banqup

QERDS - Practice Statement

v.1.5

We ensure compliance

and business growth

www.banqup.com

1. Document History

1.1. Version History

Version	Date	Status	Description
1.0	23/09/2019	Superseded	Created the initial version of the practice statement.
1.1	21/10/2019	Superseded	Monitoring third parties Sender authentication via MSSL.
1.2	22/01/2020	Superseded	Added extra information about storage of documents and personal data.
1.3	24/04/2020	Superseded	Configuration reviews for information systems.
1.4	08/09/2022	Superseded	Updated to add onboarding via API.
1.5	02/07/2026	Published	Moving trust service to Banqup. Updated Practice Statement to align with the latest ETSI controls and European Commission implementing regulations.

1.2. Document Approval

Version	Date	Status	Approved by
1.1	15/01/2020	Approved	Governance Board
1.2	04/02/2020	Approved	Governance Board
1.3	04/05/2020	Approved	Governance Board
1.4	08/09/2022	Approved	Governance Board
1.5	01/07/2026	Approved	TSP Authority

1.3. Related Documents

Document	Relation
Solution Specific Terms for Qualified Trust Services	Establish the contractual terms applicable to customers for the provision of trust services, and are aligned with and subordinate to the Certification Policies and trust service practice statements.

Table of Contents

2. Introduction

This document describes the practices and policies applied by Banqup in offering the qualified trusted service for electronic registered delivery service. This document is intended for both the senders and receivers of electronic registered deliveries.

2.1. Banqup CA Policy Management Authority

The qualified trusted service for ERDS is governed by the Banqup CA Policy Management Authority (TSP authority). The TSP authority comprises the necessary functions including policy, compliance, legal and architecture that are required to provide strategic direction and continuously supervise the ERDS operations.

The TSP authority consists at least of:

- The TSP manager
- A representative from Banqup's board
- A representative from the IT security team

The TSP authority is the highest-level management body with final authority and responsibility to:

- Maintain compliance with the legal and normative requirements,
- Define the ERDS trust service and approve its delivery model,
- Define, maintain and approve the ERDS policies and practices,
- Conduct regular supervision activities on the ERDS operations team,
- Get involved in major incidents, when applicable,
- Ensure the QERDS service described in this practice statement is implemented and operated in a non-discriminatory manner within the limits of what current technologies allow.

This practice statement is reviewed annually by the TSP Authority.

2.2. Policy administration

2.2.1. Organization administering the document

Banqup, through the Banqup CA Policy Management Authority, is bearing responsibility for drafting, publishing, maintenance and interpretation of this trust service practice statement and other policies and practices within the trust service domain.

The TSP authority is appointed to conduct the following policy administration tasks:

- Drafting, amending, maintaining and interpreting this trust service practice statement.
- Approve and publish this practice statement and its updates after the completion of a review process. The updated practice statement is published on the Banqup trust services repository as promptly as possible and, in any case, no later than its effective date (as indicated on the first page).

2.2.2. Contact person

TSP authority may be contacted at the following addresses:

- Email: qtsp@banqup.com
- Postal address: Banqup, Av. Reine Astrid 92A, 1310 La Hulpe, Belgium

The TSP authority accepts comments regarding this trust service practice statement only when they are addressed to the contact above.

2.3. Definitions and acronyms

API	Application Programming Interface
BMID	Belgian Mobile ID
B-T	PAdES Baseline signature with an embedded qualified electronic Timestamp
CA	Certification Authority
CIR	Commission Implementation Regulation
CISO	Chief Information Security Officer
DPO	Data Protection Officer
eID	Electronic Identity
eIDAS	Electronic IDentification, Authentication and trust Services
ERDS	Electronic Registered Delivery Service
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
ISO	International Standards Organization
mTLS	Mutual Transport Layer Security
PAdES	PDF Advanced Electronic Signatures
PDF	Portable Document Format
QERDS	Qualified Electronic Registered Delivery Service
QTSP	Qualified Trust Service Provider
REM	Registered Electronic Mail
REMS	Registered Electronic Mail Service
S&N	Store and Notify
SSL	Secure Sockets Layer
TLS	Transport Layer Security
TSP	Trust Service Provider
WORM	Write Once, Read Many

