Groupe de travail Réseau
Request for Comments : 2276
Catégorie : Information
Traduction Claude Brière de L'Isle

K. Sollins
MIT/LCS
janvier 1998

Principes de l'architecture de résolution de nom de ressource uniforme

Résumé
Le présent document traite des questions de la découverte des services de résolveur de nom de ressource uniforme (URN, *Uniform Resource Name*) qui vont ensuite traduire directement les URN en localisateurs de ressource uniformes (URL, *Uniform Resource Locator*) et en caractéristiques de ressource uniforme (URC, *Uniform Resource Characteristics*). Le document comporte trois grandes parties : les hypothèses qui sous-tendent le travail, les lignes directrices d'un service viable de découverte de résolveur (RDS, *Resolver Discovery Service*) et un cadre de conception des RDS. Les lignes directrices entrent dans trois domaines principaux : la capacité d'évolution, la capacité d'utilisation, et la sécurité et confidentialité. Un RDS qui se conforme à ce cadre ne sera pas forcément conforme à ces lignes directrices. La conformité aux lignes directrices devra être validée séparément.

Table des matières

1. Introduction

L'objet du présent document est de poser les critères d'ingénierie pour ce qu'on appelle un service de découverte de résolveur (RDS, *Resolver Discovery Service*) un service pour aider à savoir où sont les résolveurs d'URN (*Uniform Resource Name*, nom de ressource uniforme). Le terme de "résolveur" est utilisé dans le présent document pour indiquer un service qui traduit les URN en URL (*Uniform Resource Locator*, localisateur de ressource uniforme) ou en URC (*Uniform Resource Characteristic*, caractéristique de ressource uniforme). Certains résolveurs peuvent fournir aussi un accès direct aux ressources. Un RDS aide à trouver un résolveur à contacter pour une résolution ultérieure. On notera que certains concepts de RDS peuvent aussi incorporer une fonction de résolveur. Cette fonction de résolution d'URN est une composante de la réalisation d'une infrastructure d'informations. Dans le cadre du présent ouvrage, cette infrastructure doit être disponible, "dans l'Internet" ou globalement, et donc, les solutions aux problèmes que nous traitons doivent être adaptables globalement. Dans le présent document, on se focalise spécifiquement sur la conception des schémas de RDS.

Le groupe de travail Identifiant de ressource uniforme a défini une architecture de désignation, qui est décrite dans une série de trois RFC, [RFC1736], [RFC1737], et [RFC1738]. Bien que plusieurs documents ultérieurs aient été nécessaires pour compléter la description de cette architecture, elle incorpore les trois fonctions centrales souvent associées à la "désignation" : l'identification, la localisation, et les mnémoniques ou la sémantique. Par localisation, on veut dire les noms de domaine pleinement qualifiés ou les adresses IP, éventuellement étendues par l'accès TCP et/ou les identifiants locaux, comme les noms de chemins. Les noms donnent la capacité de distinguer une ressource d'une autre, en distinguant leurs "noms". Les noms peuvent aider à fournir l'accès à une ressource en incluant les informations de "localisation". De plus, les

noms peuvent avoir d'autres informations de sémantique ou de mnémoniques qui aident les utilisateurs humains à se souvenir ou à se représenter les noms, ou à inclure d'autres informations sémantiques sur la ressource désignée. Le groupe de travail URI est arrivé à la conclusion qu'il était nécessaire d'avoir des identifiants persistants, uniques au monde, distincts des informations de localisation ou autres informations sémantiques ; c'est ce qui a été appelé des URN. Ces "noms" fournissent une identité, en ce que si deux d'entre eux sont "les mêmes" (d'après une règle simple de canonisation) ils identifient la même ressource. De plus, le groupe a décidé que ces "noms" étaient généralement pour la machine, plutôt que pour la consommation des humains. Finalement, avec ces lignes directrices pour les RDS, ce groupe a reconnu la valeur de la séparation entre la gestion de l'allocation du nom et la gestion de la résolution du nom.

À l'opposé des URN, on peut imaginer divers schémas de désignation lisibles par l'homme (HFN, *human-friendly naming*) prenant en charge différentes suites d'applications et de communautés d'utilisateurs. Ils devront prévoir des transpositions en URN selon des couplages étroits ou lâches, selon l'espace de noms. Ce sont ces HFN qui seront les mnémoniques, à contenu plein, et peut-être mouvant, pour retracer les changements de l'usage et de la sémantique. Ils peuvent fournir des surnoms et autres noms de remplacement, relatifs ou abrégés, des noms sensibles au contexte, des noms descriptifs, etc. Leur définition ne rentre pas dans le cadre de notre travail, mais ils joueront évidemment un rôle important à long terme.

Les URN décrits dans la RFC1737 sont définis globalement ; ils sont omniprésents en ce que un URN dans n'importe quel contexte identifie partout la même ressource. Cette exigence étant donnée sur les URN, on doit se demander quelles sont ses implications pour un RDS. L'ubiquité implique t-elle la garantie de la résolution du RDS en tout lieu ? Implique t-elle la résolution en les mêmes informations que la résolution en tout lieu ? Dans les deux cas, la réponse est probablement non. On ne peut pas donner des garanties globales pour l'ensemble du système, sauf à un prix au de là de toute raison. De plus, il peut y avoir des raisons de politique aussi bien que techniques pour ne pas résoudre partout de la même façon. Il est tout à fait possible que la résolution d'un URN en une instance d'une ressource puisse atteindre différentes instances ou copies dans des conditions différentes. Donc, bien qu'un URN se réfère partout à la même ressource, dans certains environnements et dans certaines conditions, et à des instants différents, du fait des caprices des conditions du réseau ou des contrôles de politique, un URN peut parfois être résoluble et dans d'autres temps et autres lieux ne l'être pas. La résolution en tous lieux ne peut pas être supposée possible simplement parce que la dénomination est valable partout. D'un autre côté, le déploiement et l'usage le plus large sera une caractéristique importante de tout concept de RDS.

Au sein de la communauté des URI a existé un concept utilisé fréquemment que faute d'un meilleur terme nous appellerons un "conseil". Un conseil est quelque chose qui aide à la résolution d'un URN ; en théorie, on transpose les URN en conseils comme étape intermédiaire de l'accès à une ressource. En pratique, un RDS peut transposer directement un URN en la ressource elle-même si il choisit de faire ainsi. Il est très vraisemblable qu'il y aura des conseils qui seront applicables à de grands ensemble d'URN, par exemple, un conseil qui indique que tous les URN avec un certain préfixe ou suffixe peuvent être résolus par un résolveur particulier. Un conseil peut aussi avoir des méta informations qui lui sont associées, comme une date d'expiration ou une certification d'authenticité. On s'attend à ce que cela reste avec un conseil plutôt que d'être traité ailleurs. On supposera dans toute la suite de l'exposé sur les conseils qu'ils comportent toutes les méta informations nécessaires tout comme les informations du conseil lui-même. Des exemples de conseils sont :

1) l'URN d'un service de résolveur qui peut aller plus loin dans la résolution de l'URN,
2) l'adresse d'un tel service,
3) une localisation à laquelle la ressource se trouvait précédemment.

La caractéristique qui définit un conseil est qu'ils ne sont que des conseils ; ils peuvent être périmés, temporairement invalides, ou n'être applicables qu'au sein d'une localité spécifique. Ils ne fournissent aucune garantie d'accès, mais ils vont probablement aider au processus de résolution. Un ensemble de conseils peut être découvert par tous moyens disponibles. Certaines combinaisons de logiciels et de choix humains vont déterminer quels conseils seront essayés et dans quel ordre.

