it is necessary to introduce legal and technological tools for addressing this matter.

A cross-border KYC utility is one of the tools that can be used for effective information sharing, it enables moving from a case by case basis to a systemic and structural solution. A cross-

border KYC utility which incorporates several individual and public data sources to ensure information exchange options is a contribution of general public importance. It is possible to distinguish several levels of cooperation. The first level deals only with the structuring of generally accessible information, the second level involves interconnection with public registers inland and abroad, third level involves sharing of customer questionnaire data and customer due diligence information

It increases efficiency of processes as several obliged entities do not have to engage in repeated acquisition of information regarding one and the same subject-matter, although it does not exempt the obliged entities of the duty to identify customers and to clarify basic information. Secondly, it significantly encumbers the "migration" of individuals engaged in unlawful or suspicious activity from being serviced by one subject of the law to another, in order to misuse the time required for the obliged entity for undergoing risk identification anew. Thirdly, without limiting the possibilities of the obliged entities possessing large resources to obtain data from other data sources, a utility creates a platform for the disclosure of the acquired data to the obliged entities with limited resources. The platform is supplied with data that potentially useful for all obliged entities. Such data may also serve the purpose of identifying (verification) of controversial information. Fourthly, the launch of the cross-border KYC utility will allow information sharing by the obliged entities therewith cutting the total investments in ensuring the compliance function.

Currently only Latvia is taking real steps to implement national wide shared KYC utility covering all obliged entities, which allows to share the data in between the obliged entities and to receive necessary data for conducting KYC from national registers without any fees. As described before, the Latvian Shared KYC Utility concept has been prepared and already introduced to the government and parliament of the Republic of Latvia. If relevant amendments of the law shall pass this year, then at the beginning of next year the Shared KYC Utility prototype will be in use and then in full cross-nationally launched during next year.

Must be acknowledged that implementation of cross-border KYC utility demands major changes in the national AMF/CFT legislation. But not only the legislation needs to be changed, but also the way of thinking and doing things. Online and cross-border KYC, with having actually access to state/government registries and proof of origin of the data, is something very new. As well to build up your personal KYC profile in mobile app, with one push of the button, is very innovative. There is much to gain but also to lose. If the harmonization and standardization of common KYC process will be unsuccessful or KYC utility providers will not be properly licensed and supervised, then it is high risk of a total failure.

Beside Latvia, who already is taking a leading role with its national-wide sharing of KYC data in between obliged entities, in Estonia during past years different workgroups, which consist of different representatives from obliged entities, have been developing solution for better and more effective KYC incl. possibility to exchange KYC data. Unfortunately, because of the lack of interest from public and governmental sector and, above all, a reluctance to find a sensible solution, which, unfortunately, also necessitates legislative changes, has led to no changes and the work of the workgroups has not borne fruit yet. At the same time, as a private sector imitative Nordic DNB Bank, Danske Bank, Nordea Bank, Svenska Handelsbanken, and Skandinaviska Enskilda Banken (SEB*)* have announced to establish their shared KYC utility, which will be owned and controlled by the founding banks, with a focus on developing an efficient, common, secure and cost-effective utility for sharing confidential customer credentials.

However, since there is tight cooperation in between three Baltic and Nordic countries, both in government and private sector levels, countries learn from each other's experience and it is rather obvious that once the positive user cases of Latvian Shared KYC Utility or Nordic banks shared KYC utility are visible, the other neighboring states will have keen interest to implement something similar. This in turn makes also cross-border KYC possible.

Viability of DIGINNO cross-border KYC utility

The improvement of customer checks and the introduction of information sharing tools for strengthening AML/CFT risk management has become a global topicality. Each state and financial institutions operating region-wide pick solutions that are most convenient for them, which make such solutions individual, therefore it is important for each state, acting together with the industry and possibly the representatives of the largest stakeholders to decide on the best form for setting up the shared KYC utility, to reach the highest compliance standards and therewith improve the reputation of the state and cut the total customer verification costs.

The introduction of the cross-border KYC utility will allow for easier identification of AML/CFT risks, considering that in case one obliged entity has performed assessment and identified high AML/CFT risk for a certain customer or its transactions, the obliged entity would feed the given data into the KYC utility and other obliged entities will have the chance to make use of these data in their operations. Thus, the obliged entities would not have to start the evaluation from zero, therewith identifying and bringing to a halt the use of proceeds from suspicious or unlawful acts considerably faster. In fact, this means that the obliged entities under AML/CFT laws not possessing sufficient IT and human resources are reasonably incapable of completing all necessary tasks to verify that the customer or its transactions cause no AML/CFT risks.

