|  |
| --- |
| BC-8: Overarching Purpose: Issuance of Digital Certificates linked with a Specific Domain |

|  |  |
| --- | --- |
| Use Case: Help a certification authority determine and validate the identity of the entity associated with a domain name that will be bound to an SSL/TLS certificate | |
| 1. User Groups (Requestors) / User characteristics | Certificate authority |
| 1. Why is non-public registration data necessary? | The certificate generation process typically fails if the information provided by the applicant cannot be matched to the information published in the Directory Service. |
| 1. Data elements that may typically be disclosed[[1]](#footnote-0) | Data elements that uniquely identify the certificate Applicant are the most useful in the context of this use case, and most CAs routinely use the data from WHOIS records as the starting point for uniquely identifying the certificate Applicant. At the low end of the certificate service scale (for DV/domain-validated certificates) these include items that can be validated in near-real time through direct contact, such as an email address, an instant messaging address, and a telephone number. At the mid and higher end of the certificate service scale (for OV/organization-validated certificates or EV/extended validation certificates) this would include personal names, an organization name, and a postal address. |
| 1. Lawful basis of entity disclosing non-public registration data to the requestor | Disclosure of non-public registration data may be justified under Art. 6 (1)(a) consent, (b) performance of contract, (f) GDPR (legitimate interest) and (e) GDPR (public interest/official authority) |
| 1. Supporting info to determine lawful basis for the requestor | Documentation or information showing domain registrant has applied for certification services. |
| 1. Safeguards (requirements) Applicable to the Requestor | The requestor:   * + Must process data in compliance with data protection laws such as GDPR, including secure transmission;   + Must only request current data (no data about the domain name registration’s history);   + Must direct requests at the entity that is determined through this policy process to be responsible for the disclosure of the requested data;   + Must provide representations about use of requested data which will be subject to auditing. |
| 1. Safeguards (requirements) applicable to the Entity Disclosing the Nonpublic Registration Data | The entity disclosing the data:   * Must supply only the data requested by the requestor; * Must return current data in response to a request; * Must monitor the system and take appropriate action, such as revoking or limiting access, to protect against abuse or misuse of the system. |
| 1. Safeguards (requirements) applicable to the data subject | The Registered Name Holder (data subject) must have the right:  •             to obtain, on reasonable request, confirmation of the processing of personal data relating to them and the communication in an intelligible form of the data processed;  •             to obtain, on reasonable request, rectification or erasure, as the case may be, of inaccurate data or data that is being, or has been, processed contrary to the provisions of this Protocol, but in the case of erasure, except where that processing is allowed, necessary, or required under applicable law for:  1.       exercising the right of freedom of expression and information;  2.       compliance with a legal obligation(s) for the performance of a task carried out in the public interest;  3.       the exercise of official authority vested in the controller;  4.       reasons of public interest in the area of public health;  5.       archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or  6.       the establishment, exercise or defence of legal claims.    •             not to be subject to a decision significantly affecting them based solely on an automated processing of data unless this is:  o   authorized by law providing appropriate safeguards, including at least the right to obtain human intervention;  o   necessary for entering into, or performance of, a contract between the data subject and a data controller;  o   authorized by applicable law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or  o   based on the data subject's explicit consent.  Note that whether decisions referred to herein can be made shall always take into account whether applicable law allows for explicit consent or processing necessary for reasons of substantial public interest.    •             to lodge a complaint with the supervisory authority, or authorities, when they consider that their data protection rights have been violated  •             to an effective remedy before an independent and impartial tribunal when they consider that their data protection rights have been violated.    Note that the right to object will be limited in instances where applicable law allows for (1) the controller to demonstrate compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject or (2) for the establishment, exercise or defence of legal claims or (3) processing where it is necessary for the performance of a task carried out for reasons of public interest. |
| 1. Safeguards (requirements) applicable to the access/disclosure system | * Requests must only refer to current registration data (historical registration data will not be made available via this mechanism). * Contracted parties are only responsible for disclosing nonpublic registration data for the domain names under their management. |
| 1. Accreditation of user group(s) required (Y/N) – if Y, define policy principles | Individuals or entities seeking accreditation as a member of this user group must also:   * Agree to only use the data for the legitimate and lawful purpose described above; * Only issue disclosure requests with respect to the domain(s) in question; * Agree to:   + the terms of service, in which the lawful use of data described;   + prevent abuse of data received;   + be subject to de-accreditation if they are found to abuse use of data. |
| 1. Authentication – policy principles |  |
| 1. What information is required to be provided for a request under this lawful basis? | Verification of identity as a certification service, and documentation or information showing domain registrant has applied for certification services. |
| 1. Expected timing of substantive response | Immediate |
| 1. Is automation of substantive response possible / desirable? | Automation is both possible and desirable. |
| 1. Expected timing of substantive response | Immediate |
| 1. How long can the requestor retain the data disclosed and what are the requirements for destruction following the end of the retention period? | Article 5 (e) of the GDPR states personal data shall be kept for no longer than is necessary for the purposes for which it is being processed. |
| 1. Other? |  |

1. For each request, the requestor will need to confirm which data elements are necessary. [↑](#footnote-ref-0)