UK e-Science Certification Authority

Certification Practices Statement

02.04.2020

The Certificate Policy (CP) associated with this CPS is 1.3.6.1.4.1.11439.1.1.1.2.2.0 (20150304).

The UK e-Science CA remains a CEDAR (Classic) authority (1.2.840.113612.5.2.5.3), following the IGTF AP 1.2.840.113612.5.2.6.1; version 1.1 (2016). This CPS is consistent with both the CP and the AP. This document is conformant with RFC 3647.

1. Introduction

Until now (April 2020), the UK e-Science CA has only used in-person identity vetting. This updated CPS adds an alternative method of identity vetting that allows remote authentication at Kantara Level 2 or above (as described below). This implementation is consistent with the CEDAR requirements as described by the IGTF AP.

1.2. Document identification

This document is the CPS for the UK e-Science CA and is identified by 1.3.6.1.4.1.11439.1.1.1.9.2.

1.3. PKI Participants

As defined in the CP, the *Subscriber* requests a certificate on behalf of the *End Entity* that is named in the certificate. In the case of personal certificates, the Subscriber is almost always the same as the End Entity; for a host, the Subscriber is generally an administrator of the host in question.

1.5 Policy Administration

The organisation managing this policy is UKRI-STFC, through the CA Manager, who can be reached through:

CA Manager
Scientific Computing Department
STFC Harwell Oxford Campus
OX11 0QX Oxfordshire, UK

ca@grid-support.ac.uk

1.6 Definitions and Acronyms

The following abbreviations are used in this CPS.

AP	Authentication Profile	IGTF	Interoperable Global Trust Federation
CN	Common Name	OID	Object Identifier
CP	Certificate Policy	RA	Registration Authority
CPS	Certification Practices Statement	RFC	Request for Comments
CSR	Certificate Signing Request	RP	Relying Party
DN	Distinguished Name	SP	Service Provider
EE	End Entity		

3. Identification and Authentication

3.1 Naming

DNs contain a CN with a representation of the EE's authenticated name, subject to the constraints described in GFD.225. The CN may contain additional non-verified data, in order to disambiguate EEs with the same name, or to allow an EE to have certificates with different DNs.

Robots are supported. EEs are neither anonymous nor pseudonymous.

3.2. Initial Identity Validation

Identity validation prior to the issuance of EE certificates are as follows.

- All requests
  - For all requests, the RA shall check that the subscriber is entitled to request a certificate on behalf of the EE, and that the EE is entitled to have a certificate.
  - The RA shall check that the DN has not been used before.
- Personal requests
  - In-person verification, using appropriate photo id (government approved or, preferably, a staff pass, provided it has both the subscriber's photo and name);

  OR

  - An identity verification process according following Kantara Level 2 or better, as described in Annex A.
- Host requests. All host requests are identified by the subscriber's personal certificate.

  The RA Operator must check that:

  - every hostname to be included in the certificate is (a) controlled by the organisation for which the subscriber works, or (b) that the name is controlled by the subscriber; and,
  - the subscriber is responsible for the host(s) or other resources named in the certificate (typically as an administrator); and,
  - that the DN has not been used before by another entity.

- Robots. Robots are associated with individuals who request them using their personal certificates, and they carry the name of the person who requested them, plus an additional CN – and OIDs – identifying them as Robots.

Information is recorded in auditable form, subject to GDPR and to the CA's privacy policy and the policy of the organisation of the RA.

3.3 Identification and Authentication for Re-Key Requests

Subscribers can rekey EE certificates based on the existing private key. In this case, the CA supports rekey after expiry up to 30 days after expiry of the EE certificate. In exceptional circumstances, the CA may at its discretion allow rekey after expiry with a period longer than 30 days.

For subscribers requesting a certificate with a DN which has been used previously, but where the subscriber does not have access to a private key of an unrevoked certificate with this DN, or is otherwise unable to prove possession of the private key, the CA, through the RA, must check that the EE named in the DN is the same as the entity to which the previous certificates were issued.

In all cases, rekey is only permitted provided the EE’s entitlement to have a certificate remains valid – specifically, that the required auditable records are still available.

4.1. Certificate Application

Subscribers generate key pairs and CSRs and submit them to the CA portal which notifies the relevant RA.

4.2. Certificate Application Processing

The RA is notified of the submission of a CSR. When processing the request, the RA Operator must decide whether to follow the face to face approval process – which also does not change from RA Operator Procedure issued previously – or the Kantara Level 2 or higher procedure described in Annex A.

4.6. Certificate Renewal

The process for renewal of certificates (typically robots with keys on tokens) does not change.

4.7. Certificate Re-Key

The process for re-key has been amended slightly for the case where a certificate is rekeyed and the Subscriber does not have access to a private key of a non-revoked certificate that is being rekeyed. The amendment is required because the RA Operator may not have access to the original authenticating information, and thus permits additional evidence.

