Category: 1SCP documents
Status: DRAFT
Document: 1SCP-certtype-robot-0.1.docx
Editor: David Groep
Last updated: Tue, 12 May 2009
Total number of pages: 3

Policy on automated client or robot entities

Abstract
This Certificate Policy stipulates that the certified entity is a non-human actively acting as an automated client towards other entities, for the purposes of this document called a Robot.

Table of Contents

1 Introduction

1.1 Overview

This Certificate Policy stipulates that the certified entity is a non-human automated client, also known as a Robot. Automated clients are entities that perform automated tasks without human intervention on behalf of named human individuals.

Production environments also typically support repetitive, ongoing processes - either internal system processes or processes relating to the applications being run by a site (or portal system). These procedures and repetitive processes are typically automated, and generally run using an identity with the necessary privileges to perform their tasks.[1] This policy on automated client will frequently be used in conjunction with a policy on private key protection.

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 automated client entities

Document Identifier: { igtf (1.2.840.113612.5) policies (2) one-statement-certificate-policies (3) entity-definition (3) automated-client (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

3.1 Naming

The common name component or components of the automated client SHALL identify both the abstract use of the robot as well as the natural person responsible for its certified key material. The Function of the robot is defined and restricted by its permissible key usage. In particular, the element describing the Function of the automated client holding the key pair to which the certificate pertains SHOULD describe what the entity 'is', not necessarily what it 'does'.

[1] Text based on draft-ggf-caops-auto-client-certs-00.txt, by Stephen Chen and Matt Crawford.

At least one common name component of the subject distinguished name must start with the string "**`Robot`**", immediately followed by the COLON character ('**`:`**') or a SLASH ('/'), which should be followed by a string describing the Function of the robot.

The natural person responsible for the automated client must be identified by a name that a bears a reasonable resemblance to the name of the person in accordance with the stipulations made on personal end-entity certificates by the issuing CA.

3.2 Initial Identity Validation

A named human individual MUST be identified as responsible person(s) for the use of the certificated key material.

3.2.3 Authentication of individual entity

The natural person responsible for the automated client should be authenticated according to all provisions for identification of personal (human) end-entities by the issuing CA.

3.3 Identification and Authentication for Re-key Requests

Re-key requests should be identified and authenticated according to all provisions for identification of personal end-entities by the issuing CA.