Network Working Group
Internet-Draft
Expires: March 5, 2004

P. Gietz
DAASI International GmbH

September 5, 2003

Relay Bag Search Control for the Federated Internet Registry Service
draft-ietf-crisp-firs-relay-00

Status of this Memo

Copyright Notice

Abstract

This document describes an LDAP search request and response control to allow additional unspecified data to be returned with a referral to the client, which can submit these data to the referred to server in support of the Federated Internet Registry Service (FIRS) described in [FIRS-ARCH] and [FIRS-CORE]. A flexible container called relay bag as required in [CRISP-REQ] is included into this extension to the LDAP search operation.

Conventions used in this document

Protocol elements are described using ASN.1 [X.680]. The term "BER-encoded" means the element is to be encoded using the Basic Encoding

Rules [X.690] under the restrictions detailed in Section 5.1 of [RFC2251].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Whenever the words "client" and "server" are used in this document, the notion is a FIRS complying client and server respectively.

1. Background and Intent of Use

The Federated Internet Registry Service (FIRS) described in [FIRS-ARCH] and [FIRS-CORE] is a distributed service for storing, locating and transferring information about the Internet Resources using LDAPv3 [RFC3377]. It is thus an implementation of a Cross Registry Information Service Protocol as specified in the requirements document [CRISP-REQ]. To completly fulfil these requirements, a feature called relay bag has to be supported.

A relay bag is a flexible container which may contain unspecified data that a server can give back to a client in addition to a referral. The data are not to be read and understood by the client, but to be forwarded by the client to the referred to server. The data transported in the relay bag are thus server operator-to-operator coordination data, e.g. for auditing or tracking.

This document specifies such a relay bag with the means of two LDAP controls extenting the LDAP search operation.

2. Relay Bag Search Request and Response Controls

Support for the relay bag search request and response controls defined in this section is advertised by the presence of their OID in the supportedControl attribute of a server's root DSE entry, which is specified in [RFC2251], section 3.4. The OID of the request control is "1.3.6.1.4.1.10126.1.15.7.2", the OID of the response control is "1.3.6.1.4.1.10126.1.15.7.3".

An LDAP control as specified in [RFC2251], section 4.1.12, is a way to specify extension information for an LDAP operation. Basically an LDAP control consists of a controlType, containing the OID for the control, a boolean field for marking the criticality of the control, and an optional controlValue containing arbitrary data with octet string syntax.

The relay bag search request and response controls are only to be used within the search operation, which is specified in [RFC2251],

section 4.5.

2.1 Relay Bag Search Request Control

The relay bag search request control is to be included in the the SearchRequest message as part of the controls field of the LDAPMessage, which is defined in section 4.1.1 of [RFC2251]. It MUST NOT be included in any other request or result message.

It has the following controlType:

relayBagSearchRequestOID OBJECT IDENTIFIER ::= 1.3.6.1.4.1.10126.1.15.7.2

The controlValue is a BER-encoded Octet string, which can contain any kind of data:

relayBagSearchRequestValue ::== OCTET STRING

The criticality may either be set to TRUE or FALSE.

2.2 Relay Bag Search Response Control

The relay bag search response control is to be included in the the SearchResultReference message as part of the controls field of the LDAPMessage, which defined in section 4.1.1 of [RFC2251]. It MUST NOT be included in any other request or result message.

It has the following controlType:

relayBagSearchResponseOID OBJECT IDENTIFIER ::= 1.3.6.1.4.1.10126.1.15.7.3

The controlValue is a BER-encoded Octet string, with the following syntax:

```
relayBagSearchResponseValue ::== SEQUENCE of SEQUENCE {
                                     ldapurl    [0]  LDAPURL,
                                     relayBag   [1]  OCTET STRING
}
```

The ldapurl part of the relayBagSearchResponseValue is an LDAP URL,

which is specified in [RFC2255]

The relayBag part of the relayBagSearchResponseValue is a BER-encoded Octet string, which can contain any kind of data:

The criticality MUST be set to TRUE.

3. Relay Bag Specific LDAP Result Codes

As specified in [RFC3383], section 3.6, it is possible to register new LDAP result codes not specified in [RFC2251]. For the relay bag controls the following LDAP result codes are defined:

firsRelayBagUnrecognizedFormat	(1050)
firsRelayBagUnacceptableData	(1051)
firsRelayBagTemporarlyRefused	(1052)

4. Operation Requirements

A client MAY evaluate if the server it initially connects to supports this feature, by checking if the controlType Object Identifier of the controls specified in this document (relayBagSearchRequestOID and relayBagSearchResponseOID) are stored in the attribute supportedControl of the root DSE entry, which is specified in [RFC2251], section 3.4.

