Category: 1SCP documents
Status: DRAFT
Document: 1SCP-vetting-ttp-0.1.docx
Editor: David Groep
Last updated: Wed, 28 May 2008
Total number of pages: 3

Policy on vetting identity by a Trusted Third Party

Abstract
This Certificate Policy defines a policy where the identity vetting is mediated by a trusted third party.

Table of Contents

1 Introduction

1.1 Overview

This Certificate Policy defines a policy on identity vetting where the identity vetting is mediated by a trusted third party.
This is a one-statement certificate policy. The numbering follows RFC 3647, but sections that do not contain any stipulation are omitted.

1.2 Document name and identification

Document Name: Policy on vetting identity by a Trusted Third Party

Document Identifier: { igtf (1.2.840.113612.5) policies (2) one-statement-certificate-policies (3) identity-vetting (2) ttp (1) version-1 (1) }

1.5 Policy Administration

1.5.1 Organisation administering the document

This Policy is administered by the European Policy Management Authority for Grid Authentication in e-Science (hereafter called EUGridPMA) for the International Grid Trust Federation (IGTF).

1.5.2 Contact Person

The Chair of the EUGridPMA is the point of contact for all communications. The chair can be contacted by email at chair@eugridpma.org.

1.5.3 Person determining CPS suitability for the policy

The IGTF determines if a CPS complies with this policy.

1.5.4 CPS approval procedures

When approving CPS suitability for this policy the IGTF follows procedures defined in its accreditation procedures documents.

3 Identification and Authentication

3.2 Initial identity vetting

3.2.1 Method to prove possession of private key

The Registration Authority (RA) MUST have positive evidence, at the time they approve certification, that the end-entity (EE) has asked for this certification and that the trusted third party (TTP) approves it. To this end

- the RA MUST contact the EE directly (best effort), and confirm that this certification request was made by the EE; and
- the RA MUST contact the TTP directly (best effort), and ask the TTP to confirm the appropriateness of this EE's certification.

3.2.3 Authentication of individual identity

The identity is attested to by a trusted third party (TTP) trusted by the Registration Authority (RA). The attestation MUST include confirmation that the end-entity (EE) is personally known to the TTP, and the TTP approves of the certification. This is sufficient evidence to permit the RA to accept the certification request.

The RA will determine who is an acceptable TTP and maintain lists of these TTPs. The TTP SHOULD be personally known to the RA.

5 Facility, Management and Operational Controls

5.5 Records Archival

5.5.1 Types of records archived

The RA or the CA MUST maintain records showing that the appropriate transactions took place. The contact methods used between RA, TTP, and EE SHOULD be logged.

5.5.1 Retention period for archive

Records MUST be kept at least as long as there are valid certificates based on this identity verification.

8 Compliance Audit and other assessments

8.4 Topics covered by assessment

All records related to this policy will be subject to audit and MUST be made available to appropriate auditors.

9 Other business and legal matters

9.11 Individual notices and communications with participants

The CA, RA and TTP SHOULD use a trusted, secure communications path for all their communications and have direct contact, or have other means of confirming the contact even if the path would not be considered trustworthy.

In cases where secure communications paths cannot be used, immediate direct contact cannot take place or evidence is incomplete, the RA MAY complete certification, provided that the incomplete evidence is documented and satisfactory evidence is acquired in a reasonable time.