Yrityksen digitalous

eReceipt

Common requirements specification

Commenting Draft

Real time economy | 13.6.2023 | Editor Antti Kettunen, Tietoevry

Version history

Version	Date	Editor	Changes
0.1	13.06.2023	Antti Kettunen, Tietoevry	Initial version for comments

1 Keywords and definitions

To ensure consistent application, keywords that appear in UPPERCASE are to be interpreted as follows:

- **MUST:** This term, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT:** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- **SHOULD**: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT:** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behavior described with this label.
- **MAY:** This word, or the adjective "OPTIONAL", means that an item is truly optional.

The above-described keywords are to be interpreted as described in BCP 14 [RFC2119].

2 Glossary

Digital receipt is a digital proof of purchase, containing information about the purchase items.

eReceipt or electronic receipt is a structured data version of a digital receipt.

Verifiable eReceipt is an eReceipt that can be verified to be authentic and immutable using secure computing methods, such as cryptographic proofs, without contacting the original receipt issuer.

Data at rest refers to the state of the eReceipt when it's being stored in a physical medium, whether it's onsite or in the cloud via another organization's hardware. It can be encrypted to guarantee that only authorized users have access to reading what's already there or writing new information altogether.

Data in transit refers to the state of the eReceipt when it is currently being transmitted from one point to another. In this document, it specifically refers to eReceipt being transmitted between parties or intermediaries.

Party in this document refers to any of the primary entities partaking in the business transactions that contain any type of an eReceipt.

Intermediary is an entity that provides various eReceipt processing capabilities, such as messaging services, on behalf of the primary party.

Trust model describes the mechanism used to establish trust between entities. In eReceipt it specifically means how trust in the authenticity and integrity of the eReceipt can be established and maintained.

3 Scope and overview

The purpose of this document is to provide a set of common requirements for

implementing electronic receipts (later eReceipts). The requirements outlined are technology and architecture agnostic and aim to facilitate the smooth exchange and utilization of eReceipts between sellers, buyers, and verifiers.

This document defines common requirements for implementing eReceipts, irrespective of the chosen implementation architecture.

In addition to the common requirements, each implementing infrastructure or service needs to define its own technology specific data formats, protocols, and interfaces that fulfill the requirements set by the common eReceipt specifications.

Figure 1 describes the relationship of the common eReceipt requirements with the implementations.

Interoperability between various implementations is made possible by defining common interoperability elements that allow services to support multiple eReceipt implementation infrastructures.

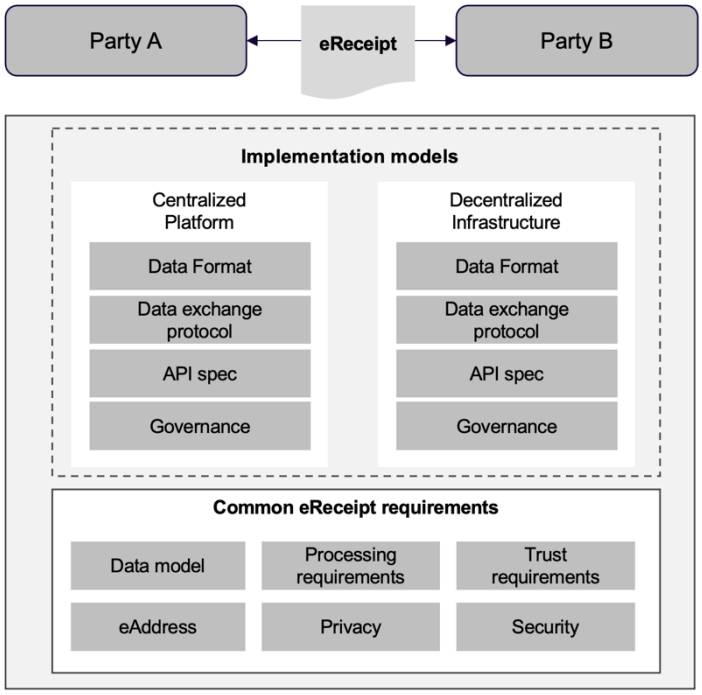


Figure 1 Relationship of common requirements and implementation specific definitions.

3.1 Common eReceipt requirements

3.1.1 Data model

Any implementation of eReceipts must ensure compatibility across different systems and platforms by supporting at least one commonly available standard data model. In addition, the implementations can also use other available data models according to their business needs.

