Category: 1SCP documents
Status: DRAFT
Document: 1SCP-private-key-filebased-1.docx
Editor: David Groep
Last updated: Tue, 12 May 2009
Total number of pages: 2

Policy on holding private keys protected in files

Abstract

This Certificate Policy defines a policy where the private key of a key pair on which a certificate is based is stored in a file or data object, either encrypted or in plain-text.

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 in files
Document Identifier:	{ igtf (1.2.840.113612.5) policies (2) one-statement-certificate-policies (3) private-key-protection (1) file-based (2) 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

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The private key pertaining to the issued certificate is kept in a machine-readable object from which the private key can be extracted. The private key thus extracted MAY be in either encrypted form or in plain-text.

The issuing authority SHOULD appropriately instruct subscribers holding private keys in this form about private key protection.