List of endorsers

CERN IT Department

CMS list of endorsers

Endorser 1:
- Real Name
- Digital Identity
- URL of VMIC

Endorser 2:
- Real Name
- Digital Identity
- URL of VMIC

...

RAL list of endorsers

Endorser 1:
- Real Name
- Digital Identity
- URL of VMIC

Endorser 2:
- Real Name
- Digital Identity
- URL of VMIC

RAL local endorsers:
- Real Name
- Digital Identity
- URL of VMIC

...

XYZ list of endorsers

Endorser X:
- Real Name
- Digital Identity
- URL of VMIC

Endorser Y:
- Real Name
- Digital Identity
- URL of VMIC

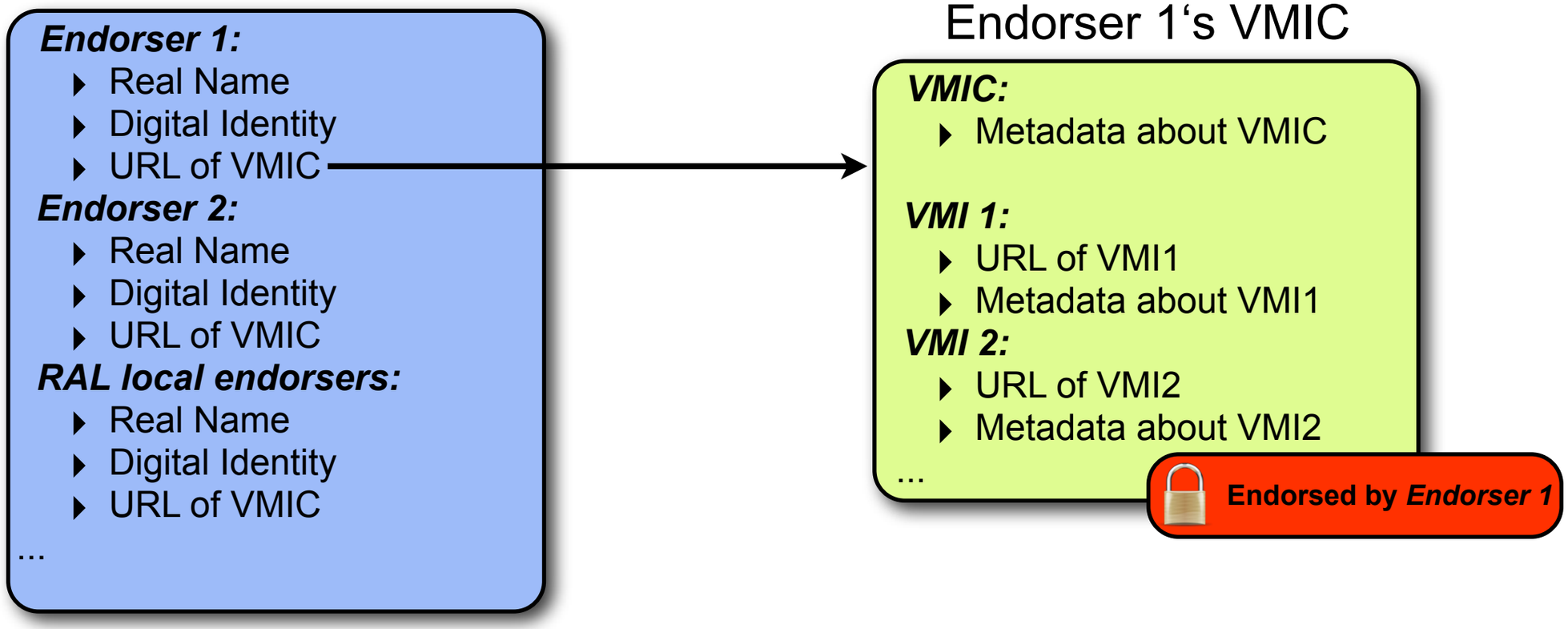
...