On doit supposer que la plupart des résolutions d'URN seront fournies par l'utilisation de conseils mémorisés localement, parce que l'entretien d'une base de données mondialement disponible, complètement à jour des informations de localisation, est infaisable pour des raisons de performances. Il y a un certain nombre de circonstances dans lesquelles on peut imaginer que les conseils deviennent invalides, soit parce que une ressource a été déplacée, soit parce qu'un service de résolveur d'URN différent a pris la responsabilité de la résolution de l'URN. On peut trouver les conseils dans divers endroits. On suppose généralement qu'un système bien conçu va entretenir ou mettre en antémémoire un ensemble de conseils pour chaque URN à chaque localisation où se trouve cet URN. Ils peuvent avoir été acquis du propriétaires des ressources, d'une recommandation de la ressource, ou d'une de nombreuses autres sources. De plus, pour les situations dans lesquelles ces conseils trouvés localement échouent, un système bien conçu va fournir un mécanisme d'échappatoire pour découvrir d'autres conseils. C'est ce mécanisme d'échappatoire, un RDS, qui est traité dans le présent document. Comme avec tous les conseils, il ne peut jamais être garanti que l'accès à une ressource sera disponible à tous les clients, même si la ressource est accessible à certains. Cependant, un RDS est supposé fonctionner avec une fiabilité raisonnable, et donc, peut résulter en un temps de réponse accru.

Le reste de ce document comporte trois sections. La première identifie plusieurs ensembles d'hypothèses sous-jacentes à ce travail Il y a trois hypothèses générales :

* les URN sont persistants ;
* l'allocation des URN peut être déléguée ;
* les décisions peuvent être prises indépendamment les unes des autres, ce qui permet de s'isoler des décisions des homologues.

La section suivante établit trois principes centraux du concept de service de découverte de résolveur. Pour chacun d'eux, nous avons identifié un certain nombre de lignes directrices plus spécifiques qui définissent plus avant et précisent le principe général. Cette section est probablement la plus critique du document, parce que tout schéma proposé de RDS doit respecter ces principes et les lignes directrices qui en sont le corollaire pour savoir si il est ou non adéquat. Les trois principes centraux peuvent être résumé par :

1) un RDS doit permettre l'évolution et la capacité de développement ;
2) la capacité d'utilisation d'un RDS par rapport à chacun des ensembles constitutifs impliqués dans l'identification et la localisation des ressources est capitale ;
3) il est d'une importance centrale que les besoins de sécurité et de confidentialité de tous les constituants soient pris en charge dans toute la mesure du possible.

Chacun des trois paragraphes majeurs de la section des lignes directrices commence par une liste résumant les lignes directrices les plus détaillées identifiées dans cette section.

La dernière section du document trace un cadre pour de tels RDS. L'objet de cette dernière section est de cadrer l'espace de recherches pour les schémas de RDS. Le concepteur de RDS devrait être conscient de l'importance primordiale du respect de ces lignes directrices ; il est possible d'y satisfaire sans se conformer au cadre. Comme on l'exposera plus en détails dans cette dernière section, une conception dans les limites du cadre ne garantit pas la conformité, de sorte que l'évaluation de la conformité doit aussi faire partie du processus d'évaluation d'un schéma.

2. Hypothèses

Sur la base des précédents projets internet et des discussions à la fois dans des réunions générales sur les URN et sur la liste de diffusion du groupe de travail URN, trois séries d'hypothèses majeures sont apparues : longévité, délégation, et indépendance. Chacune d'elle sera discutée séparément.

Les exigences pour les URN de la [RFC1737] déclarent qu'un URN doit être un "identifiant persistant". Bien que rien ne dure pour l'éternité, dans le cadre temporel des ressources, des utilisateurs de ces ressources, et des systèmes qui prennent en charge ces ressources, l'identifiant devrait être considéré comme étant persistant ou comme ayant une plus longue durée de vie que ces autres entités. Deux hypothèses sont impliquées par la longévité des URN : la mobilité et l'évolution. La mobilité va survenir parce que les ressources peuvent être déplacées d'une machine à une autre, les propriétaires des ressources peuvent changer d'organisation, ou les organisations elles-mêmes peuvent fusionner, se scinder, ou se transformer d'une façon ou d'une autre. L'Internet est en évolution continuelle ; les protocoles sont révisés, de nouveaux sont créés, alors que les politiques et les mécanismes de sécurité évoluent aussi. Ce ne sont que des exemples. En général, on doit supposer que presque toutes les pièces de l'infrastructure de support de la résolution d'URN vont évoluer. Afin de traiter les deux hypothèses de mobilité et d'évolution qui découlent de l'hypothèse de longévité, on doit supposer que les usagers et leurs applications peuvent rester indépendants de ces détails mouvants de l'infrastructure de support.

La seconde hypothèse est que les autorités de désignation et de résolution peuvent déléguer une partie de leur autorité ou de leurs responsabilités ; dans les deux cas, la délégation d'une telle autorité est la seule méthode connue qui permette la sorte d'adaptation attendue. Il est important de noter qu'une caractéristique significative du présent travail est le potentiel de séparer l'allocation des noms, qui est la tâche d'étiqueter une ressource avec un URN, de la résolution du nom, qui est la tâche de découvrir la ressource connaissant l'URN. Dans les deux cas, on s'attend à des délégations en cascade. Il peut y avoir des schémas de RDS qui fusionnent ces deux ensembles de relations de responsabilités et de délégation ; en faisant cela, elles lient ensemble ou surchargent deux activités clairement distinctes, entravant probablement ainsi la croissance.

La troisième hypothèse est celle de l'indépendance ou isolement d'une autorité par rapport aux autres, et au moins dans une certaine mesure, de son autorité parente. Lorsque une autorité délègue une partie de ses droits et responsabilités à une autre autorité, le délégataire peut opérer dans ce domaine indépendamment de ses pairs et dans les limites spécifiées par la délégation, indépendamment du délégant. Cet isolement est d'une importance critique pour permettre l'indépendance des politiques et des mécanismes.

Cette troisième hypothèse a plusieurs corollaires. D'abord, on suppose que l'éditeur d'une ressource peut choisir le service de résolveur, indépendamment des choix faits par d'autres. À un moment donné, le propriétaire d'un espace de nom peut choisir un service de résolveur d'URN particulier pour cet espace de noms délégué. Un tel service de résolveur d'URN peut être en dehors du modèle de service RDS, et n'être qu'identifié ou localisé par le service RDS. Ensuite, il doit être possible

de faire un choix parmi les services de RDS. L'existence de plusieurs services de RDS peut venir de l'évolution d'un service de RDS, ou du développement de nouveaux. Bien qu'à un moment donné il est vraisemblable qu'il n'y aura qu'un seul de ces services, ou un petit ensemble d'entre eux, leur nombre va probablement augmenter pendant une période de transition d'une architecture à l'autre. Donc, on doit supposer que les clients peuvent faire un choix parmi un ensemble probablement très restreint de RDS. Ensuite encore, il doit y avoir indépendance dans le choix des niveaux et modèles de sécurité et d'authenticité requis. Ce choix peut être fait par le propriétaire d'un sous-espace de dénomination, en contrôlant qui peut modifier les conseils dans ce sous-espace. Une autorité de désignation peut déléguer ce choix aux propriétaires des ressources désignées par les noms qu'elle a alloués. Il peut y avoir des limitations à cette liberté de choix afin de permettre à d'autres participants d'avoir le niveau de sécurité et d'authenticité qu'ils requièrent, par exemple, afin de maintenir l'intégrité de l'infrastructure de RDS globale. Enfin, on suppose l'indépendance du choix de la règle de canonisation des URN au sein d'un espace de noms, limitée par toutes restrictions ou contraintes qui peuvent avoir été établies par l'espace de noms parent. Ceci est un choix fait par les autorités de désignation sur leurs propres sous-espaces de noms. Les règles de canonisation seront discutées dans la section sur les cadres. Donc, il y a des hypothèses d'indépendance et d'isolement pour permettre une autorité déléguée et indépendante dans divers domaines.

