Electronic registered delivery service

Practice statement

V1.1

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com

Table of Contents

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com

1 Document Control

Version History

Version	Date	Status	Author	Approval	Comments
1.0	23/09/19		Glenn Callaerts	Governance board	Created the initial version of the practice statement
1.1	21/10/19	Active	Glenn Callaerts	Governance board	Monitoring third parties Sender authentication via MSSL

Approval Status

Revision	Approval date	Approver	Approver Role
1.1	26/12/2019	Tom Van Acker	General Manager - COO
1.1	03/01/2020	Kris Van Kelst	Product Manager
1.1	15/01/2020	Soâd El Bouchtaoui	Senior Legal Council
1.1	03/01/2020	Jeroen Mabille	CSO

This document is reviewed annually by the TSP's governance board[1]

[1] The governance board is described in the general term and conditions

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com

This document describes the practices and policies applied by Unifiedpost 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 Overview

2.1 General

UnifiedPost SA, with headquarters in 1310 La Hulpe, Avenue Reine Astrid 92A and registered under enterprise identification 0471.730.202 is offering the electronic registered delivery service as an add-on to its already established electronic delivery products. The electronic registered delivery is provided in accordance with eIDAS regulation (EU) No. 910/2014 of the European Parliament and Council. 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 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

2.2 Electronic registered delivery service

The service offers a typical communication between 2 parties in one direction, where there is a sender of the communication and a receiver. The offering of UP will offer different functionalities to both parties, being the sender or the receiver, keeping in mind that one party can be the sender for one communication and the receiver for another communication. UP ensures that the document uploaded by the sender will be sent electronically to the specific receiver defined by the sender. As we rely on the information provided by the sender, we can't ensure that the receiver will receive the notifications about the document, or the right receiver will be notified. In either case, the receiver will need to identify himself to get access to the content of the document. When the identity of the receiver matches the identity sent by the sender, the respective receiver will get access to the content of the document.

2.2.1 Onboarding

The service as a sender is open for all natural persons and legal persons having signed a sender contract with UP and has passed the KYC process at UP. They receive then an account and a signed certificate so they can upload documents via mutual SSL to the electronic registered delivery service.

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com

2.2.2 Notify of receipt

The potential receiver of a communication can be notified by either email, SMS or adminBOX, for active adminBOX web-based users. The receiver does not need any formal account creation on the UP platform but will need to identify himself using Itsme before getting access to the content of the communication.

3 Policies

3.1 Terms and conditions

The terms and conditions are made available on the website of UP.

3.2 Security policy

Current applicable version is 2.0, which was last reviewed on 10/9/2019 by the Information Security Steering Committee.

- Risk analysis: UP follows a risk-based approach to information security. Risks are continuously identified, monitored, assessed and then evaluated to see whether an intervention with protective measures is needed. The appropriateness of measures should be evaluated (a) based on the observation that UP offers services that highly rely on trust and confidence as well as (b) their merits taking into account effectiveness, efficiency, cost, and practical feasibility.

  An overall risk assessment of the information systems should be performed annually unless a particular business or process warrants a shorter period. Such a risk assessment shall identify, quantify and prioritize the risks according to the relevant criteria for acceptable risks.

  The CSO shall be responsible for ensuring that the risk management processes are coordinated in accordance with the policy. Each of the key roles identified above shall be responsible for ensuring that risk management processes are implemented within their domains in accordance with the policy. Risk management must be carried out in accordance with the criteria approved by management and risk assessments must also be approved by management.

  Any risk assessment that reveals risks that exceed the acceptable level, measures must be implemented to reduce the risk to the acceptable level.

  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

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com

- Applicable laws and regulation

3.3 HR policy

All personnel involved in the operation and/or development of the service is assessed during the hiring process on the necessary qualifications and experience to perform the role for which they are (or will be) hired. The same assessment applies to consultants hired on a temporary or permanent basis.
In addition to the employment/consultancy contract, each employee/consultant signs and applies the UP Group Security Policy. This Security Policy and the employment/consultancy contract include a confidentiality clause, stipulating that the employee/consultant shall respect and protect the secrecy of the intellectual property and all confidential information of UP and its customers.
All personnel working on the offered service has a role assigned defined in line with the Unifiedpost Trusted Roles Policy.

3.4 Asset management

UP 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.

3.5 Access control

The UP 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 Unifiedpost Trusted Roles Policy.

