

Groupe de travail Réseau  
**Request for Comments : 3983**  
 Catégorie : En cours de normalisation  
 Traduction Claude Brière de L'Isle

A. Newton, VeriSign, Inc.  
 M. Sanz, DENIC eG

janvier 2005

## Utilisation du service d'informations de registre Internet (IRIS) sur le protocole extensible d'échange de blocs (BEEP)

### Statut de ce mémoire

Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

### Notice de copyright

Copyright (C) The Internet Society (2005).

### Résumé

Le présent document spécifie comment utiliser le protocole extensible d'échange de blocs (PEEP, *Blocks Extensible Exchange Protocol*) comme sous strate de transport d'application pour le service d'informations de registre Internet (IRIS, *Internet Registry Information Service*).

### Table des Matières

1. Introduction et motivation.....	1
2. Terminologie du document.....	2
3. Identification du profil BEEP.....	2
4. Paquetages de message IRIS.....	3
5. Schémas de message IRIS.....	3
5.1 Schémas dépendants du registre.....	3
5.2 Schéma par défaut.....	3
6. Méthodes d'authentification de serveur.....	3
6.1 Méthodes qui dépendent du registre.....	3
6.2 Méthode de base d'authentification de serveur.....	3
7. Définitions de transposition de transport IRIS.....	4
7.1 Schémas d'URI.....	4
7.2 Étiquette de protocole d'application.....	4
7.3 Jeux de caractère admis.....	4
7.4 Transposition de BEEP.....	4
8. Enregistrements.....	4
8.1 Enregistrement de profil BEEP.....	4
8.2 Enregistrement de schéma d'URI.....	4
8.3 Enregistrement d'accès TCP bien connu.....	5
8.4 Enregistrement de S-NAPTR.....	5
9. Liste de contrôle de définition de registre.....	5
10. Considérations d'internationalisation.....	5
11. Considérations relatives à l'IANA.....	5
12. Considérations sur la sécurité.....	5
13. Références.....	6
13.1 Références normatives.....	6
13.2 Références pour information.....	6
14. Adresse des auteurs.....	7
Déclaration complète de droits de reproduction.....	7

### 1. Introduction et motivation

La proposition du présent document décrit le lien de transport d'application IRIS [RFC3981] qui utilise BEEP [RFC3080]. Les exigences d'IRIS et la spécification du présent document sont précisées dans CRISP [RFC3707].

Le choix de BEEP comme sous couche de transport est principalement motivé par le besoin de réutiliser un protocole existant bien connu avec toutes les caractéristiques nécessaires pour prendre en charge ces exigences. Cela donnerait aux mises en œuvre une riche palette d'outils et de moyens de débogage à utiliser dans la construction des serveurs et des clients et permettrait aux opérateurs d'appliquer leur expérience existante dans les problèmes de déploiement. La construction d'un simple transport d'application pour les besoins spécifiques de IRIS donnerait un standard similaire, bien que probablement plus restreint et moins complet, après avoir pris en considération des sujets comme le tramage et l'authentification.

Les utilisations précédentes d'autres mécanismes de transport dans des applications en couches ne semblent pas avoir satisfait aux objectifs de conception d'IRIS. HTTP [RFC2616] offre de nombreuses caractéristiques employées par des applications similaires. Cependant, IRIS n'est pas destiné à des utilisations telles que les passages de pare-feu, le mélange de schémas d'URI, ou toutes autres méthodes qui pourraient conduire à une confusion entre IRIS et les applications traditionnelles de la Toile mondiale. Au delà de l'adhésion aux directives énoncées dans la [RFC3205], l'utilisation de HTTP offre aussi de nombreux autres défis qui émoussent rapidement son attractivité. Par exemple, l'utilisation appropriée de TLS [RFC2246] avec HTTP est définie par la [RFC2817], mais l'utilisation courante, telle que décrite dans la [RFC2818], est généralement la seule méthode dans la plupart des mises en œuvre.

Finalement, l'utilisation de IRIS directement sur TCP, comme c'est spécifié par EPP-TCP [RFC4934], n'offre pas les caractéristiques de négociation de client nécessaires pour une application de référence dans laquelle un seul client, en traitant une interrogation, peut traverser plusieurs serveurs fonctionnant avec des paramètres différents.