There is actual need existing for such cross-border KYC utility, since:

- reduces the resource for collecting and analyzing data and for transmitting data (time and money), automated data management and analysis (eg XBLR), better and more accurate risk prevention / detection. Better information management
- speed of data collection and data quality (and reliability), faster and more accurate response, less additional movements and bureaucracy. More consistent information
- more effective risk detection and risk prevention = A more reliable country (less corruption, tax evasion, money laundering, and other criminal activities)
- cheaper and easier to create new relationships with a potential client

Perhaps most important of all is, that the state itself does not have to contribute financially for a such shared or cross-border KYC utility. Once the legislative amendments are implemented (incl. harmonization and standardization and licensing principles), due to market pressure, this KYC utility or even several competing utilities shall be created by interested parties themselves, without a need to involve any resource from public sector. One should not forget that there are already many competing products on the market, however, their usability currently is limited by lack of access to necessary data and legislative restrictions for using their data.

ANNEX 1. DIGINNO KYC showcase workgroup activities

In 2018 was in Latvia establish a public-private information sharing partnership. The roots of such model can be found in the United Kingdom. On November 23, 2018, high-level workshops were held in Riga on the topic of the best available technological solutions for "Know Your Customer" principle's implementation, and for information sharing partnerships that would lead to more effective combating of financial crime "AML/CFT: RegTech & Partnerships". These events were organized by Finance Latvia in collaboration with ACAMS Baltics Chapter, Microsoft and Citadele.

In parallel, from November 2018 under DIGINNO project, the KYC showcase national workgroups started to envision their "KYC to-be " under DIGINNO KYC showcase. Such workgroups were established in Estonia, Latvia and Lithuania, but unfortunately already at the early spring of 2019 the Lithuanian workgroup dissolved without delivering any of agreed documents under KYC showcase.

Between December 2018 to March 2019 national DIGINNO KYC workgroups were brainstorming and developing their "KYC to-be" future vision.

In February 2019 was held in Riga first DIGINNO KYC showcase international meeting, where Estonian and Latvian national workgroups presented their first ideas about the future. Also at roundtable where shared activities and information from each other national levels, discuss next steps and how to develop the showcase, KYC to-be envisioning, feasibility study structure, DIGINNO service canvas etc. In the meeting were also representatives from Lithuania and Denmark participating.

In March 2019 was held in Kaunas the second DIGINNO KYC showcase international meeting, where only Estonia and Latvia were participating. In the meeting was stressed the importance to activate the involvement of Lithuania and Denmark and was decided to held "stand-alone" special seminar for Lithuania in Vilnius and were agreed main principles for filling business canvas.

In April 2019 was held in Pärnu DIGINNO KYC Estonian and Latvian workgroups joint meeting. The aim of the meeting was to develop and agree on a common view on the future preferred situation in the development of an example of KYC. As a result of this meeting was adopted Estonian-Latvian "KYC to-be" vision and business canvas. Also was decided the structure of "KYC as-is" document and principles for feasibility study. Was decided, taking into account the enormous scale of DIGINNO KYC showcase and complexity of the problems, that feasibility study will be done by the members of the DIGINNO KYC workgroups and in simplified manner.

In May 2019 in Vilnius was held "stand alone" seminar "KYC as cross-border service", organized by the Estonian Embassy in Lithuania and Ministry of Economic Affairs and Communication of the Republic of Estonia. Aim of the seminar was discussion about possibilities to conduct KYC across borders without unreasonable and unnecessary steps and actions, transmit personal data and data exchange channels built for G2B and B2G etc., as well to get participants approval of the "KYC to-be" vision and to find among participants possible future partners to cooperate on this matter. The presentations of the seminar were made by the members of Estonian and Latvian national DIGINNO KYC showcase workgroup members.

At the beginning of June 2019 in DIGINNO KYC showcase were finalized and delivered the Baltic KYC to-be vision (Annex 3), Baltic KYC as-is overview (Annex 2) and Cross-border KYC utility business canvas (Annex 4).

