OSG PKI Enrollment and Vetting Workflows

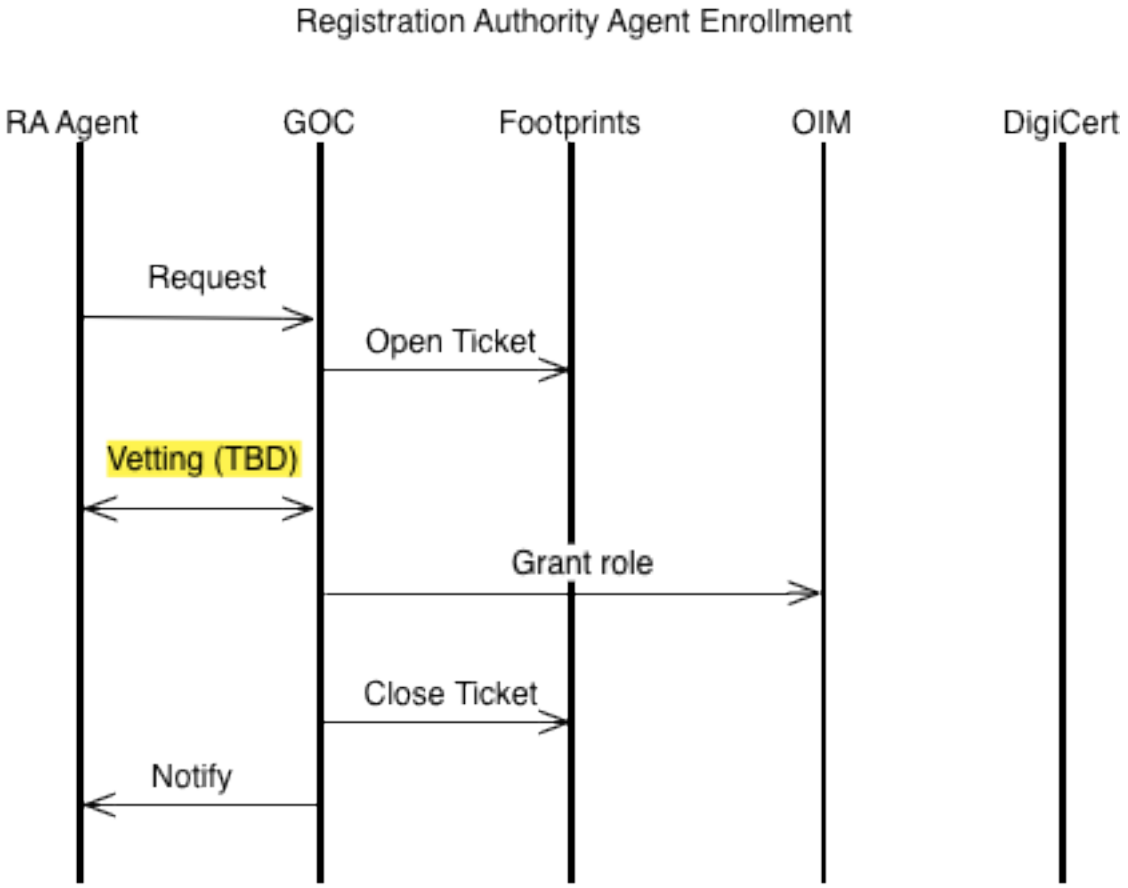
DRAFT May 8th, 2012 DRAFT

Von Welch

1 Introduction

This document captures workflows for enrolling Registration Authority Agents (to vet user certificate requests) and Grid Admins (to vet host certificate request) in the new PKI.