This document recommends using CEN/TS 16931-8:2022 (E) “Electronic invoicing – Part 8: Semantic data model of the elements of an e-receipt or a simplified electronic invoice” as the commonly supported data model.

3.1.2 Privacy & Security

The implementations should prioritize the security and privacy of eReceipt processing and transportation. Robust encryption mechanisms, data integrity measures, and secure storage practices should be employed to protect the sensitive information contained within eReceipts.

3.1.3 Trust requirements

Trust requirements define generic requirements for ensuring trustworthiness of the eReceipt processing and transmission. Trust requirements include how authenticity and integrity is maintained during the eReceipt lifecycle.

Common trust requirements define higher level requirements, but more implementation specific trust models are defined in the governance of the implementation.

3.1.4 eAddress

For transmitting eReceipts to its requested location, the parties and intermediaries need a mechanism for sharing and discovering delivery endpoints (e.g. API address). The eAddress is a concept of a private digital address for a natural or legal persons. An eAddress allows a person to indicate which digital service they want to use in various life events and digital interactions.

For example, an eAddress can refer to a unique interface for the person's own wallet, to the accounting interface of the organization or a third-party service provider’s platform interface.

eAddresses are contextual and the end-user can choose to use one eAddress for all transactions, a unique eAddress for each transaction, or anything in between the two.

One potential design approach is to use W3C Decentralized identifier standard (W3C DID Core) as the core standard for eAddresses. Although there has been tested designs, there is not yet a published eAddress specification.

3.2 Implementation specific definitions

Each implementation infrastructure should define at least data format, data exchange protocol, API specifications and governance description of what are specific for its implementing infrastructure. These definitions provide a foundation for understanding and implementing eReceipt systems, regardless of the chosen architecture. They establish a common language and technical framework that enables seamless communication and interoperability within the eReceipt ecosystem.

3.2.1 Data format

The implementation should define a standardized data format for encoding and transmitting the eReceipt. The format should be widely supported, well-documented, and easily interoperable across different systems and platforms within the implementing infrastructure. The data format should allow for extensibility, enabling the addition of custom or optional fields to accommodate specific implementation requirements.

3.2.2 Data exchange protocol

The implementation should support a secure data exchange protocol for transmitting eReceipts between parties within the eReceipt ecosystem. The protocol should ensure data confidentiality, integrity, and authenticity during transit, employing encryption, digital signatures, or other cryptographic measures as appropriate.

The chosen data exchange protocol should be scalable and capable of handling a high volume of eReceipt transactions efficiently. It should optimize network utilization, minimize latency, and provide mechanisms for handling large payloads without compromising system performance.

3.2.3 API interface

For implementations utilizing APIs for eReceipt integration, a clear and comprehensive API specification should be provided. This specification should define the endpoints, request/response formats, supported operations, and authentication mechanisms required for interacting with the eReceipt system.

The API interface is recommended to be based on commonly accepted best practices, utilizing popular libraries and tools where appropriate.

If the API specification is used for interoperability between intermediaries or parties, it should be accompanied by comprehensive documentation that provides detailed explanations of each API endpoint, its parameters, and expected behavior. Additionally, it should include code examples and sample requests/responses to assist developers in implementing eReceipt integrations effectively.

The specific requirements for data format, data exchange protocol, and API specification may vary depending on the chosen implementation architecture (centralized or decentralized) and the underlying technologies or standards.

3.2.4 Governance

Governance of the implementation infrastructure must be defined when there is more than one party involved in processing the eReceipt. Governance documentation may take different forms and scopes. For example, a decentralized infrastructure may define their governance in a collective agreement, where the agreement is made between the signee and a separate governance entity. In platform infrastructures, the parties may be part of a collective agreement, or have separate bilateral agreements between each other.

Defining governance is crucial to ensure the efficient and effective operation of the ecosystem. Among other things, the governance framework should describe how it audits and enforces the requirements of its members.

Governance should include definitions for forming the trust model. For example, where applicable, cryptographic measures like digital signatures and hashing can be employed to detect any tampering attempts, and authenticity checks may involve the use of digital signatures, certificates, or other cryptographic techniques to verify the origin of the eReceipt data.

The trust model defines how trust relationships between different parties within the eReceipt ecosystem are formed, and what is the basis of trust between the data exchange parties and their intermediaries.

