

The title page:

Version 2.3 > Version 2.4

May 15, 2014 > June 7, 2021 (This date will be updated after this CP/CPS is approved by EUGridPMA)

Table of Content:

Table of content of the CP/CPS document is regenerated.

1.1 Overview:

...CP/CPS as of May 15, 2014, 09:00 UTC > ...CP/CPS as of June 7, 2021, 09:00 UTC
(This date will be updated after this CP/CPS is approved by EUGridPMA)

1.2 Document Name and Identification

Document Version: 2.3 > Document Version: 2.4

Document Date: May 15, 2014 > Document Date: June 7, 2021

...(OID): 1.3.6.1.4.1.23658.10.1.2.3 > ...(OID): 1.3.6.1.4.1.23658.10.1.2.4

1.3.2 Registration Authorities

“The TR-GRID CA assigns the authentication of individual identity to Registration Authorities (RA). Based on this CP/CPS document, RAs are not allowed to issue certificates. The list of RAs is available on the TR-GRID CA website.”

>

“TR-GRID CA is integrated with the e-Government System of Turkey as a part of Turkish Science e-Infrastructure (TRUBA).

The e-Government System can be used by all citizens of Turkey over the age of 18 for public services like tax payments, land transactions, health systems, etc. All citizens and foreigners have an identity number and a password for using the e-Government System. The password of the e-Government system is given by Republic of Turkey Ministry of Transport and Infrastructure Turkish Post Office (PTT) branches when a citizen requested personally with his/her photo ID card which includes his/her identity number.

Since PTT is a state institution that has at least one office in every province, district and neighborhood in Turkey, every researcher (citizens and foreigners) can easily access and obtain their passwords for the e-Government System. Every researcher who wants to benefit from TRUBA services is firstly registered to TRUBA Membership Portal. The researcher is authenticated by the online e-Identification system used by the e-Government system and redirected TRUBA Membership Portal for authentication.

In addition, TRUBA Membership Portal provides a link for authorization with the Council of Higher Education System (YOKSIS) via the web service. Researcher who is registered TRUBA Membership Portal to benefit from TRUBA services is authorized directly with the name of the university or research institution, title and education level which are provided from YOKSIS with the credentials coming from the e-Government System.

The researchers, who want to benefit from existing research infrastructures, can request user, host and service certificate directly from TRUBA Membership Portal. Since they have already

authenticated with e-Government System and authorized with YOKSIS, TR-GRID CA Operator can check their requests from TRUBA Membership Portal.

The TR-GRID CA assigns the authentication and authentication of individual identity to TRUBA Membership Portal since it authenticates and authorized the person with e-Government System and YOKSIS. Therefore, there are no need RA Operator.

TR-GRID CA is based on this CP/CPS document, only TR-GRID CA Operators are allowed to issue certificates.”

1.5.1 Organization Administering the Document

E-mail: ca@grid.org.tr > E-mail: ca@truba.gov.tr

Address: YOK Binası B5 Blok 06539
Bilkent/ANKARA

>

Address: Universiteler Mah. ODTU Kampusu
MODSIMMER Binası Kat:2 06800
Çankaya/ANKARA

1.5.2 Contact Person

Address : YOK Binası B5 Blok 06539
Bilkent/ANKARA

>

Address: Universiteler Mah. ODTU Kampusu
MODSIMMER Binası Kat:2 06800
Çankaya/ANKARA

Website : <http://www.grid.org.tr/ca> >
<http://www.truba.gov.tr/index.php/en/certification-authority/>

1.6. Definitions and Acronyms

The following items are added :

PTT: Republic of Turkey Ministry of Transport and Infrastructure Turkish Post Office. PTT is a state institution that has at least one office in every province, district and neighborhood in Turkey, every researcher (citizens and foreigners) can easily access and obtain their passwords for the e-Government System.

TRUBA: Turkish Science e-Infrastructure.

TRUBA Membership Portal: TRUBA membership portal is a portal designed to validate and authorize the identity information of the persons and individuals with e-Government System and YOKSIS systems, update any information changes directly, and keep the registration information of TRUBA researchers up-to-date. This portal is used by TRUBA researchers who want to benefit from TRUBA services which includes certification processes.

YOKSIS: Council of Higher Education Information System that holds research units, researchers and students' institution, faculty, department, title information. YOKSIS can be integrated with the other information system with web services.

2.1 Repositories

“TR-GRID CA will maintain a secure online repository at <https://www.grid.org.tr/ca> that includes:” >

“TR-GRID CA will maintain a secure online repository at <https://www.truba.gov.tr/index.php/en/certification-authority/> that includes:”

3.1.1 Types of Names

DNs of examples are changed.

