2021

Operational and Governance Framework for Cross-Border E-Servicess delivery

COMPILED BY
IDONGESIT WILLIAMS
AALBORG UNIVERSITY COPENHAGEN

EUROPEAN REGIONAL DEVELOPMENT FUND

DINNOCAP

Operational and Governance Framework for Cross-Border E-Service delivery

The report is produced by the DINNOCAP project. An EU Interreg BSR finances the project.

The report is reviewed and edited by DINNOCAP showcase leads and working groups associated with the showcases. The showcases leads are namely Heiti Mering, Digilogistika Keskus, Estonia, for eCMR; Sirli Heinsoo, Head of Real-Time Economy, Ministry of Economic Affairs and Communications Estonia, for eReceipt; and Rainer Osanik, Managing partner R.O.S.Law OU, for KYC. The eCMR working group editors are namely Ulrika Hurt, a member of the Digital Transport and Logistics Forum (DTLF), Eva Killar, Executive Officer at transport development issues, Ministry of Economic Affairs and Communications for Estonia, Riho Vedler, Ramena OÜ, and Kristi Aruküla, Project manager, DINNOCAP, Ministry of Economic Affairs and Communications, Estonia.

Table of Contents

EXECUTIVE SUMMARY

The overall aim of the DINNOCAP project is to develop the capacity of SMEs to enable their digital transformation initiatives and activities. This fits into the overall aim of the EU towards the development of a Single Digital Market. As more SMEs embark on the digital transformation journey especially in the provision of data of their goods and services, the EU as a region and the Baltic Sea Region towards becoming a digital economy and eventually a Digital Single Market. However, digital transformation in SMEs is not just an SME activity. There is a need for the digitalization of e-government or e-Services that will enable SMEs to deliver their services digitally within the member state and between member states. The absence of which either, forces the SME to expand its capacity to develop end-to-end national and Cross-Border solutions or forces the SME to digitize only aspects of their service delivery processes.

Hence, in the work package 3 of the DINNOCAP project e-Services developed in the DIGINNO project (of which DINNOCAP is an extension) are further developed to open the possibility for SMEs to digitize their service delivery processes. It also enables SMEs to deliver these services digitally across borders in the Baltic Sea Region and the EU at large. In a way, these e-Services will encourage SMEs to develop their capacity to digitize.

The purpose of this report is to present proposals on operational principles (framework) and governance frameworks for Cross-Border data exchange for selected e-Services. The e-Services covered in this document are Cross-Border eCMR, Cross-Border KYC, and Cross-Border eReceipt. These are some of the e-Services developed in DIGINNO. The operational principles are rule statements like business rules. The governance framework is a structural framework of the interaction of Cross-Border stakeholders working only semantic interoperability of individual e-Service. The difference between this framework and other frameworks is that it is bottom-up and that it is granted legitimacy by contributions from stakeholders from the public sector and SMEs and service providers from the EU member states from the Baltic Sea Region.

Input to the development of both frameworks is from the feasibility studies for the e-Services, developed in DIGINNO, Stakeholder workshops, and questionnaire feedback organized and elicited respectively in the DINNOCAP project. DINNOCAP partners from Infobalt (Lithuania), Ministry of Economic Affairs and Communications (MKM) (Estonia), Digilogistika Keskus, Estonia, and Aalborg University (Denmark) coordinated the workshops. DINNOCAP partners from Latvia, Norway, Russia (Kaliningrad), and Norway supported them. The inputs from the feasibility studies, workshop notes extracted from the recorded sessions at the stakeholder workshop were analyzed, condensed, and produced as proposed frameworks at Aalborg University, Denmark. The outcome of the analysis and the process at which the outcomes were arrived at are presented in this report.

PREAMBLE

A challenge facing the delivery of Cross-Border e-Service is the absence of semantic interoperability. Hence different e-government services owned by public authorities in different member states are unable to exchange data unambiguously due to the differences in the semantics governing data exchange of the national systems. In the DINNOCAP project, an attempt is made to provide a foundation for the development of common vocabulary and semantic syntax for e-Services. This is done by providing proposals via the creation of a framework of guiding operational Cross-Border principles that will provide a harmonized Cross-Border approach to the delivery of selected e-Services. Based on these rules, common vocabularies for the delivery of the selected e-Services can be created and depending on the technical standards used for the delivery of the e-Services, different stakeholders can develop semantic syntax that can be implemented in a manner where semantic interoperability is achieved. Hence common vocabularies will be used. Although this document does not propose vocabularies for the selected e-Services, it provides a foundation for doing so.

The selected e-Services are the three mentioned earlier in the executive summary namely, KYC (Know your customer), eReceipt, and eCMR. These are e-Services that will enable the digital transformation in the service delivery operations of SMEs operating in specific vertical markets and horizontal markets. eCMR caters to a vertical market – the transport sector. KYC caters to the financial sector and other sectors of the economy where SMEs must conduct due diligence on clients. eReceipt caters to every sector in the economy. This is because receipts are issued at the end of most financial transactions in all sectors of the economy. These are the services for which the operational principles are created. As mentioned earlier, DINNOCAP is building on the work done in developing the Cross-Border technical systems for these e-Services in the DIGINNO project (see https://www.diginnobsr.eu).

The proposals are presented in two sections of this report. The first section describes the operational principles (framework) for Cross-Border eCMR, KYC, and eReceipt. The second section describes the proposed governance framework for the development of these services. The proposals are designed to contribute to ongoing efforts and discussions aimed at the semantic interoperability of e-Services in the BSR and EU.

The report is an aggregation of suggestions and contributions from public and private stakeholders from the Baltic Sea Region on their vision for eCMR, KYC, and eReceipt. Hence this document is not authoritative but contains proposals on the way forward. About 130 stakeholders consisting of SMEs and Public authorities, from Lithuania, Norway, Sweden, Latvia, Denmark, Estonia, Kaliningrad (Russia), Poland, Estonia, and Finland provided inputs at stakeholder workshops, and surveys. Inputs from these workshops and surveys are used in the development of this report.

SECTION 1 – SEMANTIC OPERATIONAL FRAMEWORK (PRINCIPLES)

1.1. INTRODUCTION

The essence of this part of the report is to develop proposals on Cross-Border processes, policies, and principles for semantic models. As mentioned in the preamble, the proposed principles will guide the further development of common semantic vocabularies and syntaxes needed to enable semantic interoperability of the selected Cross-Border e-Services. The word principles here is used in the place of rules (inspired from business rules). The proposed Cross-Border processes, policies, and principles also provide a harmonized Cross-Border framework where different stakeholders involved in the delivery of an e-Service can identify their roles and responsibilities in the data exchange process. For example, if a stakeholder is a service provider involved in routing data, the principles provide the rules governing data routing and the potential data set as well as procedures required in the routing process. The principles are the same for such service providers, irrespective of their native member state. Based on these principles, common vocabularies on data sets can be agreed upon by different service providers in all member states. Furthermore, depending on standards used by each member state, syntaxes with unambiguous terms can be used in the Cross-Border data exchange, resulting in Cross-Border semantic interoperability.

In this section of the report the proposed Cross-Border processes, policies, and principles for further semantic modeling for Cross-Border eCMR, KYC, an eReceipt will be presented. An eCMR is a digital waybill. KYC is a due diligence process conducted by obliged entities to combat money laundering. eReceipts are digital receipts delivered by a merchant to their customer at the end of a purchase.

These services were not e-government services originally. However, due to the advancement in the digital transformation process in the EU and the push from SMEs, there is growing government interest in these e-Services. This implies these e-Services are of value to both the SMEs themselves and the public authorities that either regulate, control or have vested interest in the delivery of the e-Services. The interest in the development of these e-Services by SMEs and public authorities is evident in ongoing national initiatives and project. The interest was visible in the DIGINNO and DINNOCAP projects, where public authorities and SMEs collaborated to develop these e-Services. Furthermore, there are other initiatives either developed or promoted by either public authorities and/or SMEs. For example, there is visible interest in eReceipts by the Public authorities in Finland eReceipts in Estonia[1] and Finland[2]. Some of these initiatives in Estonia are promoted under the Real-time-economy flagship. There is also interest in eReceipt from public authorities

[1] E-Estonia, (2016) EReceipts take the hassle out of accounting, https://e-estonia.com/eReceipts-take-the-hassle-out-of-accounting/

[2] Finance Finland, (2017) Finnish eReceipt saves money and nature, https://www.finanssiala.fi/en/news/finnish-eReceipt-saves-money-and-nature/

involved in the Nordic Smart government initiative[3]. The interest in eReceipt by SMEs and larger corporations can also be found in the private sector, in the Nordic and Baltic Countries. This in part is via a larger involvement of NETs in this market, but also smaller service providers in Estonia, Finland, Denmark (Storebox) etc. There is also similar interest for eCMR in the transport sector. This is evident in the Digital Transport and Logistics Forum – a Pan EU Public private collaborative stakeholder forum promoting digital transformation in the transport and logistics sector[4]. There was considerable interest in eCMR from public authorities and SMEs in the DIGINNO project. They participated in the protoyping of the eCMR, exchanging data between four countries (Estonia, Poland, Latvia, and Lithuania) in the Digi-proto project, financed by the Nordic Council of Ministers. Similar interest is evident in the DINNOCAP project where the number of countries that joined the prototyping process grew as observers grew. Furthermore, in the DIGINNO project, there was great interest in KYC from KYC providers, public agencies in Latvia and Estonia. The interest in these services has grown in the DINNOCAP project and that is evident in the number of stakeholders from the BSR that gathered to discuss what the principles should be.

The interest expressed by public authorities and SMEs for the selected e-Services indicates that these services are of value to both public authorities and SMEs in the Baltic Sea Region (BSR) and EU as well. Hence the development of the proposed principles presented in this report serves as an input to ongoing interest and discussions by different stakeholder groups in Europe working on developing the semantic framework for these e-Services. The proposals build on the Cross-Border e-Service architecture, and the operational policies developed in the DIGINNO project. The e-Service architectures and operational policies are presented in this report. They are supplemented by inputs to the architecture and the operational suggestions gathered from the more than 130 different stakeholders, via questionnaire surveys and webinars, from the public and private sectors in the DINNOCAP project. Based on these Cross-Border operational policies, rule statements that govern the critical processes in the data exchange process of the three e-Services are presented. These rule statements dictate and provide constraints to the data exchange processes and stakeholder actions within each e-Service ecosystem. In this report, these rule statements are referred to as principles. The critical Cross-Border processes considered in the data exchange process are those about the access of national and Cross-Border critical systems by authorized parties, data exchange between systems (within member states and Cross-Border), data privacy, and data security of these systems. There is however greater emphasis on Cross-Border processes related to system access. These are identification, authentication, time-based, and location-based processes. The latter processes are relevant only for eCMR.

This section of the report will be of benefit to public digitization agencies; eCMR controlling agencies; national registrars; eCMR service providers, KYC utility operators; eReceipt service providers; SMEs in the transport

[3] https://nordicsmartgovernment.org/digitalisation-receipts-boost-finlands-move-real-time-economy
[4] https://transport.ec.europa.eu/transport-themes/digital-transport-and-logistics-forum-dtlf_en

sector (in the case of eCMR); SMEs required by Anti Money Laundry laws to perform due diligence on their customers (in the case of KYC); all SMEs (in the case of eReceipts); Data exchange infrastructure operators, and financial institutions.