To maintain transparency and accountability, the implementations should support some level of auditability features. This includes the ability to track and log actions related to eReceipt processing, ensuring that any modifications or exchanges are traceable to the responsible parties.

4 Key components

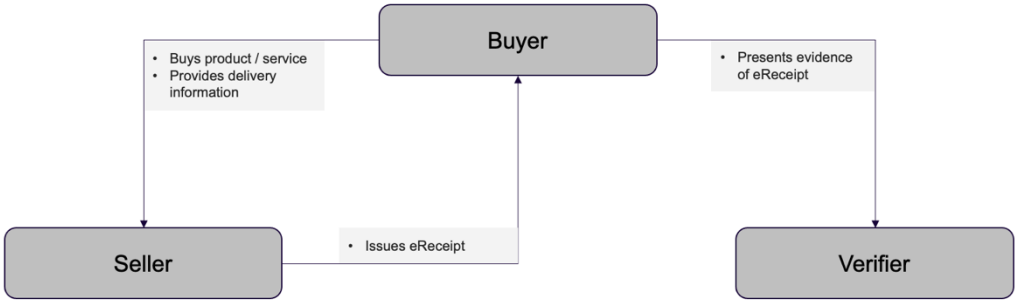
4.1 Roles

The eReceipt ecosystem contains three main roles:

- **Buyer** is the role that executes a purchase on their own or an organization’s behalf. The buyer is entitled to receive an electronic receipt of their purchase, delivered to their chosen target system. The buyer is always a private person, although they may represent an organization.
- **Seller** is the role that provides a product or service to the buyer and is required to produce a receipt of the purchase. The seller is usually a

merchant offering services to natural and legal persons.

- **Verifier** is the role that requires access to receipt information in order to offer their services to buyers. They utilize the eReceipt provided by the buyer to validate or process transactions, provide additional benefits, or perform related activities. Examples of organizations acting in the verifier role are insurance companies, banks, accounting firms and customs.



Each of the roles represent a *contractual party* in the purchase and verification process. They do not represent technical or implementation roles, as each role's responsibilities and processes can be implemented in several ways.

Whenever a requirement is defined for the specific role, that means that that party is responsible for ensuring that the requirement is fulfilled. Fulfillment of the requirement can be delegated to a service provider, but it is the responsibility of the role fulfilling party to ensure compliancy with the requirement, unless defined otherwise by regulation.

4.2 Implementation patterns

The requirements specified in this document aim to be implementation agnostic. As described in Chapter 3: Scope and overview, different implementation infrastructures may fulfill the requirements differently.

In this chapter we describe two implementation patterns as an example of how an eReceipt system can be implemented. These example patterns are conceptual, and do not actually represent how eReceipts should be implemented.

4.2.1 Dedicated intermediary pattern

An implementation model where each party has their own dedicated intermediary that handles processing and transmission of eReceipts. Each intermediary is an independent deployment, with no access to each other's data. Whenever eReceipt needs to be transported, the participating intermediaries need to establish a connection between each other and execute the eReceipt delivery according to established data transfer patterns.

An example of a dedicated intermediary pattern is digital wallets, where intermediaries are service providers of various digital wallet services.

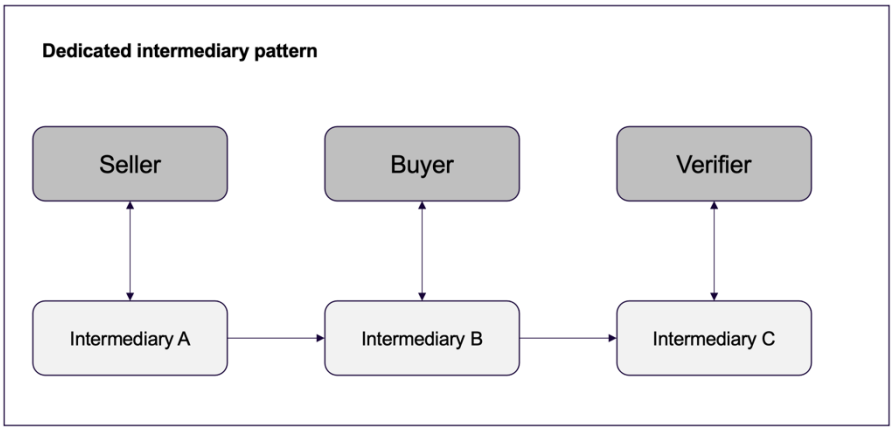


Figure 2 Dedicated intermediary pattern

4.2.2 Shared intermediary pattern

An implementation model where an intermediary service may be shared by multiple parties. In this pattern, the intermediary acts as a data platform to its users, enabling access to receipt data for privileged parties within the same platform.

As described in Figure 3, the same intermediary may span across multiple parties (seller and buyer), removing the need to transport the eReceipt data as both the seller and buyer have access to the same intermediary platform.

If a party is not serviced by the intermediary, then data needs to be transferred to the other intermediary servicing that party.

In the case that the intermediary serves all the parties involved in the value chain (seller, buyer, and the verifier), then eReceipt data is readily available to all parties, and only permission to use the data within the intermediary platform needs to be provided.

Example of a shared intermediary pattern is eReceipt operator platforms.

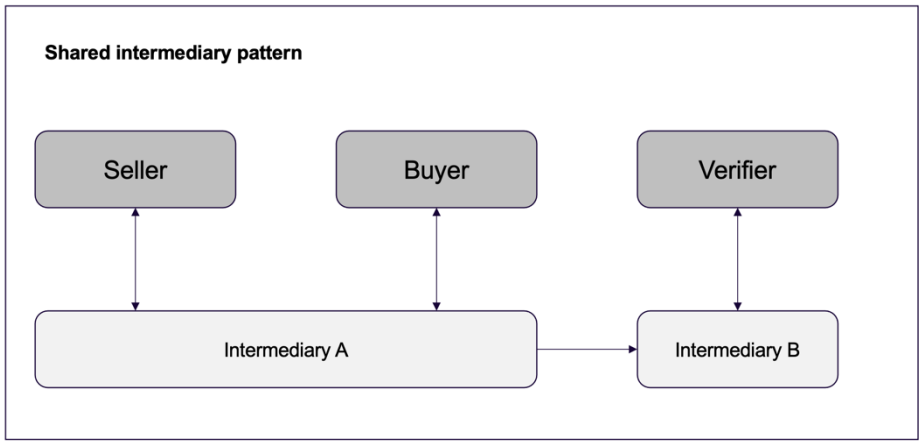


Figure 3 Shared intermediary pattern.

4.3 Receipt forms

During its lifecycle, the receipt may be transmitted and processed in different forms and by multiple systems and entities. It is important to ensure that the receipt data remains unchanged during all lifecycle states, and how trust in its authenticity and integrity can be formed.

This specification recognizes three different receipt forms, which all have different uses, features, and trust models.

The three forms include unstructured digital receipt, structured eReceipt and Verifiable eReceipt.

The common requirements focus on defining requirements for the use of structured eReceipts and Verifiable eReceipts.

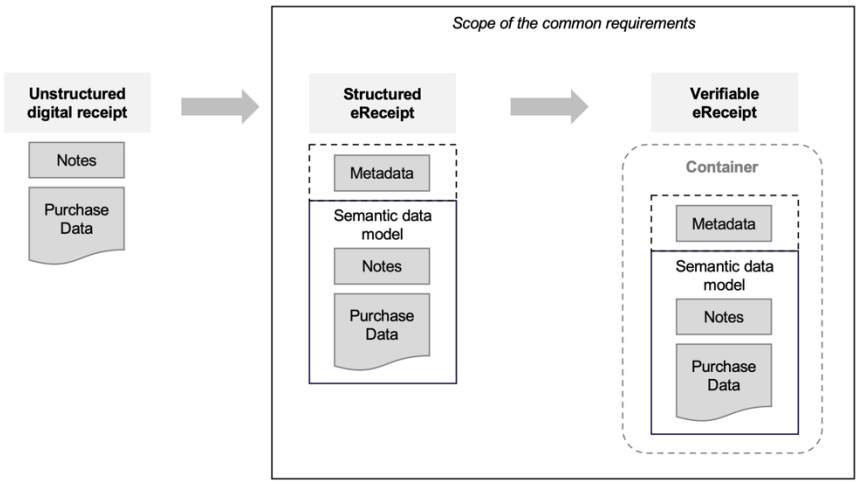


Figure 4 Three forms of eReceipts. An eReceipt may exist in all of the forms during its lifecycle.

4.3.1 Unstructured digital receipt

An unstructured digital receipt is used when the receipt is contained within the boundaries of the seller's system. It can be in any format that the seller's system requires it to be in. This type of receipt is considered 'data at rest' and is not intended to be transferred across the system boundaries.