If the server supports this control the Client MUST use it when sending a search request to the server. In the initial server contact the controlValue of the relayBagSearchRequest sent by the client SHOULD be empty.

When the server sends back the search response, it MUST include the control identified by the controlType field. The controlValue MAY contain data that at least give the information that the server had referred the client to another server.

For each LDAP URL listed in the control value of the SearchResultReference message response the relay bag part of the control value MUST contain some kind of data. The semantics for such information is not defined in this document and is to be specified by the service operators.

The semantics MAY include a mechanism to make sure that the data have not been changed, e.g. by digitally signing a hash value of the contents.

The semantics MAY also include a mechanism to make sure that only the referred to server can read the contents of the relay bag, e.g. by encrypting the contents with the Public Key of the refered to server, so that only that server can decrypt the contents with its private key.

A server may send back referrals without a relay bag, referrals with a relay bag and a combination of both.

Referrals without relay bag MUST be submitted via the SearchResultReference construct specified in RFC 2251, section 4.5.2 for this purpose.

If the server only sends back referrals without relay bags, the controlValue of the SearchResultReference MUST be empty.

When the client follows a referral given without a relay bag, it MAY nonetheless use the relay bag request control while contacting the referred to server. In this case the controlValue of the relayBagSearchRequest sent by the client MUST be empty.

Referrals with a relay bag MUST be submitted inside the controlValue field as specified above, without redundantly storing the referrals in the SearchResultReference construct.

When the client follows a referral given with a relay bag part in the response control value, it MUST use the control and send the data given by the referring server in the respective relay bag part of controlValue field unchanged in the controlValue field of the search request.

If only referrals with relay bag are submitted, the server MUST store a dummy-referral in the SearchResultReference construct. The dummy referral, which MUST be ignored by the client, is:

```
ldap:///
```

If no referrals are submitted at all, the response message of the server is another than SearchResultReference, namely SearchResultDone or SearchResultEntry. In these cases no relay bag control will be included in the response message.

If the refered to server does not recognize the format of the Relay Bag included in a search request it MUST respond with the result code firsRelayBagUnrecognizedFormat (1050). This has to be interpreted by the client as permanent failure.

If the relay bag included in a search request contains data unacceptable to the refered to server, the server MUST respond with the result code firsRelayBagUnacceptableData (1051). This has to be interpreted by the client as permanent failure.

If the relay bag included in a search request contains data that according to the policy of the referred to server indicate that processing should be refused at this time, the refered to server MUST respond with the result code firsRelayBagTemporarlyRefused (1052). This has to be interpreted by the client as transient failure.

If the relay bag included in a search request contains data that according to the policy of the refered to server indicate that processing should be refused at any time, the refered to server MAY respond with the result code unwillingToPerform (53).

Servers that support the relay bag control MAY decide to only serve clients that support and use this control. If a server wants to thus enforce the control, every search request without this control SHOULD be responded to with the resultCode unwillingToPerform (53).

5. Relationship to Other Search Controls

The relay bag search control is not intended be used together with any other existing search controls. Nonetheless there should not be a problem to do so. Clients have to be aware though that if using the relay bag control, some referrals may be found in the controlValue instead of the referral list. In cases other than a SearchResultReference, there are no effects in the server response at all caused by the relay bag control.

If a new search control is to be used in combination with the relay bag search control the document, describing that new search control has to deal with possible implications not foreseable now.

6. Security Considerations

The relay bag search control can be used in services to provide data only to clients that have properly authenticated to one server, by passing over the authentication status of the client to the referred to server.

To make sure the client has not changed the contents of the relay bag, it is possible to use the PKI feature of digitally signing the contents of the relay bag, e.g. by using X.509 based PKI with certificates as specified in [RFC3280].

To make sure the client cannot understand the contents of the relay

bag, which is only meant to be understood by the referred to server, it is possible to use the PKI feature of encrypting the contents of the relay bag with the help of the public key of the referred to server, so that only that server can decrypt the contents.

Obviously any usage of this search control is dependant on the services that use it, since this document does not specify and enforce any semantics of the controlValue field. Thus every service, using this control has to be aware of the possible security implications.

7. IANA Considerations

7.1 Object Identifiers

This document uses the OIDs 1.3.6.1.4.1.10126.1.15.7.2 and 1.3.6.1.4.1.10126.1.15.7.3 to identify an LDAP protocol element defined herin. This OID was assigned by DAASI International Ltd., under its IANA assigned private enterprise allocation [PRIVATE], for use in this specification.

