**ILNAS/PSCQ/F005**

**Security Incident Notification Form**

Modifications: minor modifications of the document

1, avenue du Swing

L-4367 Belvaux

Tél.: (+352) 247 743 50

Fax: (+352) 247 943 50

confiance-numerique@ilnas.etat.lu

<https://portail-qualite.public.lu>

### Information about the form

This notification form is to be used when a trust service provider established in Luxembourg intends to communicate incidents related to a breach of security or loss of integrity.

According to the 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 (eIDAS Regulation) - Article 19 - Security requirements applicable to trust service providers:

**“Qualified and non-qualified trust service providers shall, 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.”**

Services in scope are those defined in Article 3 (16) of the eIDAS Regulation, namely

“‘trust service’ means an electronic service normally provided for remuneration which consists of:

“(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(b) the creation, verification and validation of certificates for website authentication; or

(c) the preservation of electronic signatures, seals or certificates related to those services;”

The TSP is responsible for notifying ILNAS – Digital Trust Department of updates to the information provided in this notification form, whenever necessary. The incident reporting framework for eIDAS Article 19 is documented under

<https://www.enisa.europa.eu/publications/article19-incident-reporting-framework>

All of the documents relating to the way in which the ILNAS – Digital Trust Department functions can be found on the following website: <https://portail-qualite.public.lu>

The duly completed notification form must be sent or taken in an envelope marked "confidential" to:

**ILNAS**

**Digital Trust Department**

**1, avenue du Swing**

**L-4367 Belvaux**

Alternatively, the notification form can be sent electronically, in a secure way, to ILNAS (Digital Trust Department). Please contact ILNAS (confiance-numerique@ilnas.etat.lu) prior to sending the form and the documents to discuss the transmission modalities.

### A. General information

**A.1. Identification of the company or the institution under whose control the Trust Service Provider (TSP) operates**

name :

street and no. :

town :

country :

postcode :

postal address :

name of legal representative:       position:

company type :

legal status :

trade register no. :

telephone :

fax :

web site :

e-mail :

### B. Trust services concerned by the breach of security or loss of integrity:

**B.1. Qualified trust service(s) concerned by the security incident:**

[ ]  Qualified certificates for electronic signatures

[ ]  Qualified certificates for electronic seals

[ ]  Qualified certificates for website authentication

[ ]  Qualified validation service for qualified electronic signatures

[ ]  Qualified validation service for qualified electronic seals

[ ]  Qualified preservation service for qualified electronic signatures

[ ]  Qualified preservation service for qualified electronic seals

[ ]  Qualified electronic time stamps service

[ ]  Qualified electronic registered delivery service

[ ]  Other qualified service

If “Other”, please specify:

Identifier of the qualified trust service(s) concerned (e.g. name and object identifier (OID)) :

**B.2. Non-qualified trust service(s) concerned by the security incident:**

[ ]  Certificates for electronic signatures

[ ]  Certificates for electronic seals

[ ]  Certificates for website authentication

[ ]  Validation service for electronic signatures

[ ]  Validation service for electronic seals

[ ]  Preservation service for electronic signatures

[ ]  Preservation service for electronic seals

[ ]  Electronic time stamps service

[ ]  Electronic registered delivery service

[ ]  Other service

If “Other”, please specify:

Identifier of the trust service(s) concerned (e.g. name and object identifier (OID)) :

### C. Details on the security incident:

**C.1. Identification of the details of the security incident**

Date of incident detection :

Duration of incident :

Description of incident :

Root causes :

Detailed causes :

Asset types affected :

**C.2. Impact of the security incident**

Category of impact:

[ ]  Confidentiality

[ ]  Integrity

[ ]  Availability

Severity of impact:

[ ]  No impact

[ ]  Insignificant impact: provider assets were affected but no impact on core services

[ ]  Significant impact: part of the customer/services is affected

[ ]  Severe impact: large part of the customer/services is affected

[ ]  Disastrous: the entire organization, all services, or all certificates are affected

Personal data impacted:

[ ]  Yes [ ]  No

Cross-border impact:

[ ]  Yes [ ]  No

**C.3. Measures to address the security incident**

Measures taken:

Measures planned to be taken:

Lessons learned:

**D Signature**

Name:

Date:

Signature of authorised signatory:

### E. Other information / Comments: