Category: guidelines document
Status: APPROVED
Document: approved-robots-20140908.doc
Editor: davidg
Last updated: Mon, 08 September 2014
Total number of pages: 4

Guideline on Approved Robots

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. 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

the European Grid Authentication Policy Management Authority in e-Science – http://www.eugridpma.org/

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 separator, in a commonName component of the subject name. The preferred separator SHOULD be a single SPACE followed by a DASH and a single SPACE (" - "). It is recommended to have the Robot RDN be the last RDN in the subject name sequence[2].

The commonName subject DN component(s) of the robot MUST include a humanly-recognisable and meaningful description of the Robot as well as either:

- an electronic mail address of a persistent group of people responsible for the robot operations; or
- the name of a single natural person responsible for the automated client; or
- the validated fully-qualified domain name of the system from which the robot shall be solely operating. The RA SHALL ensure that the requestor is appropriately authorized by the owner of the associated FQDN or the responsible administrator of the machine to use the FQDN identifier asserted in the certificate. In this case the CA SHOULD have a facility to obtain at least the contact information contained in the public certificate about the owner of the FQDN based on the subject name of the certificate to any requester.

4 Key material

4.1 Generation

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

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.

[1] Text based on draft-ggf-caops-auto-client-certs-00.txt, by Stephen Chen and Matt Crawford.
[2] Since some interpreting software will log only the last cN RDN to the log file.

the European Grid Authentication Policy Management Authority in e-Science – http://www.eugridpma.org/

4.2 Storage and transport

The private key pertaining to a robot certificate[3] MUST be stored either:

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

Robots that comply with this Guideline MUST include the OID 1.2.840.113612.5.2.3.3.1 (the 1SCP "Policy on Automated Clients or Robot Entities") as a *Policy* in the *certificatePolicies* extension of any certificate issued to a robot.

Robot certificates must include, as a *Policy* in the *certificatePolicies* extension, the 1SCP for private key protection in accordance with the way the private key material was generated.

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.

6 Responsibilities

In case a persistent group of persons is named, this persistent 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 traceability to a single responsible natural person that

[3] 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.

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.
Subscribers are responsible for complying with the private key storage protection criteria and for maintaining appropriate access controls and traceability.

the European Grid Authentication Policy Management Authority in e-Science – http://www.eugridpma.org/