Client Request Access Protocol
Design Specification

v.1.2.0a September 2010

I. Introduction

This document outlines the design specification for the Client Request Access Protocol (CRAP), a proprietary network protocol used by BustiCo Software for content database searches. This document is for private internal use only; **not for public dissemination**.

The Client Request Access Protocol is used by BustiCo client applications to allow users access to content stored in BustiCo EZHaQ Database systems. This protocol specifies how a client authenticates and performs requests for data stored in the database. This robust and secure protocol provides fast data access to properly authenticated users, and supports the use of multiple BustiCo AuthSecure credential stores, allowing extensive network scalability.

II. Protocol Specification

Illustrated below is a diagram representing a possible network layout implementing the Client Request Application Protocol:

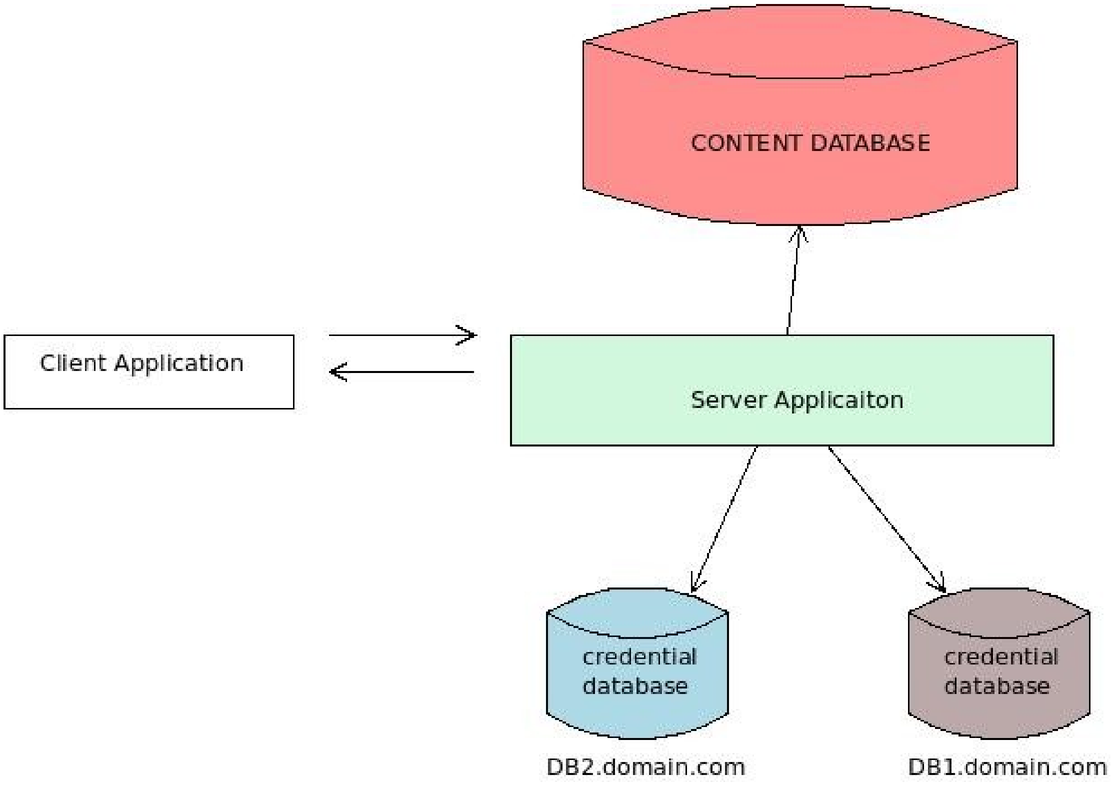

Diagram 1 – basic architecture

As can be seen above, there are several components which talk to each other. Most notably, is the client-to-server communication. Additionally it can be seen that application server talks to credential databases, as well as a content database. All communication between client and server is encrypted. Displayed below is a diagram of a request message from the client to the server:

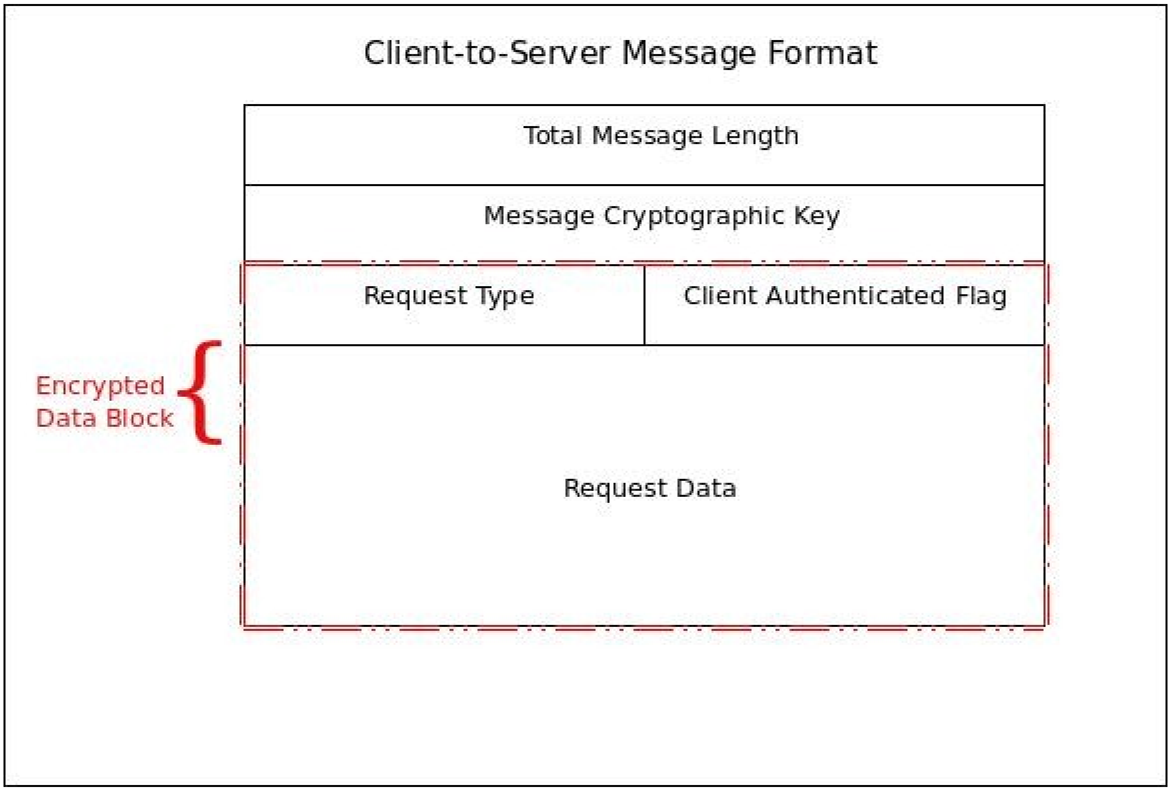
Client-to-Server Message Format
Total Message Length
Message Cryptographic Key
Request Type
Client Authenticated Flag
Encrypted Data Block
Request Data

Diagram 2 – message format

The message from client to server includes:

- message length field
- symmetric cryptographic key
- an encrypted data block

The message length field is for the server to ensure the correct amount of data was read from the network. The symmetric cryptographic key is used to decrypt the encrypted data block. This encryption is used to protect sensitive information such as user credentials which may be sent by the client.

Inside the encrypted data block is:

- request type field
- authenticated flag field
- request data

Inside the data block, the “type field” specifies one of two possible requests: authentication request, or data lookup request. The “authenticated flag” field is used to tell the server whether or not the client is already authenticated (this field is described further on in the document). If this field is not set, the user may not yet perform a data lookup request, as they must first authenticate by sending an authentication request message.