Unstructured digital receipts are not in the scope of the requirements set in this document.

Trust in unstructured digital receipt is based on the trustworthiness of the seller to uphold their legal requirements, and the security guarantees of their platform.

Generally, the seller does not give any authenticity or integrity guarantees for use outside of seller's system guarantees.

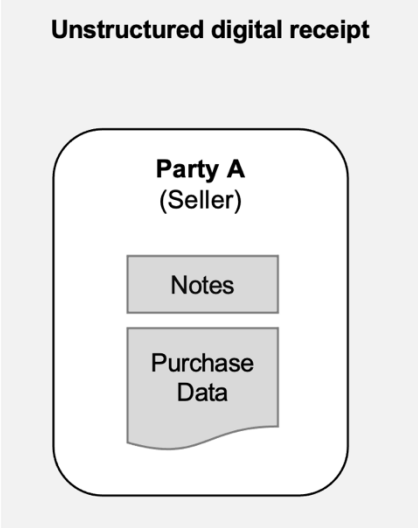


Figure 5 Unstructured digital receipt is used at rest within the seller's system

Digital receipt	
Type	unstructured data
Purchase data	Information about the purchased items, tax calculations, etc.
Notes	Optional information relating to the purchase or the customer relationship, that is not part of the purchase data.

4.3.2 Structured eReceipt

Structured eReceipt is used when transporting the eReceipt outside of the seller's system using a centralized platform. The verification features of the eReceipt are reliant on the capabilities of the seller's platform. When eReceipt is stored within the platform, it is considered 'data at rest'. When it is transported to another party, it is 'data in transit'.

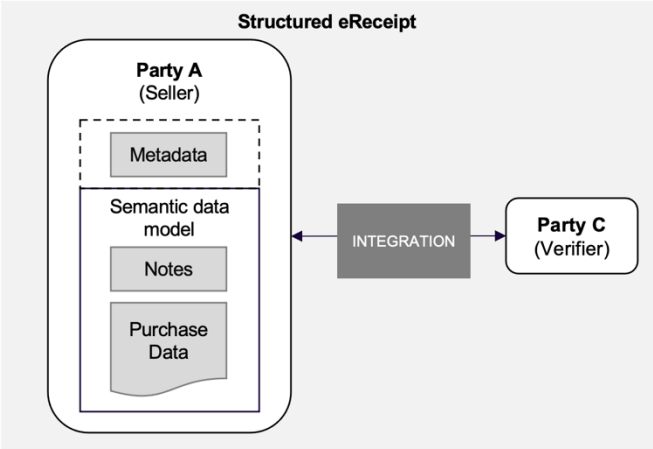


Figure 6 Structured eReceipt is used when transporting eReceipts using centralized platform.

The eReceipt is structured into a semantic data model, with additional metadata appended to the eReceipt. The eReceipt is not intended to cross the boundaries of the intermediary system, except through controlled integrations.

Trust guarantees with structured eReceipt are generally based on the trustworthiness of the eReceipt platform, and the bilateral integrations and contracts existing between the parties and their intermediaries. Authenticity and integrity guarantees are usually achieved through the platform-specific verification capabilities.

Structured eReceipt	
Type	Digital receipt + metadata + semantic data model
Metadata	Additional information provided by the intermediaries or applications processing the eReceipt.
Notes	Optional information provided by the seller, relating to the purchase or the customer relationship, that is not part of the purchase data.
Semantic data model	Receipt data structured in a semantic eReceipt data model, with purchase data and notes.

4.3.3 Verifiable eReceipt

Verifiable eReceipt is used when eReceipt is transferred outside the boundaries of the controlled system (Party A) to another system (Party B) without creating a dependency with the seller's system. In other words, Party B can verify the Verifiable eReceipt without relying on Party A's infrastructure.

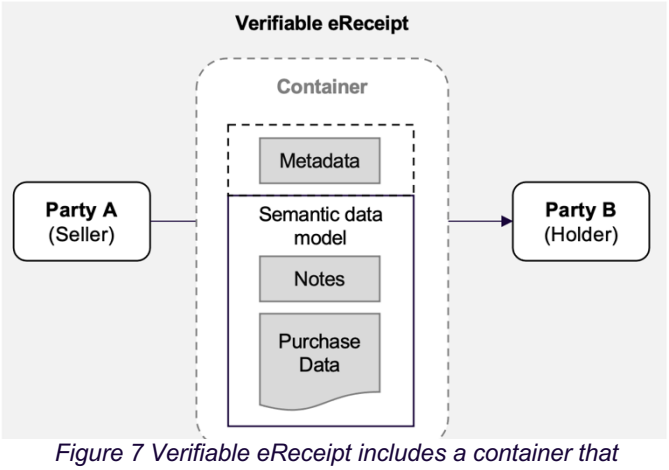


Figure 7 Verifiable eReceipt includes a container that enables verification of the eReceipt outside its originating platform.

