# Terms and conditions

## Use, acquisition and management of qualified certificates.

INCERT GIE
ZI Am Bann 2
Rue de Drosbach
L-3372 Leudelange - Luxembourg
Luxembourg Trade and Companies Register number: C101 / VAT number: LU25655759

This document describes the terms and conditions applied to the Electronic Signing certificate service provided by INCERT, but also include the PKI Disclosure Statement (PDS), as required by European standard ETSI EN 319 411-1 V1.

# 1-Definitions and acronyms

| Terms and acronyms | Definition |
|---|---|
| **CA** | Certification authority: structure responsible for issuing and verifying electronic certificates and certificate Revocation Lists with electronic signature. |
| **Certificate** | An electronic file containing the identification elements of the user: Public Key, together with additional information, laid down in the Certificate Profile rendered unforgeable via encipherment using the Private Key of the Certificate Authority which issued it |
| **CP** | Certificate Policy for qualified certificates. |
| **CPS** | Certification Practice Statement |
| **CRL** | Certificate Revocation List: Lists of blocked certificates, periodically issued by the CA |
| **OCSP** | Online Certificate Status Protocol |
| **RA** | Registration Authority: entity that is in charge of carrying the processes related to the registration of the User. |
| **Public Key** | The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by Relying Parties to verify electronic signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key. |
| **Private Key** | The key of a key pair that is assumed to be kept in secret by the holder of the key pair, and that is used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key. |
| **PIN code** | Personal Identification Number: activation code for the Qualified Certificates for Electronic Signatures |
| **Renewal** | Procedure enabling the User to renew his or her Subscribed Service when its validity has expired. In the case of Subscribed Services using Certificates, renewal enables the Certificate to be re-keyed or the User to receive another Certificate whose initial generation data remain the same but whose key changes. |
| **eIDAS** | Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. |

| | |
|---|---|
| **Qualified Certificate** | Qualified Certificate is a Certificate issued by a CA which has been accredited and supervised by authorities and meets the requirements of eIDAS. |
| **User** | A person/entity to whom the certificates are issued. |
| **Relying Party** | Entity that relies on the information contained within a Certificate. |
| **Qualified trust service** | A trust service, as defined in eIDAS, that meets the applicable requirements laid down in this Regulation. |
| **Qualified trust service provider** | A trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body. |
| **Subscriber** | An entity subscribing with Trust Service Provider who is legally bound to any subscriber obligations. |
| **Terms and conditions** | Present document that describes the obligations and responsibilities of the Subscriber while using the Certificates and the obligations and responsibilities of the provider while delivering certificates. |

## 2-Contact Information

**2.1**-Any requests regarding the subscribed service must be made exclusively by one of the following means:

**(a)** By postal letter sent to the following address, the communication deemed to have been received within three (3) business days after the date of dispatch:

-Zi Am Bann 2, Rue de Drosbach L-3372 Leudelange, Grand Duchy of Luxembourg.

**(b)** By mail sent to the following address, the communication deemed to have been received within four (4) business hours after its dispatch:

-contact@incert.lu

**(c)** By fax to the following number, the communication deemed to have been received within four (4) business hours after its dispatch:

FAX: +352 27 32 67 29

# 3-General terms

**3.1-**Present General Terms and Conditions describe main policies and practices followed by INCERT and provide PKI Disclosure Statement (PDS) for Qualified Signing Certificate.

**3.2-** The Terms and Conditions govern Subscribers' use of the Certificates and constitute a legally binding contract between subscriber and INCERT.

**3.3-** The Subscriber has to be familiar with the Terms and Conditions and accept them upon receipt of the Certificates.

**3.4-** INCERT has the right to amend the Terms and Conditions at any time should INCERT have a justified need for such amendments. Information on the amendments shall be published on the website https://incert.lu

**3.5-**The subscriber can apply for:

**(a)** Qualified Signing Certificate.

# 4-Certificate Acceptance

**4.1**-Upon submitting an application for a certificate, the subscriber confirms that the information.

**4.2**-If the certificate re-keying is performed the subscriber confirms that he/she has read and agrees to the terms and conditions.

**4.3**-Certificate type, validation Procedure and Usage

| Certificate Type | Usage | Certification Policy Applied |
|---|---|---|
| **Qualified Signing certificate** | Qualified Electronic Signature Certificate is intended for creating Qualified Electronic Signatures compliant with eIDAS. | ETSI EN 319 411-2 Policy: QCP-n-QSCD |

**4.4**-The use of the Subscriber´s Certificates is prohibited for any of the following purposes:

**(a)** Unlawful activity (including cyber-attacks and attempt to infringe the Certificate);

**(b)** Enabling other parties to use the Subscriber's Private Key;

**(c)** Enabling the Certificate issued for electronic signing to be used in an automated way;

**(d)** Using the Certificate issued for electronic signing for signing documents which can bring about unwanted consequences (including signing such documents for testing purposes).