ANNEX 2. Baltic KYC as-is overview

	ESTONIA	LATVIA	LITHUANIA
Owners (e.g Ministry of Finance, Ministry of Internal Affairs, etc)	Ministry of Finance	Ministry of Finance (Ministry initiating changes in AML law); Ministry of Environmental Protection and Regional Development (Owned of platform providing access to services/data from state registries); ministries in charge of maintaining specific state registries	Ministry of Finance or Bank on Lithuania
Stakeholders (as established locally)	Ministry of Finance, Ministry of Justice, Ministry of Economy and Communication (RTE – Real Time Economy), Anti Money Laundering Bureau, Financial Supervisory Authority, Ministry of Internal Affairs (eIDAS), Data Protection Inspectorate, Estonian Accountants' Assembly (XBRL - eXtensible Business Reporting Language), Tax and Customs Board, clusters (Finance Estonia, ICT), professional associations (eg ITL), trade unions (Banking Association, Notaries Chamber, Bar Association, Board of Auditors), Bank of Estonia, obliged entities	AML obliged entities (or rather associations representing them e.g. Finance Latvia), government entities supervising AML compliance (e.g. Financial Intelligence Unit, Financial and Capital Market Commission; State Revenue Service, Consumer Rights Protection Centre, etc.)	Lithuanian Parliament Government of the Republic of Lithuania (Government) Ministry of Finance Market participants financial institutions and obliged entities as per AML law, clause 2, section 7&10. Financial Intelligence Unit (FIU) – Financial Crime Investigation Service under the Ministry of Interior Financial Supervisory Authority (FSA) – Bank of Lithuania (BOL)
Obligated persons (as listed in the local laws and regulations)	Obliged entities as defined in AML law, clause 2: Credit institutions; financial institutions; gambling operators; persons who mediate transactions involving the acquisition or the right of use of real estate; traders within the meaning of the Trading Act; persons engaged in	Obliged entities as defined in AML law, clause 3: Credit institutions; financial institutions; tax advisors, external accountants, sworn auditors and commercial companies of sworn auditors; sworn notaries, sworn lawyers, other independent providers of legal services when they, acting on behalf and for their	Obliged entities as defined in AML law, clause 2. Financial institutions: credit institutions and financial undertakings as defined in the Law of the Republic of Lithuania on Financial Institutions, payment institutions as defined in the Law of the Republic of Lithuania on Payment Institutions,

	buying-in or wholesale of precious metals, precious metal articles or precious stones; auditors and providers of accounting services; providers of accounting or tax advice services; providers of trust and company services; providers of a service of exchanging a virtual currency against a fiat currency; providers of a virtual currency wallet service; a central securities depository where it arranges the opening of securities accounts and provides services related to register entries without the mediation of an account operator; undertakings providing a cross-border cash and securities transportation service; pawnbrokers; notaries, attorneys; enforcement officers; bankruptcy trustees; interim trustees; providers of other legal services where they act in the name and on account of a customer in a financial or real estate transaction; non-profit associations for the purposes of the Non-profit Associations Act and to other legal persons governed by the provisions of the Non-profit Associations Act as well as to foundations for the purposes of the Foundations Act where they are paid or they pay over 5000 euros in cash or an equal amount in another currency, regardless of whether it is paid in a lump sum or by way of several linked	customer, assist in the planning or execution of transactions, participate therein or carry out other professional activities related to the specific transactions described in law providers of services related to the establishment and provision of operation of a legal arrangement or legal person; persons acting as agents or intermediaries in immovable property transactions; organizers of lotteries and gambling; persons providing cash-in-transit services; other legal or natural persons trading in means of transport, cultural monuments, precious metals, precious stones, articles thereof or trading in other goods, and also acting as intermediaries in the abovementioned transactions or engaged in provision of services of other type, if payment is carried out in cash or cash for this transaction is paid in an account of the seller in a credit institution in the amount of or equals to 10000 euros or more, regardless of whether this transaction is carried out in a single operation or in several mutually related operations; debt recovery service providers.	electronic money institutions as defined in the Law of the Republic of Lithuania on Electronic Money and Electronic Money Institutions, operators of currency exchange offices as defined in the Law of the Republic of Lithuania on Currency Exchange Operators, operators of crowdfunding platforms as defined in the Law of the Republic of Lithuania on Crowdfunding, operators of peer-to-peer lending platforms as defined in the Law of the Republic of Lithuania on Consumer Credit and the Law of the Republic of Lithuania on Credit Relating to Immovable Property, insurance undertakings engaged in life insurance activities and insurance brokerage firms engaged in insurance mediation activities relating to life insurance as defined in the Law of the Republic of Lithuania on Insurance as well as investment companies with variable capital and collective investment undertakings intended for informed investors and management companies managing only those undertakings; branches of these foreign financial institutions set up in the Republic of Lithuania as well as electronic money institutions and payment institutions whose registered office is in another European Union Member State providing services in the Republic of Lithuania through agents, natural or legal persons. Other obliged entities: 1) auditors engaged in audit activities in a self-employed capacity or audit firms (hereinafter: ‘auditors’);