References

BIP0008 – Legal Admissibility and Evidential Weight of Information Stored Electronically

CP 2.0 - http://www.ngs.ac.uk/ukca/docs/cp-2.0.pdf

IGTF AP v 1.1 - https://www.igtf.net/ap/authn-assurance/igtf-authn-assurance-1.1.pdf

Kantara Initiative levels of assurance (KIAF-1200) - https://kantarainitiative.org/download/6171/

GFD.169 - Guidelines for Auditing Grid CAs - http://www.ogf.org/documents/GFD.169.pdf

GFD.225 - Interoperable Certificate Profile - http://www.ogf.org/documents/GFD.225.pdf

Annex A – Amended RA Operator Procedure – Remote Identity Vetting

This section describes the additional procedure. It supplements but does not replace the RA Operator Procedure for face to face identity checks.

A.1 Introduction and Risk

In the absence of individual RP's risk assessment (cf. NIST SP800-53), the main risks associated with misuse of the UK e-Science CA – specifically mis-issuance of credentials are:

- Inconvenience/distress/reputational.
- Misuse of computer resources. The UK has a misuse of computer act.

Specifically, UK e-Science CA certificates are not permitted to be used for financial transactions (including web sites managing credit card details), nor for safety critical infrastructure ("government agency and public interest"), or personal safety, where a failure could result, e.g., in loss of life. The IGTF community has therefore judged Kantara Level 2 as an acceptable minimum.

A.2. Procedure for Identity Vetting (Personal Requests)

For a personal request using the process described here, the subscriber must be the EE who is named in the certificate. The description below should take place after the subscriber has submitted their request for a personal certificate.

A.2.1. Initial Request

1. The RA operator must check that the DN has not been used before.
2. The RA operator must check that the request was submitted with an organisational email address managed by the subscriber's home organisation.
3. The RA operator must initiate a video call with the subscriber. This call should have sufficient security to protect OFFICIAL SENSITIVE discussions.
4. The subscriber must read the serial number of their request to the RA operator and provide the PIN to the operator. The operator must check that the serial number matches theirs and validate the PIN.
5. The subscriber must show photo id – of the type described in 3.2, and something that the RA operator recognises - where the video link must be sufficient to:
    a. Read the person's name;
    b. Verify the likeness of the photo id;
    c. As much as is practicable, verify that it looks like a valid id of the type it appears to be. Specifically for organisational id with photo, name, and holographic material, it is recommended that the subscriber hold the id at different angles to allow the operator to reasonably verify the presence of the holographic material.
6. The RA must take a screenshot of this interaction which shows the photo id.
7. The subscriber must then initiate a screen share with the RA operator, with a browser open.
8. The Subscriber must then, with the screen share remaining active throughout, use their browser to go to https://test.ukfederation.org.uk/ and authenticate to this service using their organisational id.
9. Once successfully authenticated, the RA operator must take a screenshot of the federation test page that shows the subscriber's name and organisational affiliation, the organisational email

checked in step 2, and principal. The operator must save these in a safe location, as described in A.3, along with the serial number of the request.

A.2.2. Reuse of Existing DN

If the requested DN has been used before, it is necessary to verify that the subscriber is the EE to whom the DN was previously associated. A proof of possession of a private key of a certificate with the DN is sufficient, provided this is recorded and no certificate associated with this private key is revoked.

If the subscriber is unable to prove possession of a private key as described above, additional evidence will be needed, and most likely, more than one piece of evidence is needed. It is recommended that the operator contact the helpdesk.

A.3. Storing Information

Unlike the paper format, information for these amended procedures are stored electronically. Due to the requirement for audits and, potentially, as evidence in investigations, BIP0008 is relevant. The implications of this are that RA Managers must consider the *duty of care* of the electronic information and must have documented processes for the management of the information. This information must address how the information is stored, and protected against unauthorised access, loss, unintentional modification. Additionally, if the RA has more than one Operator, the Manager should consider whether there are appropriate measures for sharing information between operators.

The RA Manager is responsible for their RA's processes and information storage.

A.4. Kantara Compliance

In order to assert that the above process is compliant with KIAF-1200 at Level 2 or higher, we note the following:

i. The operator has witnessed the subscriber authenticating to a resource using their home organisation identity, through a connection which is secure between the subscriber and the service.
ii. Safety against eavesdropping is achieved through secure channels, and using secured video communications.
iii. Safety against replay is achieved by the subscriber reading the serial number. It is not possible to approve the same request twice.
iv. Serial numbers are not easily guessable, although someone in possession of a recent serial number might make a guess of another. However, they would not know the DN, and would be unable to authenticate as anyone other than themselves.
v. The remote authentication is based on both the presented photo id and the successful authentication to the UK Access Management Federation test SP. It would thus be a Level 3 authentication (two factor) if we could reliably verify that the photo id is valid (unless the same photo id were used to prove identity to the organisation). For some type of id – organisational ids with holographic material embedded, it is generally possible to verify validity by turning it in the light.

We therefore claim that the procedure described in A.2 is consistent with Kantara Level 2 or higher which in turn is consistent with the operation of a Classic (CEDAR) CA.

A.5. Amendments

Should any part of this process need changing or amending to improve the Kantara compliance, the steps needed shall be identified by the CA Manager according to GFD.169. The RA Manager, in turn, is responsible for the timely implementation of these amendments in the RA.

Annex B. Changelog

03.04.2020	Updated to document Kantara compliance of remote working	J Jensen; J Kewley