Different communities/sites/groups maintain a list of "valid endorsers"

- The list may built from scratch
- The list may also be based on existing list
  - With a mandatory synchronization mechanism to the original source
- Each community/site/group must document but is free to:
  - Complement the JSPG policy with more criteria to maintain the list
  - Decide how changes are managed/announced

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

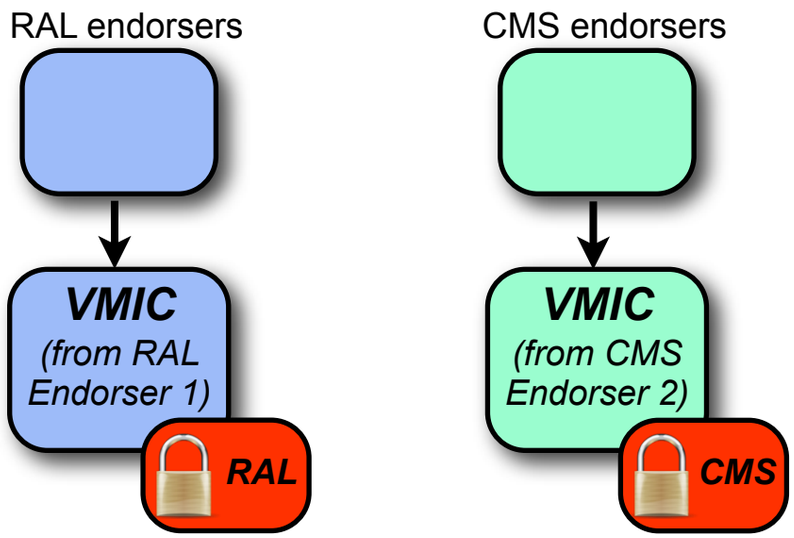
VM VMIs Catalog

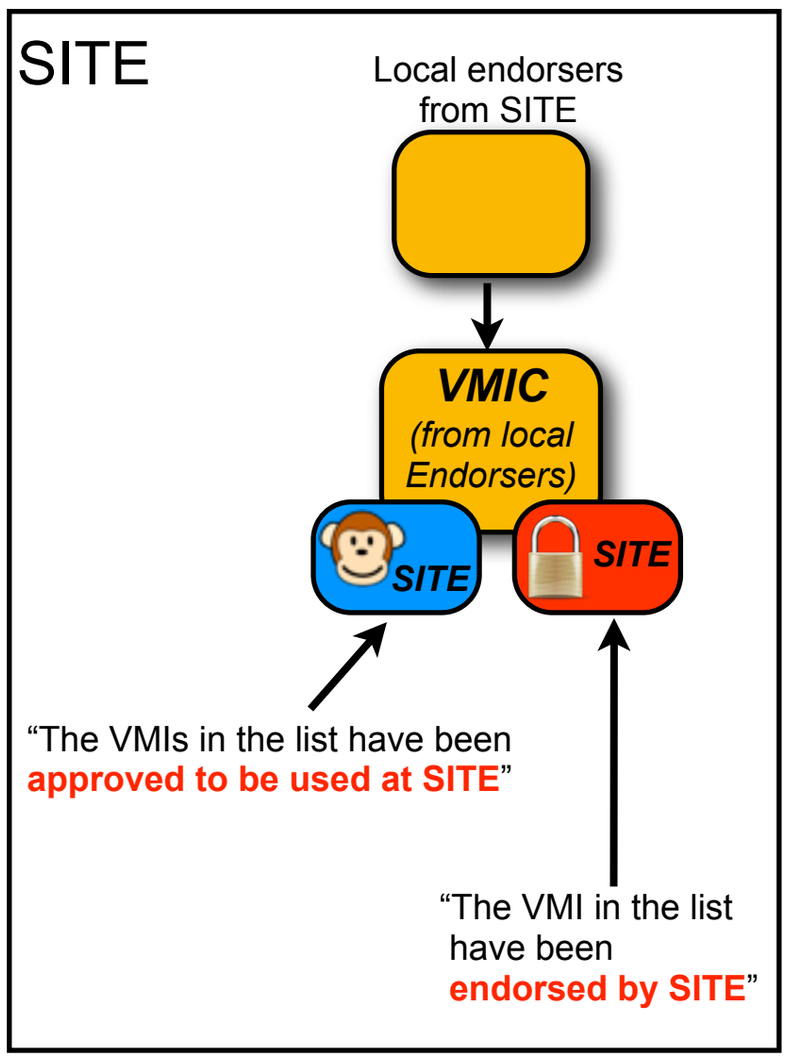


- **Each endorsers publishes a VMIC**
  - The VMIC is signed by the digital identity of the endorser
- **Some metadata is included for the VMIC and for each VMI**
  - As defined in the VMIC design document:
    - VMIC: Real Name and digital identity of the endorser, max lifetime;
    - VMI: UUID, VMI checksum, OS version and 64/32bit status, hypervisor requirements, endorser’s digital identity, date produced, date endorsed, VO tag;