	payments over a period of up to one year.		2) judicial officers and judicial officer's agents; 3) undertakings providing accounting or tax advisory services and persons providing such services in a self-employed capacity (hereinafter: 'undertakings providing accounting or tax advisory services'); 4) notaries, notary's agents and persons entitled to perform notarial actions, as well as advocates and advocates' assistants, whether by acting on behalf of and for their client or by assisting in the planning or execution of transactions for their client concerning the purchase or sale of immovable property or undertakings, management of client money, securities or other assets, opening or management of bank or securities accounts, organisation of contributions necessary for the establishment, operation or management of legal persons and other organisations, emergence or creation and operation or management of trust or company incorporation and administration service providers and/or related transactions; 5) providers of trust or company incorporation or administration services not referred to in points 1, 3 and 4 of this paragraph; 6) persons engaged in economic and commercial activities involving trade in precious stones, precious metals, movable

			cultural goods, antiques or any other property the value whereof is equal to or exceeds EUR 10 000, or an equivalent amount in foreign currency, irrespective of whether the transaction is carried out in a single operation or in several operations which are linked, provided that payments are made in cash; 7) gaming companies and lottery companies; 8) closed-ended investment companies; 9) estate agents/brokers, whether by acting on behalf of and for their client or by assisting in the execution of transactions for their client concerning the purchase or sale of immovable property and/or related transactions. As per upcoming regulation (effective September 2019): custodian crypto currency wallet providers and crypto currency exchanges.
List of direct regulations involved (except ministerial regulations)	Money Laundering and Terrorist Financing Prevention Act; International Sanctions Act; Strategic Goods Act; Notaries Act; Creditors and Credit Intermediaries Act, Investment Funds Act; Code of Commerce; Credit Institutions Act; Securities Market Act; Auditors Activities Act; Insurance Activities Act, EU directives, FATF recommendations	AML law; EU Directives; FATF recommendations	FATF guidelines (non-mandatory) EU AMLD 4 (upcoming EU AMLD5) Law on the prevention of Money Laundering and Terrorist Financing Law on the implementation of Economic and other International Sanctions Regulations and guidelines issued by the FSA Regulations and guidelines issued by the FIU
Short description of the situation (incl. recent AML violation cases,	During recent year some credit institutions were closed because of	Failure to implement, and disregard for, effective AML/CFT and sanctions policies	FinTech center. Lithuania has positioned itself as a FinTech center and attracted a

ongoing processes/exchanges in KYC area.	inability to follow AML/CFT regulations. The biggest breach of AML/CFT happened in Danske Bank A/S Estonian branch where billions of euros were washed. Ministry of Finance and Financial Supervisory Authority have been applied ne regulations for credit institutions, which are enforced with harsh sanctions. Resulting with credit institutions to close banking account of foreigners and even to the legal persons who are residence, but who have beneficiaries or member of the board. There are no regulations to enable obliged entities to exchange AML/CFT information or allowed to rely on data already collected by someone else. Therefor same data for KYC is collected again and again. The access to state registers are limited if non-existing as well if state provides access, it is very costly (state fees are high). Credit institutions have been involved to several initiatives (incl. Diginno KYC) to find solutions how to make KYC data exchangeable and reusable. There are several KYC service providers in the market, but because of lack of the regulations and trust, services are not used by obliged entities. At the government sector there is no initiative to standardize or re-regulate KYC, since there is believe that Money Laundering	and procedures[1]	number of companies from abroad to obtain their operating licenses in Lithuania. Since January 2018, Bank of Lithuania has issued 25 e-money, 13 payment and 2 specialized banking licenses. Therefore, the pressure put on the FIU and FSA to supervise the entire financial market has increased. Lithuania's dynamic FinTech sector is experiencing dramatic growth, doubling in size over the last two years. In 2018, the number of companies in the country's close-knit FinTech ecosystem grew by 45%, with 700 new positions created. Today, almost 2,700 specialists are employed in the sector across a wide range of positions and functions. Lithuania's FinTech landscape also includes accelerators, incubators, several innovative sandboxes for product and business development and over 20 co-working and flexible rental office spaces. FinTech action plan. Ministry of Finance early in 2019 presented Action Plan on the development of FinTech market in Lithuania to the Government. It is attempted to continue improving legal environment for FinTech companies, increasing supply and demand of the financial products and services as well as promoting their export, given a special attention to the ML/TF risk management and consumer protection. As explained, one of the main priorities are to improve

[1] https://www.fincen.gov/news/news-releases/fincen-names-ablv-bank-latvia-institution-primary-money-laundering-concern-and https://danskebank.com/about-us/corporate-governance/investigations-on-money-laundering