## 2. Terminologie du document

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

## 3. Identification du profil BEEP

L'identifiant de profil BEEP pour IRIS est un URI composé de l'URN de schéma IRIS, suivi par une barre oblique, suivi par un type de registre IRIS (qui est un URN).

Dans cet identifiant de profil, le schéma IRIS DOIT être abrégé conformément aux règles de IRIS. Ceci est possible parce que l'URN de schéma IRIS est conforme à XML\_URN [RFC3688].

L'URN type de registre DOIT être abrégé conformément aux règles de IRIS (voir la [RFC3981]). Ceci est possible parce que l'URN de type de registre est conforme à XML\_URN [RFC3688].

Voici un exemple d'identifiant de profil IRIS pour BEEP. Il identifie la version de IRIS pour correspondre à celle spécifiée par "urn:iana:params:xml:ns:iris1" avec un URN de type de registre de "urn:iana:params:xml:ns:dreg1" :

```
http://iana.org/beep/iris1/dreg1
```

L'ABNF complet [RFC2234] suit, avec certaines valeurs incluses de IRIS [RFC3981] :

```
profile = profile-uri "/" iris-urn-abbrev "/" registry-urn-abbrev
profile-uri = "http://iana.org/beep/"
iris-urn-abbrev = // comme spécifié par IRIS
registry-urn-abbrev = // comme spécifié par IRIS
```

Cet URI est utilisé dans l'élément "profile" dans BEEP durant la création de canal. Conformément aux règles de BEEP, plusieurs éléments "profile" peuvent être offerts, permettant donc la négociation de la version de IRIS à utiliser pour chaque type de registre servi.

Une fois que ce profil est accepté et que le canal est créé, le canal est considéré prêt à échanger des messages IRIS. Un serveur DOIT honorer les interrogations pour tous les types de registres annoncés sur tout canal ouvert avec un URI de profil IRIS.

## 4. Paquetages de message IRIS

Le profil BEEP pour IRIS transmet le XML [XML] qui contient les demandes et réponses pour les registres IRIS. Ces instances XML DOIVENT être codées en Unicode [Unicode] en utilisant le type de support de "application/xml" conformément à la [RFC3023].

Les processeurs XML sont obligés de reconnaître les deux codages UTF-8 et UTF-16 [Unicode]. XML permet des mécanismes pour identifier et utiliser d'autres codages de caractères au moyen de l'attribut "encoding" dans la déclaration. L'absence de cet attribut ou d'une marque d'ordre des octets (BOM, *byte order mark*) indique par défaut le codage UTF-8. Donc, pour des raisons de compatibilité, et selon la [RFC2277], l'utilisation de l'UTF-8 est RECOMMANDÉE avec cette transposition de transport. UTF-16 est FACULTATIF. D'autres codages NE DOIVENT PAS être utilisés.

Un type de registre PEUT définir d'autres paquetages de message qui ne sont pas des instances XML IRIS (par exemple, des images binaires référencées par une réponse IRIS).

## 5. Schémas de message IRIS

### 5.1 Schémas dépendants du registre

Parce que chaque type de registre est défini par un profil BEEP distinct (voir la [RFC3981]) chaque type de registre PEUT définir un schéma de message différent. Ces schémas DOIVENT être dans la portée admissible de BEEP [RFC3080]. Si un type de registre ne définit pas explicitement un schéma de message, le schéma par défaut est utilisé (voir le paragraphe 5.2).

Cependant, chaque type de registre DOIT être capable de prendre en charge le schéma par défaut (paragraphe 5.2) à utiliser avec l'interrogation <lookupEntity> dans IRIS.

### 5.2 Schéma par défaut

Le profil BEEP par défaut pour IRIS a seulement un schéma de message de demande/réponse biunivoques. Cet échange implique d'envoyer une instance XML IRIS, d'où résulte une réponse d'une instance XML IRIS.

Le client envoie la demande en utilisant un message "MSG" contenant une instance XML IRIS valide. Le serveur répond par un message "RPY" contenant une instance XML IRIS valide. Le message "ERR" est utilisé pour envoyer les codes de fautes. La liste des codes de fautes admis figure dans BEEP [RFC3080].

