Context

In its capacity as Solution Provider of the eDelivery Building Block, the Directorate-General for Informatics (DIGIT) makes available the eDelivery PKI service[1] to organisations participating in eDelivery-based projects operated by European Union (EU) and European Economic Area (EEA) public administrations. Such public administrations first have to establish themselves as "PKI domain owners" in relationship to the service. The organisations who are authorised by the PKI domain owner to be part of their domain can then use the eDelivery PKI service to obtain digital certificates.

The digital certificates can be used exclusively for the purpose of digital encryption and/or signing by eDelivery components, i.e., eDelivery Access Points (AP) and/or Service Metadata Publishers (SMP).

The eDelivery PKI service uses the CommisSign-2 PKI service of the European Commission to issue digital certificates. In relationship to the CommisSign-2 PKI service DIGIT plays the role of Local Registration Authority (LRA) for all digital certificates issued via the eDelivery PKI service. As LRA, DIGIT ensures the segregation by PKI domain of the digital certificates it issues.

This document contains the General Terms and Conditions of using the eDelivery PKI service for the **DOMAIN NAME** PKI domain (hereinafter referred to as "the project"). As LRA, DIGIT issues, revokes and renews the certificates of this project. The owner of the project, the **PROJECT OWNER NAME** is established as the PKI domain owner and is involved in these tasks by approving, rejecting or deferring the certificate applications received from the organisations.

Terms of Service

Agreement of the PKI domain owner

By agreeing to the present General Terms and Conditions, the PKI domain owner understands and confirms that:

- the service is delivered according to the project-specific Service Offering Description document of the eDelivery PKI service[2], which is itself subject to future changes. Such changes will be notified to the PKI domain owner.
- it is subject to the roles and responsibilities, practical modalities and terms and conditions defined in the project-specific Service Offering Description document of the eDelivery PKI service.
- before approving an organisation's certificate application, it is responsible to ensure that the latter was informed about and agreed to the parts of the present General Terms and Conditions and of the project-specific Service Offering Description document of the eDelivery PKI service that are relevant to it.

[1] A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates.
[2] The latest version of the generic Service Offering Description document is available at https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/PKI+Service.

Limitation of use

The PKI Service can be used to have up to 60 active certificates issued at any given time for all concerned eDelivery-related systems and environments necessary for the PKI Domain. Once this limit is reached, requests to issue further certificates will be rejected until the expiration or revocation of active certificates. A domain requiring more than 60 active certificates will have to rely on other Certification Authorities for obtaining certificates.

Disclaimer on liability

In no event shall the European Commission be liable to the PKI domain owner, the organisation[3], anyone claiming through the PKI domain owner or anyone claiming through the organisation, for any kind of damages resulting from reliance on the service or on the certificate issued by the eDelivery Public Key Infrastructure (PKI) service.

The European Commission accepts no responsibility or liability whatsoever with regard to the content of the certificate which remains exclusively with the certificate owner. It is the responsibility of the certificate owner to check the accuracy and appropriateness of the certificate content.

The European Commission accepts no responsibility or liability whatsoever with regard to the use of the certificate by its owner, who is a third legal entity outside the European Commission.

This disclaimer is not intended to limit the liability of the European Commission in contravention of any requirements laid down in applicable national law or to exclude its liability for matters which may not be excluded under that law.

Processing of personal data by PKI domain owner

The processing of personal data by the PKI domain owner as part of the provision of the eDelivery PKI service shall meet the requirements of Regulation (EU) 2018/1725 and be done exclusively in order for the PKI domain owner to implement its role as defined in this document and the project-specific Service Offering Description document. For the purposes of this agreement, the PKI domain owner acts as a data processor.

The localisation of and access to the personal data processed by the PKI domain owner to approve the request shall comply with the following:

- the personal data shall only be processed within the territory of the European Union and the European Economic Area and will not leave that territory;
- the data shall only be held in data centres located with the territory of the European Union and the European Economic Area;
- no access shall be given to such data outside of the European Union and the European Economic Area;
- any transfer of personal data to third countries or international organisations shall fully comply with the requirements laid down in Chapter V of Regulation (EU) 2018/1725[4].

