

Trusted Appliances

Trust between users, cloud administrators, and appliance creators is critical for an effective and dynamic cloud ecosystem.

The StratusLab Marketplace, an appliance registry,

Endorsers

1. Evaluate appliances based on security or other criteria
2. Sign (endorse) appliances that they

End-Users

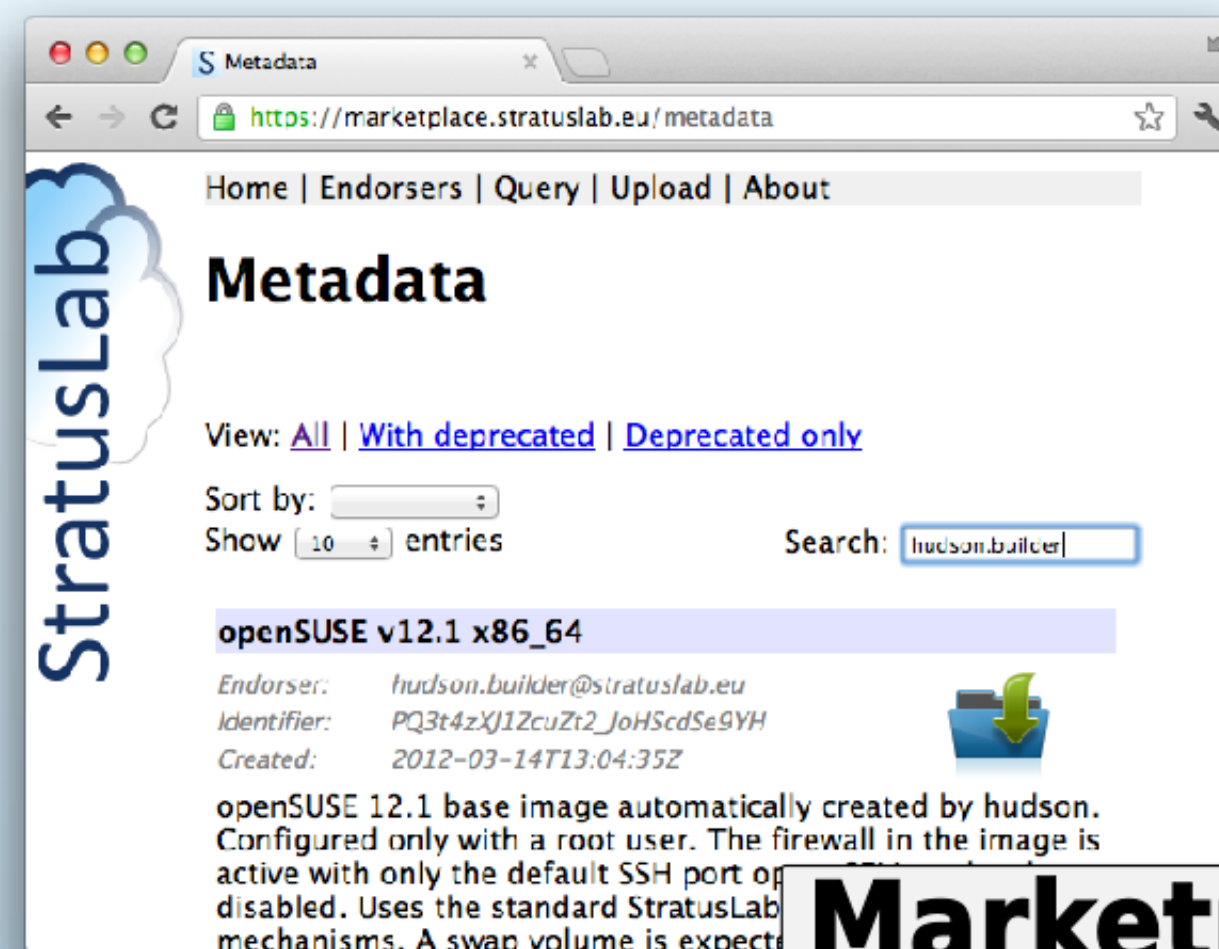
1. Scientists and engineers browse the Marketplace for useful appliances
2. Easily launch machine instances using the

Cloud Administrators

1. Define appliance acceptance policy
2. StratusLab tools enforce

Domain Experts

1. Create specialized appliances
2. Upload appliances to cloud or web storage
3. Create and sign appliance metadata
4. Upload metadata to the Marketplace



Marketplace

- Acts as neutral broker for appliance metadata
- Enforces individual timelines for

Metadata Handling

Client tools provide commands to **build image metadata**, **sign** the metadata entries, **upload** the entries to the Marketplace, and to validate them.

