

Procedura de certificare

Utilizatorul poate obține certificat prin intermediul RA RENAM (Autorității de înregistrare – persoana de legătură între utilizator și centru de certificare, responsabilă de colectarea cererilor și eliberarea documentelor). Dacă numărul utilizatorilor din cadrul unei organizații depășește 10 persoane, în cadrul organizației este creată o unitate RA. Pentru unitățile RA este organizat un seminar cu explicarea procedurilor de interacțiune cu utilizatorii și CA, este semnat un acord precum că RA a făcut cunoștință și va respecta prevederile descrise în CP/CPS (Certificate Policy and Certification Practice Statement) al MD-Grid CA. În rezultat colaboratorului RA i se emite certificat digital personal.

Ordinea pașilor de cerere a certificatului digital.

1. Utilizatorul este consultat de RA în privința procedurii de certificare;
2. Utilizatorul completează formularul propus, unde indică locul de muncă, necesitatea de a obține certificat digital, este informat de drepturile și obligațiunile lui;
3. Utilizatorul personal se prezintă la sediul RA, și prezintă originalele și copiile documentelor care pot confirma identitatea sa, formularul completat și întărit de la locul de muncă și confirmarea necesității de a obține un certificat digital;
4. Utilizatorul poate genera cererea desinestător sau cu ajutorul RA. Pentru generarea cererii utilizatorul trebuie să acceseze Linux/xNIX sistem, direct sau utilizând client(ex. *putty+winscp*)

Ordinea creării cererii

1. Este creat fișierul *openssl.cnf*, cu următorul conținut:

```
distinguished_name = 1  
[ 1 ]
```

2. În terminal în mapa cu fișierul *openssl.cnf* se execută instrucțiunea:

```
openssl req -config openssl.cnf -newkey rsa:2048 -keyout privatkey.pem -out request.csr  
-subj "/DC=MD/DC=MD-Grid/O=XX/CN=YY1 YY2"
```

где:

XX - numele organizației (participantului MD-GRID NGI, din cadrul unei liste specificate mai devreme)

YY1 - Nume (exact cum este în document, ex : Valentin)

YY2 - Prenume (exact cum este în document, ex : Pocotilenco)

Пример:

```
openssl req -config openssl.cnf -newkey rsa:2048 -keyout privatkey.pem -out request.csr  
-subj "/DC=MD/DC=MD-Grid/O=RENAM/CN=Valentin Pocotilenco"
```

În procesul executării instrucțiunii va fi cerută parola care va proteja cheia privată generată. Parola va fi introdusă de două ori și trebuie să conțină nu mai puțin de 12 caractere

Atenție!!! Parola trebuie memorizată sau notată într-un loc sigur, în caz că parola a fost pierdută sau uitată, ea nu poate fi restabilită. În acest caz trebuie inițiată o nouă procedură de emiter.

3. În rezultatul executării instrucțiunilor specificate, vor fi generate:

userkey.pem - fișierul cheii private, care este strict personal și este protejat de parolă;

request.csr – fișierul cerere pentru semnarea certificatului, care este expediat către RA.

Ambele fișiere sunt copiate pe purtător și șterse din sistem.

5. Utilizatorul prin intermediul cutiei poștale corporative va expedia fișierul *request.csr* către RA utilizând textul specificat mai jos:

=====

To the RA of the MD-Grid CA:

In the attachment you can find user certificate request for < **requestor's name and surname** >.

My contacts are given below. Please do not hesitate to contact me if any further information is needed.
Name: <requestor's name and surname >
Institution: <organization name>
Address: <e-mail>
E-mail:
Phone: +373 22 (office)
+373 (mobile)

=====

Exemplu:

=====

*To the RA of the MD-Grid CA:
In the attachment you can find user certificate request for Valentin Pocotilenco.
My contacts are given below. Please do not hesitate to contact me if any further information is needed.
Name: Valentin Pocotilenco
Institution: RENAM
Address: 5, Academiei str., of. 324, Chisinau 2028, Moldova
E-mail: valentin.pocotilenco@renam.md
Phone: +373 22 333 444
+373 555 66666*

=====

6. RA, primește scrisoarea cerere, și o redirecționează către CA, semnând scrisoarea cu certificatul său;

7. După revizuirea cererii, în decurs de maxim 3 zile lucrătoare, CA semnează cererea cu cheia centrului de certificare, și expediază o scrisoare către RA și utilizator, prin intermediul poștei electronice, cu următorul conținut:

=====

Find attached your x509v3 digital certificate signed by theMD-GRID CA.

Please return a digitally signed email at ca@renam.md,
stating that you accept your certificate and that you adhere to the
MD-GRID Certification Policy:

<http://ca.grid.md/files/MD-Grid-CP-CPS.pdf>

A template e-mail can be found at the end of this email.

Information on how to import your certificate in various mail clients or internet browser can be found by contacting RA or using address below:

<http://www.grid.auth.gr/pki/seegrid-ca/documents/certificateImport/>

If the MD-GRID CA operators do not receive an acknowledgment email within 7 days, the signed certificate will be revoked.

Regards,
Valentin Pocotilenco
MD-GRID CA Operator

Appendix I:EmailTemplate

-----Cut here-----

To whom it may concern,
With this email I state that

1. I, <put yourname here>, accept my x509v3 digital certificate with

DN: /DC=MD/DC=MD-GRID/O=<put your institution's name here>/CN=<put requestor's name here>

Serial Number: <certificate's serial number>

signed by /DC=MD/DC=MD-GRID/O==RENAM/OU=Certification Authority/CN=MD-Grid-CA

2. I adhere the MD-GRID CA policy and usage rules found at:

<http://ca.grid.md/files/MD-Grid-CP-CPS.pdf>

(O.I.D. 1.3.6.1.4.1.31194.10.1.1.3)

-----Cut here-----

=====

8. Utilizatorul, la rândul său, în decurs de 7 zile după semnarea certificatului trebuie să răspundă cu un mesaj către CA, utilizând client poștal, semnat cu certificatul digital personal. Șablonul scrisorii este următorul:

To whom it may concern,

With this email I state that

1. I, <put yourname here>, accept my x509v3 digital certificate with

DN: /DC=MD/DC=MD-GRID/O=<put your institution's name here>/CN=<put requestor's name here>

Serial Number: <certificate's serial number>

signed by /DC=MD/DC=MD-GRID/O==RENAM/OU=Certification Authority/CN=MD-Grid-CA

2. I adhere the MD-GRID CA policy and usage rules found at:

<http://ca.grid.md/files/MD-Grid-CP-CPS.pdf>

(O.I.D. 1.3.6.1.4.1.31194.10.1.1.3)

9. Din momentul expedierii scrisorii către Ca și RA, certificatul digital, valabil timp de un an, poate fi utilizat în cadrul infrastructurii MD-GRID, pentru accesul la sisteme informaționale care acceptă certificatele eliberate de centru și pentru semnarea documentelor sau scrisorilor electronice.