Verifiable eReceipt includes a container that wraps around the eReceipt and metadata. The container adds verification

capabilities for the content and the transportation.

Trust in the Verifiable eReceipt is generally based on the combination of cryptographic capabilities of the container and the decentralized governance model. The verifiable container can be used to verify the integrity and authenticity of the eReceipt, and issuance can be traced back to the originating seller. The container requires use of commonly agreed protocol that adheres to security and privacy best practices.

Verifiable eReceipt	
Type	eReceipt + container
Container	An envelope that provides additional technical capabilities for eReceipt processing and transmission. The container can be used to verify the integrity and authenticity of its content and to guarantee the privacy and confidentiality of its transportation and presentation.

5 Requirements

5.1 General requirements

General requirements that apply to all implementations and roles. It guides the infrastructure implementations and role implementors in taking note of the important features their eReceipt implementations should include.

A key requirement is to ensure that the regional regulations, directives, and industry best practices are applied. For example, in EU these would include the European General Data Protection Regulation (GDPR), Digital Markets Act (DMA), the Digital Services Act (DSA), the Data Governance Act (DGA) and the Data Act.

General requirements are identified with identifier prefixed “ER-G” + index.

Requirements

ID	Requirement
ER-G1	Implementations SHOULD enable interoperability with other implementations.
ER-G2	Implementations MUST ensure privacy-preserving and secure processing and transmission of eReceipts.
ER-G3	Implementations MUST specify how authenticity, integrity, and confidentiality of the eReceipt are guaranteed during eReceipt’s lifecycle.
ER-G4	Implementations SHOULD support data exchange protocol that supports confidentiality, privacy, and security best practices.
ER-G5	Implementations SHOULD document their governance model and how implementing parties are audited and rules are enforced.
ER-G6	Implementations SHOULD document their trust model.
ER-G7	The eReceipt contents MUST remain unchanged during its lifecycle, after it is generated by the seller.

ER-G8	The eReceipt metadata MAY be changed at any time during the eReceipt lifecycle.
ER-G9	The eReceipt implementations and implementing parties MUST adhere to the regional regulations, directives, and industry best practices.

5.2 eReceipt issuance

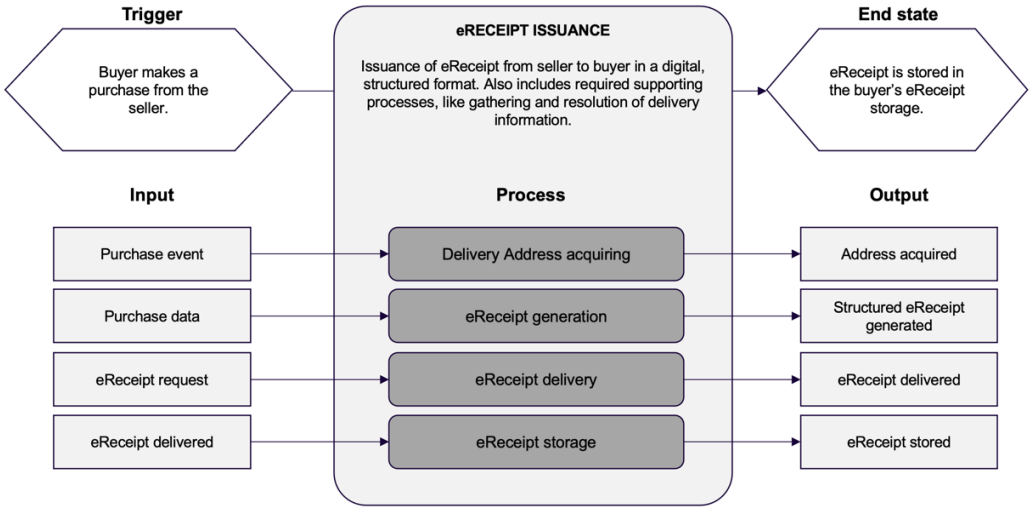


Figure 8 Issuance describes requirements for the activities around issuance and storage of eReceipts.

