Процедура выдачи сертификата.

Пользователь может получить сертификат через RA RENAM (Registration Authority – сотрудник, работающий с пользователями, ответственный за прием заявок и выдачу сертификатов). Если организация имеет больше 10 пользователей, в данной организации создается структура RA. Для RA-сотрудников организации проводится курс-тренинг по процедурам работы с пользователями и CA. Подписывается договор с RA о том, что он ознакомлен, согласен и обязывается соблюдать политики и процедуры, описанные в CP/CPS (Certificate Policy and Certification Practice Statement) от MD-GRID CA (MD-Grid Certification Authority). После этого RA-сотрудникам выдаются цифровые сертификаты.

Последовательность действий для получения сертификата:

1. Пользователь консультируется с RA организации или RA RENAM по процедуре получения сертификата.

2. Пользователь получает в своей организации официальное письмо стандартной формы (Запрос на получение пользовательского сертификата MD-Grid) с подписью руководителя и печатью своего учреждения (шаблон на сайте ca.grid.md). В письме указывается информация о том, кто он, где работает и подтверждение руководства, что ему необходимо получить цифровой сертификат.

3. Пользователь встречается с RA, имея при себе следующий список документов: подписанное руководителем письмо-запрос на получение сертификата; оригинал и копию документа удостоверяющего личность (документ с фотографией и подписью пользователя). С собой желательно иметь USB носитель.

4. Пользователь может сгенерировать цифровой запрос сам или с помощью RA. Для генерации и копирования результатов на USB носитель понадобится доступ у Linux/xNIX системе в терминальном режиме и возможность скачивания файлов. Для операционной системы Windows рекомендуется использовать программы PUTTY (для работы в терминальном режиме) и WinSCP (для скачивания файлов).

Порядок создания запроса

1. Создаем файл *openssl.cnf*, который понадобится при генерации запроса. Содержимое файла:

distinguished_name = 1
[1]

2. В терминальном режиме в каталоге с файлом *openssl.cnf* выполняется команда:

*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 — название организации-участника MD-GRID NGI из утвержденного списка.
YY1 — Имя пользователя (как в документе, например: *Valentin*)
YY2 — Фамилия пользователя (как в документе, например: *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"

В ходе выполнения команды система запросит у пользователя парольную фразу (длинной не менее 12 символов), которая будет защищать генерируемый закрытый (первичный) ключ *privatkey.pem* от незаконного использования. Вводится 2 раза.

Внимание!!! Пароль необходимо сохранить. Если пароль утерян, невозможно будет работать с сертификатом. Сертификат придется отозвать и генерировать новый.

3. После выполнения команды создаются файлы:

privatkey.pem — (закрытый или первичный ключ — файл и пароль никогда никому

не передается, используется только пользователем);

request.csr — файл запроса сертификата, отправляется RA и в центр сертификации.

Файлы переписываются на флэшку, в Linux/xNIX системе удаляются.

5. Пользователь отправляет RA письмо определенного образца с файлом *request.csr* в приложении. Если пользователь работает вместе с RA, письмо может быть отправлено сразу с адреса RA в центр сертификации. Формат письма с запросом:

==========

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)**

==========

Например:

==========

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 отправляет MD-Grid Certification Authority (CA) подписанный своей цифровой подписью письмо-запрос (см п. 5), с файлом *request.csr* в приложении к письму.

7. Время рассмотрения заявки до 3 рабочих дней. Если заявка принимается, CA в течение трех рабочих дней отправляет пользователю и RA письмо с подписанным ключом сертификационного центра СЕРТИФИКАТом. Письмо следующего содержания:

==========

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. Пользователь в ответ в течение 7 дней высылает письмо, используя почтовый клиент, подписанное слепком своего сертификата. Шаблон для письма следующий:

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. С момента отправки и получения RA и CA этого письма, сертификат сроком действия 1 год может использоваться в MD-GRID-инфраструктуре для доступа к информационным системам, доверяющим выданным сертификатам, а так же для подписи электронных документов и писем.