C=TR, O=TRGrid, OU=Ulakbim, CN=Asli Zengin > C=TR, O=TRGrid, OU=TUBITAK-ULAKBIM, CN=Asli Zengin

C=TR, O=TRGrid, OU=Ulakbim, CN=host1 > C=TR, O=TRGrid, OU=TUBITAK-ULAKBIM, CN=www.truba.gov.tr

C=TR, O=TRGrid, OU=TRGrid, CN=ldap/ldap.grid.org.tr > C=TR, O=TRGrid, OU=TRUBA, CN=ldap.truba.gov.tr

3.2.3 Authentication of Individual Identity

“Certificate of a person:

- The subject should contact personally the RA staff in order to validate his/her identity.
- The subject authentication is fulfilled by providing an official document (ID-card, driving license or a passport) declaring that the subject is a valid end entity.

In exceptional cases such as remote geographical location of the subject, identity validation may be performed by video conference. In this case, an authenticated photocopy of the required document (ID-card, driving license or a passport) must be delivered by mail or courier to the RA staff prior to this online meeting. Authenticated photocopy refers to the verification made by a legally accepted notary public under Turkish law.”

>

“Certificate of a person:

- The subject should contact personally the PTT branches in order to validate his/her identity.
- The subject authentication is fulfilled by providing an official document (ID-card, driving license or a passport) declaring that the subject is a valid end entity by PTT officers.
- PTT branches provide to the subject an e-Government password to be able to authenticate e-Government system.
- The subject authenticated by e-Government Authentication System to be a member of TRUBA Membership Portal.
- The subject is authorized by YOKSIS to verify the knowledge of being in an academic institution.
- CA Operator checks all authentication and authorization information through the TRUBA Membership Portal.

The authentication and authorization process is described in detailed in Section 1.3.2. After the person becomes a member of the TRUBA Membership Portal, his identity is verified by the e-Government system at each TRUBA Membership Portal entry. Moreover, YOKSIS

information is checked by the CA Operator for the authorization of the person in each certificate process.”

3.2.4 Non-verified Subscriber Information

During the initial identity validation the requester's e-mail is not verified. > No stipulation.

4.1.2 Enrollment Process and Responsibilities

- **User enrollment:**

“The subject should fill the membership form which could be seen both CA and RA operators. Then the subject should contact personally the RA staff in order to validate his/her identity. The subject is authenticated with his/her official identity document by RA. RA communicates with CA operator that authenticates user via SSL protected HTTP transport for the membership application or with signed e-mail.

After successful membership application, the CA operator sends an active HTTPS request link which includes randomly generated hash string that uniquely identifies the user with the following details: first and last name, organization, e-mail address, name of institution and department. The subject should use this link for certificate request. The subject is connected to online CA web site with the given link and should need to fill a minimum eight character pin before submitting the requests. The subject private key is generated on the browser of the user and the request is taken by online CA. Upon successful submission of certificate request, RA operator authenticates his/her submission by personal application of the user with his/her official identity card and the pin which is given in the request form.

CA operator checks the authentication procedures of the subject and issues the certificate and informs the RA and the requester via e-mail which describes how to download the certificate from the online CA website with the browser from which the request is submitted.”

>

“- The subject who contact personally the PTT branches officer in order to validate his/her identity before and authenticated with his/her official identity document by PTT branches officer to be able to get e-Government password. After he/she is identified by the PTT branches, the subject could use e-Government system and also connect to TRUBA Membership Portal to be a member.

- When the subject connected to TRUBA Membership Portal with his/her identity number and e-Government password:

- TRUBA Membership Portal is getting the subject all identity information including Name, Surname, Second Surname (if it is existing), Date of Birth, Date of Place, etc. for Certificate Subject from e-Government System.

- Also, TRUBA Membership Portal is connected with YOKSIS to get up-to-date institute, department, title and other academic information of the subject.

- The subject can request personal certificate from TRUBA Membership Portal. All needed information for the certificate DN is filled from e-Government and YOKSIS.

All communications of TRUBA Membership Portal and the other information systems are via SSL protected protocols.

- The subject private key is generated on the browser of the user and the request is taken by TRUBA Membership Portal.
- TRUBA Membership Portal send an e-mail to CA Operator for this new certificate request.

CA operator checks the authentication procedures of the subject and issues the certificate and informs the requester via e-mail which describes how to download the certificate from the TRUBA Membership Portal with the browser from which the request is submitted.”

- **Host enrollment:**

“Host certificates can only be requested by the administrator responsible for the particular host. In order to request a host certificate, the administrator must already possess a valid personal TR-GRID CA certificate. Applicants can make host/service certificate requests to the RA via e-mail signed by a valid TR-GRID CA certificate. Applicant's public keys are delivered to the RA in an email containing the certificate request. RA should ensure that the applicant is appropriately authorized by the owner of the associated FQDN. The public key arrives at the TR-GRID CA in an email signed by the RA.

CA operator checks the authentication procedures of the subject and issues the certificate and informs the RA and the applicant via e-mail.

Applicants can make host/service certificate requests via SSL protected HTTP certification request service provided by the RA”

>

“Host certificates can only be requested by the administrator responsible for the particular host. In order to request a host certificate, the administrator must already possess a valid personal TR-GRID CA certificate. Applicants can make host/service certificate requests to the CA Operators via e-mail signed by a valid TR-GRID CA certificate. Applicant's public keys are delivered to the CA Operators in an email containing the certificate request. CA Operator should ensure that the applicant is appropriately authorized by the owner of the associated FQDN.

