Category: guidelines document
Status: DRAFT
Document: approved-robots-20100101.doc
Editor: davidg
Last updated: Fri, 01 January 2010
Total number of pages: 4

Guideline on Approved Robots

Abstract [DRAFT]
This document describes guidelines on the generation and storage of private key material, naming, and permissible key usage of automated clients (robots) that can hold credentials issued by IGTF Accredited Authorities. It defines requirements and recommendations for issuing authorities and applicants, and indicates the permissible 1SCP policies to assert in the Certificate Policies extension of the robot certificate.

This document is an EUGridPMA Guidelines Document, to be referred to as the “Guideline on IGTF Approved Robots”, with OID 1.2.840.113612.5.4.1.1.1.6.

Table of Contents

1 Abstract

This document describes guidelines on the generation and storage of private key material, naming, and permissible key usage of automated clients (robots) that can hold credentials issued by IGTF Accredited Authorities. Footnotes are non-normative explanatory text, and may be removed or updated any time.

2 Robots

Robots, also known as automated clients, are entities that perform automated tasks without human intervention. Production ICT environments typically support repetitive, ongoing processes - either internal system processes or processes relating to the applications being run (e.g. by a site or by a portal system). These procedures and repetitive processes are typically automated, and generally run using an identity with the necessary privileges to perform their tasks.[1]

3 Naming

The subject distinguished name of a robot MUST unambiguously identify the entity as a robot by including the string “Robot”, followed by a non-alphanumeric, non-whitespace separator, in a commonName component of the subject name. The separator SHOULD be either a COLON (“:”) or a forward SLASH (“/”) character.

Naming Alternative 1
The natural person responsible for the automated client MUST be identified by a name that bears a reasonable resemblance to the name of the person in accordance with the stipulations made on personal end-entity certificates by the issuing CA. The named person thereby assumes responsibility for actions undertaken by the robot and for the actions of those persons that have access to and or can activate the private key pertaining to the robot relating to the robots activities.

Naming Alternative 2
The natural person responsible for the automated client SHOULD be identified by a name that bears a reasonable resemblance to the name of the person in accordance with the stipulations made on personal end-entity certificates by the issuing CA, or both a humanly-recognisable description as well as electronic mail address of a persistent group of people responsible for the robot operations MUST be included in a commonName component of the subject name.
The group of responsible people must react appropriately within the certificate revocation grace period to any request for information, and the issuing authority MUST keep the name of a single responsible natural person that assumes responsibility for actions undertaken by the robot and for the actions of the all persons in the group of people responsible for the robots operation.

Naming Alternative 3
The subject name of the robot SHOULD contain a humanly-recognisable description as well as electronic mail address of a persistent group of people responsible for the robot operations MUST be included in a commonName component of the subject name, or the name of a single natural person responsible for the automated client.
The group of responsible people must react appropriately within the certificate revocation grace period to any request for information, and the issuing authority MUST keep the name of a single responsible natural person that assumes responsibility for actions undertaken by the robot and for the actions of the all persons in the group of people responsible for the robots operation.

[1] Text based on draft-ggf-caops-auto-client-certs-00.txt, by Stephen Chen and Matt Crawford.

4 Key material

4.1 Generation

The key material based on which a robot certificate is issued MUST be generated

1. Inside a secure hardware token

2. Locally on an appropriately secured computer system

    a. of which the natural person responsible for the robot is the sole user and administrator, or

    b. to which only those people responsible for the robots operation have access,

    and where the key material is generated using trustworthy cryptographic software.

4.2 Storage and transport

The private key pertaining to a robot certificate[2] MUST be stored

1. On a secure hardware token

2. On a local file system on an appropriate computer system to which only those people responsible for the robots operation have access – and to which no other people have any access, either privileged or unprivileged

The computer system where the private key is stored MUST be appropriately secured, be actively monitored for security events, and MUST be located in a secured room where access is controlled and limited to only authorized personnel.

The private key pertaining to a robot certificate SHOULD NOT

- be left in plain-text form for extended periods of inactivity

- be sent over any kind of network unprotected

and the private key and activation data MUST NOT be sent in clear text over any kind of network.

5 Required certificate extensions

5.1 Key usage

The *keyUsage* and *extendedKeyUsage* extensions MUST be set, and MUST be at least as restrictive as those for certificates issued to human individuals. The extensions SHOULD be restricted to only those needed for correct operation of the robot.

5.2 Certificate Policies

[Naming Alternative 1] Robots that comply with this Guideline MUST include the OID 1.2.840.113612.5.2.3.3.1.1 (the 1SCP "Policy on Automated Clients or Robot Entities, version 1") as a *Policy* in the *certificatePolicies* extension of any certificate issued to a robot.

[2] These requirements apply to the key material on which the issued robot certificate is based. Derived credentials may be protected by other means, where compensatory measures are applied to offset security risks. In particular, the life time of derived credentials can be limited, and derived credentials can be stored in secured repositories such as *MyProxy* stores. Similarly, such stores can be used to make short-lived derived credentials available to systems that themselves are not and cannot be located in fully secured environments.

[Naming Alternative 2 and 3, that require a new 1SCP or a new version of 1SCP igtf.2.3.3.1] Robots that comply with this Guideline MUST include the OID 1.2.840.113612.5.2.3.3.1.2 (the 1SCP "Policy on Automated Clients or Robot Entities, version 2") as a *Policy* in the *certificatePolicies* extension of any certificate issued to a robot.

Robots where the private key material has been generated on a Secure Hardware Token from which it cannot be exported in any form MUST include the 1SCP OID 1.2.840.113612.5.2.3.1.3 ("Private Key Protection: Non-exportable Keys on a Secure Hardware Token") as a *Policy* in the *certificatePolicies* extension of any certificate issued to a robot.

Robots where the private key material has been generated on any other type of Secure Hardware Token MUST include the 1SCP OID 1.2.840.113612.5.2.3.1.1 ("Private Key Protection: Secure Hardware Token") as a *Policy* in the *certificatePolicies* extension of any certificate issued to a robot.

Robots where the private key is held in a file, either in encrypted or in plaintext form, MUST include the 1SCP OID 1.2.840.113612.5.2.3.1.2 ("Private Key Protection: Key material held in files") as a *Policy* in the *certificatePolicies* extension of any certificate issued to a robot.

5.3 Subject Alternative Names

The *subjectAlternativeName* extension of the certificate MUST include at least one *email* attribute with an email address of the responsible natural person, or an email address that addresses a persistent group of people responsible for the robot operations that will react appropriately, within the certificate revocation grace period, to valid requests for information.