Shown below are diagrams for the two possible request types:

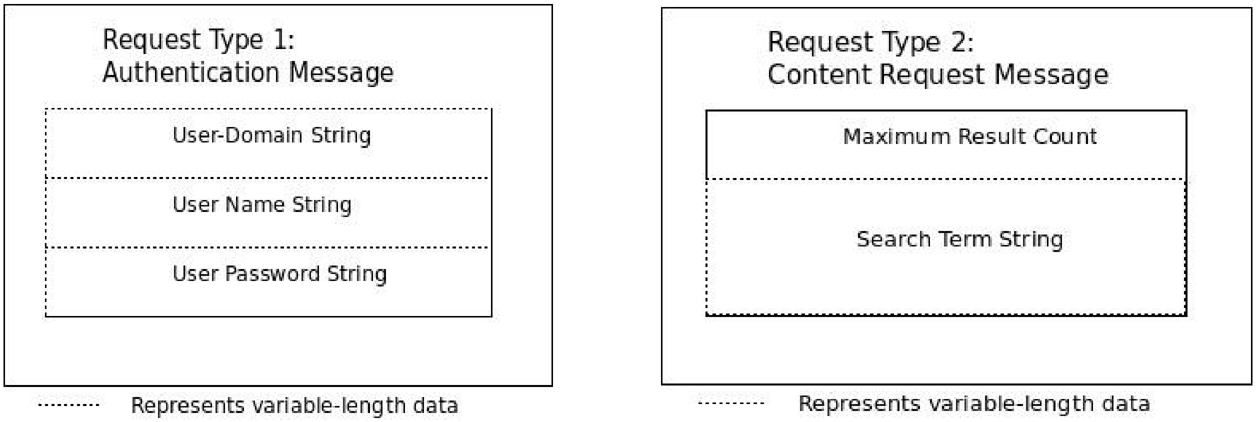

Diagram 3 – request messages

Request type 1 is an Authentication Message request. The “User-Domain” string is given to tell the application server the location of the credential database associated with the user's account. This string must be a fully qualified domain name, such as “login-storage.domain.com”. The application server then connects to the credential storage database and compares the provided user credentials (username and password) with the credentials stored in the database in order to determine if the user is allowed to authenticate.

Request type 2 is a Content Request Message. This contains a “Maximum Result Count” field, indicating the maximum number of results the server should return for any data lookup. Following this is a variable length “Search Term String”, which is a string containing the search terms for the data lookup.

After evaluating each request, the server sends a response message back to the client. This response is encapsulated in an encrypted block similar to the client request shown previously in diagram 2. Shown below are diagrams of the response messages:

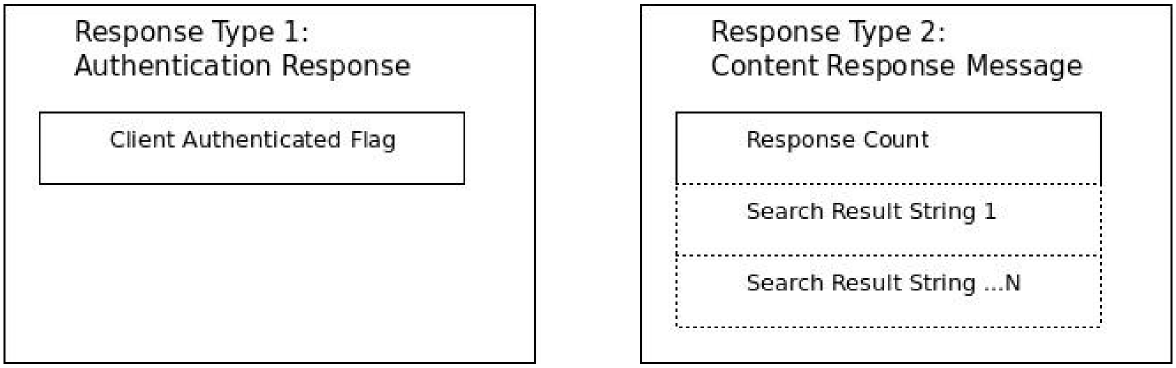

Diagram 4 – server response messages

Response type 1 is Authentication Response. This response contains only a Client Authenticated Flag. This flag is either the value 0 or the value 1. If the returned value is 0, the authentication request failed. If the value is 1, the authentication was successful, and this flag is later reused by the client for the “Client-Authenticated Flag” field in any following data lookup requests.

Response type 2 is a Content Response message. This response includes a numeric count field indicating how many results are contained in the response, which will be no more than the “Maximum Result Count” specified during the client's request. Following this is a series of strings, each string containing a matching result for the lookup request. This is what ultimately supplies the client with data from the content database system.

III. Closing Thoughts

The protocol is still in an early phase, and will require further development before being perfect, however the designers are confident in the security model behind the BustiCo EZHaQ Database system.