Any certificate or key can be used to sign metadata entries. **Email addresses are verified** to ensure

The **policy engine** uses metadata information and the **cloud administrator's policy** to decide whether or not to **start an image**. Standard policies allow white/black lists of image endorsers and image identifiers. Any policy

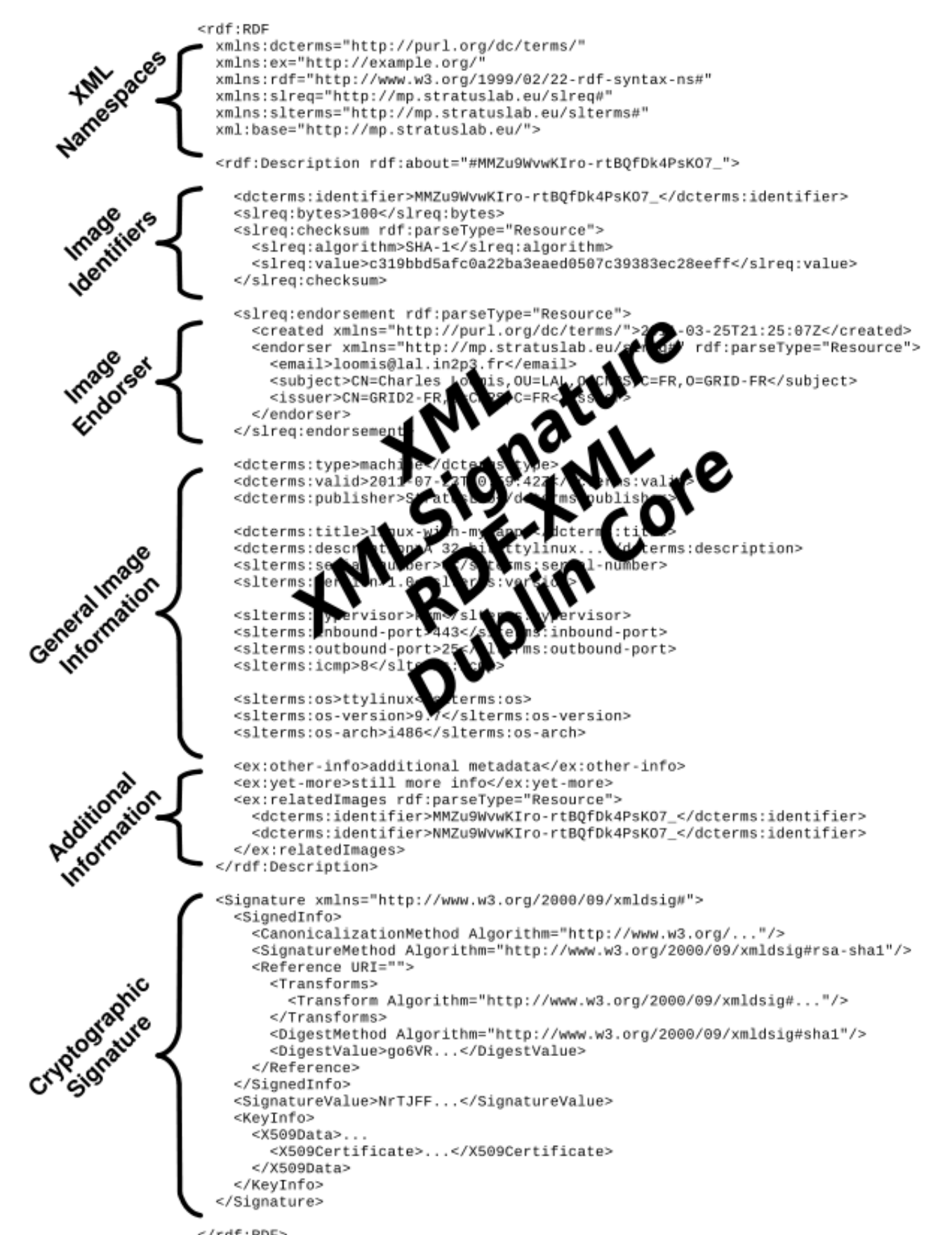
Security

A consistent metadata timeline is critical for understanding the evolution of an image and for auditing the metadata if there are problems. The **Marketplace ensures a valid timeline for each endorser** by requiring that all entries are dated and accepting only

A hacker in the Marketplace could not forge new entries but could alter the timeline by deleting entries. **Marketplace servers must be managed following best practices** and keeping

Appliances may contain **proprietary software** or other protected material. To avoid Intellectual Property Rights (IPR) issues, the **Marketplace stores only the metadata**. The appliance is stored elsewhere,

To **avoid man-in-the-middle attacks**, the Marketplace is run over HTTPS. This ensures that the server's identity is validated and that messages are not intercepted or altered in transit.



As **protection against altered or corrupted images**, the SHA-1 checksum and size of the image (stored in the metadata) are verified. to allow validation of the downloaded data. Additional checksums further reduce this risk.