2 Registration Authority Agent (RAA) Enrollment

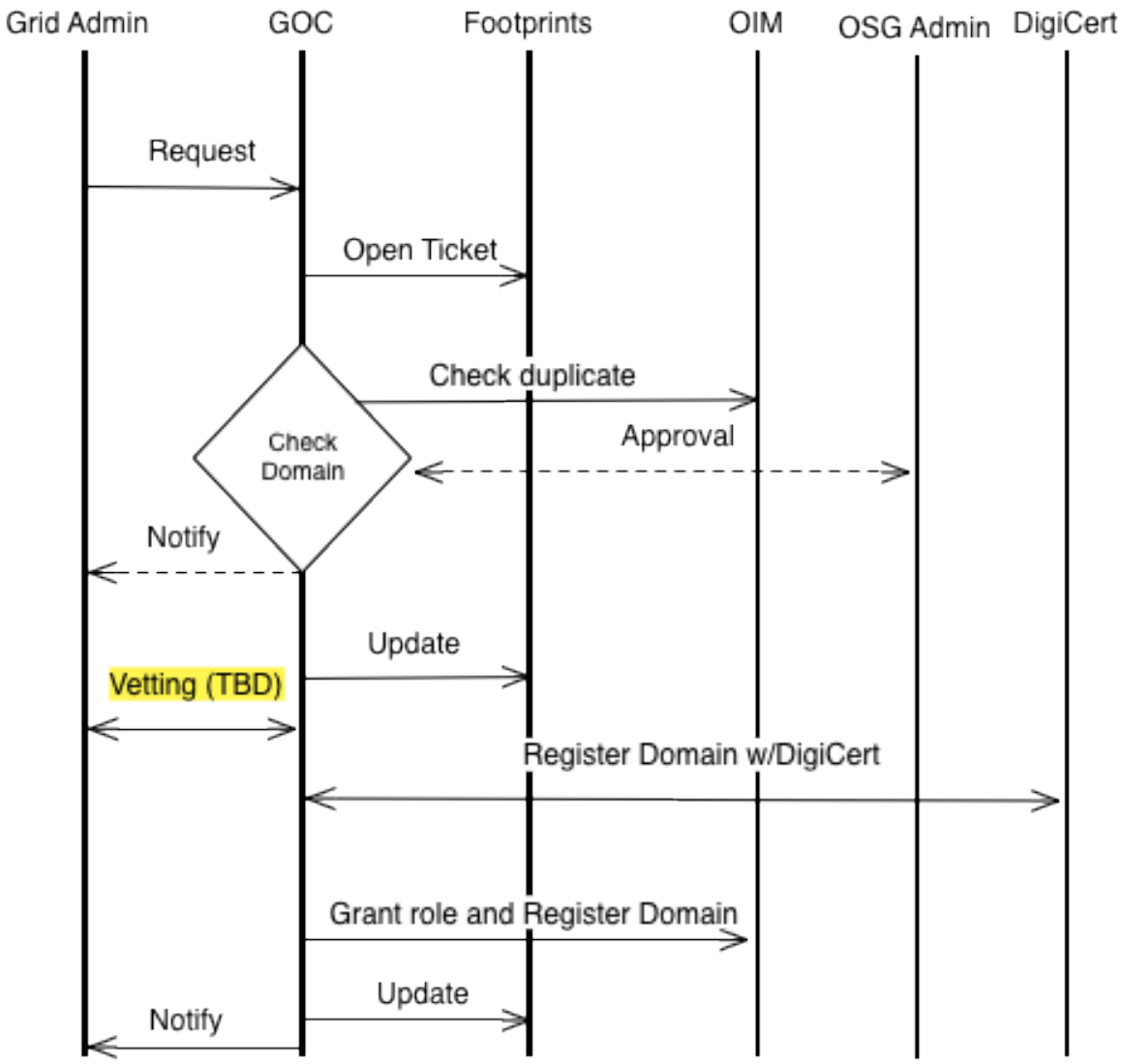


- Request: An authenticated (w/DigiCert certificate) request to become a RAA for a given VO.
- Open Ticket: A footprints ticket is opened to track the request.
- Vetting: process TBD, this is a placeholder.
- Grant role: The requestor is granted the RAA role in OIM, allowing them to approve subsequent user certificate requests for the VO in question.
- Update: The previously opened ticket is updated with the fact the user has been granted RAA role and the ticket is closed.
- Notify: The user is notified of the result of the vetting process.