## 5-Reliance limits

**5.1**- Certificates become valid as of the date specified in the Certificate.

**5.2**- Certificates become invalid on the date specified in the Certificate or when the Certificate is revoked.

**5.3**- Audit logs are retained on-site for no less than 7 years. Physical or digital archive records regarding Certificate applications, registration information and requests or revocation are retained for at least 7 years after the expiry of the relevant Certificate.

## 6-Subscriber's rights and obligations

**6.1**-The Subscriber has the right to submit an application for issuing the Certificate.

**6.2**-The Subscriber is obligated to:

**(a)** Warrants that he or she will provide all the information or documents required by the State Registration Authority for the Subscribed Service;

**(b)** Is solely liable for the Subscribed Service used by him or her;

**(c)** Is liable with regard to INCERT and to third parties for any errors or fraud committed by him or her using the Subscribed Service, as well as for any case in which the Device or the Access Codes are compromised by him or her, whether purposely or inadvertently;

**(d)** Warrants that he or she will use the Subscribed Service in conformity with the Contract, the Procedures and any and all regulations regularly communicated by INCERT;

**(e)** Warrants that he or she will take the necessary security precautions in order to prevent the Subscribed Service from being compromised;

**(f)** Is solely liable for implementing, maintaining and developing a technical infrastructure

(including hardware and software) which permits the use of the Subscribed Service;

**(g)** Is liable, jointly and severally (as the case may be) with the Recipients or any third parties, for the content of messages or transactions signed by means of the Subscribed Service.

**(h)** Immediately notify INCERT in case of a change in personal details.

**(i)** Protect his/her private key and must have the sole control on it**.**

## 7-INCERT's rights and obligations

**7.1**-INCERT has the right to revoke Certificates if it has reasonable doubt that the Certificate contains inaccurate data or is out of control of its owner and can be used without Subscriber's permission.

**7.2**-As a service provider, INCERT is obligated to:

**(a)** Provide the Subscribed Services under the Terms and Conditions specified in the Contract and the Procedures;

**(b)** Guarantee the availability of the Subscribed Services within the limits set out in the Contract;

**(c)** Ensure access to the updated Revocation Lists for the public and, more specifically, for the User, on a 24/7 basis;

**(d)** Put in place an online verification service to determine the status of the Subscribed Service, available 24/7.

**(e)** Provide security with its internal security procedures;

**(f)** Ensure that the certification keys are protected by hardware security modules and are under control of INCERT.

## 8-Certificate status checking obligations of relying parties

**8.1**-Relying Parties studies the risks and liabilities related to acceptance of the Certificate. All those who rely on the information contained in certificates must verify that certificates are revoked. Such

verification can be performed by consulting the list of revoked certificates (CRL) published by the CA or by querying the OCSP service provider by the CA, at the URLs addresses contained in certificate themselves.

**8.2**-INCERT ensures availability of Certificate Status Services 24 hours a day, 7 days a week.

## 9-Limitation of liability of INCERT

**9.1**-INCERT shall not be liable for any direct and indirect consequences as the result of:

**(a)** Lack of compatibility between the Subscribed Service, including the Device and the equipment, and the applications, procedures or infrastructures of the User or the Recipient or of any third party;

**(b)** Any unavailability of the Subscribed Services subsequent to any deactivation or renewal permitted under the Contract;

**(c)** Any security flaw originating from the User, the Recipient or any third party and, more generally, of any security flaw not directly attributable to INCERT;

**(d)** Consequences of errors and/or fraud committed by the User, the Recipient or a third party;

**(e)** Any unavailability or malfunction of electronic communications systems or networks;

**(f)** Any unavailability of the Subscribed Services in the event of imminent risk to the security of INCERT systems;

**(g)** The User's inability to decrypt some or all of the data encrypted using the User's public key, where the User does not have access to his or her private key;

**(h)** The respective contact information which are incorrect or not updated by the User.

**9.2**-INCERT ensures that:

**(a)** Certificates are revoked after the request's legality has been verified. The revocation of

the Certificate is recorded in the Certificate database of INCERT and in CRL no later than 24 hours after an application has been submitted. The CRLs of the issuing CAs are published every one (1) hour and at least once every 24 hours.

**(b)** It has compulsory insurance contracts covering all INCERT services to ensure compensation for damages caused by INCERT's breach of obligations.

**(c)** The certification keys are protected by hardware security modules (i.e. HSM) and are under sole control of INCERT.

**(d)** The certificate has a validity period of three (3) years.

## 10-Applicable agreements, CPS, CP

**10.1-**More details on the supported certificate policies (CP) and the Certification Practice Statement (CPS) are available in the "PPKI1 Certificate Policy" and the "PPKI1 Certificate Practice Statement" documentation, available on the INCERT web site.

## 11-Privacy policy and confidentiality

**11.1**-INCERT follows the Principles of Client Data Protection and complies with the GDPR (UE regulation N°679/2016) acts when handling personal information and logging information.