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Endorsed vs approved

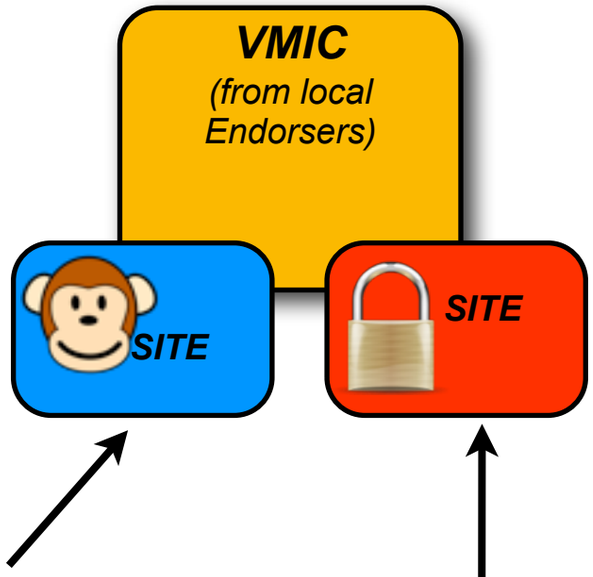




- **Distinction between:**
  - Endorsed (endorser decision):
    - Role defined in the policy document
    - Scope: VMI production & maintenance
  - Approved (site decision):
    - Marks the VMI "valid for use" by the site
    - Scope: operating the VMI
- **For a VMI to run, it must be both:**
  - Endorsed by an endorser (i.e. Part of the VMIC endorsed)
  - Approved by the local site
- **The VMI is run only when the two conditions are met**
  - The site has control over VMIs being run
  - The endorser has control over VMIs being produced/endorsed/published