The eReceipt Issuance process describes the interactions between buyer and seller relating to the issuance of the eReceipt. The eReceipt issuance process begins after the completion of the purchase transaction between the seller and the buyer and ends once the eReceipt is received and stored at the recipient systems.

The eReceipt issuance requirements are identified with identifier prefixed “ER-I” + index.

5.2.1 Delivery Address acquiring

The seller, if not already possessing the required eReceipt delivery information, needs to acquire the delivery address for the eReceipt. This process requires that the buyer presents a delivery address to the seller.

Requirements

ID	Requirement
ER-I1	The buyer MUST present a URI-based eAddress to indicate where the eReceipt should be delivered.
ER-I2	The buyer MAY use another identifier to reference a previously presented eAddress.
ER-I3	The seller SHOULD support acquiring of the eAddress via optical presentation methods, such as QR-code.
ER-I4	The seller SHOULD support acquiring of the eAddress via digital card, such as magnetic stripe, smart card chip, or contactless

	mechanisms.
ER-I5	The seller SHOULD support acquiring of the eAddress via smart personal device using radio-based transport mechanisms, such as NFC or Bluetooth.
ER-I6	The seller MAY support acquiring of the eAddress via a unique identifier that can be resolved to the eAddress using a separate registry.
ER-I7	The seller MAY support additional mechanisms for establishing connectivity between the buyer and seller.
ER-I8	The seller MAY support NFC-tags that the buyer can read during the checkout process, which enables initiating the eReceipt delivery.

5.2.2 eReceipt generation

Once the delivery information is available to the seller, and the seller is ready to deliver the eReceipt, the seller initiates the generation of the eReceipt. The seller's system compiles the transaction data into the appropriate data format and semantic data model, ensuring that all required fields are populated accurately and completely.

Requirements

ID	Requirement
ER-I9	The seller MUST ensure that the purchase data in the eReceipt is identical to that in the seller’s purchase data system.
ER-I10	eReceipt data MUST include at least the data that is required by the local authorities.
ER-I11	eReceipt MAY contain additional metadata section that can be changed without affecting the verifiability of the eReceipt contents.
ER-I12	eReceipt SHOULD NOT have personal information that enables unique identification of the buyer based on that information alone.
ER-I13	The seller MUST support generating the eReceipt according to CEN/TS 16931-8:2022 (E) data model.
ER-I14	The seller MAY support generating the eReceipt according to other eReceipt data models.
ER-I15	The seller MUST provide means to verify the eReceipt’s integrity and authenticity.
ER-I16	The seller MUST NOT make any changes to the eReceipt after it is generated.

5.2.3 eReceipt delivery

The seller's system may provide various options for delivering the eReceipt to the buyer. This can include sending the eReceipt via an eReceipt platform, digital wallet or directly to a third-party system that the buyer is using.

Requirements

ID	Requirement
ER-I17	The seller MUST deliver the eReceipt according to its supported implementation specifications.
ER-I18	The seller MUST NOT issue more than one valid instance of an eReceipt at a time.

5.2.4 eReceipt storage

The eReceipt must be stored according to the data protection best practices, ensuring privacy-preserving access control mechanism and secure encryption schemes.

Requirements

ID	Requirement
ER-I19	The buyer MUST be able to verify the contents of the eReceipt as soon as it is received.
ER-I20	The buyer MUST be able to verify the authenticity of the eReceipt.
ER-I21	The buyer MUST be able to verify the integrity of the eReceipt.
ER-I22	The eReceipt MUST be stored according to local and regional regulations.
ER-I23	Access to the eReceipt MUST be restricted to those with legal permission.