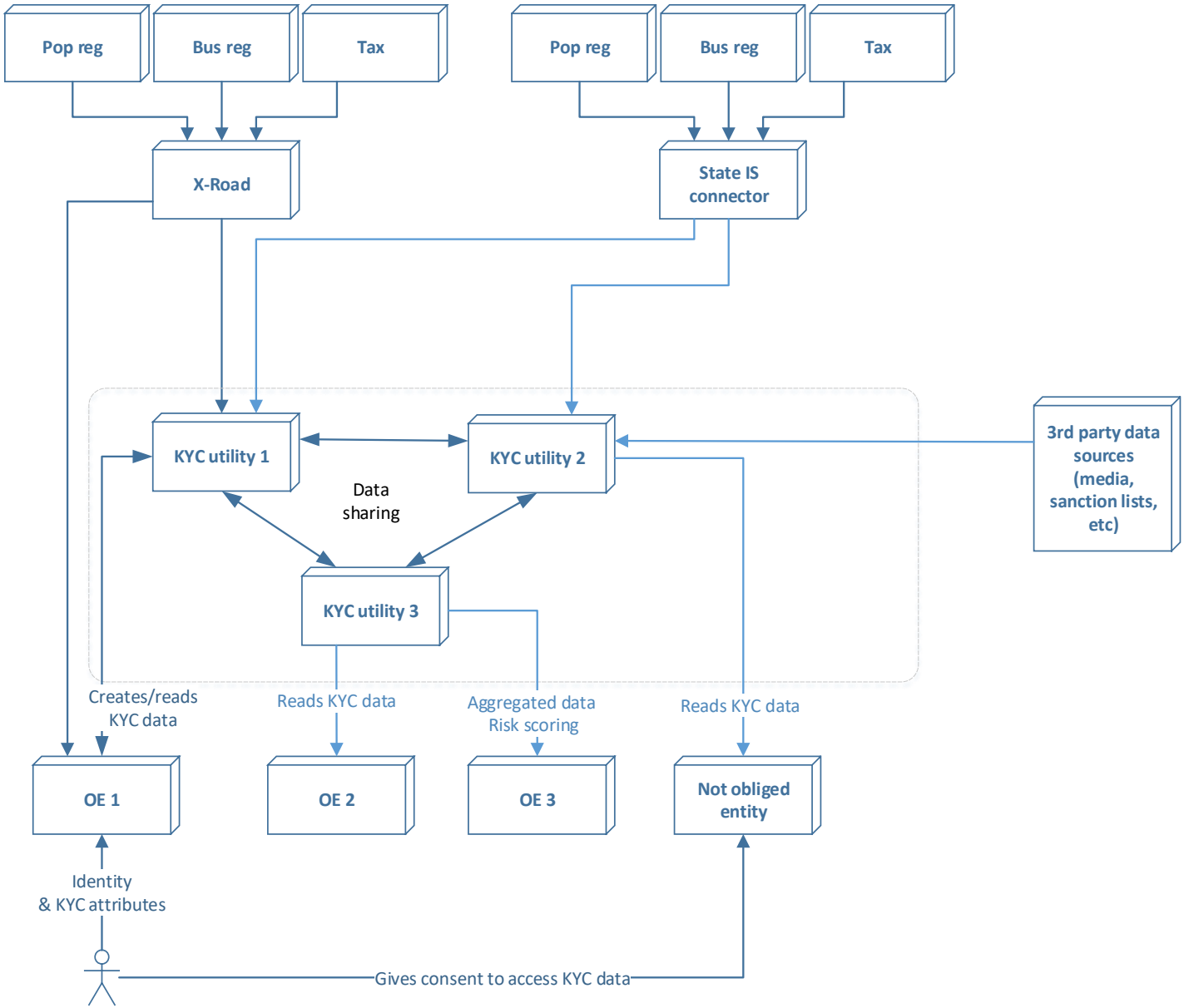
	and Terrorist Financing Prevention Act is already sufficient.		the means through which customers can be determined or initiate driver's license to be approved as a legitimate document to determine customer's identity (just like a passport or ID card already is). However, the inititative continues to hinder: Lithuanian Parliament decided to postpone this decision. Fines. Since the beginning of 2018, FSA imposed three warnings and two fines (exceeding EUR 700,000, one of which was EUR 700,000 and another only EUR 3176) on financial institutions for non-compliance with AML/CTF laws. There are no commonly agreed policy on KYC exchange between either the financial entities themselves or financial entities and third party providers/governmental institutions.
Technical description of the situation (standards, data exchange standard, data exchange solutions)	Beside regulations already involved as listed above, there is no standards, data exchange standards or data exchange solutions existing, which are recognized by the state as valid or official solution. There are many different service provides which provide different KYC services, but which are not standardized at the level of the State (Creditinfo, Infobank, Inforegister, Bisnode, id.credit, KYC-pass, Verif etc)	Extent of information required from state registries differ depending on KYC process phase (identification, verification, monitoring), customer (company, individual) and its residence (resident, non-resident). Separate integration is required to access each state register, no central hub for KYC related information from state registries	There are no data exchange standard, data exchange solutions set.
Policy for implementing KYC (tool, system, action plan, roadmap)	There is no such policy existing. At current moment the State does not feel itself as an owner of KYC and mostly presumes this is something that private sector should solve in between themselves	Adopt legal framework that allows private companies to create KYC solutions for obliged entities in a controlled manner to minimize the risk of unlawful access to sensitive data required for KYC purposes in state registries	No official policy has been approved but several initiatives occurred. For example, Lithuanian Payments Council presented the Feasibility Study on new methods to determine customer's identity and compliance with AML laws. Still no