CA operator checks the authentication procedures of the subject and issues the certificate and informs the applicant via e-mail.

In addition, applicants can make host/service certificate requests via SSL protected HTTP certification request service provided by the TRUBA Membership Portal. Applicant can upload certificate request file to TRUBA Membership Portal. CA Operator should ensure that the applicant is appropriately authorized by the owner of the associated FQDN.

CA operator checks the authentication procedures of the subject and issues the certificate and informs the applicant via TRUBA Membership Portal which send an automatic e-mail to the applicant.”

4.2.1 Performing Identification and Authentication Functions

“For a certificate to be issued, the subject authentication must be successful and proper as specified in this document. Applicants will be informed about the status of their certificate whether it is issued or rejected.”

>

“For a certificate to be issued, the subject authentication must be successful and proper as specified in this document. Applicants will be informed about the status of their certificate via e-mail whether it is issued or rejected.”

4.3.1 CA Actions during Certificate Issuance

The following line is deleted.

“CA will ensure secure communication with RAs by signed e-mails, SSL protected private web pages and voice conversations with a known person.”

4.9.3 Procedure for Revocation Request

“Revocation requests should be submitted in one of the following ways:

- by email sent to ca@grid.org.tr
- personally at the RA/CA

All revocation requests should be properly authenticated as described in 3.4.”

>

“Revocation requests should be submitted in one of the following ways:

- by email sent to ca@truba.org.tr
- personally at the CA
- by TRUBA Membership Portal

All revocation requests should be properly authenticated as described in 3.4”

5.1.2 Physical Access

“Physical access to the hardware (entering the computer room) is restricted to the authorized personnel.”

>

“Physical access to the hardware is restricted to the authorized personnel.”

5.3.3 Training Requirements

“Internal training is available and applied to the TR-GRID CA and RA operators”

>

“Internal training is available and applied to the TR-GRID CA operators.”

5.3.4 Retraining Frequency and Requirements

“TR-GRID CA will perform operational audit of the CA and RA operators once a year. Retraining is applied if the audit results are not satisfactory.”

>

“TR-GRID CA will perform operational audit of the CA operators once a year. Retraining is applied if the audit results are not satisfactory.”

5.3.8 Documentation Supplied to Personnel

“Operational manual for CA and RA operators is supplied to the new TR-GRID CA personnel.”

>

“Operational manual for CA operators is supplied to the new TR-GRID CA personnel.”

5.4.1 Types of Events Recorded

“The login/logout/reboot information of the issuing machine is archived. In addition, annual operational audits of CA/RA staff must be performed.”

>

“The login/logout/reboot information of the issuing machine is archived. In addition, annual operational audits of CA staff must be performed.”

5.5.1 Types of Event Recorded

“The TR-GRID RA will archive the following items:

- Application data (certificate and revocation requests)
- Issued certificates and CRLs
- All e-mail messages correspondence with TR-GRID CA and RA
- The login/logout/reboot information of the issuing machine
- The official identity documents (ID-card, driving license or a passport) of end entities.”

>

“The TR-GRID CA will archive the following items:

- Application data (certificate and revocation requests from TRUBA Membership Portal records)
- Issued certificates and CRLs
- The login/logout/reboot information of the issuing machine”

5.8 CA or RA Termination

“Inform the subscribed users and RAs” > “Inform the subscribed users”

6.1.3 Public Key Delivery to Certificate Issuer

“Applicants can make host/service certificate requests to the RA via e-mail signed by a valid TR-GRID CA certificate. Applicant's public keys are delivered to the RA in an email containing the certificate request. The public key arrives at the TR-GRID CA in an email signed by the RA.

Applicants can make user/host/service certificate requests via SSL protected HTTP certification request service provided by the RA”

>

“Applicants can make host/service certificate requests to the CA operators via e-mail signed by a valid TR-GRID CA certificate or via TRUBA Membership Portal. Applicant's public keys are delivered to the CA Operator in an email containing the certificate request.

Applicants can make user/host/service certificate requests via SSL protected HTTP certification request service provided by the TRUBA Membership Portal.”

6.1.4 CA Public Key Delivery to Relying Parties

<http://www.grid.org.tr/ca> > <http://www.truba.gov.tr/index.php/en/certification-authority/>

6.5.1 Specific Computer Security Technical Requirements

“The operating systems of CA/RA servers are protected at a high degree of security by applying all the relevant patches.”

>

“The operating systems of CA servers are protected at a high degree of security by applying all the relevant patches.”

9.4 Privacy of Personal Information

“TR-GRID CA does not collect any confidential or private information except for the case when CA or RA archives copies of ID documents for identity validation of a user certificate request. TR-GRID CA guarantees that this personal information will not be used for any other purposes.”

>

“TR-GRID CA does not collect any confidential or private information except authentication and authorization data of an end entity that is taken from e-Government System and YOKSIS for certificate request. TR-GRID CA guarantees that this personal information will not be used for any other purposes.”