GWD-R, GWD-I or GWD-C

CAOPS-WG

David Groep, Nikhef
Jens Jensen, STFC

Version 20080916
Updated: Sept 16, 2008

Relying Party Defined Namespace Constraints Policies in a Policy Bridge PKI Environment

Status of This Document

This document is a DRAFT. This document provides information to the Grid community. It does not define any standards or technical recommendations. Distribution is unlimited.

Abstract

Relying Party Defined Namespace Constraints (RPDNC) are limitations on the subject namespace issued by X.509 certificate authorities (CAs) that are defined and enforced by the end-point at the relying party side. As grid authentication based on X.509 credentials provides the subject distinguished name as a handle that identifies the authenticated entity, the capability to ensure subject name uniqueness is of critical importance in ensuring overall integrity of the authentication system.

This document described the rationale and use cases for relying party defined name space constraints, and lists the set of desired features a policy language expressing such constraints should have.

Contents

1. Introduction

This document described the rationale and use cases for relying party defined name space constraints in X.509 Certificate Authorities, and lists the set of desired features a policy language expressing such constraints should have.

2. Rationale for Relying Party Defined Namespace Constraints (RPDNC)

Relying Party Defined Namespace Constraints (RPDNC) are limitations on the subject namespace issued by X.509 certificate authorities (CAs) that are defined and enforced by the end-point at the relying party side[1]. As grid authentication based on X.509 credentials provides the subject distinguished name as a handle that identifies the authenticated entity[2], the capability to ensure subject name uniqueness is of critical importance in ensuring overall integrity of the authentication system.

RPDNC policies empower relying parties to limit the capability of a CA to sign in a particular name space, thereby enabling the following non limitative set of use cases:

- name space policies are written to prevent overlapping name spaces by the CAs. RPDNC allows relying parties to ensure that within the ensemble of PKIs in which they participate there are no inadvertent overlaps in the subject names issued by the diverse CAs.
- the RPDNC mechanism allows CAs to sub-divide their subject name space and apply different policies to different branches of this namespace in absence of any other mechanisms. For example, a specific part of the namespace may be reserved for end-entity certificates or subordinate CA certificates that comply with specific additional requirements requested by relying parties, and these relying parties can opt to accept only the part of the namespace where such requests are honoured[3].

Authority-defined namespace constraints policies are common in PKI Bridging architectures that use a Bridge Certification Authority [RFC4158] to express trust relationships between the participating authorities. In a *policy bridge* architecture, this technical means of expressing relationships and coordinating the namespace for the subject directory names does not exist. With a policy bridge, it is up to the relying parties to enforce limitations on the subject namespace

[1] It implements a trust anchor constraint as defined by the Trust Anchor Management group strawman charter (see draft-ietf-pkix-ta-mgmt-problem-statement version 1, visited June 4 2008 at http://www.ietf.org/internet-drafts/draft-ietf-pkix-ta-mgmt-problem-statement-01.txt):
A trust anchor is an authoritative entity represented via a public key and associated data. The public key is used to verify digital signatures and the associated data is used to constrain the types of information for which the trust anchor is authoritative. A relying party uses trust anchors to determine if a digitally signed object is valid by verifying a digital signature using the trust anchor's public key, and by enforcing the constraints expressed in the associated data for the trust anchor.

[2] There are multiple handles that identify the authenticated entity, but the subject distinguished name is used most frequently as the primary handle, since it is persistent and uniquely assigned to the entity. This handle can then be used directly, but is also frequently used in an indirect manner when obtaining other attributes that are associated to this 'handle' of the authenticated entity. For example, an attribute issuance service such as VOMS relies on the subject distinguished name to provide attributes associated with the authenticated entity.

[3] For example, in absence of an RPDNC mechanism a root CA can issue any number of subordinate CAs, and credentials issued by these subordinates would automatically be trusted since the root is part of the trust anchor repository.

of each of the participating authorities in order to guarantee subject name uniqueness across the PKI as seen from that specific relying party.

3. RPDNC Policy Language and Expression Requirements

A quick-scan in the community of Relying Parties, e-Science grid deployment projects and Grid Certification Authorities, as polled in September 2005, indicated the following features to be important for expressing a Relying Party Defined Namespace Constraints Policy.