3. Overview

Banqup SA (hereafter to be referred to as: “Banqup”, “we”, “us” or “our”), with headquarters in 1310 La Hulpe, Avenue Reine Astrid 92A and registered under enterprise identification NTRBE-0649860804 is offering the electronic registered delivery service as an add-on to its already established electronic delivery products. The Qualified Electronic Registered Delivery Service (QERDS) is provided by Banqup in accordance with eIDAS regulation (EU) No. 910/2014 of the European Parliament and of the Council (eIDAS).
This regulation stipulates that an ‘electronic registered delivery service’ means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorized alterations.This practice statement claims conformity with:

- ETSI EN 319 401 (V3.2.1 (2026-01)) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 521 (V1.1.1 (2019-02)) Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 531 (v1.1.1 (2019-01)) Policy and security requirements for Registered Electronic Mail Service Providers.

3.1. Electronic Registered Delivery Service

3.1.1. General

The service offers a typical communication between two parties in one direction, where there is a sender of the communication and a receiver. The Banqup service offers different functionalities to both parties: the sender and receiver, keeping in mind that one party can be the sender in one communication and the receiver in another. Banqup ensures that the document uploaded by the sender is sent electronically to the specific receiver defined by the sender. A receipt of sending will be available to the sender, including the seal and timestamp provided by Namirial.

3.1.2. Modifications

Banqup modifies the PDF document as provided by the sender only in the following ways:

- We add a cover page as mentioned in paragraph 3.2.
- We seal the combination (cover page and the provided PDF document).

3.1.3. Onboarding via API

The sender service is open to all legal persons who have signed a sender contract with Banqup and have passed the identity proofing process at Banqup. They will then receive an account and a Banqup self-signed advanced certificate allowing the senders to upload documents to the electronic registered delivery service using mutual SSL.

3.1.4. Onboarding via WebPortal

The sender service is open to all legal persons who have signed a sender contract with Banqup and have passed the identity proofing process at Banqup. Users then receive an account that is verified through itsme, allowing them to upload documents to the web application using itsme login to access the electronic registered delivery service.

3.1.5. Identifying receivers and senders

To verify the identity of the sender, we use Itsme during onboarding. Once the identity proofing has been completed successfully, the sender receives an account that is bound to their identity. The account is always subject to two-factor authentication.

To verify the identity of a recipient, we request identity information by using Itsme. The data provided by itsme to Banqup will not be retained and will only be used to verify the identity data submitted by the sender against the identity shared by the recipient via itsme.

The identification mean of Itsme is an eID with level of assurance "eIDAS High" and is an official notified eID for level of assurance "eIDAS High".

3.1.6. Authenticating receivers and senders

In the case of API usage by the sender, authentication is performed using the mutual SSL certificate. In the case of using the web portal, authentication of the sender is performed using the account issued to the sender.

For receivers, we do not maintain a separate authentication binding between an identity and a reusable authentication credential. Instead, authentication is performed before each delivery to the receiver, through the external identity provider itsme.

Access to the delivery is only granted if the identity confirmed during authentication matches the identity of the receiver determined during the identification process.

3.1.7. Notify of receipt

The potential receiver of a communication can be notified by email, SMS or adminBOX, for active adminBOX web-based users. The receiver does not need to create a formal account on the Banqup platform but will need to identify themselves using itsme before gaining access to the content of the communication.

3.2. Which personal information is stored and used

The personal data, together with the document, is stored for a period of 7 years. The data and document can be requested via the Banqup platform by the sender and/or receiver in the first year following the sending of the electronic registered delivery. After one year, the document must be requested via the service desk by means of a "document request" document. In addition to the content of the document, the following data is stored on the cover page which is added by the electronic registered delivery service:

- Name of the sender
- Date and time on which the electronic registered delivery service received the document
- Electronic signatures to ensure the integrity of the document
- A unique reference assigned by the electronic registered delivery service
- The contact name of the recipient (as provided by the sender)
- The postal address of the recipient (as provided by the sender)

In case the document is accepted:

- Date and time on which the recipient accepted the document
- The identity details of the recipient that gave a positive match (as provided by the sender)
- Unique itsme reference for acceptance with itsme

In case the document is not accepted before the expiry date:

- Date and time on which the document has expired

Only authorized employees in a trusted role and contractors who have signed a Data Protection Agreement have access to this information.

Data provided to Banqup via itsme will not be retained and will only be used to verify the identity data submitted by the sender against the identity shared by the recipient via itsme.