			roadmap or action plan.
Concerns (from the point view of obligated parties)	Ownership of KYC data is taken as competitive advantage, limited access to state registers, limited access to global/other countries databases, lack of trust in between obligated parties, lack of analytical skills, data is fragmented, obtaining the relevant information even from state registers is too expensive (state fees).	Ownership of KYC data and cost of AML compliance is becoming a competitive advantage for large obliged entities vs their smaller competitors. Limited access to state registers, limited access to global/other countries data bases, fragmented data, lack of trust in between obliged entities continue to increase compliance cost reducing ability of obliged entities to implement effective AML/CFT and sanctions policies and procedures.	Same as LV and EE, GDPR compliance (KYC vs GDPR's data minimization and sharing), lack of political will to ease the KYC process for private sector, lack of cooperation among institutions, competition among the private sector players (not willing to share) etc.
Market awareness/communication about AML/CFT risks both in government and ultimate client level	There is no communication or what so ever plan from governmental or public sector. Awareness of AML/CFT risks become known to everybody after Danske money-laundering case. From government level there have heard statements that the regulations should be further tightened. Credit institutions at the same time are close banking account of foreigners and even to the legal persons who are residence, but who have beneficiaries or member of the board. This has turned ridiculous the whole e-residency project of the State. In the media there are sometimes articles about the indigent clients who had to fill at the bank some "ridiculous" forms (for KYC) or file documents that are available at the state databases. Sometimes there are also printed similar thoughts from reputable persons. Still from the State side there are no comments or no plans how to make KYC more efficient and how to	Government has adopted AML/CFT action plan (Ministru kabineta (turpmāk – MK) 2018. gada 11. oktobra rīkojums Nr. 512 "Par Pasākumu plānu noziedzīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas novēršanai laikposmam līdz 2019. gada 31. decembrim) Based on this action plan further activities and plans are carried out on level of ministries and industry associations.	Market participants have been active in the field: established FinTech association regularly discusses initiatives within the field and represents itself at regulatory institutions, government and separate events. FSA has been initiating a discussion with market participants and provided FAQ on AML tools, launched an initiative of the banking association to provide guidelines for AML compliance. FSA provided regulatory sandboxes for testing financial inno-vations, accelerated the development of RegTech solutions, and created a platform (LBChain) for blockchain-based solutions to be created whilst under the watchful eye of the BOL. FIU has been more silent on the matter and will have to become much more involved by the time it becomes a supervisory authority of the crypto-market operating in Lithuania. Government of the Republic of Lithuania has been active in the field: adopted

	reduce unreasonable burden		strategic plan of the development of FinTech sector and assigned Ministry of Finance and FSA (BOL) to report to the Government on the progress of the application of the measures discussed. Lithuanian Parliament has been more conservative of revolutionary takeover of the market so there has been an initiative by the Chairman of the Committee of the Budget of Finance of the Lithuanian Parliament questioning the risks particular foreign FinTech companies bring along with the foreign investments.

