

Instructions on Receiving the Certificate

After installing the **Certification Authority Certificate** it is necessary to advance a request for User certificate. To launch a Request for User Certificate, you need to:

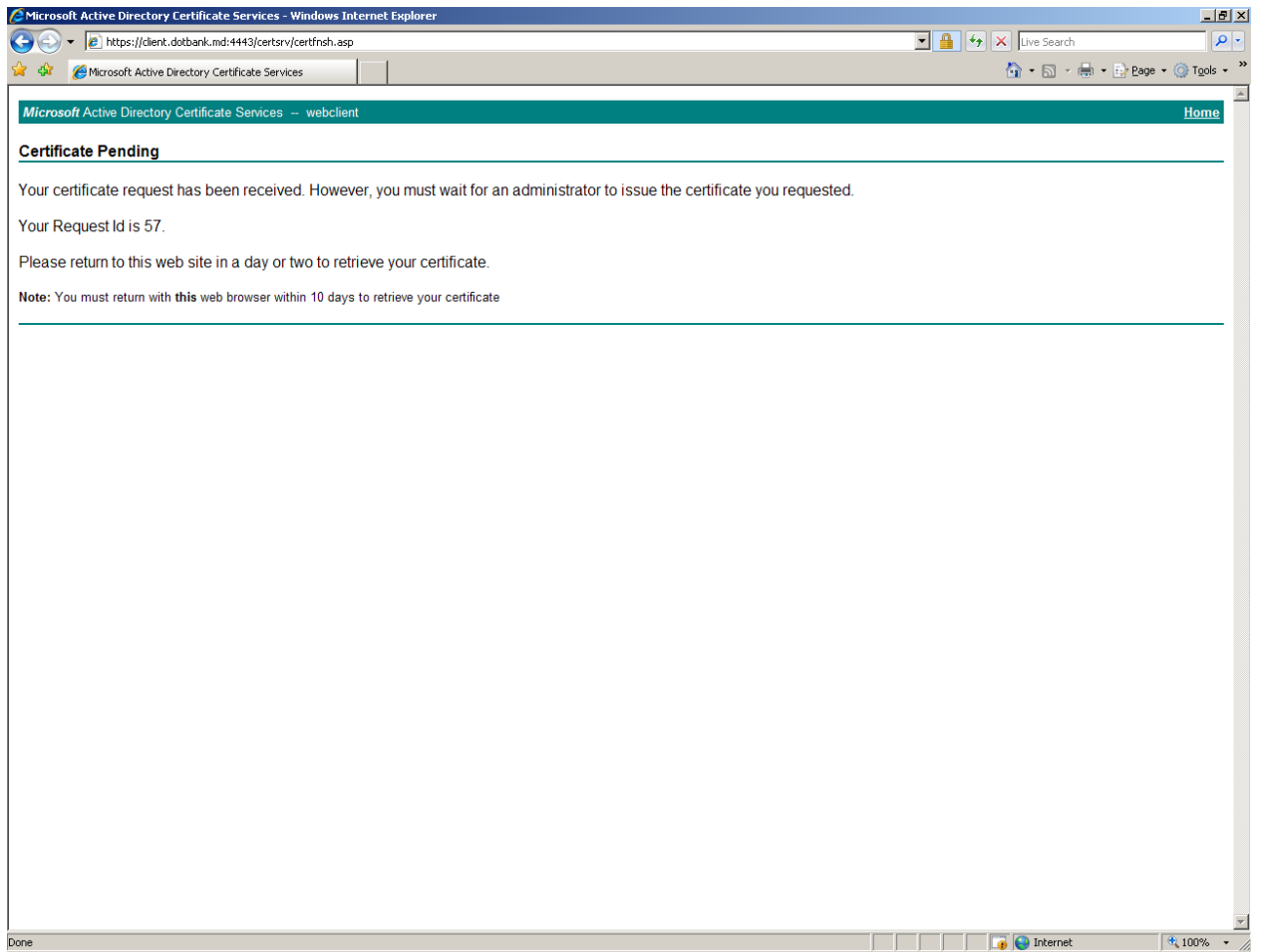
1. Click on the following web address link: <https://client.dotbank.md:4443/certsrv/certrqma.asp>.
As a result, a window will be displayed (as in the image below) where you should fill in the required fields as follows:
 - a) In the **"Name"** field – you should enter name and surname of the person for whom a Certificate is requested.
 - b) In the **"E-mail"** field – enter the email address of the person who requested the Certificate.
 - c) In the **"Company"** field – enter the full name of the company for which the person works.
 - d) In the **"Department"** field – indicate the Department where this person works and job title.
 - e) In the **"City"** field – enter the name of the Municipality/city where the respective company operates.
 - f) In the **"Country/Region"** field – enter the abbreviation MD.
2. After having filled in form, submit this Request to the server of the Certification Authority. To submit the Request to the server you should:
 - a) check **"Mark keys as exportable"** option
 - b) choose **PKS10** option
 - c) click **Submit**.

The screenshot shows a web browser window titled "Microsoft Active Directory Certificate Services - Windows Internet Explorer". The address bar shows the URL "https://client.dotbank.md:4443/certsrv/certrqma.asp". The page content is titled "Advanced Certificate Request" and contains the following sections:

- Identifying Information:**
 - Name: Ion Tonu
 - E-Mail: ion.tonu@mail.mail
 - Company: Compania SRL
 - Department: Administrativ
 - City: Chisinau
 - State: Chisinau
 - Country/Region: MD
- Type of Certificate Needed:**
 - Client Authentication Certificate
- Key Options:**
 - Create new key set Use existing key set
 - CSP: Microsoft Enhanced Cryptographic Provider v1.0
 - Key Usage: Exchange Signature Both
 - Key Size: 1024 (Min: 384, Max: 16384, common key sizes: 512, 1024, 2048, 4096, 8192, 16384)
 - Automatic key container name User specified key container name
 - Mark keys as exportable
 - Enable strong private key protection
- Additional Options:**
 - Request Format: CMC PKCS10
 - Hash Algorithm: SHA-1 (Only used to sign request.)
 - Save request
 - Attributes: [Empty field]
 - Friendly Name: [Empty field]

A "Submit >" button is located at the bottom of the form.

3. After you have clicked the **Submit** button, the system will display a new window (as in the image below) and a message saying that your request has been sent to the administrator.



4. After receiving the request, the administrator will issue the requested certificate.