L'hypothèse de modularité de la délégation et d'isolement implique l'indépendance de décision et de mise en œuvre, conduisant à une décentralisation qui apporte un certain degré de sécurité contre le déni de service. Sur la base de ces hypothèses et en conjonction avec celle de longévité et de celles pour les URL et les URN qui sont détaillées dans les RFC 1736 et 1737, on peut maintenant se tourner vers les lignes directrices pour un RDS.

3. Lignes directrices

Les lignes directrices qui s'appliquent à un RDS se concentrent sur trois principes de conception importants dans les domaines de la capacité d'évolution, d'utilisation, et de sécurité et confidentialité. Le cœur d'une fonction de RDS est de fournir des conseils pour accéder à une ressource connaissant son URN. Ces conseils peuvent aller de l'applicabilité locale à globale, et de la courte durée à la longue durée. Ils peuvent aussi varier dans le degré d'authenticité vérifiable. Bien qu'il puisse n'être jamais faisable ni nécessaire que les mises en œuvre initiales prennent en charge toutes les ligne directrices, chaque mise en œuvre doit prendre en charge l'évolution vers des systèmes qui prennent plus complètement en charge ces lignes directrices.

Il est important de noter qu'il y a des exigences, non applicables spécifiquement à un RDS, qui doivent aussi être satisfaites. Un système d'URN complet va consister en noms dans des espaces de noms, en informations de résolution pour eux, et en une transposition des noms dans les espaces de noms en informations de résolution (ou conseils). Les URN eux-mêmes doivent satisfaire aux exigences de la [RFC1737]. De plus, les espaces de noms eux-mêmes doivent satisfaire à certaines exigences décrites par le groupe de travail URN [GTURN]. Bien que ces exigences et lignes directrices ne soient pas décrites ici, elles doivent être respectées pour donner un système acceptable.

Chacun des paragraphes ci-dessous commence par un résumé des points soulignés dans cette section. Il y a un certain degré de chevauchement entre les domaines, comme de permettre l'évolution des mécanismes de sécurité, etc., et donc des questions peuvent être traitées dans plus d'un paragraphe. Il est aussi important de reconnaître que la conformité aux lignes directrices va souvent être subjective. Comme pour de nombreuses lignes directrices et exigences de l'IETF, beaucoup d'entre elles ne sont pas quantifiables et donc la conformité est une affaire de jugement et une question de degré. Enfin, le lecteur pourra estimer que certaines d'entre elles sont d'applicabilité générale pour les systèmes répartis et que certaines sont spécifiques de la résolution d'URN. Celles d'applicabilité générale sont incluse par souci de complétude et ne sont pas distinguées comme telles.

3.1 Évolution

Les questions qui se posent dans le premier domaine, qui est celui de la capacité d'évolution, sont :

1.1) un RDS doit être capable de prendre en charge l'adaptation dans au moins trois dimensions : le nombre de ressources pour lesquelles les URN seront nécessaires, le nombre d'éditeurs et d'usagers de ces ressources, et la complexité de la délégation, lorsque augmente l'autorité pour la résolution et qu'elle reflète éventuellement la délégation d'autorité de désignation ;

1.2) Un environnement de conseil de résolution doit prendre en charge l'évolution des mécanismes, en particulier pour :

* un ensemble croissant de schémas d'URN ;
* de nouvelles sortes de services locaux de résolveur d'URN ;
* de nouveaux schémas d'authentification ;
* des schémas de RDS de remplacement actifs simultanément ;

1.3) un RDS doit permettre le développement et le déploiement de mécanismes de contrôle administratif pour gérer le comportement humain par rapport à des ressources limitées.

Une des leçons de l'Internet que l'on doit incorporer dans le développement des mécanismes de résolution des URN est qu'on doit être préparé au changement. De tels changements peuvent arriver suffisamment lentement pour être considérés comme des modifications dans le cadre de l'évolution des services existants, ou assez brutaux pour être considérés comme révolutionnaires. Ils peuvent infiltrer l'univers de l'Internet bit par bit, coexistant avec les premiers services ou ils peuvent prendre l'Internet d'assaut, causant une apparente transformation complète en très peu de temps. Il y a plusieurs directions dans lesquelles on peut prédire le besoin d'évolution. Au strict minimum, la communauté et les mécanismes proposés devraient être prêts pour cela.

D'abord, l'adaptation est une question primordiale, en conjonction avec l'évolution. Le nombre d'utilisateurs, à la fois humains et électroniques, aussi bien que le nombre de ressources, vont continuer de subir une croissance exponentielle pendant au moins le prochain terme. Donc le nombre d'URN va subir une croissance similaire. De plus, avec la croissance en nombre absolu viendra vraisemblablement aussi la croissance des délégations aussi bien d'autorités de désignation que d'autorités de résolution. Ces faits signifient qu'un concept de RDS doit être prêt à traiter un nombre croissant de demandes d'inclusion, mise à jour et résolution, dans un ensemble de serveurs RDS dont les interrelations seront peut-être plus complexes. Cela ne veut pas dire qu'il y aura nécessairement plus de mises à jour ou de résolutions par URN ; on ne peut pas prédire cela pour le moment. Mais, même ainsi, l'infrastructure peut devenir plus complexe à cause de la délégation, qui peut (comme on le voit à la Section 4 sur le cadre) conduire à des règles plus complexes pour la réécriture ou l'extraction des termes d'une résolution. Tout concept a vraisemblablement une limite de performances optimales, de sorte qu'il vaut la peine d'examiner les limitations à la croissance de chaque solution de remplacement pour le concept.

Ensuite, on s'attend à ce qu'il y ait des ajouts et des changements aux mécanismes. La communauté comprend déjà qu'il doit y avoir une place pour de nouveaux schémas d'URN, comme décrit dans [GTURN]. Un schéma d'URN va définir un ensemble d'URN qui satisfasse aux exigences pour les URN de la [RFC1737], mais peut subir d'autres contraintes sur la structure interne de l'URN. L'intention est que les schémas d'URN puissent être libres de spécifier des parties de l'URN qui sont laissées opaques dans la description générale. En fait, un schéma d'URN peut choisir de rendre public ou de garder privé les algorithmes pour de telles parties "opaques" de l'URN. Dans tous les cas, on doit être prêt à un nombre croissant de schémas d'URN.

Souvent en conjonction avec un nouveau schéma d'URN, mais éventuellement indépendamment de tout schéma d'URN particulier, de nouveaux types de services de résolveurs peuvent évoluer. Par exemple, on peut imaginer un service de résolveur spécialisé fondé sur la structure particulière de l'ISBN qui améliorerait l'efficacité de la recherche de documents grâce à leur numéro ISBN. Autrement, on peut aussi imaginer un service de résolveur à finalité générale qui fasse un compromis entre performances et généralité ; bien que son niveau de performance ne soit que moyen pour la résolution des numéros ISBN, il compense cette faiblesse par la compréhension de tous les schémas d'URN existants, de sorte que ses clients peuvent utiliser le même service pour résoudre les URN sans considération du schéma de désignation. Dans ce contexte, il y aura toujours de la place pour des améliorations de services, à travers des améliorations des performances, une meilleure adaptabilité aux nouveaux schémas d'URN, ou de plus faibles coûts, par exemple. De nouveaux modèles pour la résolution d'URN vont évoluer et nous devons être prêts à permettre leur participation au processus global de résolution des URN.