1.2. BRIEF DESCRIPTION OF THE 3 E-SERVICES

1.2.1. HIGH-LEVEL DESCRIPTION OF ECMR

A CMR is a waybill with information and instructions regarding the cargo that is being transported by the cargo carrier[5]. It is a strongly regulated document. It is often inspected by controlling agencies such as the police or customs agents who verify that the goods transported are what is documented in the CMR. eCMR serves the same purpose, but the waybill is digital. Hence now we are trying to digitize it. The proposed Cross-Border e-Service is digital. The verifications are performed digitally. The e-Service is delivered via a combination of national eCMR indexes governed and managed by the public sector and private sector eCMR infrastructure. The public sector infrastructure serves as the data-exchange access point for eCMR data transmitted across borders as a cargo truck moves from one jurisdiction to the other in the BSR. The beneficiaries of these e-Services are SMEs who are cargo transporters in the BSR. The service will save time in the verification process.

1.2.2. HIGH-LEVEL DESCRIPTION OF KYC

KYC is a due diligence process conducted by obliged and non-obliged entities during the customer onboarding process. Obliged entities can identify and judge the suitability and risks associated with the customer being onboarded. To ease the process of creating and aggregating customer data for the onboarding process, A KYC utility is proposed. The KYC utility aggregates data from national registers for Politically Exposed Persons (PEP) and third-party sources to create the KYC profile (KYC passport) of the customer. The SMEs benefiting from the e-Service are obliged entities such as financial institutions, gaming companies, and non-obliged entities whose business process calls for conducting due diligence on prospective clients.

1.2.3. HIGH-LEVEL DESCRIPTION OF ERECEIPT

An eReceipt is a digital receipt delivered in a structured, standardized, and machine-readable format. The proposed Cross-Border eReceipt service (delivery) is a four-corner model where Cross-Border data exchange occurs between access points. The issuance of a receipt denotes the end of a transaction. Hence eReceipts will perform the same functions but in an automated manner, making fully digital business transactions possible for SMEs in all sectors of the economy. eReceipt has been one of the building blocks in recent years in the EU

[5] https://unece.org/fileadmin/DAM/cefact/brs/BRS_Waybill_v1.pdf

to move towards the Real-Time Economy. So far, SMEs have had the possibility of automating their internal accounting and auditing processes using ICT. The missing piece of the puzzle has always been the automated data exchange of accounting and audit information between the SMEs and the relevant government agencies such as tax authorities etc. eReceipt has the potential of making it much easier to achieve more automated reporting for real-time structured machine-readable data exchange between SMEs and relevant controlling institutions. This process results in automated accounting processes for SMEs. Receipts will be archived automatically in the entrepreneur's digital accounting systems. Hence, data is entered once, and there is a reduction in bureaucracy and fraud as the transaction, expense account reporting, and auditing processes are automated and occur in real-time.

1.3. HOW THE PRINCIPLES WERE DEVELOPED

The first step to the development of the principles for each e-Service, developed in the DIGINNO project between 2017-2020, was to analyze:

- The data exchange processes relevant for Cross-Border access to e-government systems
- The data exchange principles for each e-Service were developed in the DIGINNO project. The policies provide a structure for which decisions are made in the Cross-Border data exchange processes for each e-Service.

The following were the guiding principles behind the analysis of data exchange processes, data exchange policies, and the eventual development of the principles within the DINNOCAP project in 2021. The focus of analysis as mentioned were data exchange processes, such as identification, authentication, location, time, data security, and privacy. Natural persons and natural persons representing legal persons have to identify themselves and their identity has to be verified digitally. The identification and authentication process also has privacy and security implications. That being that the identified person should not have access to any of the e-Services if they are not authorized by the business process or by law to do so. It is important to note that this may not always be the case for eReceipts. Receipts are anonymous by nature and that might be the case with most eReceipt solutions that do not include receiver identifier information. Nevertheless, the identification and authentication process prevent access to data by unauthorized persons. Aside, from the identification and authentication process, privacy and security are crucial to the smooth operation of the e-Services. It is important that authorized persons only have access, transmit, receive, and or process data within the scope of their authorizations. Hence, the principles of data privacy become important. Furthermore, the various operators of systems within the ecosystem must adopt security measures at the point of authentication and at various data exchange nodes to avoid cyber security incidents. Hence, the security bit was considered in the development of the principles. When it comes to eCMR, transparency on the movement of the cargo from one country to the other becomes vital. Hence, the need for the location and time where various activities occur as the cargo is transported from one jurisdiction to the other.

The second stage involved engagement with public and private stakeholders responsible and operating in these service areas respectively. The stakeholders were from Estonia, Lithuania, Latvia, Poland, Russia (Kaliningrad) Norway, and Denmark. The stakeholder engagement processes were via stakeholder workshops and questionnaire surveys.

Two workshops were organized for eCMR stakeholders in 2021. The first set of workshops was aimed at agreeing on the standards and datasets that should be used for Cross-Border eCMR data exchange. The second set of workshops was on the basic security measures needed for eCMR data exchange. As input to the workshops, there were questionnaire surveys filled out by the eCMR stakeholders. eCMR stakeholders in the

workshop were from Estonia, Lithuania, Latvia, Poland, Russia (Kaliningrad), Norway, and Denmark. The third workshop was a broad workshop with three tracks focused on Semantic Instruments for Interoperable Cross-Border e-Services. Stakeholders in the different showcases (eCMR, KYC, eReceipt) had discussions aimed at agreeing on minimum viable semantic data relevant for Cross-Border e-identification, authentication, and data exchange for those. The focus on identification and authentication attributes is important as it guides against impersonation and fraud, thereby eliciting trust in the service delivery process. The vision of developing a common vocabulary for each e-Service turned out to be overambitious. Nevertheless, the input from the interaction with stakeholders enabled the additional fine-tuning of the principles which in turn served as input to the principles presented in this report.

1.4. THE PROPOSED OPERATIONAL FRAMEWORKS (PRINCIPLES)

1.4.1. THE ECMR OPERATIONAL FRAMEWORK

The proposed Cross-Border eCMR e-Service is a federated data infrastructure, where each national data infrastructure exchanges data using REST API. As seen in figure (1) below there are national data infrastructure owned by cargo companies (private sector) and public agencies (public sector) respectively. The idea behind the service is to ensure that waybills (CMR) are created, stored, transferred, inspected, and validated electronically as the cargo is transported from one BSR country to the other.

Public and private sector stakeholders have vested interest in the implementation of this e-Service. Private sector stakeholders are involved on the supply side, mostly dealing with cargo and logistics (shipping and delivery companies who own their eCMR systems) and eCMR service providers. The demand side cargo and logistic companies do not always own their eCMR system. The public sector stakeholders are government agencies that either act as controlling or enforcement bodies. Examples of such institutions include road transport agencies, the police, tax authority, customs, and other relevant agencies involved in Cross-Border cargo movement.

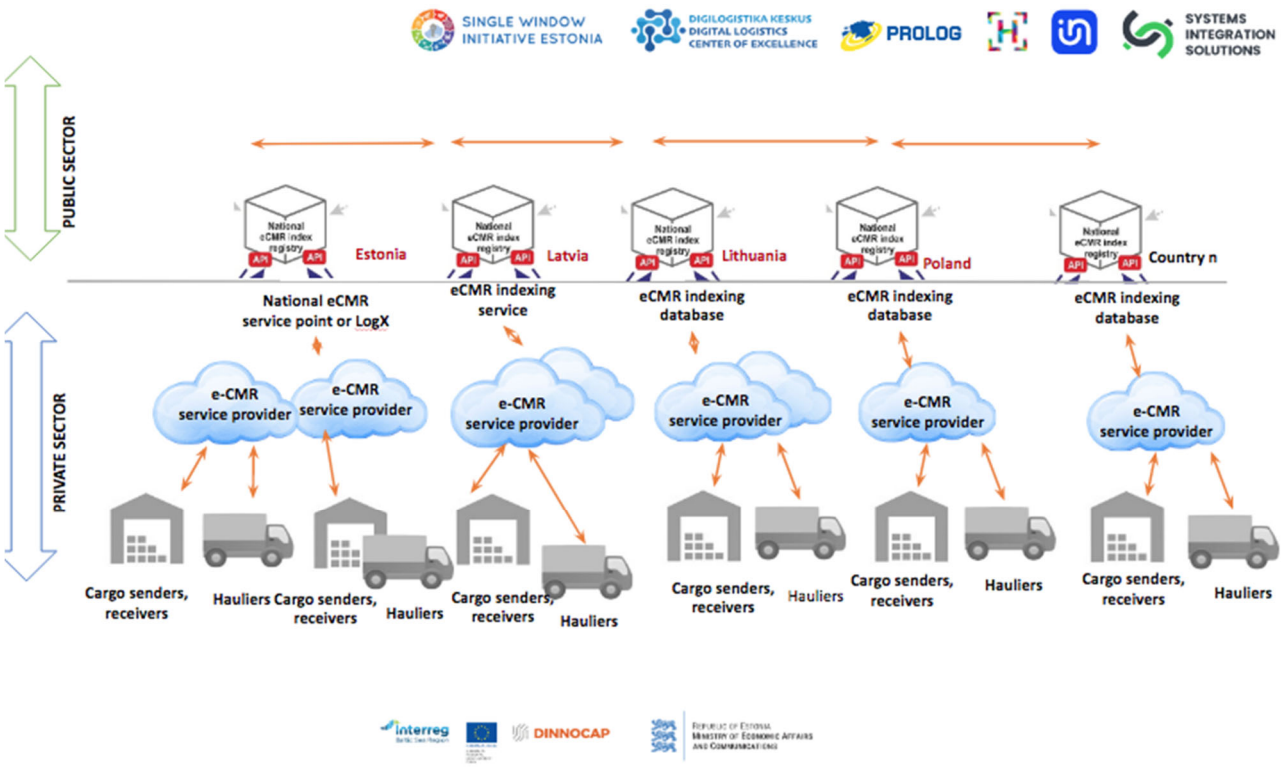

Figure 1. Cross-Border eCMR Architectural data exchange solution.

Source: DINNOCAP project documentation.

The core of the proposed eCMR architecture consists of two ecosystems. The first ecosystem is the national ecosystem where the infrastructure of carriers, consignees, and cargo receivers via eCMR service providers exchange data eCMR with national eCMR indexes (owned by public sector agencies) via an Electronic Data Interchange (EDI). The eCMR service providers serve as the EDI operators and own the EDI platforms. Furthermore, as represented in figure 2, competent authorities that either ensure waybill compliance and/or process the eCMR can exchange data with the eCMR via an API. As expressed in figure 2, the national eCMR indices serve as the national access point for the Cross-Border exchange of eCMR. The second ecosystem is the Cross-Border ecosystem where national eCMR indexes exchange eCMR data as the carrier moves from one jurisdiction to another.