## 6. Méthodes d'authentification de serveur

### 6.1 Méthodes qui dépendent du registre

Lorsque on utilise le profil de réglage TLS [RFC2246] dans BEEP, il est possible de vérifier l'authenticité du serveur. Cependant, une convention est nécessaire pour effectuer cette authentification. Cette convention impose le nom de l'autorité qu'utilise un client pour demander les accreditifs d'authentification afin que le serveur sache quel ensemble d'accréditifs passer. Parce que cela dépend du composant d'autorité de l'URI, chaque type de registre DEVRAIT définir une méthode d'authentification de serveur.

Si un type de registre ne définit pas explicitement une méthode d'authentification de serveur, on utilise la méthode de base d'authentification de serveur (paragraphe 6.2).

### 6.2 Méthode de base d'authentification de serveur

La méthode de base d'authentification de serveur est la suivante :

1. Lorsque il se connecte à un serveur, le client DOIT présenter le nom de l'autorité au serveur en utilisant le mécanisme BEEP [RFC3080] serverName. Par exemple, si l'URI "iris:dreg1//com/domain/example.com" est à résoudre, le client va utiliser l'attribut serverName="com" durant l'instanciation de session BEEP.
2. Durant la négociation TLS, le serveur présente au client un certificat pour l'autorité donnée dans serverName. Ce certificat DOIT être un certificat X.509 [RFC3280]. Ce certificat DOIT contenir l'autorité soit dans le subjectDN, soit dans l'extension subjectAltName du type dNSName.

3. Le certificat DOIT être vérifié cryptographiquement conformément aux procédures de TLS.
4. Le client vérifie ensuite le "subject" du certificat selon une correspondance insensible à la casse dans l'ordre suivant :
  1. tous les types dNSName dans le subjectAltName,
  2. le subjectDN consistant seulement en composants "dc", dans lesquels chaque composant "dc" représente une étiquette provenant du nom de l'autorité (par exemple, example.com est dc=example, dc=com),
  3. un subjectDN dans lequel le composant le plus à gauche est un composant "cn" contenant le nom de l'autorité. Un caractère générique (\*) PEUT être utilisé comme étiquette de gauche du nom dans le composant "cn".

Si le sujet du certificat ne correspond à aucun de ces composants de nom, le certificat est invalide pour représenter l'autorité.

## 7. Définitions de transposition de transport IRIS

Cette section fait la liste des définitions requises par IRIS [RFC3981] pour les transpositions de transport.

### 7.1 Schémas d'URI

Le nom de schéma d'URI spécifique de BEEP sur IRIS DOIT être "iris.beep".

### 7.2 Étiquette de protocole d'application

L'étiquette de protocole d'application DOIT être "iris.beep".

### 7.3 Jeux de caractère admis

Voir les Sections 4 et 10.

### 7.4 Transposition de BEEP

La transposition d'IRIS dans le présent document est spécifique de la [RFC3080]. Cette transposition DOIT utiliser TCP comme spécifié par la [RFC3081].

## 8. Enregistrements

### 8.1 Enregistrement de profil BEEP

Identification de profil : <http://iana.org/beep/iris1>

Messages échangés durant la création du canal : aucun

Messages commençant les échanges de un à un : instance XML IRIS

Messages dans les réponses positives : instance XML IRIS

Messages dans les réponses négatives : aucun

Messages dans les échanges de un à plusieurs : aucun

Syntaxe de message : instances XML IRIS comme défini par IRIS [RFC3981]

Sémantique de message : échanges de demande/réponse comme défini par IRIS [RFC3981]

Informations de contact : Andrew Newton <[andy@hxr.us](mailto:andy@hxr.us)> et Marcos Sanz <[sanz@denic.de](mailto:sanz@denic.de)>

### 8.2 Enregistrement de schéma d'URI

Nom de schéma d'URL : iris.beep

Syntaxe de schéma d'URL : définie au paragraphe 7.1 et dans la [RFC3981]

Considérations de codage de caractères : comme défini dans la [RFC2396]

Usage de destination : identifie une entité IRIS rendue disponible en utilisant le profil BEEP pour IRIS

Applications qui utilisent ce schéma : défini dans IRIS [RFC3981]

Considérations d'interopérabilité : non disponible

Considérations de sécurité : définies à la Section 12.

