GFD-C
Category: Community Practice Documents
CA Operations WG

March 2004

OCSP Requirements for Grids

Status of this Memo

This is an informational track document.

.

Copyright Notice

Abstract

Grids use X.509 certificates for authentication and authorization. These certificates have built-in lifetimes, but this is insufficient: lists of revoked certificates are required by many relying parties, and should be used by every relying party, in order to eliminate lost, compromised, or otherwise-invalid certificates from use. Commercial credit and debit cards are managed in an analogous fashion. The Online Certificate Status Protocol (OCSP) is a protocol that can be used to provide this service for Grid stakeholders. OCSP is a simple query protocol, relieving its clients of the burden of managing lists of revoked certificates. Since the OCSP server is not specified in detail, certificate validation services beyond reporting of contents of certificate revocation lists (CRLs) could be provided. The Grid presents considerable challenges for such a service, however. To be suitable for Grid use, OCSP services must be discoverable. Grid administrators need to develop interoperability methods, "chaining" methods from one OCSP to another, and replication techniques.

Table of Contents

1 Introduction

Grids use X.509 certificates for authentication and authorization. A reliable, secure Grid infrastructure depends on the integrity of these certificates. X.509 certificates have built-in lifetimes, but this is not adequate to deal with every aspect of certificate life cycle and management. Certificates can be lost by their owners, can be "compromised", or the justification for holding the certificate may no longer apply. These certificates need to be revoked before the certificate expiration date is reached. Distribution of certificate revocation lists (CRLs) support this need. Distribution of these in the Grid have proved difficult, but more burdensome still is the necessity of supporting validation functions on every client. Online Certificate Status Protocol (OCSP) provides a simple query protocol for clients to perform basic validation lookups on certificates without the need to maintain sets of CRLs from different certificate authorities.

OCSP is a product of the IETF PKIX working group, and the current version is described in [RFC2560].

[From here on, describe what we need to do:

practical considerations

over all service

client requirements

server requirements

CA or certificate "requirements"

]

2 Practical Considerations

[In this section, we discuss which software packages support this, such as revisions of openssl, gsi, java, and any other important support api's; browser support; Apache web servers; other web servers or the like.

We may need to discuss incompatibility or limitations (for instance, Microsoft IE doesn't support OCSP directly). Identify missing software / software requiring development or integration issues that stakeholders may need to deal with]

3 Service

[Issues related to the protocol (see RFC 2560 section 2) and Appendix A.1 We are only interested in supporting OCSP over HTTP – rqmt. Any other transports? WS description

There are some changes proposed for OCSP – see below & PKIX list. Also examine the large-scale VeriSign OCSP service.

]

4 Client Requirements

[See 3. Clients will have to have the ability to POST (http) their requests.

Caching should be provided. How do we specify/lifetime ?

Clients may wish to mix OCSP and CRL – or other validation services – do we deal with this or skip it?

How do clients discover this service:

Can we use DNS

Built-in

Default local OCSP server

AIA extension in certificates

Discovery is the most important issue. We need to define a reasonable default, but allow some flexibility for different circumstances.

How does client deal with failure: "unknown" response from OCSP server

How does client deal with failure: OCSP responder doesn't perform, not there &c

Bottom line: need a basic configuration file spec

]

5 Server Requirements

[

Track discussion in IETF/PKIX about changes to standard

Gathering of CRL's

Performance – a lot of signed data!

Special / custom lists – Relying Parties want "Rapid Response" to security incidents

Underlying database – we probably care about this because

- We want replication
- Need to provide local lists
- Integration with proxy cert issuers & services

Integration with CAS/VOMS?

Our experience with OCSP servers has been with a commercial product which has considerable capabilities but also some limitations. A server based on open-source software such as openssl or a java implementation should be developed in tandem with this requirements definition.

]

6 CA / Certificate Issuer Requirements

[AIA extension for OCSP – see RFC 3280 & 2560. There shouldn't be much to do here. This is a SHOULD not a MUST; formatting and conventions for using the PKIX extension will be defined. Commercial practices (to the extent they can be found) should be followed if possible to insure future interoperability.

Glossary

None

Intellectual Property Statement

Full Copyright Notice

References

[PKIX]

[RFC2560]

[RFC3280]

Change History

24 February 2004 Initial rev