ANNEX 3. Baltic KYC to-be vision

- Harmonization of a minimum list of questions, documents and collectable data that are needed to conclude KYC (i.e. shall be listed which data will be collected from business register, population register, PEP register, beneficial owners register, state revenue register, land book, vehicle register, criminal records database, document register, credit bureaus data etc.)
- An agreed normative, substantive, and best practice for data transmission framework (i.e. possible data exchange standards XML, XBRL, JSON or other) under which service providers can create their services.
- Adopted cross -border (or transnational) acts/regulations to guarantee cross -border usage/applicability of such services and adopted that for obliged entities to fulfill the AML/CFT regulations is not needed to obtain consent from the person.
- Access to state registers is granted to obliged entities and licensed entities (e.g. credit institutions, audit firms, credit bureau, service provider etc.) free of charge or with reasonable costs.
- Other States accept the KYC data that is recognized by the first State (transnational agreements).
- State confirmation of the data it has/owns (i.e. symbolically confirms their accuracy as these data come from national registers) except. beneficial owners and PEPs data which shall be checked each and every time by the obliged entities and/or licensed entities.
- State acceptance of licensed entities (e.g. credit institutions, audit firms, credit bureau, service provider etc.) to validate the information entered by persons about themselves (e.g. data about foreign beneficiaries, PEPs etc.)
- An ability to create a KYC profile, which consists of both automatically collected (query -based) and self - contained data (documents that cannot be obtained from national databases based on inquiries).
- Profile can be created by person itself or by obliged entities and/or licensed entities (e.g. credit institutions, audit firms, credit bureau, service provider etc.)
- Profile (i.e AML passport), which has already created, is interoperable in all cases where obliged entities want or need to carry out KYC.
- It shall be created on once-only principle and updated (incl. automatic updates) every time the profile is used again.
- On the basis of existing and entered data, visual display is created of inter-dependency links between the person(s) and the company(s).
- Contradictions between the data collected, the data provided by the person itself and the data entered by licenses entities must be visible. Licensed entities are entitled to check which data is correct in case of inconsistencies (if possible)
- Voluntary KYC should be available using the same principles, but the consent of person should be obtained once, when the profile is created or used again.



Idenity attributes

Name, Address, Date of Birth, Nationality, and Occupation.

Legal name, Address, Unique Identifier.

KYC attributes

PEP status,

Source of funds, Tax and Fiscal residence, Beneficial

Owner Identity, Source of funds, Brand name

(Public) Service Model Canvas *Know-Your-Customer*

Name of Service
Cross-border KYC utility

Vision

Harmonized minimum list of questions, documents and collectable data that are needed to conclude KYC. Agreed normative, substantive, and best practice for data transmission framework under which service providers can create their services. Adopted cross -border (or transnational) acts/regulations to guarantee cross -border usage/applicability of such services. Access to state registers is granted to obliged entities and licensed entities free of charge or with reasonable costs. Other States accepts the KYC data that is recognized by the first State. State. symbolically confirms their accuracy as these data come from national registers. .State acceptance of licensed entities (e.g. credit institutions, audit firms, credit bureau, service provider etc.) to validate the information entered by persons about themselves. An ability to create a KYC profile, which consists of both automatically collected (query -based) and self -contained data. Profile can be created by person itself or by obliged entities and/or licensed entities. Profile (i.e AML passport), which has already created, is interoperable in all cases where obliged entities want or need to carry out KYC. It shall be created on once-only principle and updated (incl. automatic updates) every time the profile is used again. On the basis of existing and entered data, visual display is created of inter-dependency links between the person(s) and the company(s). Contradictions between the data collected, the data provided by the person itself and the data entered by licenses entities must be visible. Voluntary KYC should be available using the same principles, but the consent of person should be obtained once, when the profile is created or used again.

Owners & Builders

State as owner (different ministries in different countries which have core interest in the AML/CFT area): Ministry of Finance, Ministry of Internal Affairs, FIU etc.

Services will be provided (built) by private sector (licensed) under standards and regulations made by public sector (State)

Key Activities

Ensure online data exchange and setting up an information exchange network (public-private-European-Global sector).
Standardized set of regulations of information (what data and in what form);
Agreed security standards.
Creating legal framework incl. national and international provision enabling cross-border data exchange.
Create framework by involvement both governmental and private sectors.

Value Proposition

KYC utility reduces the resource for collecting and analyzing data and for transmitting data (time and money), automated data management and analysis (eg XBLR), better and more accurate risk prevention/ detection.

KYC utility minimize the need for data processing for AML/CFT purposes.

KYC utility allows to build up automatic data analyze systems and additional services (client credit rating etc) which shall make this service more demanded and desirable.

KYC utility allows to serve client faster and cheaper (i.e. green corridor, interoperable profile).

KYC utility allows to the obligated entities cheaper and more professional access to the data which must and shall be collected for AML/CFT purposes.

KYC utility will result with less consumption of paper and therefor helps to save the environment.