Publications pertinentes : BEEP [RFC3080] et IRIS [RFC3981]  
Informations de contact : Andrew Newton <andy@hxr.us> et Marcos Sanz <sanz@denic.de>  
Auteur/Contrôleur des changements : IESG

### 8.3 Enregistrement d'accès TCP bien connu

Numéro de protocole : TCP  
Formats, types, Opcodes, et séquences de message : défini aux Sections 3, 4, et 5.  
Fonctions : défini dans IRIS [RFC3981]  
Utilisation de diffusion/diffusion groupée : aucune  
Nom proposé : IRIS sur BEEP  
Nom abrégé : iris.beep  
Informations de contact : Andrew Newton <andy@hxr.us> et Marcos Sanz <sanz@denic.de>

### 8.4 Enregistrement de S-NAPTR

Étiquette de protocole d'application : iris.beep  
Usage de destination : identifie un serveur IRIS utilisant BEEP  
Considérations d'interopérabilité : non disponible  
Considérations de sécurité : définies à la Section 12.  
Publications pertinentes : BEEP [RFC3080] et IRIS [RFC3981]  
Informations de contact : Andrew Newton <andy@hxr.us> et Marcos Sanz <sanz@denic.de>  
Auteur/Contrôleur des changements : IESG

## 9. Liste de contrôle de définition de registre

Les spécifications de types de registre DOIVENT inclure les définitions explicites suivantes :

- o schéma de message -- une définition du schéma de message à utiliser avec BEEP, ou une déclaration d'utilisation du schéma de message par défaut du paragraphe 5.2.
- o méthode d'authentification du serveur -- une définition de la méthode à utiliser pour l'authentification du serveur avec TLS, une déclaration d'utilisation de la méthode de base d'authentification du serveur du paragraphe 6.2, ou une déclaration de pas du tout d'authentification du serveur.

## 10. Considérations d'internationalisation

Voir la Section 4.

## 11. Considérations relatives à l'IANA

Les enregistrements auprès de l'IANA sont décrits à la Section 8.

## 12. Considérations sur la sécurité

Les mises en œuvre devraient être pleinement conscientes des considérations sur la sécurité données par IRIS [RFC3981], BEEP [RFC3080], et TLS [RFC2246]. En ce qui concerne l'authentification du serveur avec l'utilisation de TLS, voir la Section 6.

Les clients DEVRAIENT être prêts à utiliser les profils de réglage de BEEP suivants :

- o <http://iana.org/beep/SASL/DIGEST-MD5> -- pour l'authentification de l'utilisateur sans avoir besoin de chiffrement de session.
- o <http://iana.org/beep/SASL/OTP> -- pour l'authentification de l'utilisateur sans avoir besoin de chiffrement de session.
- o <http://iana.org/beep/TLS> utilisant le chiffrement TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA -- pour le chiffrement.
- o <http://iana.org/beep/TLS> utilisant le chiffrement TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA avec des certificats côté client -- pour le chiffrement et l'authentification de l'utilisateur.

- o <http://iana.org/beep/TLS> utilisant le chiffrement TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA -- pour le chiffrement. Voir la [RFC3268].
- o <http://iana.org/beep/TLS> utilisant le chiffrement TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA avec des certificats côté client -- pour le chiffrement et l'authentification de l'utilisateur. Voir la [RFC3268].
- o <http://iana.org/beep/TLS> utilisant le chiffrement TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA -- pour le chiffrement. Voir la [RFC3268].
- o <http://iana.org/beep/TLS> utilisant le chiffrement TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA avec des certificats côté client -- pour le chiffrement et l'authentification de l'utilisateur. Voir la [RFC3268].

L'accès de client anonyme DEVRAIT être considéré selon une des deux méthodes suivantes :

1. Lorsque aucun profil de réglage d'authentification n'a été utilisé.
2. En utilisant le profil SASL anonyme : <http://iana.org/beep/SASL/ANONYMOUS>

IRIS contient un mécanisme de référence dans son fonctionnement standard. Cependant, il faut veiller à ce que les mécanismes d'authentification d'utilisateur ne passent pas les accreditifs d'utilisateur à des serveurs qui ne sont pas de confiance. Donc, les clients NE DEVRAIENT PAS utiliser le profil de réglage <http://iana.org/beep/SASL/PLAIN>. Comme spécifié par SASL/PLAIN, les clients NE DOIVENT PAS utiliser le profil de réglage <http://iana.org/beep/SASL/PLAIN> sans avoir d'abord chiffré la session TCP (par exemple, comme avec le profil de réglage <http://iana.org/beep/TLS>).