Banqup has defined a set of rules to perform the identity check. It is the following data that the service requests from the recipient via itsme in order to verify the identity as accurately as possible.

- family_name
- given_name
- birthdate
- email
- phone_number
- street_address
- locality
- postal_code
- country

Banqup ensures to have implemented the technical and organizational measures to protect personal information in accordance with the requirements of the GDPR directive 2016/679.

3.3. Obligations of parties

This section defines the obligations of the sender, the receiver and any relying parties in relation to the electronic registered delivery service.

A relying party is any entity that relies on the evidence generated by the service. This may include the sender, the receiver or a third party (e.g. auditor, court or supervisory authority).

3.3.1. Sender obligations

The Sender is responsible for:

- providing correct and sufficient identification data of the intended Receiver;
- ensuring that the personal data used for identification is accurate at the time of submission;
- selecting the correct receiver and delivery parameters;
- using the service in accordance with applicable legal and contractual requirements, such as this practice statement and the applicable general and trust service terms and conditions.

We rely on the data provided by the sender and do not verify the correctness of such data beyond the identity matching process described in this practice statement.

3.3.2. Receiver obligations

The Receiver is responsible for:

- identifying themselves using the provided identification mechanism;
- completing the identification and authentication process to access the delivered content;
- ensuring that the identity information shared during the identification process is correct.

Access to the content is only granted when the identity confirmed during authentication matches the identity determined during the identification process.

3.3.3. Relying Party obligations

Relying parties are responsible for:

- validating the evidence associated with electronic registered deliveries;
- verifying the integrity and origin of documents using the provided electronic seals and timestamps;
- interpreting the evidence in accordance with applicable legal and regulatory requirements.

We provide the technical means to support validation of the evidence but do not control or guarantee how relying parties interpret or use such evidence. Where the sender or receiver relies on the evidence for legal or operational purposes, they act in the role of relying party.

3.4. Evidence

For each electronic registered delivery, we generate an evidence set consisting of multiple evidence elements related to the delivery process.

A representation of the evidence set is included in the document cover page. Additional evidence elements may be retained within the service and made available via the platform or upon request.

The following event types are captured as part of the evidence set:

Event	Evidence	Interpretation	Access to evidence	Validity
Submission	Timestamped confirmation of receipt, including unique reference and electronic seal	Confirms that the Sender submitted the document and that it was received by the service	Part of the evidence set; available via the platform and reflected in the cover page where applicable	Valid from timestamp of submission; retained in accordance with evidence retention period (7 years)
Receipt of sending	Evidence record including timestamp and electronic seal	Confirms that the document was processed and accepted for delivery	Part of the evidence set; reflected in the document cover page and available via the platform	Valid from timestamp of submission; retained in accordance with evidence retention period (7 years)
Notification	Record of notification attempt (email, SMS or equivalent)	Confirms that the Receiver was notified of the document	Part of the evidence set; not necessarily included in the cover page; available via the platform or logs upon request	Valid as operational evidence; may be subject to shorter retention depending on logging policies

Event	Evidence	Interpretation	Access to evidence	Validity
Identification & authentication	Identity confirmation from the external identity provider (e.g. itsme), including unique reference	Confirms that a natural person successfully identified and authenticated	Part of the evidence set; relevant identity attributes are reflected in the cover page; additional data not stored or only temporarily used	Valid at the time of authentication; only referenced identifiers retained as part of evidence set
Acceptance (handover)	Timestamped record of successful access, including identity match and electronic seal	Confirms that the identified Receiver obtained access to the document	Part of the evidence set; relevant identity attributes are reflected in the cover page; additional data not stored or only temporarily used	Valid from timestamp of access; integrity ensured by seal and timestamp for the full retention period
Expiry (non-acceptance)	Timestamped record indicating that the document was not accessed within the defined period	Confirms that the document was not accepted before expiration	Part of the evidence set; relevant identity attributes are reflected in the cover page; additional data not stored or only temporarily used	Valid from expiry timestamp; retained as part of evidence set for the defined retention period

Each evidence element includes information on the event type, timestamp, involved identities and integrity protection.