User Journeys

As an example, clients from Latvia desires to open the banking account in Estonia. He logs in into local (Latvian) KYC utility or goes to the bank office in Estonia and the bank opens the KYC profile in the local (Estonian) KYC utility. Client/bank selects the KYC package suitable for such transaction. The KYC utility collects in accordance to the package the available and needful data from public registers (directly or via other KYC utility tools in other countries) and will reply also which data is missing or where are mismatches. The bank informs the client which additional data (documents) is needed, if any. The bank opens the banking account at the spot, if all relevant information is received. Next day the person wants to buy real estate in Lithuania. Notary at Lithuania checks that this person has KYC profile established, makes additional inquires to receive information needed for this transaction. No additional declaration by the client shall be filled.

Users & Customers

Everybody who has the obligation or need to carry out KYC (obliged entities stated by the AML/CFT regulations) and the one who is required to provide data for KYC (private sector) or entities who are doing it on voluntary bases i.e the enterprises, obliged entities: banks, financial institutions, notaries, attorney offices/attorneys, auditors, debt collection companies, accountant companies etc. and private person/entities who open itself the profile/enters data (for example as obligated persons it concerns at least 30000 entities within Baltics)

Partners & Enablers

Ministry of Finance, Ministry of Justice, Anti Money Laundering Bureau, Financial Supervisory Authority/Financial Intelligence Unit/ Financial and Capital Market Commission/ Ministry of Internal Affairs (eIDAS), Data Protection Inspectorate, Accountants' Assembly (XBRL - eXtensible Business Reporting Language), Tax and Customs Board/State Revenue Service, clusters (Finance Estonia, Finance Latvia, ICT/Likta etc), professional associations (eg ITL), trade unions (Banking Association, Notaries Chamber, Bar Association, Board of Auditors), Bank of Estonia, obliged entities

Resources and prerequisites

Legislation – eIDAS Regulation (EU), Plan on AML/CFT activities for implementation, Report on solutions for the circulation and access to information in the public administration
Needs: public data, technological solutions. Policy planning and legal solutions, Financial Resources, Human Resources, Technological Solutions.

Ways of service

Customer can establish KYC profile and/or the obligated person opens the KYC profile for customer, which consists of both automatically collected (query based) and self-contained data (documents that cannot be obtained from national databases based on inquiries, eg actual beneficiary data, related parties etc). On the basis of existing and entered data, visibility links between the person(s) and the company(s) (eg a spider chart) are displayed visually. It shall be driven from once-only principle, possible to update and amend, but no need to start over every time. Data belongs to the data owners.

Beneficiaries

Citizens because living in country with less AML/CFT risks.

Society by lower AML/CFT risk the business is more transparent and gray economy is lower, leading to higher GDP.

Government by having lower risk level for the state and better reputation.

Costs

Demands further analyzes (cost of exchanging the legislation, cost of developing KYC utility, cost of collecting the information from databases (state fees), cost of maintaining the KYC utility working (service fees) etc)

Benefits

Reduces the resource for collecting and analyzing data and for transmitting data (time and money), automated data management and analysis (eg XBLR), better and more accurate risk prevention/detection, fights against grey economy.

Elevator pitch

KYC utility will allow for easier and cheaper identification of AML/CFT risks, considering that in case one obliged entity will has performed assessment and identified high AML/CFT risk for a certain customer and its transactions, the obliged entity will feed the given data into the KYC utility and together with the query based collected data from State registers (all) obliged entities will have the chance to make use of these data for their operations based on their data access needs (obliged entities will see only data what is assigned them in accordance to the standard i.e. banks will see much wider range of data than notaries etc). The data collected is machine-readable and usable for risk-assessments modules/analyses. The obliged entities will not have to start the assessment again and again from zero, therewith bringing to a half the use of proceeds from crime considerably faster.

Interreg Baltic Sea Region
EUROPEAN UNION
EUROPEAN REGIONAL DEVELOPMENT FUND
DIGINNO

ANNEX 5. List of persons who contribute for preparing this document

From Latvia

- Linda Austere, Finance Latvia
- Edgars Pastars, Finance Latvia
- Janis Timermanis, Credit Information Bureau

From Estonia

- Rainer Osanik, R.O.S Law Office
- Ragnar Toomla, SEB Bank Baltic division
- Anne Kalberg-Sägi, SEB Pank

Other persons within DIGINNO workgroups whose help, knowledge and wisdom has been used:

- Toma Matikiūnienė, Spectro Finance
- Ege Metsandi, Krediidiinfo
- Heiki Pruul, Swedbank
- Gatis Ozols, Ministry for Environmental Protection and Regional Development of Latvia
- Reet Reismaa, Ministry of Economic Affairs and Communication of Estonia