3 Grid Admin (GA) Enrollment

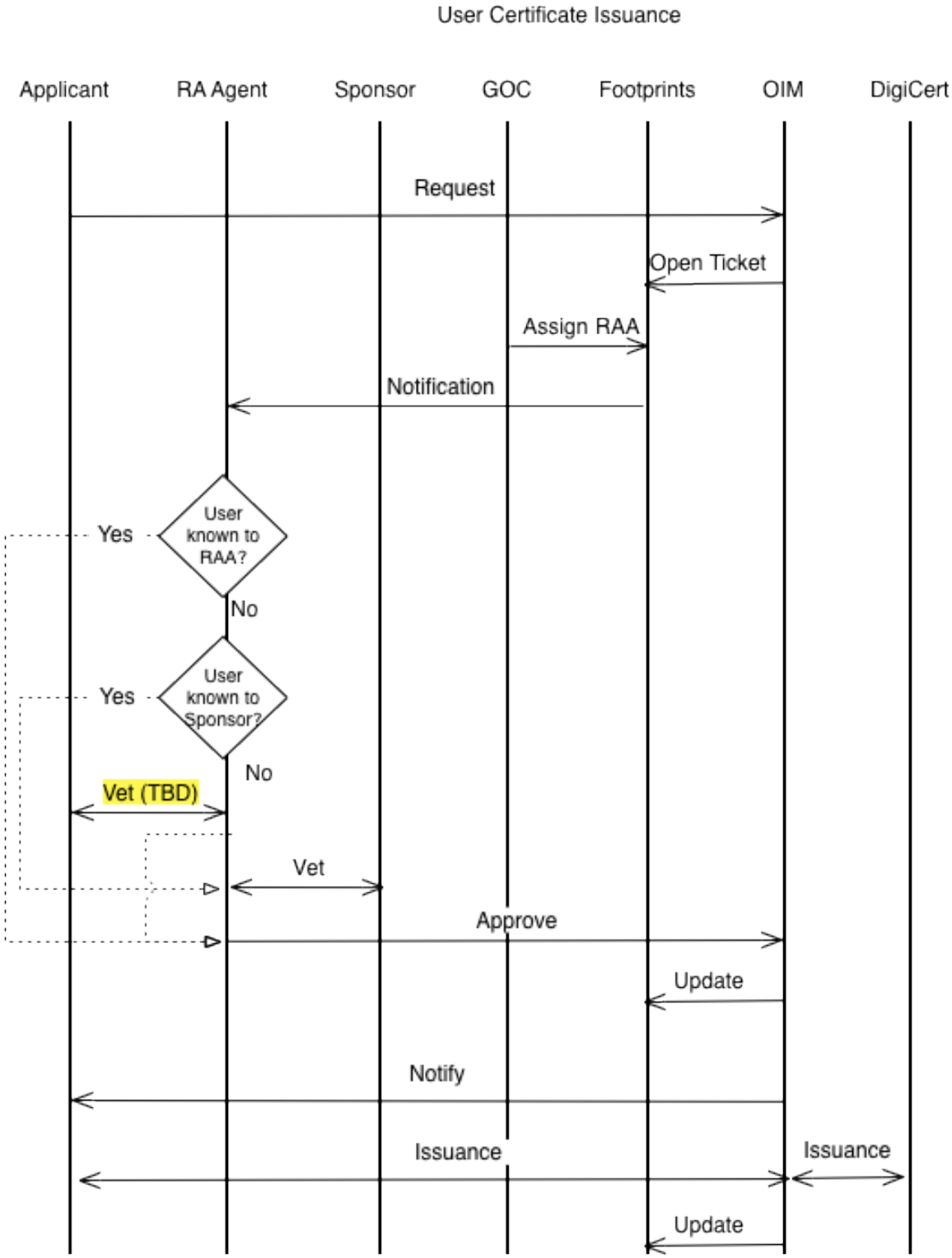
- Request: An authenticated (w/DigiCert certificate) request to become a Grid Admin. Request includes the intended domain for which the Admin wishes to be authoritative for.
- Open Ticket: A footprints ticket is opened to track the request.
- Check Domain: The requested domain is checked as follows:
    - If it overlaps with an existing registered domain then the request most be approved by existing Grid Admins for the overlapped domain.
    - If it is outside the following domains, it is rejected: .edu, .org, .gov, .net, and .us.
    - If it is less than a third-level domain (e.g., example.edu as opposed to physics.example.edu), the Grid Admin must be an authoritative representative of the domain owner (e.g., from the IU department of the university or project that registered the domain) or obtain an exception from the OSG management.
- Update: The previously opened footprints ticket is updated at various steps with results of those steps.
- Register Domain w/DigiCert: The domain is registered via email to the OSG DigiCert POC. Registration is acknowledged.
- Grant Role and Register Domain: The Requestor is granted Grid Admin privileges for the given domain in OIM.
- Notify: The user is notified of the result of the vetting process.