3.6 Cryptography

The Cryptography Policy ensures the proper management of cryptographic keys throughout their lifecycle.
This is the case for all cryptographic keys that are being used in relation to the services.

3.7 Physical and environmental security

The physical and environmental security policy ensures to prevent unauthorized access or damage to IT services. To prevent the loss of, damage to, or compromise to information assets. The IT infrastructure for the trusted service is located in cloud data centers. Only the IT OPS employees have access to the servers in the cloud data centers. None of the UP personnel has physical access to cloud data centers.

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com

3.8 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. UP ensure that changes are performed in a controlled fashion

3.9 Information security incident management

The management of security incidents and improvements is integrated within the overall operations model and the standard incident management procedures there. Incidents are logged and assigned based on their classification. Security and privacy incidents are also/automatically forwarded to the CSO or DPO respectively, to keep him/her informed, and take immediate appropriate action.

On a monthly basis, incidents and events are reviewed on the Operational Management Committee, in order to further determine appropriate actions for further mitigation if required.

3.10 Business continuity management

The service is designed with availability in mind. The business continuity management policy ensures to continue the service as fast and smooth as possible without loss of data in case of a disruption.

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

3.11 Network security

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

4 External Components

4.1 Itsme

Itsme is used in the process to identify the recipient and asking the recipient for confirmation. Itsme is a trust service provider.

4.2 Namirial

The seals attached to the documents are provided by Namirial. The seals in the PDF document are of type PAdES LTV (long term validation). Beside the seal service, we also use the qualified timestamp service. Namirial is a trust service provider.

4.3 AWS

All infrastructure is hosted by AWS. All physical resources are located in the Ireland (eu-west-1) region. AWS has many compliance programs (notably ISO27001) and is regularly audited for compliance.

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com

4.4 Monitor third parties

UP created a tool that will monitor the third-party solutions. When one of the third parties will lose their TSP certificate for whatever reason, an alert is triggered and UP will take the appropriate actions to define the next steps.

5 Termination plan

UP created a termination plan which describes the procedures to follow in case of cessation of Qualified electronic registered delivery services.

5.1 Notification of termination

Unifiedpost will inform the Federal Public Services Economy as soon as the decision to terminate the service has been taken by Unifiedpost.

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.

5.2 Continuation of the service

UP will contact all qualified trusted service providers of the electronic registered delivery services in order to find a successor for the service. FPS Economy will be kept up to date of these contacts and possible negotiations.

In case a successor is found, UP will make all the necessary arrangement 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, UP will settle an agreement with the Supervisory Body.

5.3 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.

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com

All documents are sealed with a seal of type PAdES LTV (long term validation). The holder of the PDF will therefore be able to check the validity of the certificate using signature validation software even after the expiration of the certificate and without intervention of Unifiedpost.

6 Compliance

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

6.1 Recurrent audit

UP will select a recognized conformity assessment body to run an audit on the compliance of UP 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 UP.
The resulting conformity assessment report will be submitted to the Belgian Federal Public Service of Economy. In case the report stipulates any non-conformity, UP will rectify the non-conformity in the delay as stated by the Federal Public Service of Economy.

6.2 Audit on request

When the Federal Public Service of Economy request ad-hoc audit, UP will select a recognized conformity assessment body to run the audit on the Trusted Service Electronic Registered Delivery, offered by UP.
The audit will be conducted at the costs of UP.
The resulting conformity assessment report will be submitted to the Belgian Federal Public Service of Economy. In case the report stipulates any non-conformity, UP will rectify the non-conformity in the delay as stated by the Federal Public Service of Economy.

6.3 Qualified trusted service application

UP will only offer the described trusted service as a Qualified Trusted Service when the Federal Public Service of Economy has published the qualification in the trusted list.
When using the EU trust mark, UP will ensure that the mark will also contains a link to the Trusted List of this Qualified Trust Service.

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com

Any shortcoming to meet the requirements of the eIDAS ruling, will be rectified by UP in the delay as stated by the Federal Public Service of Economy.

Unifiedpost SA
Avenue Reine Astrid 92A
B-1310 La Hulpe

KBC 734-0128028-94 - SWIFT KREDBEBB
IBAN BE87 7340 1280 2894
RPR Nivelles - TVA BE 0471730202

Tel: +32 2 634 06 28
Fax: +32 2 633 46 61
www.unifiedpost.com