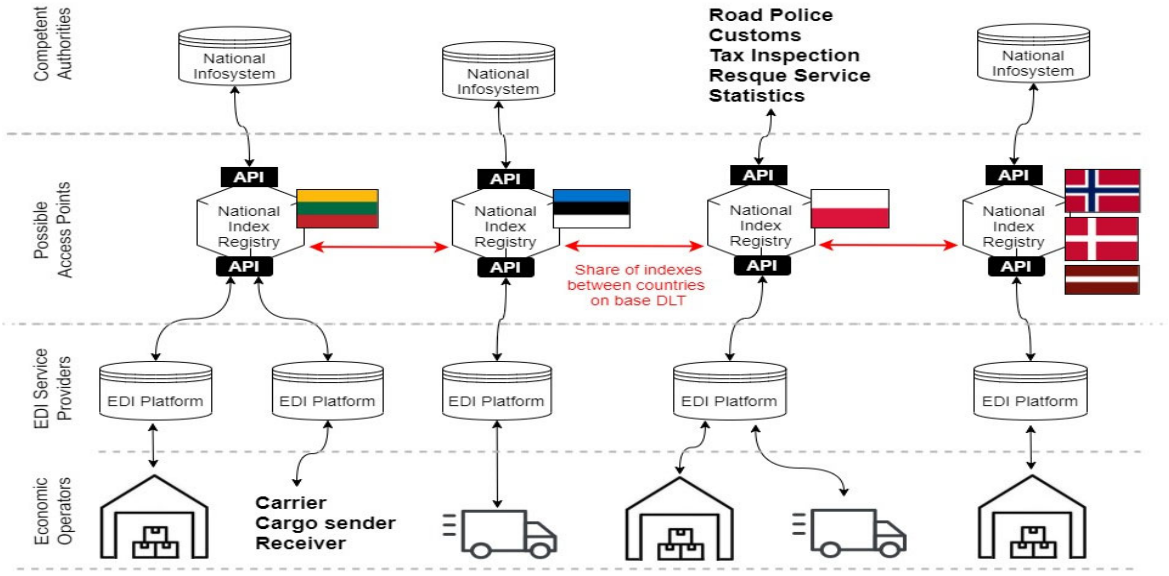

Figure 2. Schema: Cross-Border eCMR indexing ecosystem.
Source: DINNOCAP project documentation.

TRANSACTION FLOW IN THE ECMR INDEXING AND QUERIES

In the proposed system, Carriers (if they own their eCMR system) and eCMR service providers create the eCMR. Their system as well as national indexes store and transmit the eCMR. The eCMR service provider and the Carrier (if they own their eCMR systems) archive the eCMR at the end of the journey. These are the systems in the eCMR ecosystem. In addition to the critical systems are third-party systems, which include, banks, e-courts, SMEs operating within the ecosystem. Data processing occurs in these three classes of systems.

These systems are accessible to natural persons that represent legal persons. The latter could be representatives of, controlling agencies, the eCMR service provider, the carrier, the sender or consignor (if legal persons), or receiver or consignee (if legal persons). Figure 3. depicts the transaction flow and query process for the eCMR between the different stakeholders.

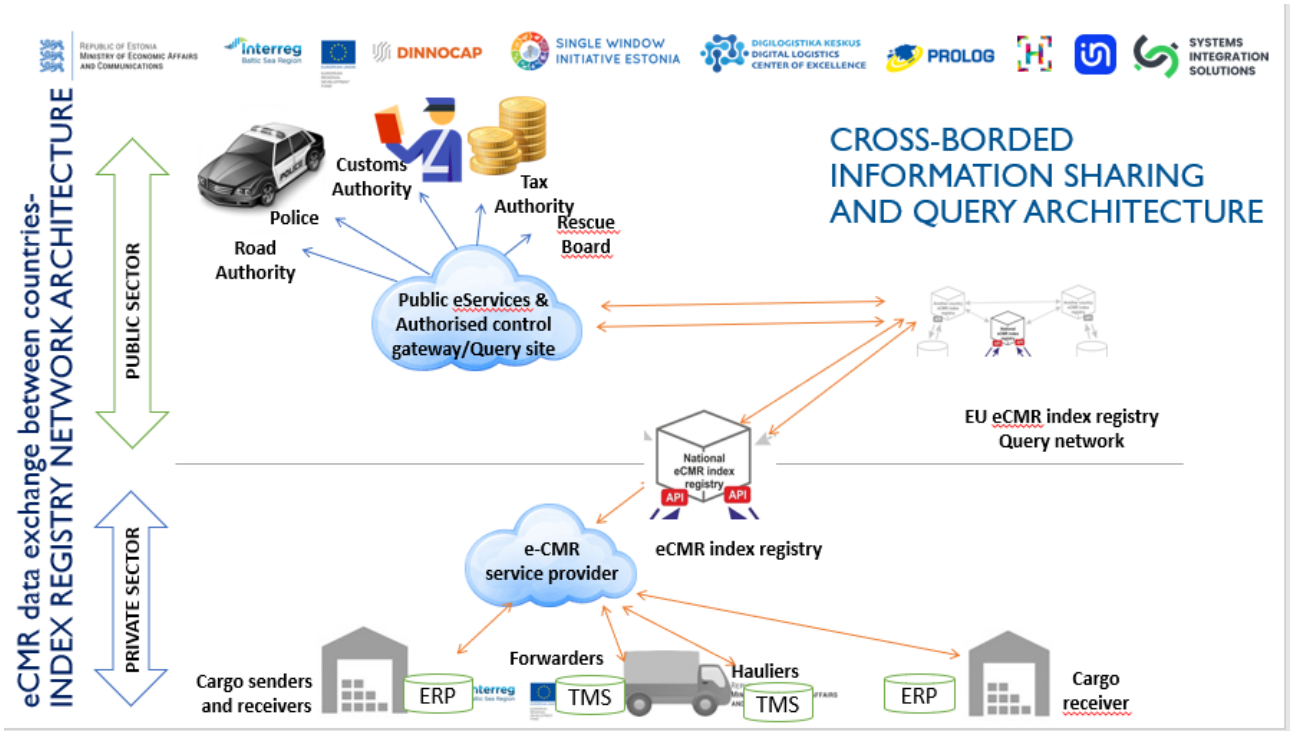

Figure 3: Cross-Border eCMR creation, indexing, and query architecture.
Source: DINNOCAP project documentation

The eCMR process begins with either the carrier or consignor accessing the system of the eCMR service provider to input the datasets required in the eCMR. The inputted data set can be accessed by the consignor, carriers (be they forwarders and/or haulers), and consignee from the system owned by the eCMR provider. The dataset is then from the eCMR service providers system is then parsed to the eCMR index using XML standard. Once the data is an eCMR national index, National controlling authorities and other eCMR national indexes in other countries in the EU can query that national eCMR national index for the eCMR data sets. Controlling authorities can only query national eCMR data sets that are already stored in their eCMR national index. To comply with the once-only principle, eCMR datasets are created once for each transaction and reused via queries from other national eCMR indices.

ECMR CROSS-BORDER DATA EXCHANGE PROCESSES

The eCMR processes for which the principles are developed are data exchange principles. The points of Cross-Border data exchange that require attention include identification, authentication, location, time, data security, and privacy data processes.

1. Proposed identification and authentication process

In the eCMR service, there is a stakeholder proposal on the need for a process of identification and identification of natural persons using the eCMR. The persons could be natural persons such as a cargo sender or natural persons representing a legal person, such as the driver of the carrier vehicle, etc. The identification and authentication processes are important to ensure that only authorized stakeholders have access to the national eCMR index, the databases, and the data query/exchange infrastructure. Secondly, the process enables the verification that an authorized person has the right to access the system in question to make uploads and queries. Currently, the authentication of CMRs is via signature. In the eCMR prototype developed in DINNOCAP, authentication is via username and password. In the proposed system, an e-signature or alternative is proposed. The authentication process is coupled with data security, as the tool used for authentication ought to be secured.

There was no firm agreement on what the common means of identification and authentication by the consulted stakeholders should be. This in part is because of the diversity in the different tools one can choose. For some stakeholders, the use of usernames and passwords created by the authorized user was enough, for others, different levels of authentication were required. Digital ID and timestamps are supported as the next-level authentication method. The use of hyper ledger (in Blockchain) via EBSI (European Blockchain Service Infrastructure) Blockchain, and biometric ID were some suggested identity and authentication possibilities. The challenge with hyperledger is that its level of adoption in the EU is low and Biometrics only secures a part of one's data. Furthermore, the sharing of biometric data across the border is challenging because the personal identity attributes of an individual will be transmitted.

However, there were proposals on the need for a harmonized approach for identification and authentication in the Cross-Border e-CMR process. The preferred solution now is eIDAS. eIDAS provides some form of harmonization in identity and authentication for the eCMR ecosystem. However, in the future EBSI platform can also be applied to the Cross-Border eCMR ecosystem. This will allow additional harmonization of the identification and authentication system for Cross-Border eCMR. The principles developed during the DINNOCAP project are based on eIDAS.

2. Location and time processes

The location and time-based processes go hand in hand with the identification and authentication processes. In the proposed system, the truck is envisaged to load, transport, undergo checks at borders, and deliver cargo. These activities occur at certain locations and at a particular time from the connection to the unloading point. The location-based and time-based processes provide transparency for the cargo sender, the cargo carrier, the cargo receiver, the eCMR service provider, and the different controlling agencies. Hence, the time and location activities have to be identified and verified digitally.

3. Data security and privacy processes

The security of data attributes exchanged in the identification, authentication, location, and time-based processes are important in the proposed eCMR solution. Aspects of data security as described in the identification and authentication of natural persons. This is that unauthorized persons should not have access to the eCMR databases in the eCMR ecosystem. Such unauthorized access could be via a systems breach by cyber-intruder or internal personnel working with any of the eCMR stakeholders. In the eCMR ecosystem, the eCMR service provider can transmit the eCMR to the national index but cannot directly modify the data in the national index. Modified entries from the service provider have to overwrite the previous submission. There has to be a timeframe by which the changes can be made to avoid fraudulent activities. Hence, the authorized person (s) at the service provider end must have their Identity validated before they can access the national eCMR index. Furthermore, authorized agencies can only read the cargo data and not amend data they access from the eCMR index. These measures are relevant to ensure that only authorized persons have access to data as ascribed by the law in the member state. Furthermore, the different systems in the eCMR ecosystem will have to adopt security measures to ensure that their systems are safe and not vulnerable to attacks.

When it comes to privacy, it was difficult for stakeholders to agree on who should have access to user data. Different stakeholders will have different interests in enhancing their services using certain user data. Controlling agencies are required by law to have access to and process relevant data for law enforcement.

OPERATIONAL POLICIES GOVERNING THE PROPOSED CROSS-BORDER ECMR SYSTEM

1. Generic ecosystem system policies

- The eCMR ecosystem should be digital by default.
- Each country should have an access point.
- The access points should operate on common principles on how the eCMR indexes should be built and data from these indexes can be accessed.

2. Operational policies for Cross-Border data flow.

The process policies developed for eCMR for the following process are as follows:

- Identification and authentication policies:
    - The Regulation on electronic identification and trust services (eIDAS)[6] framework, governed by the European Commission supported by European Union Agency for Cybersecurity (ENISA), should be the basis of e-Identification and authentication of natural and legal persons, who are either consignors, carrier agents operating the vehicle, or consignees.

    - Digital/electronic signature and/or seal (e-Seal) standard, which is provided by the same eIDAS framework, must be used to verify the identity of natural and legal persons, who are either consignors, carriers, or consignees.

- Location and Time:
    - Digital timestamp by eIDAS should be used to record the timing of when the eCMR is created, validated at various transit points, and when it is closed. This policy caters to location and time-based identification.

- Data security and privacy

    The technical implementation of eIDAS for identification and authentication processes must take into considerations cybersecurity guidelines provided by the ENISA.

    E-Security standards relevance for eGovernance and secure data exchange must be implemented in data exchange infrastructure.

- General data exchange processes
    - All standards used for Cross-Border eCMR data exchange must be compatible with the international eCMR standard developed by United Nations Economic Commission for Europe (abbreviated UNECE).
    - The data exchange delivery standards should be based on eDelivery and possibly other (building block) standards developed in support of the Connecting Europe Facility (CEF).
    - The indexing format should be standardized.

