A Guideline on Robot Certificates

beyond the 1SCP stage

January 19, 2010

18th EUGridPMA Dublin meeting

Robots

1SCP

BACKGROUND

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.

Acceptable Robots

- We know what Robots are

- Which robots are acceptable end-entities?
  - De-facto standard set by UKeScience
    naming, private key handling, keyUsage
  - Conservative approach chosen
    Full name in subjectDN, hardware token
  - Copied by INFN and DutchGrid CAs
  - Initial consent by EUGridPMA was never formalised

- So, what are 'acceptable robots'?

Definitions of a Robot

- Via the 1SCP documents?
  - No, since the 1SCP series was designed to be orthogonal for RP trust evaluation purposes, not to be normative
- 1SCP 'Robot Entities' { igtf.2.3.3.1 }
  - Describes the type on entity
  - NOT whether a particular robot implementation is 'acceptable'
- 1SCP 'PKP Secure Hardware Token' { igtf. 2.3.1.1}
  - Says the key is on a hardware token
  - Not whether this is needed for a Robot, or for a person, or for a Martian

Guideline on Approved Robots

- Approved Robots are those robots that meet our criteria for acceptance under the Classic (or MICS, or SLCS) profile:

  "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's a Guidelines document, not a 1SCP or an AP
  - Managed by the EUGridPMA, on IGTF request
  - Assigned OID { igtf.4.1.1.1.6 }
  - https://www.eugridpma.org/objectid/?oid=1.2.840.113612.5.4.1.1.1.6
  - https://www.eugridpma.org/guidelines/robot/

But What Do We Approve Of?

Items to reach consensus on

- Naming
- Key generation
- Key storage
- Extensions
  - keyUsage
  - certificatePolicies
- Required contact information in EEC

Naming

- Basic naming requirement:
  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.
- Then the rest of the name? We discussed:
  1. *MUST have the full name of a responsible natural person*
  2. *SHOULD have full name of responsible person OR MUST have recognisable description PLUS email address of a persistent group of people responsible for the robot operations in the CommonName*
  3. *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, OR MUST have have on single responsible natural person*

Alternative 1

Maintaining the current, confusing, status-quo ☹:

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.

Alternative 2

'current process is OK, but operationally responsive team is equally good as long as all CAs do it the same way':

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.

Alternative 3

'Operationally responsive team is preferred, with all CAs doing it the same way, but current practice is also still OK':

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.

Key Material

- Long discussion on the list on the usefulness of hardware tokens in the presence of proxy authentication and permissible derived credentials
- In practice hardware token is always activated or activation data stored on the file system
- Actual risk not affected by the use of hardware tokens or file-based storage

Proposal: generation of keys

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.

Proposal: storage of keys (not proxies)

The private key pertaining to a robot certificate 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.

Extensions

- keyUsage:
  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.

- subjectAlternativeName
  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.

Extensions: certificatePolicies

- For robots require appropriate assertion of 1SCPs
- For naming alternative 2 and 3 we need
  - A new 1SCP for these robots
  - Or a new version of { igtf.2.3.3.1}

Next steps

Based on discussions today:

- Approve the Guidelines document
- Propose to TAGPMA and APGridPMA

- Start working under the new guideline
  - May be more permissive for current Cas
  - Entice new CAs to issue robot certs
  - Resolve Alexey's problem, I hope …