# Annex F

Trust Service Providers Information – Regulation EU 910/2014 (eIDAS)

**Part 1 – Registration**

This part applies only to Trust Service Provider which apply for certification according to Regulation EU 910/2014 (commonly known as eIDAS Regulation) and supporting standards ETSI EN 319 4xx.

Please fill-in the following information. **For sections 1 to 7 check the description (a, b or c) which best describes your organization. In case of multiple sites, which have significant differences between them, please fill in a separate Annex F form for each different site.**

|  |  |  |
| --- | --- | --- |
| Factors related to business and organization (other than IT) | | |
| 1. Complexity of the ISMS (e.g. criticality of information, risk situation of the ISMS, etc.) | | Check | |
| a) | Only little sensitive or confidential information, low availability requirements  Few critical assets (in terms of CIA)  Only one key business process with few interfaces and few business units involved | ... | |
| b) | Higher availability requirements or some sensitive / confidential information  Some critical assets  2-3 simple business processes with few interfaces and few business units involved | ... | |
| c) | Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, banking) or high availability requirements  Many critical assets  More than 2 complex processes with many interfaces and business units involved | ... | |
| 1. The type(s) of business performed within scope of the ISMS | | | |
| a) | Low risk business without regulatory requirements | ... | |
| b) | High regulatory requirements | ... | |
| c) | High risk business with (only) limited regulatory requirements | ... | |
| 1. Previously demonstrated performance of the ISMS | | | |
| a) | Recently certified  Not certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system | ... | |
| b) | Recent surveillance audit  Not certified but partially implemented ISMS: Some management system tools are available and implemented; some continual improvement processes are in place but partially documented | ... | |
| c) | No certification and no recent audits  ISMS is new and not fully established (e.g. lack of management system specific control mechanisms, immature continual improvement processes, ad hoc process execution) | ... | |

--- part 1 continues to page 2 ---

|  |  |  |
| --- | --- | --- |
| Factors related to IT environment | | |
| 1. Extent and diversity of technology utilized in the implementation of the various components of the ISMS (e.g. number of different IT platforms, number of segregated networks) | | | |
| a) | Highly standardized environment with low diversity (few IT platforms, servers, operating systems, databases, networks, etc.) | ... | |
| b) | Standardized but diverse IT platforms, servers, operating systems, databases, networks | ... | |
| c) | High diversity or complexity of IT (e.g. many different segments of networks, types of servers or databases, number of key applications) | ... | |
| 1. Extent of outsourcing and third party arrangements used within the scope of the ISMS | | | |
| a) | No outsourcing and little dependency on suppliers, or  Well-defined, managed and monitored outsourcing arrangements  Outsourcer has a certified ISMS  Relevant independent assurance reports are available | ... | |
| b) | Several partly managed outsourcing arrangements | ... | |
| c) | High dependency on outsourcing or suppliers with large impact on important business activities, or  Unknown amount or extent of outsourcing, or  Several unmanaged outsourcing arrangements | ... | |
| 1. Extent of information system development | | | |
| a) | No in-house system development  Use of standardized software platforms | ... | |
| b) | Use of standardized software plat- forms with complex configuration / parameterization  (Highly) customized software  Some development activities (in-house or outsourced) | ... | |
| c) | Extensive internal software development activities with several ongoing projects for important business purpose | ... | |
| Multi-site Information | | |
| 1. Number of sites and number of Disaster Recovery (DR) sites | | | |
| a) | Low availability requirements and no or one alternative DR site | ... | |
| b) | Medium or High availability requirements and no or one alternative DR site | ... | |
| c) | High availability requirements e.g. 24/7 services  Several alternative DR sites  Several Data Centers | ... | |

--- part 1 continues to page 3 ---

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HSM Information | | | | | |
|  | HSM Site  (only sites which host Hardware Secure Modules) | Number of HSMs at this site | Are any private keys loaded in these HSMs? | Are HSMs at this site managed similarly to HSMs in the other sites? | |
|  | ... | ... | ... | ... | |
|  | ... | ... | ... | ... | |
|  | ... | ... | ... | ... | |
| Remote HSM | | | | | |
| 1. Remote signature HSMs in the organization’s infrastructure or externally but operating within organization’s responsibility | | | | | | |
| ... | | | | | | |
| National Trusted List | | | | | |
| 1. Services declared to the national supervisory body (i.e. EETT) for inclusion in the Trusted List | | | | | | |
| ... | | | | | | |
| 1. CAs declared to the national supervisory body for inclusion in the Trusted List (in case Creation of Certificates is provisioned) | | | | | | |
| ... | | | | | | |
| Ca Hierarchy and Sizing | | | | | |
| 1. Complete hierarchy of all the organization’s Certification Authorities issued (in case Creation of Certificates is provisioned) | | | | | | |
| ... | | | | | | |
| 1. Number of Certificates issued per class / type (in case Creation of Certificates is provisioned) | | | | | | |
| ... | | | | | | |
| Certification-related options | | | | | |
| 1. Full surveillance audits are requested for each year (required by some Browser Root CA programs) | | | | | ... | |
| 1. Vulnerability Assessment and Penetration Testing services are requested | | | | | ... | |
| Other | | | | | |
| 1. Document other significant information / particularities which might affect the Certification | | | | | | |
| ... | | | | | | |

Instructions:

* Part 1 of this form is always to be send along with Organization Profile (F-2503 form)

---Part 1 ends---

# Part 2 – Surveillance

Trust Service Providers Information – Regulation EU 910/2014 (eIDAS)

This part applies only to Trust Service Providers already certified by QMSCERT and in the process of a surveillance audit according to Regulation EU 910/2014 (commonly known as eIDAS Regulation) and supporting standards ETSI EN 319 4xx.

For the optimal planning of the audit, please fill-in the following, regarding changes and information for the examination period.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Organization Name | |  | | | | | **Examination Period** | |  | | |
| Organization Address(es) | |  | | | | | Registration No. / Date | |  | | |
| Standard(s) | |  | | | | | | | | | |
| Scope of Changes  Please denote the boxes according to changes that occurred in the examination period | | | | | | | | | | | |
|  | Legal entity | | |  | Organizational management | | | | | | |
|  | Standards | | |  | Partners and contractors | | | | | | |
|  | New services | | |  | Infrastructure | | | | | | |
|  | Updates in existing services | | |  | DR | | | | | | |
|  | Policies | | |  | Certificate profiles | | | | | | |
|  | Cryptographic devices | | |  | Location | | | | | | |
|  | Legislation | | |  | Risk management records (provide attachment) | | | | | | |
|  | Changes in personnel | | |  | UTC(k) laboratories for timestamping | | | | | | |
| Please describe the changes (based on the denoted boxes): | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Please provide certificate statistics and incidents (if any) for the examination period: | | | | | | | | | | | |
|  | | | | | | | | | | | |
| Organization Representative | | |  | | | Signature | |  | | Date |  |

Instructions:

* Part 2 of this form is always to be sent prior to Surveillance Audit’s scheduling.

---Part 2 ends---