All documents are sealed with a qualified electronic seal in PAdES B-T format, with an embedded qualified electronic timestamp. The qualified seal and qualified timestamp ensure the integrity and proof of existence of the document at the time of sealing. All documents and evidence are archived in write-once (WORM) form for the applicable retention period of 7 years. The documents and evidence can be retrieved by the sender and/or receiver via the Banqup platform during the first year following the delivery, and thereafter via the service desk by means of a document request.

3.5. Limitations on the use of service

The use of the electronic registered delivery service is subject to the following limitations:

- We rely on the identification data provided by the sender. Incorrect or incomplete data may result in failed or incorrect identification of the intended receiver.
- The identification of the receiver is based on a matching process using data provided by the sender and data obtained from an external identity provider. We do not guarantee that a match will always be successfully established.
- Notification of the receiver (e.g. via email, SMS or other communication channels) is not guaranteed. Failure to receive a notification does not prevent the availability of the document within the service.
- Access to the delivered content requires successful identification and authentication of the receiver. If the receiver does not complete this process, the document will not be accessed.
- Documents are only available for access within a defined validity period. After expiry of this period, the document can no longer be accepted by the receiver.
- The identification and authentication process depends on external identity providers. The availability and correct functioning of these providers are outside our control.

- Evidence is provided in the form of digitally sealed PDF documents (PAdES B-T format). The correct interpretation and validation of such evidence may require suitable software capable of verifying electronic seals and timestamps.
- We do not control the software environment or validation tools used by relying parties and cannot guarantee the correct interpretation of evidence outside the provided environment.

3.6. Supported user agents

The electronic registered delivery service is accessible through the following user agents:

- API interfaces supporting system-to-system integration, secured using mutual TLS authentication;
- Web-based user interfaces (web portal), accessed through standard web browsers and requiring user authentication via an external identity provider;
- Notification channels used to inform the receiver of the availability of a delivery, including email, SMS and, where applicable, other supported communication channels.

We do not impose specific requirements on the type of web browser or end-user device, provided that the user is able to access the service securely and use the required identification and authentication mechanisms.

The correct display and validation of delivered documents requires support for PDF documents and, where applicable, software capable of validating electronic seals and timestamps.

3.7. Delivery model and interoperability

3.7.1. Store and Notify (S&N) model

The electronic registered delivery service operates using a Store and Notify (S&N) model.

In this model:

- the document submitted by the sender is stored by the Trust Service Provider;
- the receiver is notified of the availability of the document via one or more notification channels;
- the receiver must identify and authenticate using the supported identification mechanism before accessing the document;
- the receiver is required to explicitly accept the document in order to complete the delivery process.

Delivery is considered to take place at the moment the receiver successfully identifies, authenticates and accepts the document. This event is recorded as part of the evidence set.

If the receiver does not accept the document within the defined validity period, the document expires. This is recorded as an expiry event within the evidence set.

The Receiver must accept the document within the validity period assigned to the delivery by the Sender (or defaulted by the service). The applicable validity period is communicated in the delivery notification and/or made visible in the user interface. If no acceptance occurs within that period, the document expires automatically.

3.7.2. Acceptance and expiry

The service requires an explicit action from the Receiver to accept the document.

- Acceptance occurs when the receiver, after successful identification and authentication, confirms access to the document.
- A timestamped record of acceptance is generated and forms part of the evidence set.
- If no acceptance occurs within the defined time period, the document expires and an expiry record is generated.

These events are reflected in the document cover page, which serves as a representation of the evidence set.

3.7.3. Messages relayed by other REM services

The service does not support the Store and Notify (S&N) model for messages relayed by another registered electronic mail service (REMS).

We process only messages submitted within our own service environment.

3.7.4. Interoperability with other REM and ERDS services

The service does not support the relaying of messages to or from other REMS or other electronic registered delivery services operated by third parties.

All messages are processed, stored and delivered within our service environment.

As a result, the service operates as a closed delivery system between the sender and the intended receiver.

3.7.5. Relation to evidence

The delivery model described above is directly reflected in the evidence generated by the service.

In particular:

- submission, notification, identification, acceptance and expiry are recorded as distinct events;
- each event results in corresponding evidence elements that form part of the evidence set;
- a representation of these evidence elements is included in the document cover page.

4. Policies

4.1. Terms and conditions

The terms and conditions are made available on the Banqup repository, which can be found at: https://www.pki.banqup.com. Banqup is liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under section 13.1 Regulation Intention or negligence of a QTSP shall be presumed, unless proven otherwise by the QTSP (see also Art. 24.2 (c) of the eIDAS regulation).

4.2. Security policy

Banqup maintains an Information Security Policy that governs the protection of all systems, data and processes involved in the provision of the Qualified Electronic Registered Delivery Service. The Security Policy is approved by the Information Security Steering Committee, communicated to all relevant employees and contractors, and reviewed at planned intervals or whenever significant changes occur.

4.3. Risk analysis

Banqup follows a risk-based approach to information security. Risks are continuously identified, monitored, assessed and evaluated to determine whether protective measures are required. The appropriateness of measures is evaluated (a) based on the observation that Banqup offers trust services that highly rely on trust and confidence and (b) their merits taking into account effectiveness, efficiency, cost, and practical feasibility.

A formal risk assessment is performed at least annually, unless a particular business or process context warrants a shorter interval. Such assessments identify, quantify and prioritize risks according to likelihood and impact, scored on a 1-5 scale across categories including regulatory/compliance, reputational, financial, fraud, privacy, and operational capacity. Results are maintained in a risk register and presented to the Information Security Steering Committee.

The CISO is responsible for ensuring that risk management processes are coordinated in accordance with policy. Each key role is responsible for implementing risk management within their domain. Risk assessments must be approved by the Information Security Steering Committee, and any risk exceeding the acceptable level requires a treatment plan to reduce it to an acceptable level, using one of the defined responses: modify, accept, transfer, or avoid.

The risk analysis includes:

- Unauthorized access to sensitive assets including but not limited to: infrastructure, hardware, data, certificates and private keys;
- Unauthorized changes to and deployment of the software;
- Protection of personal data against theft, unauthorized access, and incorrect disposal or alteration;
- Availability of the platform;
- Applicable laws and regulation.

To keep the information systems secure, various forms of configuration reviews are performed including:

- Yearly configuration review of the infrastructure and systems against our security policies;
- Continuous evaluation of the infrastructure and systems for unauthorized changes.

4.4. HR policy

All personnel involved in the operation and/or development of the QERDS service are vetted for a trusted role in accordance with the Roles & Responsibilities Policy.

In addition to the employment or consultancy contract, each employee and consultant signs and acknowledges the Banqup Group Security Policy. Both the Security Policy and the employment or consultancy contract include a confidentiality clause, stipulating that the employee or consultant shall respect and protect the confidentiality of all intellectual property and confidential information of Banqup and its customers.

4.5. Asset management

Banqup maintains updated inventories of its assets, including information assets. Security level of an asset is assigned in accordance with the risk assessment. Media containing sensitive data is securely handled and disposed when no longer required. This includes a thorough erasure process or secure disposal for physical media containing sensitive data.

4.6. Access control

The Identity & Access Control Policy ensures that system access shall be limited to authorized individuals keeping in mind principles such as segregation of duties and least privilege principle. These principles are also reflected in the Banqup Trusted Roles Policy.

4.7. Cryptography

The Cryptography Policy ensures the proper management of cryptographic keys throughout their lifecycle. This applies to all cryptographic keys used in relation to the services.

4.8. Physical and environmental security

The Physical Security Policy prevents unauthorized access to and damage to IT services, and protects information assets against loss, damage or compromise. The IT infrastructure for the trust service is located in cloud data centers. Only employees in specific trusted roles have access to the servers in these cloud data centers.

4.9. System acquisition, development and maintenance

Every organization needs to make changes to their IT environment. Those changes are, most of the time, driven by business needs. In other cases, those changes are necessary to prevent impact on the system's integrity or availability. Banqup ensures that changes are performed in a controlled manner.

4.10. Information security incident management

The management of security incidents and improvements is integrated within the overall operations model and the standard Incident Management Procedures. Incidents are logged, classified by impact level, and assigned accordingly. Security incidents are escalated to the CISO, who leads evaluation, containment, and reporting; privacy incidents involving personal data are additionally forwarded to the DPO. A lessons-learned process ensures that identified risks, corrective actions, and indicators of compromise are formally recorded to prevent recurrence.

4.11. Security & personal data breach notification

Banqup will, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

Banqup will also notify the [likely adversely affected] natural or legal [customer] of the breach of security or loss of integrity without undue delay.

