



Category: 1SCP documents
Status: DRAFT
Document: 1SCP-private-key-hardwaretoken-
1.docx
Editor: David Groep
Last updated: Sun, 25 May 2008

Policy on holding private keys protected on a secure hardware token

Abstract

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

Table of Contents

1	Introduction	2
1.1	Overview	2
1.2	Document name and identification	2
1.5	Policy Administration	2
1.5.1	Organisation administering the document.....	2
1.5.2	Contact Person	2
6	Technical Security Controls	2
6.1	Key pair generation and installation.....	2
6.1.1	Key pair generation.....	2
6.2	Private key protection and cryptographic module engineering controls.....	2
6.2.1	Cryptographic module standards and controls	2
6.2.6	Private key transfer into or from a cryptographic module	3
6.2.7	Private key storage on cryptographic module.....	3

1 Introduction

1.1 Overview

This Certificate Policy and Practice Statement 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: { igt (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.

1.5.2 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 contact by email at chair@eugridpma.org.

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

Secure hardware tokens are those hardware security cryptographic devices or hardware security modules that operate on and hold asymmetric cryptographic key pairs in such a way that the private part of the key pair cannot ever be extracted in unencrypted form, can only be unencrypted inside the device, and the encrypted form, if available, uses 128 bit symmetric key encryption or equivalent or stronger, and where the key pair can be generated inside the cryptographic device. Any tampering, any substitution or extraction of keys, and any unauthorized modification of the activation data, must leave evidence on the secure hardware token.

Secure hardware tokens and hardware security modules that comply with the requirements of FIPS 140-1 level 2 or higher, or FIPS 140-2 level 2 or higher, and where the key pair has been generated inside the module, are adequate to meet the requirements set forth above. 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.

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 must be held exclusively on a secure hardware token.