Si on commence par un plan global pour la résolution des URN, dans lequel pourraient s'intégrer les améliorations décrites ci-dessus, on doit aussi être prêt pour une évolution des schémas d'authentification qui seront considérés utiles ou nécessaires à l'avenir. Il n'y a pas un seul schéma d'authentification qui soit d'acceptation universelle, et il se peut qu'il n'y en ait jamais. Même si il en existe un, un jour, nous devons toujours être prêts à passer à de nouveaux meilleurs schémas, parce que les anciens deviennent trop faciles à deviner et à mystifier.

En termes de mécanismes, bien qu'on puisse développer et déployer initialement un seul schéma de RDS, on doit être prêt à l'évolution du modèle de niveau supérieur. Donc, si le modèle de RDS prend en charge un schéma apparemment centralisé (du point de vue de la politique) pour l'insertion et la modification des informations d'autorité, on doit être prêt à évoluer à l'avenir vers un modèle différent, peut-être avec un modèle plus réparti d'autorité et d'authenticité. Si le modèle n'a pas de cœur mais plutôt une découverte d'informations partielles en cascade, on pourrait trouver que cela devient ingérable lorsque l'accroissement d'échelle se fait sentir. Quel que soit le modèle, on doit être prêt à le voir évoluer avec des changements d'échelle, de performances, et de contraintes de politique comme celle de sécurité et de coût.

La troisième question en matière d'évolution est même encore plus mécanique que les autres. À tout moment, la communauté est susceptible d'adopter un compromis sur la question de la résolution. On va probablement fonctionner dans une situation d'équilibre entre la faisabilité et l'idéal, peut-être avec des contrôles de politique utilisés pour aider à stabiliser l'utilisation du service. Idéalement, le service devrait fournir exactement ce que veut le consommateur qui, quant à lui, ne demanderait pas plus que ce dont il a besoin, mais cela semble extrêmement peu vraisemblable. Comme on sera presque toujours dans une situation dans laquelle certaines ressources de fourniture de service seront à court, certaines formes de contrôle de politique seront généralement nécessaires. Certains contrôles de politique peuvent être réalisés par des mécanismes au sein des serveurs ou dans le détail des protocoles, alors que d'autres ne peuvent être réalisés qu'à l'extérieur du système. Par exemple, si on suppose que des entrées de conseils sont soumises dans une telle quantité que les serveurs

de conseils excèdent leurs capacités et aient besoin d'espace disque. Deux suggestions pour le contrôle de politique sont les prix et l'administration. Avec les changements de technologie et le changement de l'équilibre des ressources qui peuvent se trouver à court, les mécanismes et les politiques de contrôle de leur usage peuvent aussi évoluer.

3.2 Capacité d'usage

Pour résumer, la directive d'utilisabilité touche trois domaines fondés sur la participation à la gestion et la découverte des conseils :

2.1) L'éditeur
- 2.1.1) L'URN sur une résolution de conseil doit être correct et efficace avec une très forte probabilité ;
- 2.1.2) Les éditeurs doivent être capables de faire un choix et de se déplacer parmi les services de résolveur d'URN pour localiser leurs ressources ;
- 2.1.3) Les éditeurs doivent être capables de créer plusieurs points d'accès pour leurs informations de localisation ;
- 2.1.4) Les éditeurs devraient être capables de fournir des conseils avec des durées de vies diverses ;
- 2.1.5) Il doit être relativement facile aux éditeurs de spécifier la gestion et l'observation de leurs informations de conseil ainsi que toutes les contraintes de sécurité nécessaires pour leurs conseils.

2.2) Le client
- 2.2.1) L'interface au RDS doit être simple, effective, et efficace ;
- 2.2.2) Le client et les applications clientes doivent être capables de comprendre facilement les informations mémorisées et fournies par le RDS, afin d'être capable de faire leurs choix en connaissance de cause.

2.3) La gestion
- 2.3.1) La gestion des conseils doit être aussi discrète que possible, en évitant d'utiliser trop de ressources du réseau ;
- 2.3.2) La gestion des conseils doit permettre les contrôles administratifs qui encouragent certaines sortes de comportements réputés nécessaires pour satisfaire les autres exigences ;
- 2.3.3) La configuration et la vérification de configuration des serveurs de RDS individuels doivent être assez simples pour ne pas décourager la configuration et la vérification.

La capacité d'utilisation peut être évaluée dans trois perspectives distinctes : celle d'un éditeur qui souhaite rendre publiques certaines informations, celle d'un client qui veut la résolution d'un URN, et celle du fournisseur ou gestionnaire des informations de résolution. Les questions d'utilisabilité seront examinées séparément pour chacune de ces trois perspectives. Il est important de reconnaître qu'il peut y avoir des situations dans lesquelles les intérêts de certains des participants (par exemple, un utilisateur et un éditeur) peuvent être en conflit ; il va bien falloir le résoudre.

On notera qu'il y a deux autres sortes de participants au processus global de dénomination, comme l'a souligné le groupe de travail URN. Ce sont les autorités de désignation qui choisissent et allouent les noms, et les auteurs qui incluent les URN dans leurs ressources. Aucun d'eux ne joue de rôle dans la conception d'un RDS et ne sera donc discuté ici.

3.2.1 L'éditeur

L'éditeur doit être capable de faire connaître les URN aux consommateurs potentiels. Du point de vue d'un éditeur, il est d'une importance primordiale que les URN soient correctement et efficacement résolubles par les clients potentiels avec une très forte probabilité. Les éditeurs misent sur des URN à longue durée de vie, car cela augmente les chances que les références continuent de pointer sur les ressources qu'ils publient.

L'éditeur doit aussi être capable de faire facilement un choix parmi divers services potentiels qui peuvent traduire des URN en informations de localisation. Pour permettre cette mobilité parmi les résolveurs, l'architecture de RDS doit prendre en charge de telles transitions, dans les limites du contrôle de la politique. Il vaut de noter que plusieurs services d'annuaire sont disponibles dans les recueils téléphoniques, ils sont généralement payants. Il n'y a rien qui empêche que des redevances soient collectées pour des sortes de services similaires par rapport aux URN.

L'éditeur doit être capable de s'arranger pour que de multiples accès pointent sur une ressource publiée. Pour que cela soit utile, les services de résolveurs devraient être prêts à fournir différentes résolutions ou informations de conseil à des clients différents, sur la base d'une diversité des informations, incluant la localisation et les divers privilèges d'accès que peut avoir le client. Il est important de noter que cela peut avoir de sérieuses implications sur la mise en antémémoire de ces informations. Par exemple, des sociétés peuvent s'arranger pour faire des copies locales de ressources populaires, et vont donner accès aux copies locales pour leurs seuls employés. Ceci est distinct du contrôle d'accès sur la ressource comme un tout, et peut s'appliquer différemment aux différentes copies.

L'éditeur devrait être capable de fournir des informations de localisation aussi bien à long qu'à court terme sur l'accès à la ressource. Les informations à long terme seront vraisemblablement des informations telles que l'adresse à long terme de la ressource elle-même ou la localisation ou l'identité d'un service de résolveur avec lequel l'éditeur a une relation à long terme. On peut imaginer qu'un arrangement avec un tel service de résolveur "d'autorité" à long terme pourrait être une

garantie de fiabilité, de résilience à la défaillance, et de mises à jour précises. Des informations à plus court terme sont utiles pour des changements à court terme dans les services ou pour éviter des problèmes d'encombrement ou de défaillance de courte durée. Par exemple, si le dépositaire réel de la ressource est temporairement inaccessible, la disponibilité de la ressource pourrait être assurée à partir d'un autre dépositaire. Ces informations de court terme peuvent être vues comme des raffinements temporaires des informations à plus long terme, et comme tels devraient être mises à disposition plus facilement et plus rapidement, mais pourraient être moins fiables. Certains concepts de RDS peuvent ne pas faire de distinction entre ces deux extrêmes.