[3] Identified by the "O=" attribute value in the Subject Distinguished Name of the issued certificate

[4] Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295/39, 21.11.2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&from=EN

The PKI domain owner shall assist DIGIT for the fulfilment of its obligation to respond to requests for exercising rights of person whose personal data is processed in relation to this contract as laid down in Chapter III (Articles 14-25) of Regulation (EU) 2018/1725. The PKI domain owner shall inform without delay DIGIT about such requests.

The PKI domain owner may act only on documented written instructions and under the supervision of DIGIT, in particular with regard to the purposes of the processing, the categories of data that may be processed, the recipients of the data and the means by which the data subject may exercise its rights.

The PKI domain owner shall grant personnel access to the data to the extent strictly necessary for the implementation, management and monitoring of the contract. The PKI domain owner must ensure that personnel authorised to process personal data has committed itself to confidentiality or is under appropriate statutory obligation of confidentiality.

The PKI domain owner shall adopt appropriate technical and organisational security measures, giving due regard to the risks inherent in the processing and to the nature, scope, context and purposes of processing, in order to ensure, in particular, as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
(e) measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed.

Irrespective of the above, the communication between the PKI domain owner and the European Commission may take place via unencrypted email and using this mode of communication shall not be considered in breach of the requirements set out in these General Terms and Conditions

The PKI domain owner shall notify relevant personal data breaches to DIGIT without undue delay and at the latest within 48 hours after the PKI domain owner becomes aware of the breach. In such cases, the PKI domain owner shall provide DIGIT with at least the following information:

(a) nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) likely consequences of the breach;
(c) measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The PKI domain owner shall assist DIGIT for the fulfilment of its obligations pursuant to Article 33 to 41 under Regulation (EU) 2018/1725 to:

(a) ensure compliance with its data protection obligations regarding the security of the processing, and the confidentiality of electronic communications and directories of users;
(b) notify a personal data breach to the European Data Protection Supervisor;
(c) communicate a personal data breach without undue delay to the data subject, where applicable;
(d) carry out data protection impact assessments and prior consultations as necessary.

The PKI domain owner shall maintain a record of all data processing operations carried on behalf of DIGIT, transfers of personal data, security breaches, responses to requests for exercising rights of people whose personal data is processed and requests for access to personal data by third parties.

The PKI domain owner shall notify DIGIT without delay of any legally binding request for disclosure of the personal data processed on its behalf made by any national public authority, including an authority from a third country. The PKI domain owner may not give such access without the prior written authorisation of DIGIT.

The duration of processing of personal data by the PKI domain owner will not exceed the latter's use of the eDelivery PKI service. Upon expiry of this period, the PKI domain owner shall effectively delete all personal data unless Union or national law requires a longer storage of personal data.

If part or all of the processing of personal data is delegated to one or more third parties, the PKI domain owner shall pass on the obligations referred to in this section in writing to those parties. At the request of DIGIT, the PKI domain owner shall provide a document providing evidence of this commitment.

Termination of the provision of the PKI service

The provision of the PKI service can be terminated by DIGIT at any time. Equally, the PKI domain owner can request the termination of the provision of the service at any time.

DIGIT reserves the right to stop providing the PKI service at any time. Under normal circumstances, DIGIT will notify the PKI Domain Owner of the service termination by email at least 3 months in advance, after which it will proceed to revoke all certificates issued for that PKI domain. In extraordinary circumstances including, but not limited to, security incidents, the service may be stopped effective immediately and all certificates may be revoked without delay. In this latter case, a notification may only be sent after the fact.

In case the PKI domain owner wishes to stop using the PKI service, it should notify DIGIT about it by email to EC-EDELIVERY-SUPPORT@ec.europa.eu. In this case, DIGIT will revoke all certificates issued for that PKI domain within a period no longer than one month.