[6] <eIDAS regulation: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

- Indexing framework could also be implemented using different Distributed Ledger Technology solutions.
- Data sharing and reuse using the once-only principle should be operational in the proposed system.

- Indexing format and standard which are applied in compliance with eGovernance principles,

CROSS-BORDER ECMR OPERATIONAL PRINCIPLES

The Cross-Border principles derived from the policies are those related to system access, eCMR data exchange, eCMR data creation, data query, data security, and data privacy principles.

1. PRINCIPLES ON CROSS-BORDER eCMR SYSTEM

The Cross-Border system access principles are principles on identification and authentication for relevant systems where the eCMR is created, processed, stored, transmitted, and archived.

As mentioned in the policies, these natural persons must be identified and verified before they can access the system. The system also must constrain non-authorized persons from accessing any of the aforementioned systems to impersonate or access eCMR data for which they have no authorization. The system access principles for the aforementioned three classes of systems are as follows.

1.1. Cross-Border system access principles for national eCMR indexes.

A. Identification principles for natural persons representing legal persons and public authorities.
- Every natural person and a legal person authorized to perform transactions in national eCMR indexes must be identified.
- Every natural person and a legal person authorized to perform queries in national eCMR indexes must be identified.
- Every login and registration session by authorized natural and legal persons to national eCMR indexes have to be via the eIDAS framework.
- National eCMR index is not accessible to unauthorized natural persons representing either an eCMR service provider, a cargo carrier, or a public agency.

B. Authentication principles for natural persons representing legal persons and public authorities.
- A verification/authentication process must either follow or simultaneously accompany every identification session at request for every access to national eCMR indexes.

- Authentication sessions for authorized natural and legal persons must be via the eIDAS framework.
- Access to authorized natural and legal persons must be denied for authorized natural and legal persons who cannot be authenticated via eIDAS or other agreed-upon Cross-Border options for authentication.

1.2. Cross-Border system access principles for eCMR service provider systems by consignors, carriers, and consignees

A. Identification principles for natural persons and legal persons
   - Consignors, Carriers/their representatives, and consignees must be identified.
   - Every login and registration session by consignors, consignees, and carriers/their representatives to a service provider's infrastructure must be via an eIDAS application too.

B. Authentication for natural and legal persons
   - A verification/authentication process must either follow or simultaneously accompany every identification session at request for every access to service provider systems.
   - Authentication sessions for authorized natural and legal persons are preferred to be done via eIDAS.
   - Access is granted to consignors, carriers/their representatives, and consignees who can be authenticated via eIDAS or other agreed-upon solutions.

2. CROSS-BORDER SYSTEM ACCESS PRINCIPLES ON DATA CREATION (INPUT) INTO THE ECMR

Data creation is the process of inputting data in the eCMR system to create the eCMR. Data creation occurs in the system of the eCMR service provider. The consignor and the carrier currently create data for existing CMRs and should be able to do so in eCMR. Hence, the data creation principles enforce constraints on who can create data and the mandatory data sets that are important for the data creation process.

The mandatory data were elicited from BSR eCMR stakeholders who suggested data that should be in the eCMR. The datasets are identifiers and cargo-related data sets. The identifier datasets identify the carrier, consignee, consignor, time-based events, location (eCMR creation, loading, transit, and unloading), and location-based events. The principles on data creation are as follows:

2.1. Principles on who should be able to create an eCMR

A. principles on data input to eCMR

- The carrier and consignor only must create an eCMR.
- The carrier and consignor only must be able to edit eCMR
- eCMRs must not be deleted once transportation begins.
- The eCMR must be created in a service provider's system.

2.2. Principles on basic identifiers of natural persons, legal persons, time, location, and means of carriage

A. Principles on data set that accompany consignor's identity (both natural and legal persons)

- Consignor's eCMR must be identified with an identifier (eCMR number).
- Consignor who is the natural person must be identified with a title, first name, and surname
- Consignors who are legal persons must be identified by legal name
- All consignors must provide a street number (optional) street name, Zip code, region, and country
- All consignors who are legal persons must provide their legal code (company registration number)
- All consignors who are legal persons must provide their VAT numbers.

B. Principles on data set that accompany consignee's identity (both natural and legal persons)

- All consignees and/or carriers must identify their consignee in the eCMR.
- Consignees who are natural persons must be identified with personal identifiers such as Gender, first name(s), and surname(s). Consignees who are legal persons must be identified by their legal name.
- Either the Consignor or carrier must document a consignee's address in the eCMR.
- The consignor or carrier must provide the consignee's street number (optional) street name, Zip code, region, and country.
- The legal code (company registration number) of consignees, who are legal persons must be documented in the eCMR.
- The VAT number of the Consignee (if they are legal persons) must be documented in the eCMR.

C. Principles on carrier's Information

- The carrier must identify on the eCMR
- The carriers must document their legal name in the eCMR.
- The carrier must document the legal code (company registration number) in the eCMR
- The carrier must provide a street number (optional) street name, Zip code, region, and country.
- The carrier must document the carrier's VAT code in the eCMR.

D. Principles on carrier's driver

- The vehicle driver must be identified in the eCMR
- The vehicle driver's license must be identified in the eCMR
- The vehicle driver's name on the driver's license must match the driver's name on the eCMR.

E. Principles on the carrier's vehicle

- The carrier's vehicle details must be identified in the eCMR.
- The vehicle's model must be identified in the eCMR.
- The Vehicle's plate number must be identified in the eCMR.

F. Principles on the date, time, and place of issue of eCMR

- All eCMRs must include the date of issue.
- All eCMRs must include the time of issue.
- All eCMRs must include the name of the Service provider who issued the eCMR
- All eCMRs must include the street number, street name, city, region, and country where the eCMR is created.

2.3. PRINCIPLES ON DATA ENTRY ON CARGO INFORMATION, TIME-BASED EVENTS, LOCATION-BASED EVENTS, DELIVERY, AND CLOSE OF CMR

A. Principles on cargo information

- The destination of goods, if different from the consignee's country, must be in the eCMR.
- The place of delivery of goods, if different from the consignee's address, must be in the eCMR
- The goods transported must be described in the eCMR.
- The nature of goods must be documented in the eCMR
- The carrier has the option to indicate if the good is hazardous
- The number of packages of goods transported must be documented in eCMR
- An option for the Gross weight/volume of the goods must be in the eCMR.
- An option for the cost associated with the carriage must be in the eCMR.
- An option for Special instruction on customs clearance must be in the eCMR.
- An option on information on subsequent modification of eCMR must be in eCMR.

B. Principles on cargo location

- The city, region, and country where the eCMR is created must be in the eCMR.
- The time when the cargo departs must be in the eCMR

- The city, region, and country where the cargo will be delivered must be eCMR.
- The time the cargo is delivered must be in the eCMR.
- Cargo stops at transit borders must be updated in the eCMR using data from GIS
- Cargo departure at transit borders must be updated in the eCMR using data from GIS
- Cargo arrival at the destination must be updated in the eCMR using data from GIS
- Cargo arrival at the destination must be recorded as the place of the takeover of goods in the eCMR
- The carrier must update the date of cargo arrival at destination in the eCMR.

C. Principles on cargo delivery
   - At delivery of goods the carrier, in the eCMR, must update the date of delivery of goods.
   - At delivery of goods, the carrier, in the eCMR, must update the date of delivery of goods.
   - At delivery, the status of the eCMR number for the cargo in all service providers and routed national eCMR indexes must be updated as delivered.

D. Principles on close of eCMR
   - The eCMR must close after the carrier updates the eCMR status as delivered.
   - The carrier and service provider must notify the consignee and consignor of delivery of the eCMR.
   - The place of delivery and time of delivery must be communicated to the consignee and consignor by automated messaging.

3. PRINCIPLES ON CROSS-BORDER DATA QUERY

Data query here implies the query of national eCMR indexes. Controlling agencies or authorized public agencies and service providers are permitted to query the national eCMR index. Those stakeholders determine the principles on the query of other eCMR indexes in the eCMR ecosystem. The national eCMR indexes are important because they facilitate Cross-Border data exchange and also serve as access points to the national eCMR ecosystems. Hence there are greater constraints on who should access it to make queries and how. The Cross-Border data query principles are as follows:

A. Principles on Cross-Border data query at transit or end of the journey by an authorized public agency
   - On the query of active eCMR numbers, authorized public agencies at transit borders and the end of the journey must access all eCMR information for that eCMR number.
   - On the query of closed eCMR number, authorized public agencies at transit borders and end of the journey must access not access eCMR information for that eCMR number.
   - A query for closed eCMR must return, “Closed eCMR”.

- Authorized public agencies at transit borders cannot edit or delete eCMR.

B. Principles on Cross-Border data query by the service provider
   - On the query of an active eCMR number, authorized service providers must access all eCMR information for that eCMR number.
   - On the query of closed eCMR number, authorized service providers must access all eCMR information for that closed eCMR number but can only print and not edit it.
   - On the query of active eCMR number, carriers at transit borders and end of the journey must access all eCMR information for that eCMR number. The
   - On the query of closed eCMR number, authorized service providers must access all eCMR information for that closed eCMR number but can only print and not edit it.

4. PRINCIPLES ON DATA EXCHANGE

The operational policy, mentioned earlier, indicates that all data exchange should occur in the eDelivery infrastructure that supports CEF standards. However, the data exchanged must be created and queried by relevant stakeholders before the transfer occurs. First, we present a set of mandatory datasets that can be exchanged coupled with additional datasets. This is followed by process principles governing the creation and query of the eCMR datasets in an eCMR transaction process. The eCMR process and the proposed eCMR policies inspire the process principles.

The selected data sets.

These are data sets that are seen as relevant for eCMR from the loading point, through transit points to the end of the journey. The XML syntaxes are not included here because they are already defined in the relevant standards.