Enfin, les éditeurs seront la source de beaucoup des informations de conseil qui seront mémorisées et servies par le gestionnaire de l'infrastructure. En dépit du fait que beaucoup d'éditeurs ne vont pas comprendre les détails du mécanisme de RDS, il doit être pour eux facile et direct d'installer les informations de conseil. Cela signifie qu'en général tous ceux qui souhaitent publier et à qui le privilège de résolution a été étendu par une délégation, peuvent le faire. L'éditeur doit être capable non seulement d'exprimer des conseils, mais aussi de vérifier que ce qui est servi par le gestionnaire est correct. De plus, dans la mesure où il y a des contraintes de sécurité sur les informations de conseil, l'éditeur doit être capable à la fois de les exprimer et de vérifier facilement leur respect.

3.2.2 Le client

Du point de vue du client, simplicité et facilité d'usage sont les valeurs suprêmes. Il est d'une importance critique pour le service efficace des clients qu'il puisse acquérir les informations de conseils à travers un protocole efficace. Comme la résolution du nom n'est que la première étape sur le chemin de l'accès à une ressource, le temps qu'on y passe doit être réduit au minimum.

De plus, il sera important d'être capable de construire des interfaces standard simples au RDS, de sorte que le client et les applications au nom du client puissent tous deux interpréter les conseils et faire ensuite leurs choix en connaissance de cause. Le client, peut-être avec l'assistance de l'application, doit être capable de spécifier des préférences et des priorités puis de les appliquer. Si la commande des conseils est seulement partielle, le client peut devenir directement impliqué dans leur chois et leur interprétation et ils doivent donc être compréhensibles pour ce client. D'un autre côté, il devrait en général être possible de configurer les préférences par défaut, avec les préférences individuelles conçues comme subrogeant toute valeur par défaut.

Du point de vue du client, bien que les URN apportent des fonctionnalités importantes, le client va très vraisemblablement n'interagir directement qu'avec des dénominations lisibles par l'homme (HFN, *human friendly name*). Comme dans une interaction humaine directe (non médiatisée par l'ordinateur) le partage des noms sera sur petite échelle, privée, ou spécifique du domaine. Les HFN seront des sortes de références et noms qui sont facile à mémoriser, à taper, à choisir, allouer, etc. Il y a aussi besoin d'un certain nombre de mécanismes pour transposer les HFN en URN. De tels services que les "pages jaunes" ou "outils de recherche" entrent dans ces catégorie. Bien qu'on mentionne ici les HFN, il est important de reconnaître que les HFN et la transposition des HFN en URN est et doit rester une fonction distincte de celle d'un RDS. Donc, bien que les HFN soient critiques pour les clients, ils ne rentrent pas dans le domaine d'application du présent document.

3.2.3 La gestion

Finalement, on doit exposer les questions d'utilisabilité par rapport à la gestion de l'infrastructure de conseil elle-même. Ce qu'on appelle "gestion" est un service qui est distinct de celui de la publication ; il est au cœur d'un RDS. Il implique la mémorisation et la fourniture des conseils aux clients, afin qu'ils puissent trouver les ressources publiées. Il fournit aussi la sécurité par rapport à la résolution des noms dans la mesure où il y a un engagement de fourniture d'une telle sécurité ; ceci est traité au paragraphe 3.3 ci-dessous.

La gestion des conseils doit être aussi discrète que possible. D'abord, son infrastructure (serveurs de mémorisation des conseils et protocoles de distribution) doit avoir aussi peu d'impact que possible sur les autres activités du réseau. On doit se souvenir que ceci est une activité auxiliaire et qu'elle doit rester en arrière plan.

Ensuite, pour rendre faisable la gestion des conseils, il peut être besoin d'un système pour des incitations et des dissuasions administratives telles que par le prix ou par des restrictions légales. La récupération des coûts du fonctionnement du système n'est qu'une des raisons de percevoir des charges. L'introduction des payements a souvent un impact sur le comportement social. Il peut être nécessaire de décourager certaines formes de comportement qui lorsqu'ils ne sont pas sous contrôle ont un sérieux impact négatif sur l'ensemble de la communauté. En même temps, toutes les politiques administratives devraient encourager les comportements qui bénéficient à l'ensemble de la communauté. Donc, par exemple, un petit montant occasionnel pour la mémorisation d'un conseil peut encourager une utilisation prudente des conseils. Si on suppose qu'il y a un coût fixe pour la gestion d'un conseil, plus son applicabilité est large à travers l'espace des URN, plus il est rentable. C'est à dire que lorsque un conseil peut servir pour toute une collection d'URN, il y aura une

incitation à soumettre un conseil général plutôt qu'un grand nombre de conseils plus spécifiques. Des politiques similaires peuvent être instituées pour décourager le changement fréquent des conseils. De cette façon, et d'autres, les comportements utiles à l'ensemble de la communauté peuvent être encouragés.

Enfin, en parallèle aux questions de capacité d'utilisation pour les éditeurs, il doit aussi être simple pour la gestion de configurer la transposition des URN en conseils. Il doit être facile à la fois de comprendre la configuration et de vérifier qu'elle est correcte. Par rapport à la gestion, la question peut avoir un impact non seulement sur les informations elles-mêmes mais aussi sur la façon dont elles sont partagées entre les serveurs du réseau qui fournissent en collaboration le service de gestion ou le RDS. Par exemple, il devrait être facile de prendre un serveur et de vérifier que les données qu'il gère sont correctes. Bien que ce ne soit pas une ligne directrice, c'est mieux que rien parce qu'on discute ici d'un service mondial et probablement en croissance, encourager la participation de volontaires suggère que, comme avec le DNS, ces volontaires puissent se sentir en confiance avec le service qu'ils fournissent et qu'il profite à la fois à eux-mêmes et au reste de la communauté.

3.3 Sécurité et confidentialité

En résumé, les lignes directrices pour la sécurité et la confidentialité peuvent être identifiées comme un certain degré de protection contre des menaces. Les lignes directrices qui entrent sous ce troisième principe, celui de sécurité, sont toutes formulées en termes de possibilités ou options pour les utilisateurs du service de demander et d'utiliser. Donc, elles visent la disponibilité de fonctionnalités, mais non leur utilisation. On reconnaît que toute sécurité est une affaire de degrés et de compromis. Cela peut ne pas satisfaire tous les consommateurs potentiels, et nous n'avons aucune intention d'empêcher la construction de serveurs plus sécurisés avec plus de protocoles sûrs pour satisfaire ces besoins. Ces lignes directrices sont destinées à satisfaire les besoins du grand public.

3.1) Il doit être possible de créer des versions d'autorité d'un conseil avec contrôle de l'accès aux privilèges de modification ;
3.2) Il doit être possible de déterminer l'identité des serveurs ou d'éviter le contact avec des serveurs non autorisés ;
3.3) Il doit être possible de réduire la menace de déni de service par une large distribution des informations à travers les serveurs ;
3.4) Il doit être possible, dans les limites des critères de politique organisationnelle de fournir au moins un certain degré de confidentialité au trafic ;
3.5) Il doit être possible aux éditeurs de garder confidentielles certaines informations telles que le tableau d'ensemble des ressources qu'ils publient et l'identité de leurs clients ;
3.6) Il doit être possible aux éditeurs de restreindre l'accès à la résolution des URN pour les ressources qu'ils publient, si ils le souhaitent.

Quand on parle de sécurité, une des principales questions est l'énumération des menaces qu'on veut atténuer. Le compromis inclut souvent le coût monétaire et de ressources de calcul et de communications, la facilité d'utilisation, la vraisemblance de l'usage, et l'efficacité des mécanismes proposés. En gardant cela présent à l'esprit, nous examinerons un ensemble de menaces.

