10.5 Client Identification and Customised Response

The service provider may wish to identify specific clients in order to offer customised responses to requests. This might be used to deny access to all or part of the potentially available information, dependent on the requesting client.

NOTE: This is not intended to implement client authentication as a replacement for established HTTP methods such as Basic Access Authentication or Digest Access Authentication.

Example scenario: A service provider may be prepared to share more detailed Service and Programme information with a user if there is a contractual agreement between them. Once the contractual agreement has been made, the service provider provides the user with a unique api-key for any client connections they make.

If the agreement is breached, the service provider can invalidate the api-key and either deny or apply different controls to the information provided.

10.5.1 Client Presentation of API Key

The client should determine the Fully Qualified Domain Name of the SPI server by using the process defined in section 10.1.1 of the current document. If the client has stored an api-key that corresponds to that Fully Qualified Domain Name, it should provide the api key using an HTTP header:

x-radiodnsspi-api-key: [api-key]

Where [api-key] is formatted as a [field-value] as defined in section 4.2 of RFC2616.

NOTE: The api-key selection is made using the FQDN of the SPI server found by resolving the _radioepg SRV record. If the client encounters an HTTP redirect response from the SPI server, it should still present the api-key to the server to which it is redirected.

10.5.2 Service Provider Response to an API Key

The service provider may respond to the presence of an API Key string with one of four actions:

- Ignore the key and proceed as if it was not provided
- Identify the key as valid, and offer a response intended for that client
- Identify the key as invalid, and proceed as if it was not present
- Identify the key as invalid, and return a HTTP 403 Not Authorised response

The response may include varying numbers of elements and attributes, and varying content within each element, but must always be a valid document.

10.5.3 Provision of API Key from Service Provider to Client

The service provider should provide an api key in the form of a key-value pair formed of the Full Qualified Domain Name of the SPI server defined in the _radioepg SRV record and the api-key value

For example

```
epg.musicradio.com : Y1u$67|{W?A779:#4xfw8OLtX7(QvU
```

This document does not specify how the key should be requested from the Service Provider, nor how it should be transported from the service provider to the client. It also does not stipulate if each client device requires a unique key or if the same key can be used by all clients.

10.5.4 Notification of API Key availability

The Service Provider may want to advise clients that a process for acquiring an API Key exists by adding a comment element to the XML document, using the <!-- --> format

This element is not intended to be machine readable, and must be ignored by client devices. It is intended for a human to read, and make contact with the Service Provider.

10.5.5 Use of HTTPS

HTTPS is mandatory for both client and server when providing the x-radiodnsspi-api-key HTTP header.

A service provider must allow HTTPS connections on port 443 if they issue api-keys, and must also allow HTTP connections for clients that do not support api-keys.

A client must use HTTPS to contact a server if it includes the api-key in the request. If the HTTPS connection fails, it may fall back to HTTP but must not include the api-key value in that retried connection. The client must use port 443 to attempt an HTTPS connection, regardless of the port value provided in the SRV record for HTTP connections.