Table 1. ECMR DATASETS HIGHLIGHTED AS NECESSARY FOR CONTROL AND USE IN THE ECMR AS SUGGESTED BY ECMR STAKEHOLDERS IN THE DINNOCAP PROJECT

Data set	Data description	CMR data field nr
Number of eCMR	This is a unique ID that is unique to the eCMR	On CMR
Name of consignor	This is the name of the cargo sender. The sender could be a natural or legal person.	1
Address of consignor	This is the address of the cargo sender.	1
Country of consignor	This is the address of the cargo sender.	1
Legal code of consignor	This is the business registration code of the cargo sender. This option is only for legal persons.	Not currently on CMR

VAT of consignor	This is the VAT number of the cargo sender. This option is only for legal persons.	Not currently on CMR
Name of consignee	This is the name of the cargo receiver. The receiver could be a natural or legal person.	2
Address of consignee	This is the address of the cargo receiver	2
Country of consignee	This is the country of the cargo receiver	2
Legal code of the consignee	This is the business registration code of the cargo receiver. This option is only for legal persons.	Not currently on CMR
VAT of consignee	This is the VAT number of the cargo sender. This option is only for legal persons.	not currently on CMR
Place of creation of consignment note	This is the location of the service provider or carrier whose system is used to create the eCMR.	21
Date of creation of consignment note	This is the date indicating when the eCMR was created	21
Place of the takeover of Goods	This is the location where the cargo was picked up	3
Date of the takeover of goods.	This is the date indicating when the cargo was picked up	3
Destination of goods	This is the country where the goods will be delivered	2
Place of delivery of goods	This is the exact location where the goods will be delivered.	4
Time of delivery of goods	This is the exact time when the goods are delivered at the place of delivery	24
Number of packages	This is the quantity of cargo being transported	11
Description of packages	This is a description of the cargo being transported	10 - 15
Nature of goods	This is an indication of the type of cargo being transported. For example, if the cargo is hazardous or not.	9
Gross weight/volume	This is an indication of the weight of the cargo being transported	14
Name of carrier	This is the name of the carrier (a legal person).	6
Address of carrier	This is the address of the carrier	6
Country of carrier	This is the address of the carrier	6
Legal code of carrier	This is the business registration code of the carrier	Not currently on the CMR
VAT of carrier	This is the VAT number of the carrier.	Not currently on the CMR
Date of issue of eCMR	This is the date on when the eCMR is created.	Not currently on the CMR
Time of issue of eCMR	This is the time when the eCMR is created	Not currently on the CMR
Vehicle and trailer number	This is the license plate details of the carrier's vehicle transporting the cargo.	10
Vehicle and trailer model	This is the brand model of the carrier's vehicle transporting the cargo.	10
The cost associated with carriage	These are costs associated with the monetary value of the cargo.	17 and 19
Necessary instructions regarding custom clearance and other formalities	These are instructions provided by the consignor as regards the clearance of goods by customs.	18
Information on subsequent modification of consignment note.	These are written descriptions highlighting modifications and reasons for such modifications in the eCMR.	Not currently on the CMR

The datasets presented in table one are some of the suggested datasets some public agent stakeholders in the BSR would like to see in an eCMR. It is important to note that the EFTI datasets proposed for 2024 will override the proposed data sets. However, these datasets are proposals that could serve as inputs to the compilation of the EFTI datasets.

The stakeholders consulted were from the following agencies. The Polish customs authority, the Polish Road Transport Inspectorate, the Polish Ministry of Infrastructure, the Polish Road Transport Inspectorate, the Polish state border guard service, the Lithuanian State Road Transport Inspectorate, the Lithuanian State border guard service, the Lithuanian State Tax Inspectorate, the Lithuanian customs authority, The Estonian Police, the Estonian Transport Administration, the Estonian State Tax Inspectorate, the Estonian Customs Authority the Estonian State border guard service, the Estonian State border guard service, the Estonian Road Transport Inspectorate, the Estonian Customs authority, Danish Organization for Road Transport (ITD), Central Statistical Bureau of Latvia, The Latvian State Tax Inspectorate, the Latvian Customs authority, and the Latvian Financial Crime Investigation Service.

The responses provided in table 1 are not the official opinion of the agencies but the individuals that provided feedback to the DINNOCAP project on the datasets.

The suggested datasets consist of datasets that are currently in the CMR document and those datasets that are not in the CMR. The datasets also denote fields in the proposed eCMR required by respondents working in controlling agencies in Latvia, Estonia, and Lithuania and an industry organization from Denmark as listed in the previous paragraph. The proposed eCMR data sets that are not in the current CMR include the legal code of the consignor, VAT of consignor, legal code of consignee, VAT of consignee, legal code of career, VAT of career, time of issue of the CMR, and date of issue of CMR. These are data sets found relevant by the respondents from the following agencies: Polish customs authority, the Polish road transport inspectorate, the Polish state Border guard service, the Lithuanian state tax inspectorate, the Lithuanian customs authority, the Lithuania state border guard service, the Lithuania state transport inspectorate, the Lithuania police, the Estonia customs authority, the Estonian transport administration, the Estonian police, the Estonian tax inspectorate, the Estonian Customs Authority, the Danish organization for road transport, and the Latvia state tax inspectorate. The datasets of relevance to the respondent from the Latvian central statistical bureau were the legal code of the consignor, VAT of consignor, legal code of consignee, VAT of consignee, legal code of career, VAT of career. This dataset related to the legal code and the VAT is because of the expectation that eCMR national registries will exchange data with national registries as expressed in figures 1, 2 and 3. Hence the datasets associated with legal code, and VAT serve as additional identifiers for the consignee, The relevance of the proposed dataset related to the date and time of issue of the CMR is to enable timestamps of events as the goods to be delivered moves from one country to the other. It also denotes when the eCMR is active. The eCMR ends and is archived when the goods are signed and delivered by the consignee.

The fields in the current CMR proposed for the eCMR by the respondents are fields 1, 2, 3, 4, 6, 9, 11, 10-15, 17, 18, 19, 21, and 24. It should be noted that the respondents only selected dataset fields they (as individuals within organizations and public agencies) prioritize. Only a few respondents that represent the agencies did not prioritize all data sets in table 1. In Poland, the respondent from the ministry of infrastructure preferred to go with datasets that align with the UNECE's datasets on eCMR. The basis is that the UNECE datasets provide a more universally accepted framework for eCMR data exchange. The dataset on the "*place of destination of goods*" was not proposed by the respondent from the Lithuanian Customs authority. The dataset on the "*number of CMR*", the unique identifier for the CMR, was not proposed by a respondent from the Estonian border. The respondent from the Latvian central statistics bureau was not interested in the identity of the sender, but in the type of goods, the origin, transit, and destination of the goods, and the carrier of the goods.

Nevertheless, the proposal in table 1 provides suggestions of what the data fields that each of the represented agencies will require in the eCMR.

The proposed datasets are already standardized in the UN CEFACT Multi-Modal standards (developed by UNECE). UNECE holds a full set of standards for global shipping trading, forwarding, multi-modal transport, and environmental holding. The advantage of UNECE is that UNECE standards are free. Standards such as open PEPPOL GS1 and UBL reuse some UN CEFACT data sets. This makes it possible for service providers to fulfill the EFTI regulation requirement of delivering eCMR in a technology-neutral ecosystem.

5. PRINCIPLES ON DATA SECURITY AND PRIVACY

As mentioned earlier, data security and privacy, principles are important. The operational policy suggests the use of cybersecurity guidelines provided by the European Union Agency for Cybersecurity (ENISA)[7]. This is relevant to prevent a breach of national eCMR indexes and systems owned by eCMR service providers. A breach could occur via system access procedures or intrusion via third-party systems. Hence there is a need for principles that will enhance data security during system access and when interfacing with third-party systems. The privacy-related principles are GDPR dependent.

The data security and privacy principles are preferred to be as follows:

5.1. Principles on data security

- Only natural and legal persons authorized can access national eCMR indexes.
- Only natural and legal persons authorized by national laws can access eCMR data in databases owned by service providers.

[7] European Union Agency for Cyber security. https://www.enisa.europa.eu/

- in transit, anyone must have designated authorized persons who can edit eCMR data.
- Request to edit or delete eCMR by a carrier can only occur, once the eCMR is active.
- All databases (service provider, national eCMR indexes) must implement firewalls to prevent hacking.
- eID assurance level at authentication must either be the same as or above national eIDAS assurance levels.
- Dealing with system compromise must be in line with the GDPR 72[8] hour requirement.
- To minimize social engineering, the interaction between service providers, carriers, consignees, and consignors should be app-based.
- The use of third-party services is optional but must be well coordinated.

5.2 Principles on data privacy (Principles on access to personal data)

1. Access to user data on eCMR service provider accounts
   - Consignors must only access personal data related to their eCMR (account) (if any) and eCMR transactions they performed.
   - Consignees must only access personal data related to their eCMR account (if any).
   - Carriers must only have access to personal data in their eCMR accounts and eCMR numbers for transactions they performed.

2. Principles on the right to inform
   - National eCMR indexes must notify Cross-Border carriers, consignees, and consignors once they receive or delete personal data from other national eCMR indexes.
   - eCMR service providers must notify Cross-Border consignees when they (eCMR) receive and delete their personal data.
   - Carriers must inform consignees when they (eCMR) receive and delete their personal data.
   - Data exchange operators must not inform either consignees, consignors, or carriers when they receive or delete personal data.

3. Principles on the processing of personal data
   - Only eCMR carriers, eCMR service providers, eCMR national indexes and authorized public agencies can process eCMR personal data.

[8] General Data Protection Regulation. https://gdpr.eu/

- eCMR service providers are not permitted to process eCMR personal data for reasons beyond the use of personal data to improve their eCMR services delivery.
- eCMR service providers must not process eCMR personal data without the written consent of the data owner (carrier, consignee, or consignor).
- eCMR national indexes are not permitted to process eCMR personal data for any reason without the written consent of the data owner (carrier, consignee, or consignor).
- Data exchange operators are not permitted to process eCMR personal data except when needed to facilitate data exchange of eCMR.

1.4.2. THE KYC OPERATIONAL FRAMEWORK

The Cross-Border KYC is an innovation that utilizes the possibilities of resource sharing based on KYC data across borders in the BSR to combat Money laundering and illegal funding of terrorism. The proposed system consists of national KYC utilities (As seen in figure 4) that identify and verify the client as well as verify the risk status of the client based on prior information about the client in national registers, systems owned by obliged entities, and third-party sources.

Stakeholders involved in the proposed KYC Utility ecosystem include:

1. The owner of the KYC utility: The owner of the KYC utility could be a public or private agency depending on the national laws that determine who should own the utility. Hence, the stakeholder operating the utility is not fixed.

2. The client (user): In the proposed system, the client is either a natural person or a natural person representing a legal person. The client is a legal resident or citizen of an EU or BSR member state. In the KYC stakeholder workshop held in the DINNOCAP projects, the clients were further classified. The client could either be:
    a. Natural persons who are either, private persons (who are citizens of an EU member state); private persons (who are not citizens but possess residency status in EU member states); and private persons (who are non-residents from a third country). However, the current design of the KYC utility does not cater to the latter from the third country.
    b. EU Legal persons who are represented by natural persons either, citizens of the EU member state; non-EU-citizens but legally resident in an EU member state; or non-EU-citizen from a third-party country.
    c. Non-EU legal persons who are represented by natural persons from third party countries who are not legal residents in the EU. The system does not cater to them either.
    d. Sole proprietors who are citizens of either the EU member states or are legal residents of the EU member state.
    e. Sole proprietors who are not legal residents in the EU member state. The system does not cater to them.
    f. Natural persons who are either citizens, legal residents of the EU member state, represent public authorities.
    g. Public authorities not domiciled in the EU. The system does not cater to them.

3. Obliged entities: These financial and non-financial institutions are obliged by Anti-Money Laundry laws and Combating Financial Terrorism (CFT) laws, in each member state, to conduct due diligence before onboarding clients.

4. Non-obliged entities: These are organizations and institutions that are not obliged to conduct due diligence to onboard clients but perform due diligence but do so for good business practice or as a form of risk assessment.

5. Third-party sources: These stakeholders host additional data sources needed for the KYC due diligence process. These include data hosted by these sources include sanctions lists, lists of Politically Exposed Persons (PEP), Media sources, and other data needed to either verify and/or perform a risk assessment on the client.

6. National registrars: These public sector agencies host various national public registers with relevant data needed for KYC processes. These registers include population registers, debt registers, tax registers, etc.

TRANSACTION FLOW IN THE PROPOSED KYC UTILITY.

To understand fully the transaction flow, how data is exchanged in the KYC Utility ecosystem is described. This is followed by a brief description of the transaction flow or how the proposed KYC utility works.

1. Overview of Data exchange in KYC utility technical architecture:

The high-level technical architectural framework for the proposed KYC ecosystem is presented in figure (4) below. The proposed KYC ecosystem is a decentralized ecosystem consisting of different sub-ecosystems. The sub-ecosystems are KYC ecosystems of the member states. As mentioned earlier, the KYC utilities serve as the national access points in the sub- ecosystems. In each sub-ecosystem, the relevant national registers and systems owned by obliged entities are interconnected using data exchange infrastructure.

