REPUBLIC OF ALBANIA
NATIONAL AUTHORITY FOR ELECTRONIC CERTIFICATION

GUIDANCE NO. 4

N0. 4 , Date 22.02.2016

ON PROCEDURES FOR ELECTRONIC IDENTIFICATION AND ELECTRONIC STAMPS

In support of Law No. 107/2015, "On electronic identification and trusted services", DCM 69, 27.01.2016 "On the adoption of the Regulation on electronic identification and trusted services", the National Authority for Electronic Certification,

INSTRUCTS

All Qualified Trusted Service Providers (QTSP) for the provision of electronic stamps and electronic identification must meet the following requirements:

1. For the provision of physical persons by electronic identification, the QTPS, performs correctly the initial identification of applicants through the official identification document that the applicant submits and documents the procedure accepted by both parties. This criterion is applicable also to foreign nationals residing in the Republic of Albania.

2. For the provision of legal persons with electronic stamp, the QTPS, executes correctly the initial identification of the applicants, through the official identification document, an official document certifying the NIPT number and the respective certificate / authorization certifying the representation of the legal person.

3. Ensures that electronic identification and electronic signature generating devices are designed in such a way that only their holder has access to and use on them; are protected by duplication and interference and physical manipulation. They should ensure connection with the subject using at least two of the three authentication factors as follows:
   a) The subject must demonstrate its ownership
   b) the subject must demonstrate its recognition
   c) The subject demonstrates that he possesses physical attributes (finger print, retina, etc)

4. It ensures in full transparency and documents the process of issuing, submitting and activating electronic identification and electronic stamping devices, which must be submitted only to their holder.

5. Creates authentication mechanisms by ensuring that:
   a. Issuance of personal identification data is preceded by a reliable verification of the validity of electronic identification tools through a dynamic authentication, which ensures an electronic test whenever required, that the subject has control of the authentication data, which is different with each authentication process between the subject and the system, which verifies its identity.
   b. In cases where personal identification data is stored as part of authentication mechanisms, this information is stored in such a manner as to protect against compromise, including offline modification attempts.
   c. Implement security controls to verify electronic identification tools so that actions like guessing access codes, interception, or manipulation of communication channels will compromise or simulate the results generated by authentication mechanisms.

6. The QTSP must have an electronic service to publish and disseminate notifications to the holders in respect of all terms of use, the responsibilities of the parties, including any limitation of service or use of the service. This service should also include a privacy policy;
   a. The procedure and policy should be implemented in a way that ensures that service users are notified without delay of changes to service definitions or in other terms of use and privacy policies for the specified service;
   b. Policies and procedures should be implemented in a manner that responds fully and correctly to any request for information by the holders.

7. The QTSP should provide for technical controls to manage the risks to the security of services, the protection of confidentiality, integrity and availability of processed information under the following conditions:
    a. Electronic communications channels, used for the exchange of personal data or sensitive information, should be protected from interception, manipulation or registration;
    b. The access to cryptographic devices and materials used for issuing identification and authentication tools as well as electronic stamping tools are limited to roles and applications that necessarily need access to them. Controls of access to such materials should never be preserved in readable text;
    c. The procedure must ensure the level of security to the changes, risks and possible incidents on it;
    d. Each personal data storage medium, cryptographic or other sensitive information storage medium is safely stored, transported and destroyed.
    e. Sensitive cryptographic materials, which are used for the issuance of identification and authentication tools and electronic stamping tools, should be protected against physical interference.

8. In the case of the implementation of electronic stamp for electronic public services:
    a. the visual format of the stamp in the received document by the electronic service should contain the following data:

<table>
<tr><td rowspan="3">Graphic presentation of the physical Stamp of the institution</td><td>Name of issuing institution</td></tr>
<tr><td>Date and time of stamping - according to timestamp</td></tr>
<tr><td>No. serial of the stamped document - linked to the code two-dimensional, if one is displayed in the document)</td></tr>
<tr><td>Note:</td><td>This document was generated and stamped by a automatic procedure from an electronic system (name of issuing institution)</td></tr>
</table>

    b. The shape of the stamp should be rectangular and its dimensions should not exceed 40% of the width of the document or 30% of its height (example: A4 format - 84mm horizontally and 89mm vertically);
    c. The electronic seal is placed at the bottom of the last page of the document.