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Endorsed vs approved

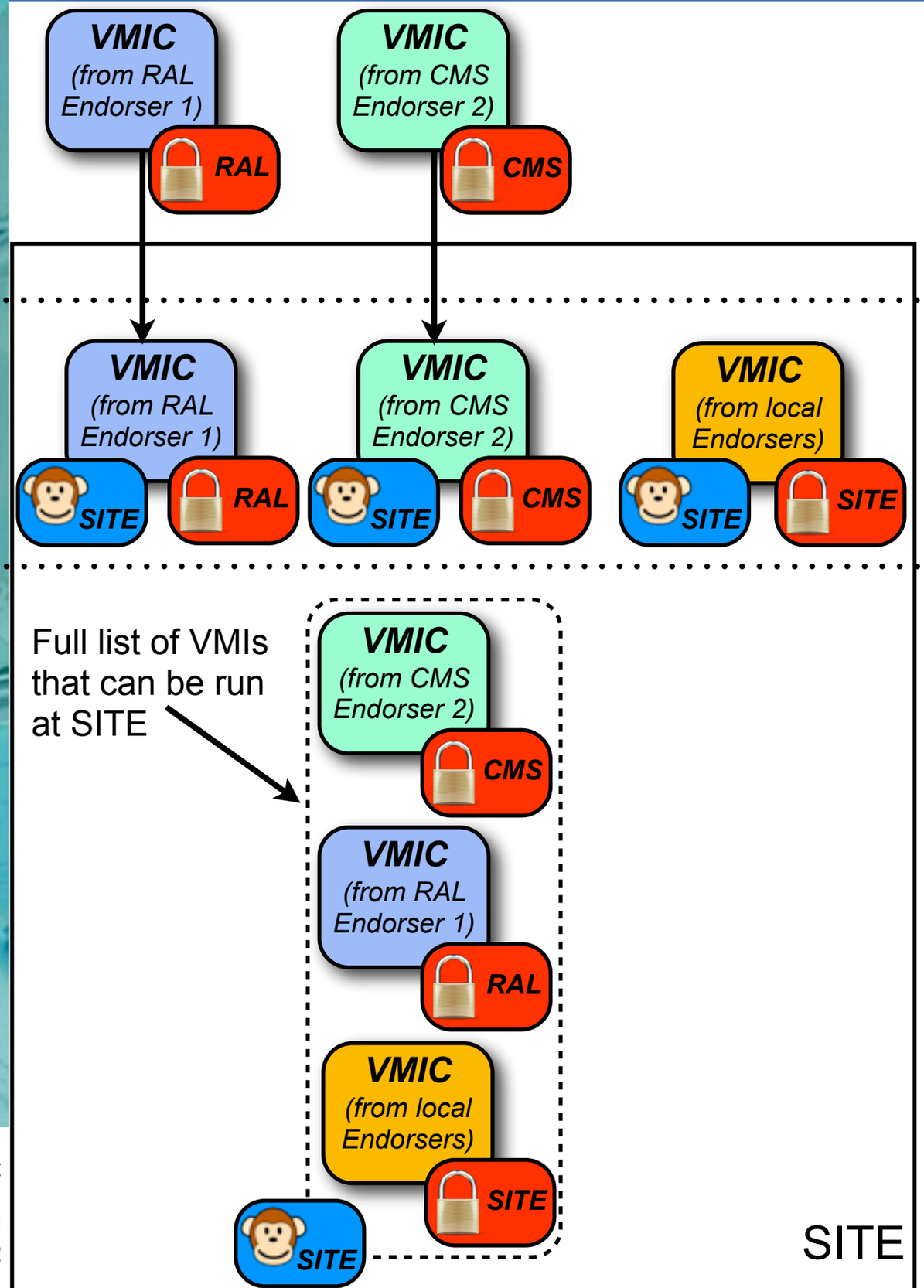


"The VMIs in the list have been **approved** to be used at SITE"

"The VMI in the list have been **endorsed** by SITE"

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Heterogenous example



1. SITE decides to approve VMIs endorsed by (XYZ) RAL and CMS

2. VMIs are approved(SITE)
Sites has fine-grained control over VMIs being approved (but can also approve them all)

3. The RAL and CMS VMIs are added to complement the VMIs produced locally

4. The resulting list of VMIs (endorsed by different entities) is approved by the local site

XYZ + SITE + SITE

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Use case 1: VMI lifecycle

1. **VMI creation**
2. **VMI endorsement + publication**
3. **VMI distribution (between sites)**
4. **VMI verification**
5. **VMI approval**
6. **VMI distribution (within each site)**
7. **VMI revocation**

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Use case 2: Endorser handling

CERN IT Department

- **Endorser:** ***"An individual who confirms that a particular VM complete image has been produced according to the requirements of this policy and states that the images can be trusted."***
- ***A new Endorser for VO XYZ enters.***
  - *The new endorser needs to be approved*
  - *All sites supporting VO XYZ must be informed*
  - *All sites supporting VO XYZ are asked to make its VMIs available for the users of this VO*
- ***An Endorser leaves VO XYZ and is not replaced***
  - *The VO wants the sites to keep running its VMIs*
  - *The VO decides to revoke all its VMIs*
  - *All sites supporting VO XYZ must be informed about this change. No **new** VMIs of this Endorser must be approved*
- ***An Endorser E1 of VO XYZ is replaced by Endorser E2***
- ***VO A elects a new Endorsers E1. Site S1 supports VO A. Site S2 does not support VO A***
  - *Site S1 needs to take action*
  - *Site S2 should not be bothered*

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Use case 3: Endorsers'

- **A new VMI is released. Endorser A blesses it for publication**
  - The new VMI is published
  - Supporting Sites are asked to make the new VMI available for the users
- **Endorser A revokes a previously blessed VMIs**
  - e.g. because a bug has been found, without replacing it
- **Endorser A wants to update an existing VMI**

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Use case 4: site actions

- A site B wants to use a site specific VMI for local users
- A site B has created a VMI which is useful for other sites and wants to share it
- A site is asked to run a VMI from a trusted endorsers, and the site policies allow this
  - the VMI integrity is ok, and the VMI can be made available
  - the VMI integrity is violated (e.g. wrong checksum, wrong signature...)
- A site is asked to run a VMI from a trusted endorser, but site policies forbid them to run it
- A site needs to stop running VMIs for type XYZ because of some reason (security, bug, wrong software,changed site policies)
- A site needs to stop running all VMIs of Endorser XYZ, which were previously trusted and used
- A site needs to make a new VMI available to their users
- Endorser A is replaced by Endorser B. VMIs of A are no longer trusted, VMIs of Endorser B are trusted.

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it