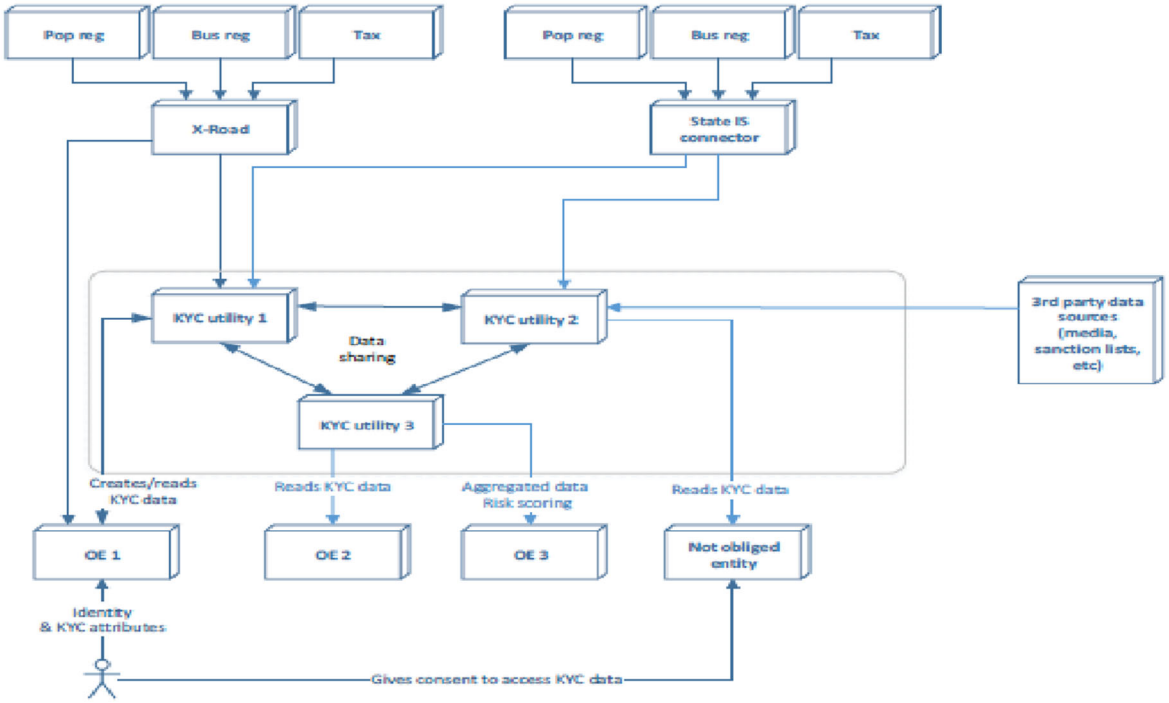

Figure 4. Main working principle of a Cross-Border KYC utility
Source. DIGINNO KYC feasibility studies

The data exchange infrastructure is technology neutral. As an example, in figure 4, in one sub-ecosystem the Estonian X-road infrastructure is used. While in another sub-ecosystem, another data exchange infrastructure is used. The different relevant registers and KYC systems owned by obliged entities supply to update the KYC utility with KYC information of prospective clients using the data exchange infrastructure. Data on the client are also extracted from third-party stakeholders are, based on agreed-upon Service Level Agreements (SLA) between the KYC utility and the third-party source also supplied to the KYC utility. The KYC utility aggregates the supplied information to create a KYC profile (KYC passport) of the client. To comply with the GDPR the compiled passport is performed when there is a request from an obliged or non-obliged entity. The data compilation is automated. However, once the passport is created in the KYC utility, it is stored there and can be reused when requested.

2. Transaction process in the KYC utility ecosystem

The transaction process begins with the onboarding process by an obliged entity. The obliged entities have various onboarding processes. In some cases, the client must be physically present when obliged entities conduct due diligence, in other cases, the client has to provide certified documentation online or physically. Such documents used in the identification and verification of the client and his/her background are uploaded to the KYC utility where the client's profile is either created or updated. When that client travels to another member state to consume a financial service, for example, the financial institution will then issue a query to

their national KYC requesting the KYC data of the Cross-Border client. That KYC utility will forward the request and retrieve the needed information from the client's national KYC utility. The client's national KYC utility will enrich the existing KYC passport, created by the obliged entity from the client's member state, with additional information from national registers and third-party sources - based on the parameters in the request -, and forward the updated KYC profile to the requesting national KYC utility. The financial institution will then read and store the information retrieved in their systems. If the KYC information provided by the KYC utility is not sufficient for the bank either because of their KYC procedure or legal requirements, they can conduct due diligence for the missing aspects and update the KYC utility. Hence, the obliged entities play a critical role in processing KYC data and updating the KYC profile of the client.

Non-obliged entities also have access to the KYC utility, but they can only query and read the KYC data of the client. They can neither edit nor update the KYC data of the client.

There is an obvious conflict between the consent principles in the GDPR and KYC. The GDPR empowers the client to decide if their data should be processed or otherwise. However, articles 6 and 7 of the GDPR, empower the processing of personal data without the consent of the user if it is required by law. AML/CFT laws require KYC for clients who consume financial services and services offered by non-financial obliged entities. Hence, when a client agrees to consume such services, the user can trigger different articles in the GDPR but the clients' consent is not required in the further processing of his/her personal data as long as it is performed as part of KYC. The client can only withdraw such consent by deciding not to consume the service.

CROSS-BORDER KYC DATA-SHARING PROCESSES

The Cross-Border data sharing process relevant for KYC is identification, authentication, data security, and privacy. Time and location-based principles were not relevant.

1. Proposed identification and authentication process

Critical Cross-Border processes for KYC include the identification and verification of the client and the risk assessment of the client. The risk assessment also consists of different verification processes. The initial Idea in DIGINNO was for the KYC passport to save as a means of identification and verification of clients based on harmonized minimum data sets. However, further stakeholder input from the DINNOCAP project indicates that that process might be difficult. This is because current legislation in some EU member states supports third-party verification processes. An example could be certifications from the court. In the stakeholder consultation process, stakeholders proposed the need for flexibility in how obliged entities identify and verify the identity of prospective clients. Anything that an individual obliged entity felt is not enough to identify a

person was seen as invalid. Hence, obliged entities proposed further means of identifying and verifying a client besides the identity extracted from the KYC utility. Suggestions on how this could operate include:

- Virtual identification (computer verification)
- Physical verification via meeting in the same room checking documents (2 persons sit in the room).
- Digital verification (digital id, digital signature).
- The combination of physical with virtual id (This is because some obliged entities do not trust KYC using the camera).
- Facial recognition if possible.

Hence, in some cases, the KYC profile could be enough in the case of virtual ID, digital verification, or facial recognition. However, in other cases, the hybrid approach of Identification based on a minimum dataset should be enough. Obliged entities can choose the means of identification they feel comes with a high assurance level.

However, when it comes to the verification of the identity of the client, the stakeholders proposed three approaches. Two of them are the use of digital signature for verification and authentication from a state register can be implemented in the KYC utility. The third approach was the verification by a third party if required by the obliged entity. This was important for some obliged entities because the verification of the individuals the obliged entity can trust was deemed important. However, the verification must reflect somehow in the KYC utility to indicate that a third party has verified the client.

Based on the adoption of this approach, obliged entities can constantly update the client's KYC profile in the KYC utility. This, at some point, will make the KYC profile the standard "passport" for KYC in the BSR.

The KYC utility also supports aspects of risk assessment processes. However, constant update of the profile also makes the profile a rich source for conducting a risk assessment on clients.

2. Privacy and security process

As mentioned earlier, the KYC ecosystem is a decentralized ecosystem. In each system, there are sub-systems. There is the KYC utility, the national registers, the obliged entities systems, and third-party systems. These systems are interconnected with one another. In this systems data creation, data processing, and data exchange/mutual recognition of data between the systems; and data storage in the individual systems, occur. As these systems are interconnected, the cyber vulnerability of one of these systems will have an impact on the KYC system. Furthermore, the integrity of the KYC system depends on its robustness when it comes to data security and privacy during the aforementioned process. Hence, cyber security measures and principles on data creation, data processing, data exchange are important.

OPERATIONAL POLICIES FOR KYC

The operational policies proposed to govern the development of Cross-Border KYC are as follows:

- Datasets/profiles are created which include a minimum list of questions, documents, and collectible data that are needed to conclude KYC (i.e., shall be listed which data will be collected from the 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.)
- All data-exchange must be done in a machine-readable way using the best practice for data transmission framework (i.e., possible data exchange standards XML, XBRL, JSON, or other)
- 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 confirms that 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 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 the 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 been created, is interoperable in all cases where obliged entities want or need to carry out KYC.
- It shall be created on a once-only principle and updated (incl. automatic updates) every time the profile is used again, no massive database shall be built
- Person should have access to the information who has used his (KYC)data and for what purpose
- Person itself should have the possibility to share/send his/her KYC data.

The first point in the policy is deemed valid but the amendment on the flexibility in approach to identification is taken into consideration.

OPERATIONAL PRINCIPLES FOR CROSS-BORDER KYC

The Cross-Border principles derived from the Cross-Border KYC policies borer on Identification, authentication, data security, and privacy.

SYSTEM ACCESS PRINCIPLES

A. Access to KYC utility

- Obliged entities, non-obliged entities, and state registrars should have direct access to the KYC utility.
- Obliged entities should possess read, write, and edit privileges to the KYC utility.
- State registers should only possess read and write privileges to the KYC utility.
- Non-obliged entities should possess only read privileges in the KYC utility.

B. Access to state registers

- Obliged entities should have direct access to state registers for manual data verification purposes.
- Obliged entities should have only read privileges in state registers.

KYC UTILITY PRINCIPLES

1. Identification and authentication principles for client data stored or uploaded to the KYC utilities.

A. Principles on valid eIDs of EU/BSR resident natural and legal persons, during the onboarding process via the KYC utility.

- Natural persons with EU/BSR recognized eIDs can be onboarded via identification data extracted from the KYC utility.
- Legal persons with EU/BSR recognized eIDs can be onboarded via identification and verification data extracted from the KYC utility.
- Data from natural persons with EU/BSR recognized eIDs must be uploaded or updated in the KYC utility.
- Only data from natural persons with EU/BSR recognized eIDs must be uploaded or updated in the KYC utility.

B. Principles on valid means of verification for EU/BSR resident natural and legal persons, during the onboarding process via the KYC utility.

- Verification of natural persons and natural persons representing legal persons can be by e-signature.
- Verification of natural persons and natural persons representing legal persons can be by from national population register or relevant register of the member state where the client either resides or is a citizen.

C. Principles on additional identification and verification of natural and legal persons during the onboarding process.
   - Information in the form of documentation on either third-party verification, verification via physical meeting, or additional digital verification must be uploaded to the client's profile in the KYC utility as an attachment.

2. Principles about the KYC profile in the KYC utility

1. Minimum mandatory datasets on the structure of KYC profile.
   - Datasets/profiles in each Member States' KYC utility must be created which include a minimum list of questions, documents, and collectible data that are needed to conclude KYC.

2. Additional datasets in the structure of the KYC profile.
   - Additional data sets, documents, and collectible data updated from previous KYC processes must reflect in the KYC profile of the client.