## 13. Références

### 13.1 Références normatives

- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.
- [RFC2234] D. Crocker et P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", novembre 1997. (*Obsolète, voir RFC5234*)
- [RFC2246] T. Dierks et C. Allen, "[Protocole TLS version 1.0](#)", janvier 1999.
- [RFC2277] H. Alvestrand, "Politique de l'IETF en matière de [jeux de caractères et de langages](#)", BCP 18, janvier 1998.
- [RFC2396] T. Berners-Lee, R. Fielding et L. Masinter, "Identifiants de ressource uniformes (URI) : Syntaxe générique", août 1998. (*Obsolète, voir RFC3986*)
- [RFC3023] M. Murata, S. St-Laurent et D. Kohn, "Types de support XML", janvier 2001. (*Obsolète, voir RFC7303*)
- [RFC3080] M. Rose, "Cœur du [protocole extensible d'échange de blocs](#) (BEEP)", mars 2001. (*P.S.*)
- [RFC3081] M. Rose, "[Transposition du cœur BEEP](#) en TCP", mars 2001. (*P.S.*)
- [RFC3268] P. Chown, "Suites de chiffrement de la norme de chiffrement évolué (AES) pour la sécurité de la couche Transport (TLS)", juin 2002. (*Obsolète, voir RFC5246*) (*P.S.*)
- [RFC3280] R. Housley, W. Polk, W. Ford et D. Solo, "Profil de certificat d'infrastructure de clé publique X.509 et de liste de révocation de certificat (CRL) pour l'Internet", avril 2002. (*Obsolète, voir RFC5280*)
- [RFC3981] A. Newton, M. Sanz, "IRIS : [Protocole central du service d'information des registres Internet](#) (IRIS)", janvier 2005. (*MàJ par RFC4992*) (*P.S.*)
- [Unicode] The Unicode Consortium, "The Unicode Standard, Version 3", ISBN 0-201-61633-5, 2000,.
- [XML] World Wide Web Consortium, "Extensible Markup Language (XML) 1.0", W3C XML, février 1998, <<http://www.w3.org/TR/1998/REC-xml-19980210>>.

### 13.2 Références pour information

- [RFC2616] R. Fielding et autres, "[Protocole de transfert hypertexte](#) -- HTTP/1.1", juin 1999. (*D.S., MàJ par 2817, 6585*)

- [RFC2817] R. Khare, S. Lawrence, "[Mise à niveau de TLS](#) au sein de HTTP/1.1", mai 2000. (*P.S.*)
- [RFC2818] E. Rescorla, "HTTP sur TLS", mai 2000. (*Information*)
- [RFC3205] K. Moore, "Sur l'utilisation de HTTP comme sous strate", février 2002. ([BCP0056](#))
- [RFC3688] M. Mealling, "[Registre XML de l'IETF](#)", BCP 81, janvier 2004.
- [RFC3707] A. Newton, "Exigences pour le protocole d'enregistrement croisé de service Internet (CRISP)", février 2004. (*Info.*)
- [RFC4934] S. Hollenbeck, "Transport sur TCP avec le protocole d'approvisionnement extensible (EPP)", mai 2007. (*Remplace la [RFC3734](#) (Remplacée par [RFC5734](#), STD 69)*)

## 14. Adresse des auteurs

Andrew L. Newton  
VeriSign, Inc.  
21345 Ridgetop Circle  
Sterling, VA 20166  
USA

téléphone : +1 703 948 3382  
mél : [anewton@verisignlabs.com](mailto:anewton@verisignlabs.com) ; [andy@hxr.us](mailto:andy@hxr.us)  
URI : <http://www.verisignlabs.com/>

Marcos Sanz  
DENIC eG  
Wiesenhuettenplatz 26  
D-60329 Frankfurt  
Germany  
mél : [sanz@denic.de](mailto:sanz@denic.de)  
URI : <http://www.denic.de/>

## Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2005).

Le présent document est soumis aux droits, licences et restrictions contenus dans le BCP 78, et à [www.rfc-editor.org](http://www.rfc-editor.org), et sauf pour ce qui est mentionné ci-après, les auteurs conservent tous leurs droits.

Le présent document et les informations contenues sont fournis sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci-encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

### Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourraient être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible ; pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à <http://www.ietf.org/ipr> .

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org) .

### Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society