4.12. Business continuity management

The service is designed with availability in mind. The Business Continuity Management Policy ensures to continue the service as fast and smoothly as possible without loss of data in case of a disruption.

Internally within Banqup, responsibilities are assigned, as well as the specification of processes to guarantee availability, continuity, security and privacy in all its services.

4.13. Network security

The network design includes network controls, security of network services and segregation of networks.

5. Third parties

5.1. BMID - itsme

itsme is used to identify the recipient and request confirmation from the recipient before viewing the communication. For this purpose, we use itsme solely as a provider of an electronic identification means (eID) with a level of assurance high.

Obligations of Itsme are:

- Delivering and Identity Proofing solution for Banqup in accordance with eIDAS High;
- Maintaining the notified status of eID at eIDAS High level.

5.2. Namirial

The seals attached to the documents are provided by Namirial. The seals in the PDF document are of type PAdES B-T, with an embedded qualified electronic timestamp. Banqup therefore also makes use of Namirial's qualified timestamping service. Namirial is a qualified trust service provider.

The document repository (including certificate policies and/or practice statements) of Namirial can be found here: https://www.namirial.com/en/documentation

Obligations of Namirial are:

- Rendering a seal service to seal the PDF documents;
- Rendering a qualified timestamping service;
- Maintaining QTSP status for qualified timestamping service;
- Maintaining QTSP status for the seal service.

5.3. AWS

All infrastructure is hosted by AWS. All physical resources are located in the Ireland (eu-west-1) region. AWS maintains many compliance programs, notably ISO 27001 and SOC 2, and is regularly audited for compliance.

AWS is not a (qualified) trust service provider.

Obligations of AWS are:

- Rendering hosting services;
- Rendering hosting services in accordance with service level agreements;
- Maintain ISO 27001 certified.

5.4. Monitor (Q)TSP status

Banqup monitors the qualification status of all involved third-party trust service providers. The qualification status is reviewed quarterly, and when a third party is found to have lost their QTSP certificate or qualified status for whatever reason, Banqup will take appropriate actions to define the next steps.

The following Qualified Trust Service Providers (QTSPs) are involved in the provision of the Qualified Electronic Registered Delivery Service:

Belgian Mobile ID (BMID) - itsme. Role: Provider of an electronic identification means (eID) at assurance level "eIDAS High", used for identity proofing and authentication of senders and recipients. itsme is a notified eID scheme under eIDAS at level of assurance High, as published in the Official Journal of the European Union.

Namirial S.p.A. Role: Qualified Trust Service Provider for electronic sealing and qualified electronic timestamping. Qualified services used:

- Electronic seal service (PAdES B-T) applied to delivered documents;
- Qualified electronic timestamping service.

Namirial is listed as a QTSP on the Italian Trusted List and its qualified services are published on the EU Trust List (EUTL).

6. Termination plan

Banqup maintains a Termination Plan that defines the procedures and responsibilities to be followed in the event of a planned or unplanned cessation of the Qualified Electronic Registered Delivery Service, ensuring continuity of evidence availability and minimal disruption to senders, receivers and relying parties.The Termination Plan, and any document associated with it, is reviewed at least annually and after any material change to ensure it remains up to date.

6.1. Notification of termination

Banqup will inform FOD Economie - SPF Economie as soon as the decision to terminate the service has been taken by Banqup.

All customers of the service will be informed at least 30 days before the actual termination of the service. The notification will include the date of termination, the termination plan and the practical arrangements to be taken.

All recipients will be informed about the termination of the service in the landing page where they are redirected to when starting the identification process. The notification will include the date of termination.

All the other parties which are involved in the electronic registered service will also be notified in order to terminate the contracts.

6.2. Continuation of the service

Banqup will reach out to relevant qualified trust service providers of the electronic registered delivery services in order to find a successor for the service, FOD Economie - SPF Economie will be kept up to date of these contacts and possible negotiations.

In case a successor is found, Banqup will make all the necessary arrangements to transfer all loggings to this successor and offer the existing customers the opportunity to move to the successor for the continuation of the service.

In case no successor is found, Banqup will settle an agreement with the Supervisory Body.

6.3. Practical arrangement after notification

Once all relying parties have been informed of the termination of the service, the following reduction of service will become effective:

- All intake accounts for existing customers will be de-activated. In doing so, no new electronic registered deliveries will be treated
- Outstanding electronic registered deliveries not yet accepted by the receiver will be kept available for acceptance by the receiver up to the given days by the sender after the notification date.
- Already accepted electronic registered deliveries will be kept live for download by the receiver for the period mentioned in the general terms and conditions.

