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

Policy on holding private keys protected on a secure hardware token

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

1.1 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.

1.2 Document name and identification

Document Name: Policy on holding private keys protected on a secure hardware token

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) }

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.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

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

6.2 Private key protection and cryptographic module engineering controls

6.2.1 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.

6.2.6 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.

6.2.7 Private key storage on cryptographic module

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