**Abstract**

This Certificate Policy defines a policy where the private key of a key pair on which a certificate is based is generated, stored, and protected exclusively on a secure hardware token.

**Table of Contents**

[1 Introduction 2](#_Toc199475903)

[1.1 Overview 2](#_Toc199475904)

[1.2 Document name and identification 2](#_Toc199475905)

[1.5 Policy Administration 2](#_Toc199475906)

[1.5.1 Organisation administering the document 2](#_Toc199475907)

[1.5.2 Contact Person 2](#_Toc199475908)

[6 Technical Security Controls 2](#_Toc199475909)

[6.1 Key pair generation and installation 2](#_Toc199475910)

[6.1.1 Key pair generation 2](#_Toc199475911)

[6.2 Private key protection and cryptographic module engineering controls 2](#_Toc199475912)

[6.2.1 Cryptographic module standards and controls 2](#_Toc199475913)

[6.2.6 Private key transfer into or from a cryptographic module 3](#_Toc199475914)

[6.2.7 Private key storage on cryptographic module 3](#_Toc199475915)

# Introduction

## Overview

This Certificate Policy defines a policy on how the private key of a key pair on which a certificate is based is protected.

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) private-key-protection (1) hardware-token (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.

# Technical Security Controls

## Key pair generation and installation

### Key pair generation

The key pair must be generated inside the secure hardware token.

## Private key protection and cryptographic module engineering controls

### Cryptographic module standards and controls

The cryptographic module should be a hardware token complying with the requirements of FIPS 140-1 level 2 or higher or FIPS 140-2 level 2 or higher.

If not FIPS certified, implementation of an equivalent security level and appropriate mechanisms on the token must be demonstrated: the vendor must have built the device with the intention of obtaining FIPS 140-2 certification at level 2 or higher, and must either intend to submit the device for certification, or have it in process of certification. The token must not have failed an attempt for FIPS certification.

### Private key transfer into or from a cryptographic module

The private key may only be transferred into or from a secure hardware token in an encrypted form that must use a 128 bit symmetric key encryption or equivalent or stronger.

### Private key storage on cryptographic module

The private key can be in plaintext form exclusively inside the secure hardware token.