7.2 Protocol Mechanisms

Registration of the protocol mechanisms defined in this document is requested in [RFC3383].

Subject: Request for LDAP Protocol Mechanism Registration

Object Identifier: 1.3.6.1.4.1.10126.1.15.7.2

Description: relay bag search request

Person & email address to contact for further information:
Peter Gietz <peter.gietz@daasi.de>

Usage: Control

Specification: RFCxxxx

Author/Change Controller: IESG

Comments: none

Subject: Request for LDAP Protocol Mechanism Registration

Object Identifier: 1.3.6.1.4.1.10126.1.15.7.3

Description: relay bag search response

Person & email address to contact for further information:
Peter Gietz <peter.gietz@daasi.de>

Usage: Control

Specification: RFCxxxx

Author/Change Controller: IESG

Comments: none

7.3 LDAP Result Codes

Registration of the LDAP result codes defined in this document is requested in [RFC3383].

Subject: Request for LDAP Result Code Registration

Result Code Name: firsRelayBagUnrecognizedFormat

Result Code Number: 1050

Person & email address to contact for further information:
Peter Gietz <peter.gietz@daasi.de>

Specification: RFCxxxx

Author/Change Controller: IESG

Comments: none

Subject: Request for LDAP Result Code Registration

Result Code Name: firsRelayBagUnacceptableData

Result Code Number: 1051

Person & email address to contact for further information:
Peter Gietz <peter.gietz@daasi.de>

Specification: RFCxxxx

Author/Change Controller: IESG

Comments: none

Subject: Request for LDAP Result Code Registration

Result Code Name: firsRelayBagTemporarlyRefused

Result Code Number: 1052

Person & email address to contact for further information:
Peter Gietz <peter.gietz@daasi.de>

Specification: RFCxxxx

Author/Change Controller: IESG

Comments: none

8. Changes from Previous Drafts

8.1 Changes in Draft 01

- Separated the control into different controls for the request and the response. The response control value now consists of a list of referrals with a relay bag attached to each referral.
- introduced FIRS specific LDAP result codes for relay bag handling of the server.
- added a number of clarifications in section Section 4
- changed section Section 5 to clarify the relations to other search controls.
- re-evaluated the MUST, SHOUD and MAY with respect to the requirements specified in [CRISP-REQ], especially with respect to the criticality of the control
- added section on IANA considerations
- some minor editorial changes

9. Acknowledgments

This document is the result of discussions taking place in the IETF CRISP WG. The concept of relay bags is derived from that activity. Especially Andrew Newton, Eric A. Hall, Steven Legg, Leslie Daigle and Marc C. Smith gave valuable input.

This document has been written in XML according to the DTD specified in RFC2629. xml2rfc has been used to generate an RFC2033 compliant plain text form. The XML source and a HTML version are available on request.

10. References

10.1 Normative References

[CRISP-REQ] Newton, A., "Cross Registry Internet Service Protocol (CRISP) Requirements", May 2003, <draft-ietf-crisp-requirements-05.txt>.

[FIRS-ARCH] Hall, E., "The Federated Internet Registry Service: Architecture and Implementation Guide", May 2003, <draft-ietf-crisp-firs-arch-01.txt>.

[FIRS-CORE] Hall, E., "The Federated Internet Registry Service: Core

Elements", May 2003, <draft-ietf-crisp-firs-core-01.txt>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2251] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[RFC2255] Howes, T. and M. Smith, "The LDAP URL Format", RFC 2255, December 1997.

[RFC3377] Hodges, J. and RL. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", RFC 3377, September 2002.

[RFC3383] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", RFC 3383, September 2002.

[X.680] ITU-T, "Abstract Syntax Notation One (ASN.1) - Specification of Basic Notation", X. 680, 1994.

[X.690] ITU-T, "Specification of ASN.1 encoding rules: Basic, Canonical, and Distinguished Encoding Rules", X. 690, 1994.

10.2 Non-normative References

[PRIVATE] IANA, "Private Enterprise Numbers", http://www.iana.org/assignements/enterprise-numbers.

[RFC3280] Housley, R., Polk, T., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 3280, April 2002.

Author's Address

Peter Gietz
DAASI International GmbH
Wilhelmstr. 106
Tuebingen 72074
DE

Phone: +49 7071 29 70336
EMail: peter.gietz@daasi.de
URI: http://www.daasi.de/

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.