FIRS and CRISP Requirements

crisp Meeting, 57th IETF
Vienna, July 16, 2003

Peter Gietz, DAASI International

peter.gietz@daasi.de

General remarks on the matrix

- Difficult to decide what to check the requirements against:
  - FIRS
  - LDAP standard
  - LDAP implementations
- The matrix may need some additional debugging

General remarks on the FIRS evaluation

- All requirements contained in the matrix can be fulfilled by FIRS/LDAP
  - In some cases there may be need for clarification
  - In some cases (relay bag) there is the need of additional specification
  - In one case (IDNs) there may be a better way to support
- In the following all problematic statements will be discussed

Section 3.1.8.1

„The protocol MUST provide a mechanism allowing a client to determine if a query will be denied before the query is submitted according to the appropriate policies of the operator.“

- LDAP has a maximum of three steps in a client server session start:
  1. Open an LDAP-connection
  2. Perform a client bind (optional)
  3. Perform the actual LDAP operation, e.g. search
- The server could give such deny information at step 2
- There are better alternatives to fulfill this requirement

Section 3.1.8.1 contd.

- Alternative solution 1:
  - the server publishes it‘s denial policy in a special entry which is pointed at in the rootDSE entry
  - The client can evaluate itself, if a query will have success
- Alternative solution 2:
  - Specification of an LDAP extended operation (request & response) that tells a client what kind of data it can request successfully

Section 3.1.9.1 b

„The protocol MUST NOT prohibit the participation by an Internet registry in federated, distributed authentication systems.“

- Authentication delegation is possible in LDAP
  - SASL external authentication
  - Authentication based on PKI certificates

Section 3.1.10

„The protocol MUST be capable of returning the following types of non-result or error responses to all lookups and searches:“

- „Permission denied“:
  - inappropriateAuthentication (48)
  - invalidCredentials (49)
  - insufficientAccessRights (50)
- „Not found“:
  - noSuchObject (32)
  - Or ldapSuccess and an empty result list
- „Insuficciant resources“:
  - Busy (51)
  - Unavailable (52)
  - unwillingToPerform (53)

Section 3.1.12.1 a

„The protocol MUST provide a means by which the end-systems can either identify or negotiate over the protocol version to be used for any query or set of queries.“

- On LDAP-level there is and most probably will ever be only one Protocol version: v3
- The client can specify an LDAP protocol version (used for v2-v3 negotiation)
- FIRS addresses this

Section 3.1.12.1 b

„All resource-specific schema MUST provide a version identifier attribute which uniquely and unambiguously identifies the version of the schema being returned in the answer set to a query.“

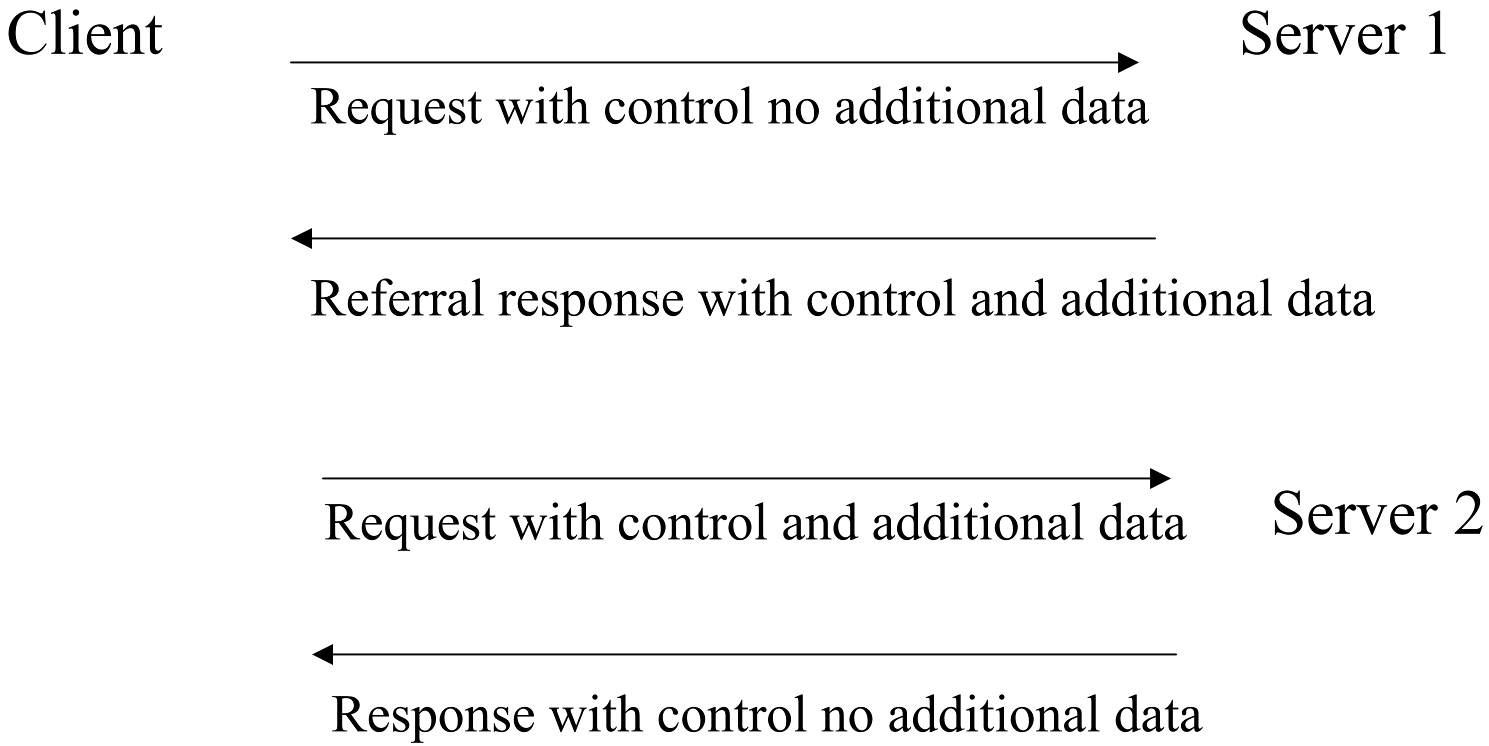
- On the schema level every schema element (like object class, or attribute type) has it‘s own OID and thus is identifiable as belonging to a specific FIRS schema version
- FIRS version support could be published by the server in the rootDSE entry
  - This is not yet specified in FIRS