3.1 Co-existence of authorities with and without RPDNC policies

It must be possible to have issuers with and without namespace constraints policies co-exist within the same trust anchor repository.

3.2 Distribution of RPDNC policies

It must be possible to distribute RPDNC policies in conjunction with each individual trust anchor, independent of any other trust anchors present in the trust anchor repository.

3.3 Support for dynamic hierarchies

It must be possible to support the concept of "subordinate" issuers in a hierarchical chain of issuers, such that a single namespace constraints policy collection (file) support the expression of namespace constraints on any subordinate issuer.

3.4 Expression of subject DN namespaces as strings

The string rendering identifier naming of directoryNames and X.500 distinguished names in the policy expression must comply with RFC4514

3.5 Usability and human readability of the policy

The format used to express RPDNC policies must be human readable in order for relying parties to visibly inspect and assess the namespace constraint policy.

3.6 Name sub-tree support and the use of wild cards in names

The policy expression must support wildcard pattern matching[4].

3.7 Sub-tree specific policies and policy-file precedence

It must be possible to explicitly set a namespace constraints policy for a subordinate issuer, without modifying the policy collection (file) for the up-stream issuer(s). Such a policy on a subordinate issuer must not be able to broaden the namespace constraints defined by higher-level CAs.

3.8 Independence of non-namespace trust anchor characteristics

A subordinate authority trust anchor must be able to change (i.e. a subordinate could be compromised and re-keyed) without having to change the namespace constraints policy in any end-system configuration.

3.9 Policy collision

The probability for collisions in the policy expression format must be vanishingly small[5].

[4] It was request to support that wildcard matching be possible anywhere in the pattern, in order to accommodate distinguished names where the most-variable part of the DN was not at the end of the string. However, this request conflicts with the request to align closely with the SubTree namespace constraints as defined in X.500

[5] Meaning that, e.g., the hash names should be used.

Some of the desired features correspond to similar namespace constraints requirements in the X.509. It is advised for a RPDNC policy language to follow closely the X.509 namespace constraints where possible.

4. Current RPDNC Policy Languages

The first RPDNC Policy language was introduced in the Globus Toolkit [GT] in 1997, based on the EACL Extended ACL language format [EACL]. In this policy, commonly referred to as the "signing policy", specific restrictions can be based on the subject namespace on a per-authority basis. For all Globus Toolkit version 2.0 and higher, this policy is stored in a per-CA policy file. The implementation allows for a list of allowed namespaces to be expressed, within certain limitations.

An alternative "namespaces" policy language [NS96] has been experimentally distributed since 2005 as part of the Common Trust Anchor distribution of the International Grid Trust Federation.

5. Security Considerations

The namespace policy is an integral part of the security and protection mechanisms of a relying party, and as such should be protected from tampering at all times. Inadvertent or malicious modification of a RPDNC policy can lead to namespace collisions, resulting in incorrect subject being authorized, or may expose a relying party to credentials issues under policies that are inappropriate or unacceptable.

In case the namespace constraints policy is distributed to the relying party by a third party, this distribution mechanism must be secured. Once obtained by the relying party, it should be adequately protected from tampering.

6. Contributors

The document is a work of the OGF CA Operations Working Group with contributions by the members of the International Grid Trust Federation (IGTF, see www.gridpma.org)

The editors,
David L. Groep, Nikhef, davidg@nikhef.nl
Jens Jensen, STFC, j.jensen@rl.ac.uk

7. Intellectual Property Statement

The OGF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the OGF Secretariat.

The OGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the OGF Executive Director.

8. Disclaimer

This document and the information contained herein is provided on an “As Is” basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

9. Full Copyright Notice

10. References

[EACL]
Anonymous (the Globus Toolkit Authors) Extended Access Control List (EACL) Format Specification (as stored on http://www.eugridpma.org/documentation/eacl-signing-policy-format.txt)

[GT]
Globus Alliance *The Globus Toolkit* http://www.globus.org/

[NS96]
D.L. Groep *Namespaces Format Specification* EUGridPMA Technical Documentation Series, 2006 (http://www.eugridpma.org/documentation/)

[RFC4158]
M. Cooper et al. *Internet X.509 Public Key Infrastructure: Certificate Path Building: RFC 4158*. September 1995.