3. Principles on creating KYC Profile (AML passport).
   - Obliged entities and licensed entities (e.g., credit institutions, audit firms, credit bureau, service provider, etc.) will be allowed to create and update the profile for natural and legal persons in the KYC utility.

   - The client may indirectly create a profile in the KYC utility using the obliged entities interface. This principle is at the discretion of the obliged entity.

   - Updates on client data in the national register, systems owned by obliged entities and third party stems about a client, already listed in the KYC utility, must be automatically updated in the KYC utility.

   - KYC utility profile (AML passport) of natural and legal persons in a member state must be automatically updated whenever there is new data for these persons in other KYC utilities.

4. Principles on retrieving KYC data from the KYC utility.
   - Only obliged entities and non-obliged entities should be able to read client data directly from the KYC utility.
   - Data retrieval is via a search query based on search parameters decided upon by the KYC utility.
   - The client can only access his/her data from the obliged entity's system.

- The search parameters for the client's access to his or her data must be provided by the obliged entity.

5. Rule on the accuracy of data from Government registers in the KYC utility.
    - The relevant must confirm that it owns the data with attestation on the validity of the data supplied to the KYC utility.

KYC DATA PRIVACY AND SECURITY PRINCIPLES

These are principles that pertain to all systems in the KYC utility ecosystem.

Principles on data ownership and sharing

- Natural persons may have unrestricted access to his/her personal data.
- All systems in the KYC utility system may inform the client on who has used his/her (KYC) data and for what purpose.
- Obliged entities and the KYC utility must enable natural persons to share/send their KYC data.
- Authorized representatives of legal persons may have access to the data of the legal entity.
- Authorized representatives of legal persons may be notified on who has used his/her (KYC) data and for what purpose.

KYC PRINCIPLES ON DATA EXCHANGES

- Only structured, machine-readable data are to be exchanged.

1.4.3. THE ERECEIPT OPERATIONAL FRAMEWORK

Receipts are provided at the end of a retail sales transaction. They serve as evidence that a transaction has occurred and is finalized (including payment) or in other words, the payment is done. Receipts, just as invoices are used for audit and accounting purposes. eReceipts as mentioned earlier are digital receipts delivered in a structured, standardized, and machine-readable format. All fields in an eReceipt are processed digitally without human effort. This implies that private persons, relevant public (tax agencies, etc.), and private stakeholders in the auditing, accounting, and tax reporting process can transmit and receive data on a particular purchase in real-time. The proposed system will enable real-time data exchange across borders, enabling the creation, transmission, and accounting reconciliation of eReceipts.

The proposed system, developed in the DIGINNO project, is a decentralized system where the systems in each member state are operated in a 4 corner of 4 party model. In the model, the parties (stakeholders) are the "the Seller", "the Buyer", "eReceipt operators" and "eReceipt, Sellers (point-of-sale)". The Seller is a commercial entity providing a service. They issue the eReceipt at the end of the service to the customer from their point-of-sale system. The point-of-sale can also be a third-party provider (for example Square) to which the Seller subscribes. The point-of-sale system transforms the structured machine-readable data produced per transaction into an eReceipt. The eReceipt, at the point-of-sale, is enriched with the e-address of the Buyer's eReceipt operator and the Buyer's user id. The eReceipt is then forwarded from the Seller's own point-of-sale or third-party point of sale to the Sellers' eReceipt operator as expressed in figure (5) below.

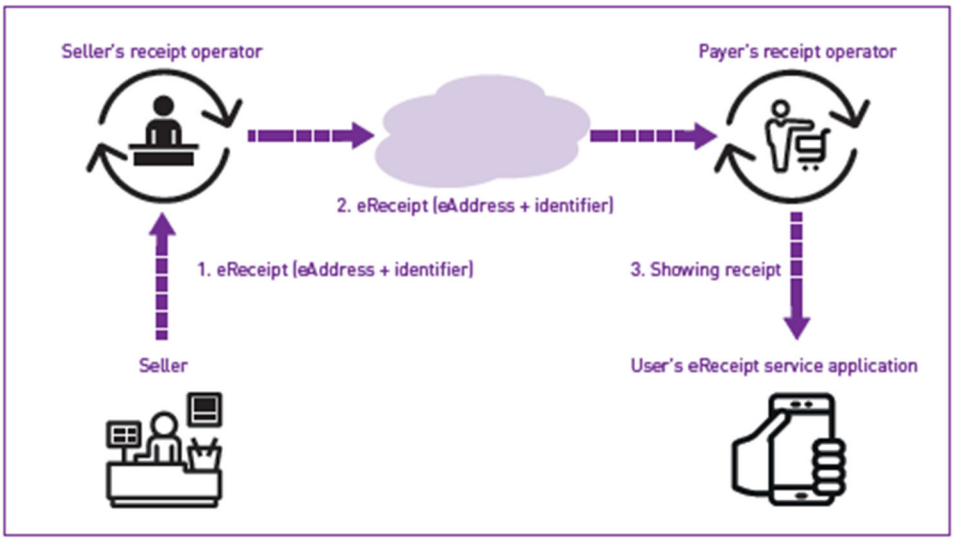

Figure 5: eReceipt four corner model ecosystem.
Source: Technology Industry of Finland[9]

[9] EReceipt guidelines.
https://teknologiateollisuus.fi/sites/default/files/file_attachments/2018_ekuitti_eng_sisus_vedos_6.pdf

The Seller eReceipt operators (service providers) then exchange data of the transaction with the Buyer's eReceipt operator (service provider) via an eDelivery network. An example of such an eDelivery network is PEPPOL. PEPPOL's disadvantage is that it does not support eDelivery to natural persons. Nevertheless, the routing in the data exchange process is guided by the e-addresses generated based on the information on the Buyer's eReceipt operator and user ID extracted at the point-of-sale from the Buyer. Once the eReceipt is delivered to the Payer's eReceipt provider, the Buyer is then able to access the eReceipt from his/her subscription account with the service provider using his/her user id. The proposed system enables the Seller to perform B2B and B2C transactions as well as automatically file VAT claims.

THE TRANSACTION FLOW OF ERECEIPT

This is how the system works nationally. A Buyer makes a purchase. The basic transactional information on purchase made is transmitted, as structured machine-readable data, to relevant agencies such as the tax authority, business registrars, and any other public agency that requires accountability from the Seller. The structured machine-readable data originates from the Seller's point-of-sale at the time of purchase. The information exchange is made by the eReceipt operator (access points) who also routes the information from the respective Sellers' point-of-Sale to the eReceipt service provider for which the Buyer is a subscriber.

The point-of-sale aggregates the data on the purchase received into an eReceipt where the user can access on their mobile device and the Seller can access on the device they use for accounting. As the Seller and Buyer continue to conduct a transaction on both ends, they do not only receive the eReceipts, but automated accounting processes are going on for the Buyer and Seller provided by the point-of-sale. If the relevant government agencies, who also receive the eReceipt data, either also use the services of the point-of-Sale or possess their automated accounting process based on data received from the eReceipt operator, then they join in the Real-time economy activity.

In the DIGINNO and in the DINNOCAP projects, it is proposed that the point-of-sale (if it is a third party) and the service provider ecosystems should be a competitive environment. Here the Seller and the Buyer can decide on subscribing to the eReceipt operator (Service providers) of their choice. If the Seller is subscribed to a third-party point-of-sale, they can also decide which point-of-sale provider they will subscribe to. Furthermore, the eReceipt operators (service providers) and third-party point-of-sale, should be able to decide on which eDelivery networks they subscribe to. Routing as mentioned earlier is an e-addressing.

The eReceipt ecosystem presented in figure (5) is the framework that serves both national and Cross-Border eReceipt systems. The proposal from DINNOCAP, in that regard, is that some member states may opt for national access points that interconnect eReceipt operators (service providers) in their respective jurisdictions.

The national access point also possessed its e-address. Hence, if a Cross-Border client purchases in one EU member state, their purchase information will be routed to the Buyer from the Seller's point-of-sale to the Seller eReceipt operator using an e-address network to the Buyer's eReceipt operator via a national access point to the Buyer's eReceipt operator and user id. The national access point could be one of the existing eReceipt operators or a newly established eReceipt operator mandated to serve as an access point. The user's ID is tied to the user's means of payment. The proposed eReceipt is expected to work on all payment instruments; hence, the user does not need to be restricted to one means of payment.

ERECEIPT OPERATIONAL POLICIES

To implement the proposed Cross-Border eReceipt service, the following policies were proposed in the DIGINNO project.

- The Buyer must have the right to select which receipt service provider of their choice.
- The merchants (Seller) can choose the receipt service provider, or they can also select a payment terminal service to forward the eReceipts.
- The form of the eReceipt should be standard. This can be either an agreed-upon standard between the Seller, eReceipt operator, and the Buyer or, bilateral standards agreed upon by eReceipt operators within a member state and/or Cross-Border eReceipt operators.
- The operating model should be the four-corner model. Closed three-corner models are also possible, but these must be able to provide information outside the system or receive it from outside if required. The Three-corner model is not acceptable for Cross-Border services and prototyping.
- The operating model should be open to new eReceipt service providers who meet the criteria.
- The eReceipt should be viewable in the display application "quickly enough" after the payment.
- EReceipt processing must comply with the eIDAS regulation, GDPR, and European Data Protection Board (EDPB) guidelines.

Operational policy suggestions from DINNOCAP input from the ongoing development of CEN-EU standards and stakeholders.

1. Operational policies on standard and minimum data sets

- Data sets needed from eReceipt should be based on upcoming EU standards.
- Ecosystem standards used for eReceipt in each member stated mapped to the dataset must that agreed upon by CEN. (Based on input from the stakeholder workshop in DINNOCAP, there were suggestions on the possibility of mapping the standards to UBL. This is because UBL is widely used in Europe for invoicing. The possibilities for mapping the datasets to the e-invoicing standards were also considered

by stakeholders. However, the proposal is that Cross-Border data exchange should be facilitated by standards agreed upon by the EU eReceipt standardization working group).

- Data sets from national standardization bodies must be considered as the basis for eReceipt data exchange within the member state.

2. Identification and identification policies

- Identification and authentication either as a person or as an avatar should occur in the B2B and B2G data exchange processes. The customer's id number is the identification. It should be noted that eReceipt customers are often anonymous. Identification of a person should be optional.
- The means and how the identification should be determined by the point-of-sale operator.
- The decision on what threshold of spending requires identification and authentication in a B2B and B2G transaction should be determined by member states.
- The service provider should decide which means of authentication to use.
- In B2C data exchange, there is no customer identification in the eReceipt ecosystem, except for VAT claims are not necessary.

3. Data exchange policies

- Means of e-addressing should be decided by services provider agreements.
- E-addressing possibilities in each member can be based on different possibilities such as:
    - The e-addressing format both in the digital payment methods and mobile number[10] addressing in B2C transactions.
    - National four corner model solutions (not PEPPOL because it does not support customer identifier. However, a similar network to PEPPOL with XML identifier space or proxies like banks who have clients and might have a sort of gateway for exchanging data. Name payment used in the Baltics is also an inspiration)
- Data exchange for transport of B2B data should be PEPPOL network. As mentioned earlier, it is difficult to deliver to natural persons using PEPPOL. Furthermore, receipts go to travel and expense systems not to ERP as a purchase invoice, and it is already paid so companies want to have a separate address for receipts. Nevertheless, the reason for the use of PEPPOL in B2B transactions is because

[10] This is in other words - the name payment where one name is related to one mobile number which is discoverable from the bank and related to IBAN code

of this network's readiness to provide such services. Also, it would stimulate the market to enable eInvoice exchange as well.