**11.2**-All information that has become known while providing services and that is not intended for disclosure (e.g. information that had been known to INCERT because of operating and providing Trust Services) s confidential. The Subscriber has the right to obtain information from INCERT about him/herself pursuant to the law.

**11.3**-INCERT secures confidential information and information intended for internal use from compromise and refrains from disclosing it to third parties by implementing different security controls.

**11.4**-INCERT has the right to disclose information about the Subscriber to a third party who pursuant to relevant laws and legal acts is entitled to receive such information.

**11.5**-Additionally, non-personalized statistical data about INCERT's services is also considered public information. INCERT may publish non-personalized statistical data about its services.

**11.6**-The registration information is retained for 7 years after the end of the Certificate validity period.

**11.7**-The Subscriber is aware and agrees to the fact that during the use of Certificates in digital identification, the person conducting the identification is sent the Certificate that has been entered in Subscriber´s Document and contains Subscriber´s name and personal identification code.

**11.8**-The Subscriber is aware and agrees to the fact that during the use Certificates for digital signature, the Certificate that has been entered in their Document and contains their name and personal identification code is added to the document they digitally sign.

## 12-Applicable laws, complaints and dispute resolution

**12.1**-All CA services provided by INCERT are subject to Luxemburgish and European laws. The applicability, execution, interpretation and validity of the CPS are governed by Luxemburgish laws and by directly applicable European laws.

**12.2**-For all legal disputes related to the INCERT's CA service, where INCERT is plaintiff or defendant, the court of justice of Luxembourg shall have exclusive jurisdiction, with the exclusion of any other court.

## 13-TSP and repository licenses, trust marks, and audit

**13.1**-INCERT has been certified ISO/IEC 27001:2013 since January 8th 2014 and manage for the state of Luxembourg the governmental CAs used for the production and verification of travel and secure

documents (i.e. ePassport, eResidence Permit and eID card). This certification has expired on January 2017 but INCERT has undertaken the process for a new certification ISO/IEC: 27001 and ISO: 9001.

**13.2**-INCERT act as operator for Luxtrust which is a Trust Service provider by managing a private PKI composed of a RA factory (receiving certificate creation and revocation requests), a CA factory OCSP responders and a CRLs publication platform to enable this organization establishing and running qualified, standard and SSL Certification Authorities compliant with ETSI standards requirements and eIDAS regulation**.**

**13.3**-INCERT act also as a Trusted Third Party for Regify by managing a trusted back-end infrastructure securely storing encryption / decryption keys used by Regify clients to exchange sensitive information (i.e. invoices, payroll, messages) through "Regimail" products.

**13.4**-Since 2016, INCERT is a member of the European Cyber Security Organization (ECSO).

**13.5**-Since January 2016, INCERT has been accredited by CSSF (Commission de Surveillance du Secteur Financier) as Financial Service Provider (PSF).

**13.6**- INCERT has undertaken a process for being compliant with eIDAS applicable requirements.

**13.7**-INCERT is subject to a compliance audit every 12 months for the following points:
-PSF audit
-Financial audit
-eIDAS regulation audit

## 14-Terms, termination and amendment of the contract

**14.1-Terms of the Contract**. The Contract will enter into force on the date indicated on the Order Form and is entered into for a period of three (3) years and one (1) month from that date. At the end of that period, the Subscribed Service must be renewed by the user, as prompted by INCERT.

**14.2**-**Termination by INCERT**. INCERT may terminate the Contract at any time as provided for by law, without recourse to the courts and without having to state any reasons, by means of advance notice of one (1) month, by informing the User by e-mail to an e-mail address provided at the time of the order. Said termination shall not give rise to any right to compensation on the part of the User.

**14.3**-**Wrong non-fulfilment**. In the event of non-compliance by one of the Parties with any of the provisions of the Contract which the Party at fault has failed to rectify within ten (10) Business Days, the latter may terminate the Contract with immediate effect as provided for by law, without recourse to the courts, at the end of that period of time. In this case, termination by INCERT shall not confer any right of compensation.

**14.4**-**Automatic termination**. The Contract will be automatically terminated with immediate effect as provided for by law, without recourse to the courts and without any prior warning, one (1) month after the deactivation or expiry of the last Subscribed Service.

**14.5**-**Amendment of the contract**. The Contract may be amended at any time:

**(a)** by mutual agreement of the two Parties, by means of a written addendum;

**(b)** unilaterally by INCERT according to the following procedure:

**(1)** INCERT notifies the User, by at least one (1) of the means of communication provided, or by any other means of communication determined by INCERT, of the planned amendment;

**(2)** The User has one (1) month from the notification mentioned in the first point to terminate the Contract by informing INCERT by registered letter with confirmation of receipt;

**(3)** In the absence of termination by the User, the amendments will enter into force one (1) month from the notification mentioned in the first point and the User will be deemed to have agreed to those amendments.

**By signing this document, the subscriber confirms that he/she approves that the information contained in the provided certificate are correct and accept all the terms and conditions mentioned above.**