**Abstract**

This Certificate Policy defines a policy where the

**Table of Contents**

[1 Introduction 2](#_Toc199662408)

[1.1 Overview 2](#_Toc199662409)

[1.2 Document name and identification 2](#_Toc199662410)

[1.5 Policy Administration 2](#_Toc199662411)

[1.5.1 Organisation administering the document 2](#_Toc199662412)

[1.5.2 Contact Person 2](#_Toc199662413)

[1.5.3 Person determining CPS suitability for the policy 2](#_Toc199662414)

[1.5.4 CPS approval procedures 2](#_Toc199662415)

[6 Technical Security Controls 2](#_Toc199662416)

[6.1 Key pair generation and installation 2](#_Toc199662417)

[6.1.1 Key pair generation 2](#_Toc199662418)

[6.2 Private key protection and cryptographic module engineering controls 2](#_Toc199662419)

[6.2.1 Cryptographic module standards and controls 2](#_Toc199662420)

[6.2.6 Private key transfer into or from a cryptographic module 3](#_Toc199662421)

[6.2.7 Private key storage on cryptographic module 3](#_Toc199662422)

# Introduction

## Overview

This Certificate Policy defines a policy XXXXXXXXXX.

This is a one-statement certificate policy. The numbering follows RFC 3647, but sections that do not contain any stipulation are omitted.

## Document name and identification

Document Name:

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

## Policy Administration

### Organisation administering the document

This Policy is administered by the European Policy Management Authority for Grid Authentication in e-Science.

### Contact Person

The Chair of the European Policy Management Authority for Grid Authentication in e-Science is the point of contact for all communications. The chair can be contacted by email at [chair@eugridpma.org](mailto:chair@eugridpma.org).

### Person determining CPS suitability for the policy

The Policy Management Authority for Grid Authentication in e-Science determines if a CPS complies with this policy.

### CPS approval procedures

When approving CPS suitability for this policy the Policy Management Authority for Grid Authentication in e-Science follows procedures defined in its accreditation procedures document.

# Identification and Authentication

## Initial identity vetting

### 3.2.3 Authentication of individual identity

The identity is attested to by a trusted third party (TTP) trusted by the Registration Authority (RA). 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. Communications between the TTP and RA SHOULD be via a trusted path. RA MUST have positive evidence, at the time they approve certification, that the EE himself has asked for this certification and the TTP approves it.

* The RA MUST contact the EE directly (best effort), and confirm that this certification request was made by the EE.
* The RA MUST contact the TTP directly (best effort), and ask the TTP to confirm the appropriateness of this EE’s certification. This confirmation MUST include confirmation that the EE is personally known to the TTP, and the TTP approves of the certification.

Direct contact means the RA employs a trusted, secure communications path to reach the TTP or EE, or has other means of confirming the contact even if the path would not be considered trustworthy. The contact method SHOULD be logged.

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.

## 5.4 Auditing section

The RA or the CA MUST maintain logs and records showing that these transactions took place. These will be subject to audit and MUST be made available to appropriate auditors. Records MUST be kept for the lifetime of the certification in question.