ERECEIPT OPERATIONAL PRINCIPLES

EReceipt operational principles, business terms, and syntaxes are being developed by CEN. Those principles supersede other principles- including the one proposed in this report. However, the principles proposed here could serve as input to the ongoing work by CEN. The focus of the proposed principles is on B2B transactions.

1. GENERIC ERECEIPT PRINCIPLES

A. Identification and authentication

- The display of a Buyer and Seller's personal data on the eReceipt is optional unless made mandatory by national regulation (the statement is to guarantee the anonymity of the Buyer, but the Seller must always be identified).
- Sellers should be authenticated every time they access their point-of-sale (if owned by a third party) eReceipt account.
- Buyers should be authenticated every time they access their account in the eReceipt service provider's application.
- The Seller's point-of-sale account should include a mandatory option for a verifiable address and legal or private personal information of the Seller. The Buyer's account should include a non-mandatory option for a verifiable address and personal information of the Buyer. If the Buyer is a legal person, then the registration number of the company (as a minimum requirement) should be on the account.

- For data exchange purposes, the location of the Buyer, Seller, eReceipt operator, and point-of-sale operator must be identified using their e-address which is mapped to their point-of-sale account. PEPPOL e-address identifier is proposed here. PEPPOL works well with UBL. The proposed principles on e-address follow next.

B. Seller's e-address

- All Sellers must be traceable using e-address identification codes.
- All eReceipt Sellers must be identified with a Seller identification code.

- The Seller's identification code should consist of the code for the point-of-sale and Seller's eReceipt operator. The Seller identification code is the Seller's e-address.

C. Buyers e-addressing

- All Buyers that are natural persons must be traceable using address identification codes.
- All Buyers that are legal persons must be traceable using address identification codes.
- All legal persons must be issued with unique Buyer identification codes.
  - The unique identification code should be linked to the legal person's means of payment.
  - If the legal person is paying by cash, the national unique Buyer code must be given to the Seller to input into the system.
  - Natural persons purchasing for a legal person within a member state must be identified with the legal person's national Buyer identification code.

D. Buyer identification codes

- The Buyer's identification code can also be the code for the national access point (for Cross-Border Buyers), the Buyer's eReceipt operator and user id to the Buyer's account,

E. Fields in the eReceipt

- The fields in the produced eReceipt must follow specifications from relevant laws governing either cash register, invoice, or receipt fields.

2. PRINCIPLES FOR END OF THE TRANSACTION

A. Principles on the transmission of purchase information

- At payment, the Seller identification code must be transmitted to the Seller's eReceipt operator.
- At payment, the date and time of transaction must be transmitted to the Buyer and Seller's eReceipt operators respectively.
- At payment, data on items purchased and their associated cost must be transmitted to the Buyer and Seller's eReceipt operators respectively.
- At payment, data on the total amount spent on purchase must be transmitted to the Buyer and Seller's eReceipt operators respectively.

- At payment, means of purchase must be transmitted to the Buyer and Seller's eReceipt operators respectively.

B. Principles on the transmission of eReceipt from the Seller to Buyer

- The transmitted eReceipt data from the point-of-sale must be in a structured and machine-readable format.
- The transmitted data goes first to the eReceipt operator of the Seller, then the eReceipt operator of the Buyer, and then to the Buyer's accounts in the eReceipt operator's system.
- The national e-address route should be Seller (and/or point-of-sale), Sellers Operator, Buyer's operator, and Buyer's account with the Buyer's operator.
- The Cross-Border e-address for Cross-Border Buyers should/can be:
    - Option 1: Seller (and/or point-of-sale), Seller's operator, Seller's national access point, Buyer's national access point, Buyer's operator, Buyers eReceipt subscription account with Buyer's operator.
    - Option 2: Seller (and/or point-of-sale), Seller's operator, Buyer's operator, Buyers eReceipt subscription account with Buyer's operator.
- The storage of the eReceipt must be in accordance with national legislation.

3. PRINCIPLES FOR POINT OF SALE

- The Seller should subscribe to a merchant account with a third-party point-of-sale provider if the Seller does not own an in-house point-of-sale system.
- The Seller may also host a point-of-sale account.

4. ERECEIPT OPERATOR ACCOUNT

- The Buyer (legal person who is a merchant) must subscribe to a merchant account with an eReceipt operator.
- The Buyer's (legal person) account with the eReceipt operator may exchange data with their expense account. This is important to avoid double data entry.
- The Buyer's (legal person) eReceipt account with the eReceipt operator, if mandated by law, must exchange data with government agencies (for example tax authority).
- A Buyer (a natural person) must subscribe to an individual's account with an eReceipt Operator.

SECTION 2 - GOVERNANCE FRAMEWORK FOR THE E-SERVICES

The development of the proposed operational principles requires a governance framework. The principles presented for each e-Service consider the data exchange activities between multiple stakeholders. But how do we bring these stakeholders together to accept the proposal, hence the need for a governance framework. Although the governance framework is developed for the operational principles, it is also presented as a separate proposal for a governance framework for the semantic implementation of e-government services in genera. Hence, the framework will be described in generic terms, which also encompasses the proposed operational principles.

The governance proposal in this report for the semantic implementation of each e-Service is Cross-Border collaborative governance. The collaborative semantic interoperability governance framework consists of sub-collaborative semantic governance groups in each member state as represented in figure 6 below.

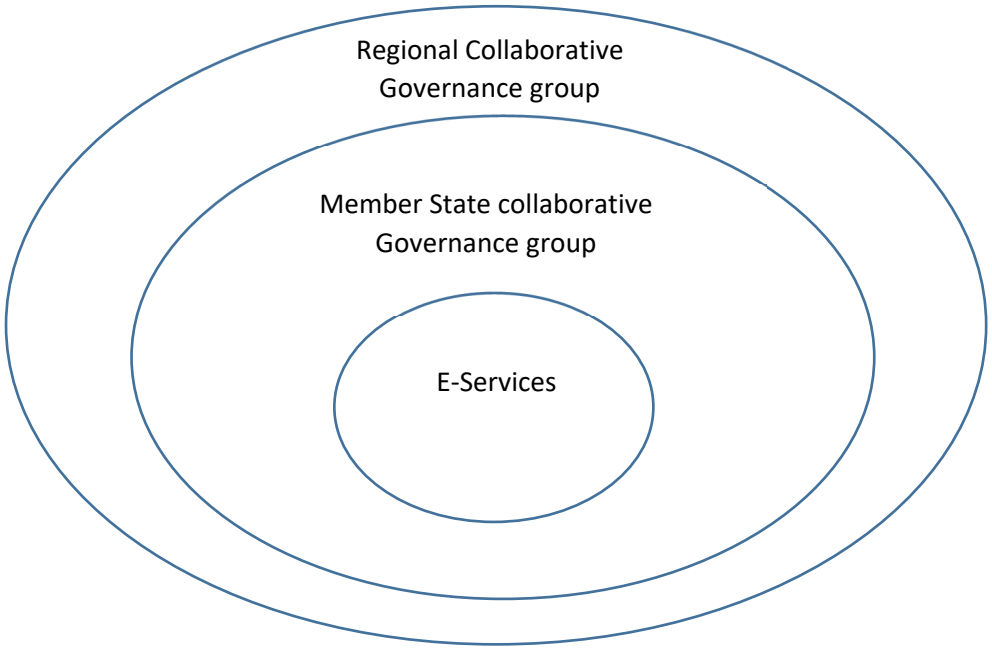

Figure 6. Illustration of the collaborative governance framework ecosystem.

Selected representatives of the sub-collaborative semantic governance groups would then make up the Regional (BSR or EU) governance group. The group should consist of technical experts from digitalization agencies, the regulatory agencies, Ministries, and agencies that have oversight over the sector, service providers, other relevant agencies, and SMEs. The task of the sub-collaborative governance group would be to:

- Develop holistic service delivery processes, semantic principles, data models, and if possible, standards that will govern semantic data transfer between government agencies and SMEs within the member state and across the border.
- Continuously evaluate the implementation as well as the need to modify the policies that govern how they implement the operational principles in their member state.
- Evaluate the national legal framework and propose amendments where necessary.
- Collaborate with other sub-collaborative groups delivering other e-Services.

At the regional level, the aim of the group would be on:

- The harmonization of minimum viable operational Cross-Border processes, policies, and principles for the Cross-Border delivery of the specific e-Service.
- The exchange of ideas on best practices.
- The evaluation of the existing semantic frameworks, propose modifications where necessary as well as continuously improve upon or replace existing semantic models.

The essence of this framework is not just to give each stakeholder a voice or help each stakeholder understand each other's processes, rather it is to enable each stakeholder to negotiate their position based on their interest. For example, SMEs could voice that the adoption of a particular data exchange standard would harm their current operations. Or the digitalization agency could argue that the government does not have the resources to implement a suggestion from the service providers. Hence being on the same table opens the possibility for hearing each other, understanding each other's concerns, and arriving at semantic frameworks that are not just good on paper but are practical.

The administrative structure within each governance group should be decided by the ministerial agency in charge of the sector in a member state. However, it is recommended that the group be led by a digitalization agency or similar agencies. Furthermore, such working groups in each member state should have some form of legitimacy granted either by national regulation or special recognition by the ministerial agency in charge of the sector. Legitimacy at the member state is what a lot of semantic interoperability working groups in Europe are lacking. For example, there is the semantic interoperability community working in collaboration with DG DIGIT's ISA[2]. Although they run pilots, the uptake of the proposals would be greater if there was also a push from member states. The proposed framework provides a bottom-up approach that will complement such groups but with a specific e-Service.

The implementation of the governance framework will require a greater interest by member states towards the development of Cross-Border e-Services. However, an incentive is and always will be the increase in trade. Developing e-Services that will enhance the service delivery operations of SMEs opens new opportunities for

innovation and a potential increase in foreign direct investment. Furthermore, the increase in datafication has resulted in the growth in the delivery of more e-Services and with the potential for globalization enabled by the internet, there is a greater yearning for Cross-Border e-Services. Hence removing the bottleneck caused by the lack of semantic data interoperability of Cross-Border e-Services should be an incentive for the implementation of the proposed governance framework.

An indirect challenge to the implementation of the proposed framework is the unripe legal environment. Currently, these proposals are futuristic and provide an insight into what these services would look like, bearing in mind that they do not currently exist as Cross-Border e-Services. There are eCMR, KYC utilities, and eReceipt services provided by the private sector. These are localized initiatives that do not cater either to the BSR as a sub-region or the EU as a region. The basic challenge is that there are no policies laws either at the member state level or the EU that drives the development and implementation of these services. Hence, in the case of eCMR, the CMR process is still paper based in most EU member states. There is a push for eReceipt from Estonia and Finland but in other member states, there are no discussions on eReceipt. The same is the case with KYC. In the absence of enabling laws, existing laws serve as a barrier for public agencies who would like to implement these services. Hence, the absence of laws serves as a barrier to the development of the service. Furthermore, the absence of laws dampens the resolve to develop a semantic interoperability framework as proposed in this report.

Hence, the first recommendation here would be the removal of national legal barriers that either prevents or does not place emphasis on the digital delivery of either CMRs or receipts. For KYC, is difficult to insist that the KYC process should be digital due to the need for third-party verification in most cases. But the proposal is that the implementation and usage of the national KYC utility in each member state should be digital. Nevertheless, the adoption of e-Service friendly laws is required for the implementation of the proposed governance framework.