Virtual Image distribution mechanism

Rubric

Authors: Martin Bly (RAL), Owen Synge (DESY)

Date: 29 March 2010

Version: v0.2

Status: Draft

Introduction

This paper describes a possible distribution mechanism for virtual images to be used at wLCG sites, addressing various issues such as validation, verification, expiry and revocation. The actual distribution technology is not discussed in detail.

Summary

Images are signed using x509 technology, distributed to sites and registered in a catalogue at the site. When an instantiation request is received, the image validity is checked. If the image is valid, the image is contextualised and then instantiated. Images that do not pass validation are not instantiated.

Description

The basic idea is that virtual images are signed at creation and approval with a x509 certificates. Each image is then given its own x509 certificate. This provides a mechanism by which a virtual image can be checked for validity: expiry, revocation, whether it has been tampered with etc, and traceability.

The image is then distributed to a site using (for example) the software distribution mechanism by the responsible VO. Information about the image (the certificate public keys, VO responsible, a unique ID, a VO tag family and a URI, inital global validity, i.e., the metadata) is registered with a local catalogue. A local validity flag may also be set by the site.

Requests for instantiation are made via the unique ID or the tag. When the local system receives an instantiation request for a particular image, the catalogue is checked for the location and global and local validity flags. If both are OK, the image is then checked for expiry and revocation using the x509 credentials. If the image passes then the image is contextualised and instantiated. Expired or revoked images are refused.

Details

Terminology

Image	A virtual image created to be instantiated at a Site
Site	The site running the Image locally
Creator	Person or role authorised to build an Image
Approver	Person or role authorised to approve an Image has been created according to the defined policies and standards
Registrar	Authority issuing x509 certificates for an Image
Catalogue	As simple database containing Image registration data
Tag	An identifier for a Family of Images
UUID	Globally unique image identifier

Image Signing

An Image will be created by a Creator and signed by the Creator's x509 certificate. The Image will then be approved by an Approver and further signed by the Approver's x509 certificate to validate that the Image has been created according to the policies and standards required. Each Image will be issued with an x509 certificate and signed by a Registrar. The Image will have an appropriate expiry for the certificate. The Image may then be distributed.

Distribution

An image may be distributed at Site by any suitable means including the existing software distribution mechanism.

Local Catalogue

A Site will have a local Catalogue which will be a registry (database) of Images which may be considered for running at the Site. The Catalogue will contain metadata for each subscribed Image: the x509 certification data, the unique UUID, a Tag, resource locator, a global validity flag field and a local validity flag field.

The Local Catalogue will subscribe to the appropriate revocation service (CRLs) and flag Images that have been revoked by setting the global validity flag.

A local validity flag may be set against an Image, to allow local administrations to 'blacklist' an Image. The local validity flag may also be set to 'run anyway' to allow expired but NOT revoked images to be run

Registration/Subscription

A distributed Image will be subscribed to the local Catalogue by the distribution mechanism. The subscriber will write the Image metadata to the catalogue and set the global validity flag by checking the latest CRLs. Images may be subscribed locally using the approved API.

Instantiation

A request to the instantiation system to run an Image will cause the instantiation system to validate the Image against its global and local validity flags and metadata in the Local Catalogue, and to check for the expiry of the Image using its x509 certificate. If an image passes all the required checks, the Image may be contextualised and then run.

Image Metadata

Images will have x509 signature/certificate metadata. Images will have a unique identifier (UUID). Images will have a Tag name which may be non-unique such that a series of images may belong to a tag family. Requests to run an image may be either via the UUID or the Tag. In the case of a Tag having more than one UUID registered the latest dated image will be considered for instantiation.