5.3 eReceipt application

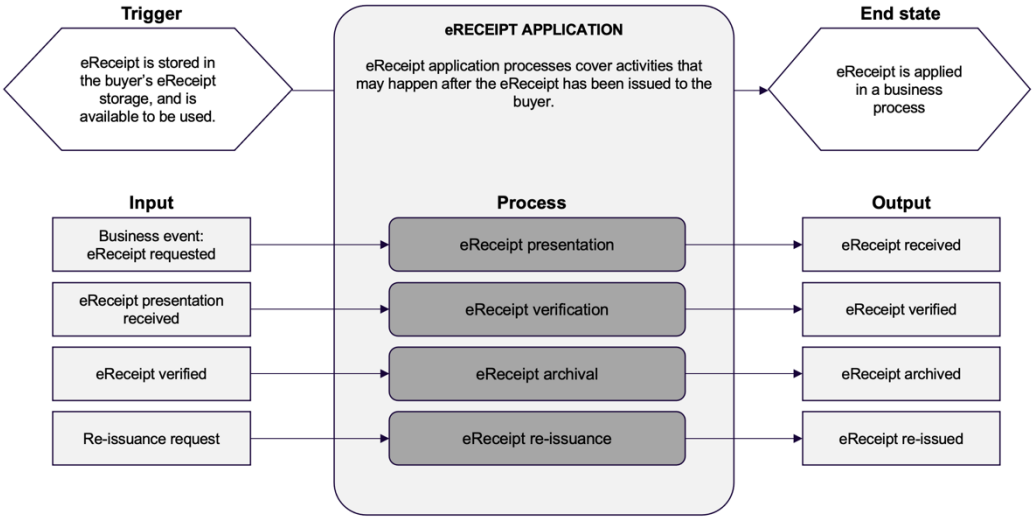


Figure 9 eReceipt application process includes the sub-processes that happen after the eReceipt has been issued.

The eReceipt application process describes the interactions and activities that may

happen after the eReceipt has been issued. These include the usage of the eReceipt with a relying party (verifier), or other activies like archival and re-issuance of the eReceipt.

The eReceipt application requirements are identified with identifier prefixed “ER-A” + index.

5.3.1 eReceipt presentation

eReceipt presentation describes the activity of presenting the eReceipt to its relying party, or verifier. Presentation includes any channels that may be used to present and receive the eReceipt data.

Requirements

ID	Requirement
ER-A1	The eReceipt MAY be presented to one or more verifiers.
ER-A2	The eReceipt SHOULD be able to be presented using a physical presentation device.
ER-A3	The verifier SHOULD be able to be read the eReceipt using a scanner or other proximity-based reader device.
ER-A4	The verifier SHOULD be able to receive the eReceipt using a remote online system.
ER-A5	eReceipt MUST be presented according to CEN/TS 16931-8:2022 (E) data model.
ER-A6	eReceipt MAY be presented in other eReceipt data models.
ER-A7	The buyer MAY selectively disclose only selected portions of the eReceipt.

5.3.2 eReceipt verification

At any point of its lifecycle, the eReceipt must be verifiable by its processor, so that they can confidently trust the receipt data and include in their business process. The verification includes at least verifications of authenticity (source), integrity and status, but other verifications may also be added.

Requirements

ID	Requirement
ER-A8	The verifier MUST be able to verify the authenticity of the eReceipt.
ER-A9	The verifier MUST be able to verify the integrity of the eReceipt.
ER-A10	The verifier MUST be able to verify if the eReceipt has been voided.
ER-A11	The verifier MAY add information to the eReceipt metadata.

5.3.3 eReceipt archival

In some cases, the eReceipt needs to be archived for long-term storage. When archiving the eReceipt, the archiving party must ensure that the verification status of the eReceipt at the time of the archival can be confirmed later. The confirmation of the verification status must be self-contained and not be dependent on external technical systems.

Requirements

ID	Requirement
ER-A12	The eReceipt MAY be archived.
ER-A13	The archived eReceipt's verification status at the time of archival MUST be provable without dependencies on any external technical systems.

5.3.4 eReceipt re-issuance

In some cases, the original receipt needs to be corrected, due to wrong information in the receipt or a product return. This requires a re-issuance of the eReceipt. The re-issuance process is system dependent, but generally it requires that the original eReceipt is voided and a new eReceipt is re-issued.

Requirements

ID	Requirement
ER-A14	The seller MUST notify the buyer if the eReceipt is voided.
ER-A15	The seller SHOULD re-issue a new eReceipt to the buyer if the original receipt was voided.
ER-A16	The re-issued eReceipt SHOULD reference the original, voided eReceipt.

6 Additional discussion topics

Row level re-issuance

It is recognized that row-level re-issuance of a receipt is possible in some systems, making it possible to make changes to the receipt rows, without needing to re-issue the whole receipt. However, the implications of making changes to the eReceipt rows after its generation may be problematic from eReceipt verification perspective. Further consideration needs to be made on this topic.

Yrityksen digitalous

Euroopan unionin rahoittama –
NextGenerationEU