Voydock et Kent [SMHLP] donnent un utile catalogue des menaces potentielles. Parmi elles, les menaces passives contre la vie privée et la confidentialité et les menaces actives sur l'authenticité et l'intégrité sont probablement les plus importantes à considérer ici. Dans la mesure où une association parasite cause des menaces pour la vie privée, l'authenticité, ou l'intégrité par rapport aux informations au sein des serveurs qui gèrent les données, elle est aussi importante. Le déni de service est probablement la plus difficile de ces zones de menaces à la fois à détecter et à empêcher, et nous la laisserons donc aussi de côté pour l'instant, bien qu'on verra que des solutions à d'autres problèmes vont aussi atténuer certains des problèmes du déni de service. De plus, comme ceci est destiné à fournir un service global pour satisfaire aux besoins de diverses communautés, les compromis d'ingénierie seront différents selon les clients. Donc, les lignes directrices sont données en termes de "Il doit être possible..." Il est important de noter que les informations qui nous concernent ici sont celles de conseil, dont il n'est, par nature, pas garanti qu'elles soient correctes ou à jour ; donc, il est vraisemblable qu'il ne vaut pas la peine de faire trop de frais pour vérifier que les conseils sont corrects, parce qu'il n'est pas garanti qu'ils seront de toutes façons encore corrects. Le choix exact du degré de secret, d'authenticité, et d'intégrité doit être déterminé par les besoins du client et la disponibilité des services auprès du serveur.

Pour éviter toute confusion, il vaut la peine de souligner la signification des termes qui ont un sens différent dans d'autres contextes. Dans ce cas, le terme "d'autorité" lorsque il est utilisé ici dénote une action ou un tampon d'approbation par un principal (là encore au sens de la sécurité) qui a le droit d'effectuer un tel acte d'approbation. Cela n'a pas d'implication sur la correction des informations, mais seulement peut-être une implication sur qui prétend être correct. À l'opposé, le terme est aussi souvent utilisé simplement pour se référer à une copie primaire d'un élément d'information pour lequel il peut aussi y avoir des copies secondaires ou des copies disponibles en antémémoire. Dans cet exposé sur la sécurité, on utilise la première signification, bien qu'il puisse aussi être important d'être capable d'apprendre si un élément d'information provient

d'une source primaire ou non et de demander qu'elle soit primaire. Cette seconde signification sera utilisée ailleurs dans le document et sera notée ainsi à ce moment là.

Il est aussi important de distinguer diverses significations possibles pour "contrôle d'accès". Il y a deux domaines qu'on peut distinguer. D'abord, il y a la question de la sorte de contrôle d'accès dont on parle, par exemple, en matière de conseils, si il s'agit d'accès réel, d'accès en lecture et écriture, ou lecture avec vérification d'authenticité. Ensuite, il y a la question de quel accès est contrôlé. Dans le contexte des désignations, cela peut être les noms eux-mêmes (ce n'est pas le cas pour les URN), la transposition des URN en conseils (c'est l'affaire d'un RDS), la transposition des URN en adresses (ce n'est pas l'affaire d'un RDS comme il sera exposé plus loin avec les questions de secret), ou la ressource elle-même (sans relation du tout avec la désignation ou la résolution de nom). Nous allons essayer d'être clairs sur ce qu'on veut dire quand on parle de "contrôle d'accès".

Il y a encore une question à régler sur ce point, qui est la distinction entre mécanisme et politique. En général, une politique est réalisée au moyen d'un ensemble de mécanismes. Dans le cas d'un RDS, il peut y avoir des politiques internes au RDS qu'il est nécessaire qu'il prenne en charge afin d'accomplir sa tâche de la façon qu'il juge appropriée. Comme, en général, il s'agit de mémoriser et distribuer des informations, la plus grande partie de ses politiques de sécurité peut concerner le maintien de sa propre intégrité, et elle est plutôt limitée. Au delà de cela, dans la mesure du possible, il ne devrait imposer aucune politique à ses abonnés, aux éditeurs et aux usagers. Ce sont eux qui peuvent avoir une politique qu'ils voudraient voir prise en charge par le RDS. À cette fin, un RDS devrait fournir une gamme "d'outils" ou mécanismes dont l'usager puisse causer le déploiement en son nom pour réaliser sa politique. Un RDS peut ne pas fournir du tout ce qui est nécessaire à un consommateur. Un consommateur peut avoir des exigences différentes à l'intérieur de ses limites administratives qu'à l'extérieur. Donc, "il doit être possible..." de capturer l'idée que le RDS doit généralement fournir les outils pour mettre en œuvre les politiques en tant que nécessaire pour les consommateurs.

La première approche de la résolution d'URN est de découvrir les conseils locaux. Pour que des conseils soient découverts localement, ils devront être distribués aussi largement que possible à ce qui est considéré comme local pour tout les locaux. L'inconvénient d'une distribution aussi large est la large distribution des mises à jour, ce qui cause des problèmes de trafic sur le réseau ou de délais dans la livraison des mises à jour. Un modèle de remplacement concentrerait les informations de conseil dans les serveurs, exigeant donc que les informations de mise à jour ne soient distribuées qu'à ces serveurs. Dans un tel modèle, les points vulnérables sont les sources de l'information et le réseau de distribution entre elles. Des attaques contre l'intégrité des informations mémorisées dans un serveur peuvent venir sous la forme d'une usurpation d'identité du propriétaire ou du serveur des informations. Une large duplication des informations parmi les serveurs augmente la difficulté de l'usurpation d'identité sur toutes les localisations des informations, tout en réduisant la menace de déni de service. Ceci nous conduit à trois lignes directrices identifiables pour notre modèle de sécurité :

* Contrôle d'accès sur les conseils : Il doit être possible de créer une version d'autorité de chaque conseil avec un contrôle de changements limité aux seuls principaux qui ont le droit de le modifier. Le choix de ces principaux, ou s'ils ne sont pas limités, doit être fait par l'éditeur d'un conseil.

* Authenticité du serveur : Les serveurs et les clients doivent être capables d'apprendre l'identité des serveurs avec lesquels ils communiquent. Ce sera une question de degré et il est possible qu'il y ait des serveurs plus dignes de foi, mais moins accessibles, pris en charge par une plus large série de serveurs moins authentifiables qui soient plus largement disponibles. Dans le pire des cas, si le client reçoit ce qui paraît être des informations non validées, le client devrait supposer que le conseil pourrait être inapproprié et la confirmation des données pourrait être recherchée auprès de sources plus fiable mais moins accessibles.

* Répartition des serveurs : Une large disponibilité assurera la résistance au déni de service. C'est seulement dans la mesure où les services sont disponibles qu'ils peuvent fournir un certain degré de confiance. De plus, la répartition des services va réduire la vulnérabilité de l'ensemble de la communauté, en réduisant la confiance mise sur un seul serveur. Cela peut être atténué par le fait que la confiance se fonde sur un ensemble de serveurs liés ; si l'un d'eux a une défaillance, toute la chaîne de confiance est défaillante ; plus il y a d'éléments dans une telle chaîne, plus elle peut devenir vulnérable.

Le secret peut être une arme à double tranchant. Par exemple, d'un côté une organisation peut considérer qu'il est d'une importance vitale que ses concurrents ne soient pas capables de lire son trafic. D'un autre côté, elle peut aussi considérer qu'il est important d'être capable de surveiller exactement ce que ses employés transmettent, à qui et de qui, pour diverses raisons, comme de réduire la probabilité que ses employés donnent ou vendent les secrets de la compagnie, ou pour vérifier que les employés n'utilisent pas les ressources de la compagnie à des fins personnelles. Donc, bien qu'il y ait vraisemblablement des besoins de secret et de confidentialité, ce qu'ils sont, qui les contrôle et comment, et par quels mécanismes, varie suffisamment largement pour qu'il soit difficile de dire quelque chose de concret sur eux ici.