7. Compliance

Banqup will monitor the evolution of legislation to make sure that the services are created and maintained in line with any applicable legal requirements. Therefore, Banqup will also select a recognized conformity assessment body every 24 months to run an audit on the compliance of Banqup and the Trusted service for Electronic Registered Delivery with the eIDAS regulation and accompanying Commission Implementation Regulations (CIR's). The TSP's management will also respect the required reviews defined in ETSI EN 319 401, ETSI EN 319 521 and ETSI EN 319 531.

7.1. Recurrent audit

Banqup will select a recognized conformity assessment body to run an audit on the compliance of Banqup and the Trusted service for Electronic Registered Delivery with the eIDAS regulation. This audit will be planned at least every 24 months and at each significant change in the application software, platform architecture or change in geographical application of the service.

These audits will be conducted at the costs of Banqup.

The resulting conformity assessment report will be submitted to the Belgian supervisory body (FOD Economie - SPF Economie). In case the report stipulates any non-conformity, Banqup will rectify the non-conformity within the timeframe stipulated by FOD Economie - SPF Economie.

7.2. Audit on request

When the FOD Economie - SPF Economie (supervisory body) requests an ad-hoc audit, Banqup will select a recognized conformity assessment body to conduct the audit on the Trusted Service Electronic Registered Delivery offered by Banqup.

The audit will be conducted at the costs of Banqup.

The resulting conformity assessment report will be submitted to the Belgian supervisory body (FOD Economie - SPF Economie). In case the report stipulates any non-conformity, Banqup will rectify the non-conformity within the timeframe stipulated by FOD Economie - SPF Economie.

7.3. Notification to the Supervisory Body

Banqup shall notify the supervisory body of any significant changes to its qualified trust services, in the following cases and using the following procedures:

The supervisory body shall be notified when Significant changes occur to:

- Service descriptions, policies, practice statements, or associated terms and conditions.
- Technical architecture of the trust services, or any trustworthy systems or products in use.
- Hosting or technical services of any components used to provide the qualified trust services.
- Cryptographic techniques or materials used in the provision of the services.
- Registration and identification procedures.
- Organisational structure or governance.
- Termination plans.
- Financial resources or liability insurance.
- Elements affecting the content of the national trusted list.
- Third parties involved in providing the qualified trust services, including subcontractors or changes to contractual terms.

Notifications to the supervisory body shall be made in a structured and timely manner. Each notification shall include:

- A description of the change or planned cessation of services.
- The scheduled date and time for the implementation of the change.
- The reasons for the change, supported by evidence where applicable.
- Any updated or amended documentation relevant to the change.

Notifications shall be submitted sufficiently in advance of the planned implementation to allow the supervisory body to review and assess potential compliance impacts. Submissions may be made electronically or in writing, in accordance with the supervisory body’s preferred communication method.

7.4. Security of transmission

We ensure the security of transmission of electronic registered deliveries against risks of loss, theft, damage and unauthorized alteration.

The following measures are applied:

- The PDF documents are transmitted between the sender, us and the receiver over secured communication channels using TLS-based encryption.
- For system-to-system integrations, mutual TLS (mTLS) is used to authenticate the sender system and to protect the integrity and confidentiality of the transmitted data.
- PDF documents are protected against unauthorized alteration by applying an electronic seal and timestamp. These ensure the integrity of the document throughout the delivery process.
- Access to the delivered content is only granted after successful identification and authentication of the receiver, ensuring that only the intended recipient can access the content.
- PDF documents and associated data are stored in controlled environments with appropriate security measures to prevent unauthorized access or modification.

These measures collectively ensure that the transmission and handling of electronic registered deliveries are protected throughout the entire delivery process.

7.5. Qualified trusted service application

Banqup will only offer the described trust service as a qualified trust service once FOD Economie - SPF Economie has published the qualification in the trusted list. When using the EU trust mark, Banqup will ensure that the mark contains a link to the trusted list entry of this qualified trust service.

Any failure (non-conformity) to meet the requirements of the eIDAS Regulation will be rectified by Banqup within the timeframe stipulated by FOD Economie - SPF Economie.