In both cases, it is the sole responsibility of the PKI domain owner to inform organisations that obtained a certificate that their certificate will be revoked. DIGIT will **not** notify individual organisations.

Changes of the General Terms and Conditions

The European Commission reserves the right to change these General Terms and Conditions under which it is providing the service. The PKI domain owner will be notified of any such future changes 30 days in advance of their entry into force. In case the PKI domain owner disagrees with the updated General Terms and Conditions, it must notify its choice to stop using the service by email to EC-EDELIVERY-SUPPORT@ec.europa.eu before the expiration of the 30 days. In this case, DIGIT will revoke all certificates issued for the PKI domain. Conversely, an absence of a reaction from the PKI domain owner during the 30 days shall be understood as agreement to the new General Terms and Conditions, which enter into force at the end of the 30 days.

Authorised/prohibited uses of certificates

Permitted usage of certificates

Once the certificate is issued, the organisation (also referred to as the "certificate owner") shall use the certificate only in the context of the project. Within this context, certificates can be used to provide the following functionalities exclusively for operating deployed eDelivery Access Points (APs) or deployed eDelivery Service Metadata Publishers (SMPs):

- authenticate the origin of data;
- encrypt data;
- ensure detection of integrity breaches of data.

Prohibited usage of certificates

Any usage not explicitly authorised as part of the permitted usages of the certificate is prohibited.

Additional obligations of the organisation

The detailed terms and conditions of the CommisSign-2 PKI service are defined in the Certificate Policy (CP)/Certificate Practice Statement (CPS)[5] of the CommisSign-2 PKI service. This document includes security specifications and guidelines regarding technical and organisational aspects and describes the activities of the Trust Centre operator in the roles of Certification Authority (CA) and Registration Authority (RA) as well as the Registration Authority's (RA) delegated third party.

It should be highlighted that:

- Only organisations authorised to participate in the project can request a certificate, as described in the Service Offering Description document of the eDelivery PKI service for the project.
- Regarding certificate acceptance, clause 4.4.1 of the CP/CPS applies, furthermore the terms of use and provisions described in the present document are deemed accepted by the organisation to which the certificate is issued when first used.
- Regarding publication of certificate information, clause 2.2 of the CommisSign-2 PKI service CP/CPS applies.
- All certificate owners shall comply with the following requirements:
    - Protect their private key against unauthorized use.
    - Refrain from transferring or revealing their private key to third parties, even as representatives.
    - Refrain from continued use of the private key following expiry of the validity period or revocation of the certificate, other than to view encrypted data.
    - The certificate owner is responsible for copying or forwarding the key to the end entity or entities.
    - The certificate owner must obligate the end entity/all end entities to comply with the present terms and conditions, including the CommisSign-2 PKI service CP/CPS, when dealing with the private key.
    - The certificate owner must provide the identification of its representatives who are authorised to request revocation of certificates issued to the organisation, providing the details of the events that led to issuing the revocation request.
    - For certificates associated to groups of persons and functions and/or legal persons, after a person leaves the group of end entities (e.g. termination of the employment relationship), the certificate owner must prevent misuse of the private key by revoking the certificate.
    - Certificate owner is responsible and has obligation to request revocation of certificate under circumstances identified in clause 4.9.1 of the CommisSign-2 PKI service CP/CPS.
- Regarding renewal or re-key of certificates, clause 4.6 or 4.7 of the CommisSign-2 PKI service CP/CPS applies.
- Regarding modification of certificate, clause 4.8 of the CommisSign-2 PKI service CP/CPS applies.
- Regarding certificate revocation and suspension, clause 4.9 of the CommisSign-2 PKI service CP/CPS applies.

[5] The latest version of the document can be downloaded from the CommisSign-2 PKI site: https://commissign.pki.ec.europa.eu/info/cp/CPS.pdf