Grid Admin Enrollment



4 User Certificate Enrollment

This reflects and should be harmonious with technically-oriented processes in the OIM certificate management design doc.

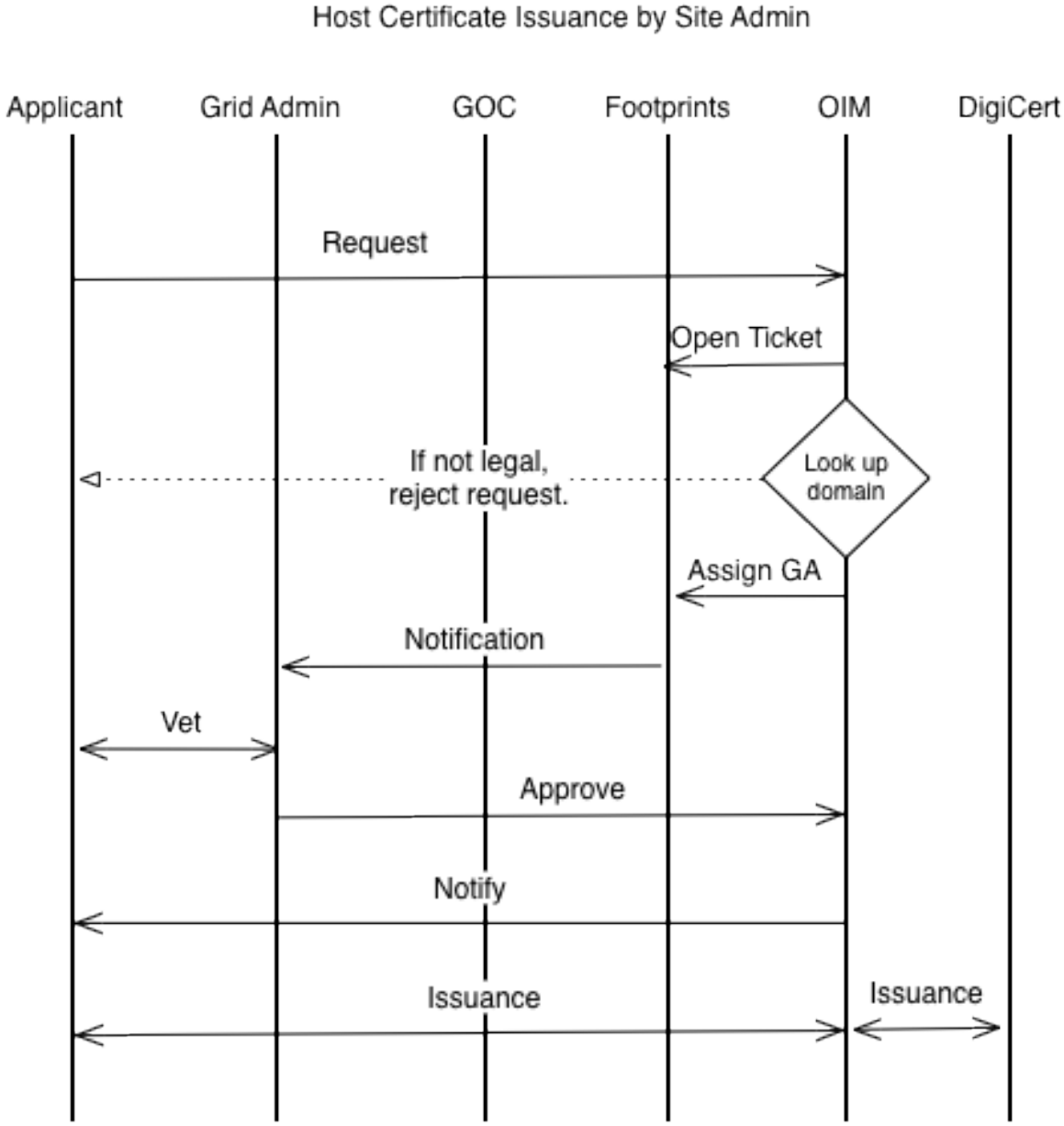


5 Host Certificate Issuance

This reflects and should be harmonious with technically oriented processes in the OIM certificate management design doc.

5.1 Host Certificate Request by Site Admin

Request for a single host certificate by a Site Admin.



5.2 Bulk Host Certificate Request by Grid Admin