Le secret des éditeurs est beaucoup plus facile à traiter. Comme ils essayent de publier quelque chose, le secret n'est en général probablement pas recherché. Cependant, les éditeurs ont bien des informations qu'ils pourraient souhaiter garder

secrètes : des informations sur l'identité de leurs clients, et des informations sur les noms qui existent dans leur espace de noms. Les informations sur qui sont leurs clients sont peut-être difficiles à collecter, mais elles dépendent de la mise en œuvre du système de résolution. Par exemple, si les informations de résolution qui se rapportent à un certain éditeur sont largement dupliquées, les touches sur chaque copie vont devoir être enregistrées. Bien sûr, déterminer si un client spécifique demande un certain nom peut être abordé par d'autres moyens, en observant le client comme on l'a vu plus haut.

Il y a vraisemblablement des éditeurs qui publient pour un public restreint. Dans la mesure où ils veulent restreindre l'accès à une ressource, cela relève de la responsabilité du dépositaire de fournir ou interdire l'accès à la ressource. Si il souhaite garder secrets le nom et les conseils pour une ressource, un RDS public peut être inadéquat pour ses besoins. En général, il est destiné à ceux qui veulent que les consommateurs trouvent leurs ressources sans contraintes.

La dernière question sur le secret pour les éditeurs a à voir avec le contrôle d'accès sur la résolution des URN. Cette question dépend de la mise en œuvre du serveur résolveur d'URN d'autorité (au sens de "primaire") de l'éditeur. Les serveurs résolveurs d'URN peuvent être conçus pour exiger des preuves d'identité afin que les informations de résolution soient produites ; si le client n'a pas la permission d'accéder à l'URN demandé, le service nie qu'un tel URN existe. Un protocole chiffré peut aussi être utilisé afin que la demande et la réponse soient toutes deux dissimulées. Le chiffrement est possible dans ce cas parce que l'identité du receveur final est connue (c'est le serveur d'URN). Donc, le contrôle d'accès sur la résolution d'URN peut et doit être fournie par les serveurs résolveurs plutôt que par un RDS.

4. Le cadre

En gardant présentes à l'esprit les hypothèses et les lignes directrices, nous conclurons par un cadre général dans lequel peut entrer la conception d'un RDS. Comme on l'a dit précédemment, bien que ce cadre soit mis en avant comme un guide suggéré pour les concepteurs de RDS, la conformité à ce cadre ne garantit en aucune façon la conformité aux lignes directrices. Une telle évaluation doit être effectuée séparément. Un tel manque de conformité devrait être clairement documenté.

La conception du cadre se fonde sur la syntaxe d'un URN telle qu'exposée dans la [RFC2141]. C"est à dire :

URN:<NID>:<NSS>

où URN: est un préfixe sur tous les URN, NID est l'identifiant d'espace de nom, et NSS est la chaîne spécifique de l'espace de nom. Le préfixe identifie chaque URN comme tel. Le NID détermine la syntaxe générale pour tous les URN au sein de son espace de noms. Le NSS est probablement partagé en un ensemble d'espaces de noms délégués et subdélégués, et cela est éventuellement reflété plus précisément dans des spécifications de syntaxe . Dans des environnements plus complexes, chaque espace de nom délégué aura la permission de choisir la syntaxe de la partie variable de l'espace de noms qui lui a été délégué. Dans les espaces de nom plus simples, la syntaxe sera verrouillée complètement par l'espace de noms parent. Par exemple, bien que le DNS ne satisfasse pas à toutes les exigences pour les URN, il a une syntaxe complètement verrouillée, telle que toute structuration supplémentaire ne doive être faite que par l'ajout d'autres précisions sur la gauche, en conservant la structure de poids fort vers poids faible, de droite à gauche. Une syntaxe déléguée pourrait faire qu'un hôte soit désigné par le DNS, mais à la droite de cela et séparée par un "@" se trouve une chaîne dont l'ordre interne est défini par le système de fichiers chez l'hôte, qui peut être défini de poids fort vers poids faible, de gauche à droite. Bien sûr, des syntaxes plus complexes et incorporées devraient être possibles, étant en particulier donné le besoin d'espaces de noms "grand pères". Pour résoudre les URN, des règles seront nécessaires pour deux raisons. Une est simplement de canoniser ces espaces de noms qui ne suivent pas un ordre direct (probablement de droite à gauche ou de gauche à droite) des composants d'un URN, comme déterminé par les autorités de désignation déléguées impliquées. Il est aussi possible que des règles soient nécessaires afin de déduire des URN les noms des serveurs de RDS à utiliser dans les étapes.

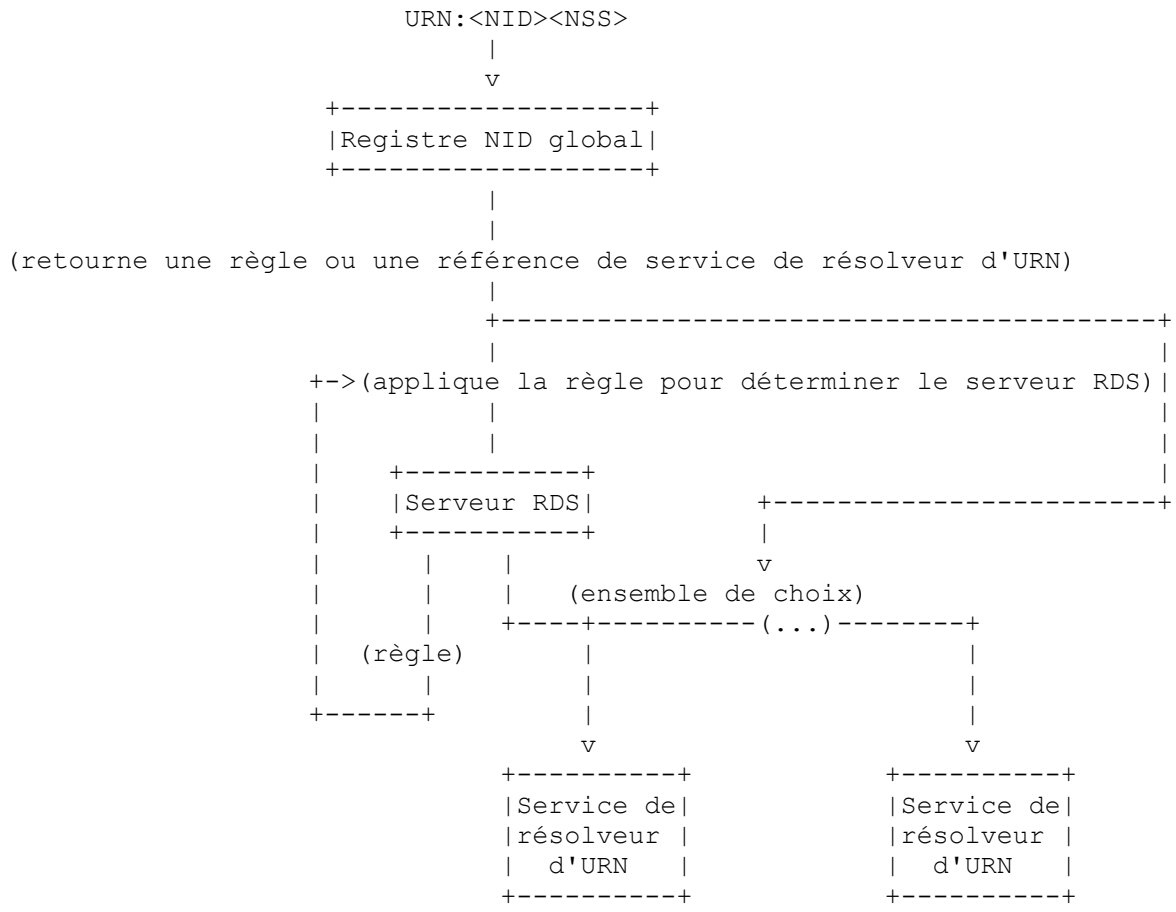

Figure 1 : Cadre de RDS

Le NID définit une syntaxe de niveau supérieur. Cette syntaxe va déterminer si le NID seul, ou en conjonction avec des extractions du NSS (pour le nom de l'autorité de désignation de niveau supérieur) est à utiliser pour identifier le serveur de premier niveau à contacter. À chaque étape de la recherche, une nouvelle règle pour générer la chaîne utilisée dans une recherche déjà effectuée (la chaîne étant l'identité d'un autre serveur RDS et éventuellement une chaîne à résoudre si elle est différente de l'URN d'origine) ou une référence en dehors du RDS à un service de résolution d'URN, mettant de côté tout autre usage du schéma de RDS. La Figure 1 décrit ce processus.

