TCS Model Process Non-SAML Personal Issuance

version v01 rev 3

Amsterdam Office
Singel 468 D
1017 AW Amsterdam
The Netherlands
+31 (0) 20 5304488

www.geant.org
info@geant.org

About this document

The primary process described and propagated by the TCS G3 CPS uses federated authentication and the exchange of entitlement attributes to authorize the issuance of Personal and eScience Personal certificates to Applicants. This process can be fully automated, but does rely on the identity management system at the Subscriber being able to interface through a SAML based identity provider with a (national) federation. The federation is then linked through electronic means with the issuance portal at DigiCert.
To cater for those incidental cases where such an automated link cannot be put in place, or is (temporarily) unavailable, as well as to support the issuance of 'Robot' (machine-to-machine) client authentication certificates, the CPS permits an alternative process to validate identity and issue certificates. The required practices are specified in section 3.2.3, but leave some room to use a few different processes. In this document, we propose a model process to manually issue Personal and eScience Personal certificates, as well as Robot (Name) Certificates.

Prerequisites

1. You have a Subscriber Administrator account in CertCentral, and have (at least) one Organisation validated for OV or Grid
2. You, the Administrator, have (read) access to your organisational identity management (IdM) system and/or HR database[1]
3. The IdM or HR database has at least a verified email address for the intended applicant that cannot be changed through self-service, and is populated from trusted sources

Verification Process

1. Obtain confirmation from the IdM data that a face-to-face[2] identity vetting has taken place

[1] The IdM and/or HR database of course *might* be a paper-based thing as well. Paper is a permissible implementation of a database *but* then you must make sure that the paper data base is backed up, managed, and you can find stuff in it. The CPS does not forbid the use or paper-based IdMs, as long as it's audited, archived, and you meet the retention requirements. And if you do go that way, think hard first …
[2] Face-to-face or equivalent process. If an identity meets the requirements of Kantara LoA 2, this is sufficient. Otherwise, either re-vet the applicant in a face-to-face meeting and check a government-issued photo identity document, or read carefully the requirements of the DigiCert CPS section 3.2.3 for "Level 2 Client Certificates and IGTF Classic/MICS Certificates" (page 14 and 15).

2. Verify that there is a name field (usually Common Name, or Given Name + Surname) is a reasonable representation of the real name
3. Prove current possession of the Applicant's mail box listed in the IdM system by the Applicant. This is implicit if the Applicant authenticates to this same IdM in order to access the mail box. The shared secret (e.g., a PIN or password) must meet or exceed proper (NIST SP 800‑63 Level 2) entropy requirements.
   If this is not possible, send a one-time challenge ('nonce') to the mail box and verify face-to-face that the prospective applicant knows this nonce. If you use this latter method, you must
   a. verify at the end of the process that the certificate has been obtained by the intended applicant
   b. you must never issue more than one simultaneous invite.
   c. if the applicant cannot by him or herself request the certificate - because the link in the invite indicates that a certificate has already been issued to a *different* entity! - all certificates resulting from invites to applicant must be revoked *at once!*
4. *For eScience Personal Certs and Robots:* derive, based on local but consistent rules (that may be specific you your IdM), what would have been the unique identifier of the applicant. This is what usually end up in the *eduPersonPrincipalName* (ePPN), which usually looks like '`userid@domain.scope`'. It may also be an opaque targeted ID, or a serial number.
   The important thing is that this identifier
   a. is never re-assigned to any other applicant, ever (not even after 99 years)
   b. will probably be the same if the very same applicant comes back in the future
5. Retrieve from the IdM at least the following
   a. Full real name of the applicant
   b. Email address
   c. The record identifier of the applicant in the IdM (i.e. personnel number, an entityUUID, an LDAP or AD distinguished name, or the user-id if that is persistent and unique)
   d. If the IdM is not always available electronically, extract contact information for the applicant: phone number, home address, potentially the last few digits or letters from the government photo ID serial number.

Technical issuance process

1. Login to CertCentral as an Administrator
2. Choose the certificate product: Grid Premium, Grid Robot Name, Digital Signature Plus, or Premium – and click "Order Now"
3. Select the Validity Period (eScience Personal and Grid Robot are at most 13 months)
4. Select the proper Organisation inside your Division (this name will end up in the certificate)
5. **Leave** "Organsational Unit" **empty**!
6. Select "SHA2" as the hash
7. **Leave** Order Options on "**Don't automatically renew**". You are *not permitted* by the CPS to have automatic renewal enabled (it bypasses the required identity checks in your IdM!)
8. Fill in the Recipient Name. You **must** construct the Recipient Name *exclusively* from data in the IdM or HR databases.
   For eScience Personal and Grid Robot Name, you **must** append a space followed by the unique identifier to the name. So e.g. "David Groep davidg@nikhef.nl".
9. Fill in the email address. You **must** take this email address *exclusively* from the data in the IdM or HR databases.
10. Click "Submit Request"

At this point, an invitation email is send to the applicant. The applicant can click on the link in the email and generate the certificate (also the Grid Robot one) in the browser. The certificate can then be exported and/or backed up by the applicant through browser-specific mechanisms.

Before leaving the order system, you now must record the auditing data you collected in the verification phase in the DigiCert order system.

1. Go to the "Orders" tab in CertCentral
2. Open the order for the request you just sent. It will be listed as "Pending"
3. Click on "Manage Order Notes"
4. In the note pad, enter at least the following information
    a. Your own name and job description (role)
    b. The name and/or URL of the IdM system or HR database used
    c. The record identifier of the applicant in the IdM (i.e. personnel number, an entityUUID, an LDAP or AD distinguished name, or the user-id if that is persistent and unique)
    d. Phone number, (home) address, and potentially the last few digits or letters from the government photo ID serial number (unless you can be sure that the IdM is always available electronically).
    e. The entitlements or attributes from the IdM on which you based your judgement that the identity has been validated in a face-to-face or equivalent way – so show how the LoA2 vetting requirement has been met.
5. If authentication to the mail box is not linked to the IdM itself, verify out-of-band (phone call, in-person meeting) that:
    a. the certificate has been obtained by the intended applicant
    b. no more than one invitation was outstanding at any one time

This should conclude the manual issuance process.
For issuing the Grid Robot email and Grid Robot FQDN products, the process can be largely the same provided that:

- for Grid Robot email, the listed email address must be used
- for Grid Robot FQDN, you must (through local means) verify that the applicant is an OV or EV verified user in CertCentral for the listed domain, *or* is authorized administrator of the listed machine, *or* a registered contact for the domain. You must only request Robot FQDN certificates for domains that are Grid Verified for your organisation.