Section 3.1.13.1 (relay bag)

a) „When issuing a referral, the protocol MUST be capable of supplying a relay bag from the server to the client“
b) „and the protocol MUST be capable of allowing the client to submit this relay bag with a query to the referred server.“
c) „The use of the relay bag MUST be OPTIONAL.“
d) „The protocol MUST NOT make any assumptions regarding the contents of the relay bag“
e) „but the relay bag MUST be described using the schema language of the protocol.“

- LDAP controls allow additional data to be sent in requests and responses of LDAP operations
- Has to be specified and to be implemented in clients and servers

Relay bag contd.



Client

Server 1

Request with control no additional data

Referral response with control and additional data

Request with control and additional data

Server 2

Response with control no additional data

Relay bag contd.

- More requirements not in the matrix:

„The protocol MUST provide different error messages to indicate whether the bag is of unrecognized format (permanent failure), if it contains unacceptable data (permanent failure), or if it contains data that means processing is refused at this time (transient failure).

There MUST be no more than one bag per referral. The protocol MUST NOT make an association or linkage between successive bags in a referral chain.

The client MUST pass the bag as part of any query made to a Referrant server as a result of a referral.“

Section 3.2.2.1 (IDNs)

„Domain name search given an exact match or reasonable subset of a name.“ A) „This search SHOULD allow for parameters and qualifiers designed to allow better matching of internationalized domain names“
c) „This search SHOULD NOT require special transformations of internationalized domain names to accommodate this search.“

- FIRS supports IDNs by specifying transformations as defined in RFC 2279 and RFC 3490
- Draft-hall-ldap-idn-00 specifies schema for IDNs which could be used in FIRS to directly store IDNs

Section 3.2.8.1

„When a value in an answer to a query cannot be given due to policy constraints, the protocol MUST be capable of expressing the value in one of three ways:

1. complete omission of the value without explanation
2. an indication that the value cannot be given due to insufficient authorization
3. an indication that the value cannot be given due to privacy constraints regardless of authorization status

The protocol MAY define other values for this purpose, but MUST define values defined above at a minimum.“

- Access control granularity in LDAP is on attribute level (only few implementations may have value level)
- For complete fulfilment we need another LDAP control or something like a reserved value.

Section 3.2.9 Internationalization

c) „The protocol MUST be able to support multiple representations of contact data, with these representations complying with the requirements in Section 3.2.3.“

- I think I got that wrong in the matrix
- This is doable in LDAP (language tag)

Why is LDAP a good choice?

- Well established & stable technology
- Database with integrated network protocol
- Scalable via distribution and replication
- Good authentication mechanisms
- Granular access controll mechanisms
- Very IETFish Standardization
- CRISP should be easily implementable with current LDAP implementations.

Why is XML a good choice?

- Very flexible technology
- Allowes a layered architecture:
  - Registry specific XML schema
  - Framework for defining specific registries
  - Application transport layer
- where transport layer can easily be exchanged
- XML gets a lot of support these days
- BEEP is a new transport protocol that has learned some lessons from LDAP experience

Why not take both?

- Two different worlds will exist for a long time side by side: LDAP world, XML world
- Interoperability is possible
  - NAPSTR for locating the appropriate service
  - IRIS interface on top of a FIRS server similiar to a LDAP2Web-Gateway
  - (FIRS interface on top of an IRIS server?)