Plusieurs points méritent d'être notés à propos du cadre de RDS. Tout d'abord, il laisse ouverte la détermination des protocoles, de l'organisation des données, de la distribution et de la duplication nécessaires pour prendre en charge un schéma de RDS particulier. Ensuite, il laisse ouverte la question de la localisation des calculs engendrés par les règles. Troisièmement, il laisse ouverte la possibilité que des partitions (répartitions) de la base de données RDS n'aient pas besoin d'être sur les mêmes frontières que la délégation de nom. Cela peut sembler radical à certains, mais si les informations sont mémorisées par exemple dans des arborescences B équilibrées, la partition peut n'être pas selon ces frontières de délégation d'autorité de désignation (voir [EGRS]). Enfin, il laisse ouvert l'accès au registre NID mondial. Est il distribué à tous les clients, ou géré dans des serveurs largement répartis ? Il est important de noter que notre intention est qu'un seul schéma de RDS prenne vraisemblablement en charge les noms provenant de nombreux schémas de désignation, comme ils sont incorporés dans leurs NID.

Un concept qui n'a pas été abordé dans la Figure 1 est qu'il peut y avoir plus d'un RDS disponible à un moment donné, afin de permettre une évolution vers de nouveaux schémas. Donc, le tableau devrait probablement plutôt ressembler à celui de la Figure 2.

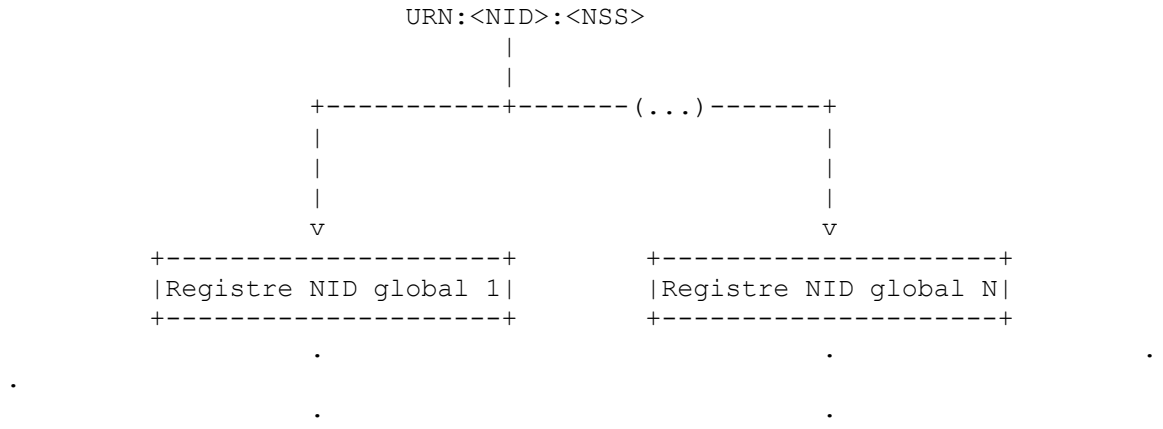

Figure 2 : Plus d'un schéma de RDS coexistent

Si on doit prendre en charge plus d'un schéma de RDS coexistants, il faudra les coordonner par rapport à la mémorisation et la propagation des informations et de leurs modifications. Le problème est que généralement on devrait supposer que toutes les informations devraient être disponibles dans tout schéma de RDS fonctionnel. On ne peut pas s'attendre à ce que les éditeurs potentiels soumettent les mises à jour à plus d'un schéma de RDS. Il devra donc y avoir une transposition directe des informations d'un de ces schémas dans les autres. Il est possible que cette transformation n'aille que dans une seule direction, parce qu'un service de RDS plus récent en remplace un plus ancien, qui n'est plus mis à jour, afin d'encourager le transfert sur le nouveau. Donc, dans une certaine mesure, les mises à jour peuvent n'être effectuées que sur le nouveau schéma et n'être pas disponibles sur le plus ancien, comme cela se fait souvent dans les catalogues des bibliothèques.

Ce cadre est présenté afin de suggérer aux concepteurs de schémas de RDS une direction pour le démarrage de leurs travaux. Il devrait être évident au lecteur que l'adhésion à ce cadre ne va en aucune façon garantir la conformité aux lignes directrices, ou même aux hypothèses décrites dans les Sections 2 et 3. Celles-ci doivent être revues indépendamment au titre du processus de conception. Il n'y a pas une seule conception correcte qui va être conforme à ces lignes directrices. De plus, on suppose que des propositions préliminaires peuvent ne pas satisfaire aux lignes directrices, mais on devrait s'attendre à ce qu'elles argumentent et justifient tout manquement à la conformité.

5. Remerciements

Les premiers remerciements pour le présent document vont à Lewis Girod, comme coauteur du document préliminaire sur les exigences pour les URN et pour ces commentaires perspicaces sur la présente version du document. Nos remerciements vont aussi à Ron Daniel en particulier pour ses nombreux commentaires sur la rédaction. De plus, je reconnais la contribution à la précédente version du document cadre des URN de groupe "Knoxville". Ils sont trop nombreux pour les remercier tous ici individuellement, mais je leur adresse un merci global. Finalement, je dois remercier les contributeurs au groupe de travail URN et à la liste de diffusion (urn-ietf@bunyip.com), pour les discussions animées sur ces sujets et ceux qui s'y rapportent.

6. Références

[RFC1736] J. Kunze, "Recommandations fonctionnelles pour les localisateurs de ressource Internet", février 1995. *(Info)*

[RFC1737] K. Sollins et L. Masinter, "Exigences fonctionnelles pour les noms de ressource uniformes", décembre 1994.

[RFC1738] T. Berners-Lee et autres, "Localisateurs uniformes de ressource (URL)", décembre 1994. *(P.S., Obsolète, voir les RFC4248 et 4266)*

[GTURN] Groupe de travail URN, "Namespace Identifier Requirements for URN Services," Travail non publié

[SMHLP] Voydock, V. L., and Kent, S. T., "Security Mechanisms in High-Level Protocols", ACM Computing Surveys, v. 15, n° 2, juin 1983, pp. 135-171.

[RFC2141] R. Moats, "Syntaxe des URN", mai 1997.

[EGRS] Slottow, E.G., "Engineering a Global Resolution Service," MIT-LCS-TR712, juin 1997. Actuellement disponible à <http://ana.lcs.mit.edu/anaweb/ps-papers/tr-712.ps>
ou à <http://ana.lcs.mit.edu/anaweb/pdf-papers/tr712.pdf>.

7. Adresse de l'auteur

Karen Sollins
MIT Laboratory for Computer Science
545 Technology Sq.
Cambridge, MA 02139
téléphone : +1 617 253 6006
mél : sollins@lcs.mit.edu

8. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'éditeur des RFC est actuellement assuré par la Internet Society.