

Data Transport Standard: An Overview

This is a protocol specification only and must be easily implementable in Java and .Net.

Data Transport Standard is a layered protocol definition, with each higher layer building on the one below it. This provides DTS implementors with manageable segments to implement, and will make managing the implementation and maintenance easier.

| |
|--|
| Applications |
| Data Transport Standard: Guaranteed Delivery |
| Data Transport Standard: Security-Authentication & Authorization |
| Data Transport Standard: Core Transport |

DTS is based on well defined standards and common uses of those standards. This is not a definition of an abstract concept, but a definition of how to utilize a set of common and functional standards to create a secure transport mechanism. Additionally, DTS defines a set of standard behaviors for specific components that provide guaranteed delivery.

This aggregation of technologies to accomplish this task is called the DTS RoadMap. Technologies standards included in the DTS RoadMap include: HTTP, SSL, SOAP, XML, Base64 Encoding(RFC 1341 part 5.2), zLib compression(RFC 1950), LDAP, and WSDL. These technologies were chosen based on the requirements laid out by the Data Transport Business Workgroup or on the best practices experience of the EEAT.

Explanation of Technologies:

HTTP

Hyper Text Transport Protocol is the client/server TCP/IP protocol commonly used on the internet for the exchange of HTML documents. Because of the Textual/XML nature of SOAP, HTTP is also used for the exchange of SOAP messages.

SSL

Secure Sockets Layer is used to produce a secure connection over which to transmit information. The secure connection is based on "session encryption" which uses keys to transparently encrypt data as it is sent and transparently decrypt data as it is received.

SOAP

Simple Object Access Protocol is a light-weight set of conventions for invoking code using XML over HTTP.

XML

Extensible Markup Language (XML) is used with the HPCP to format the data being transmitted. Use of XML, allows for flexibility and expandability of the

data being sent - including both the business application data, and additional data useful to the transport subsystem itself, such as optional information items, message correlation identifiers, and system performance and status information. Most importantly, use of XML allows for changes to the data being sent - such as the inclusion of additional data - in the future with minimal change to the transport subsystem. All that is required to process new data is for the sender to add the data to the transmission and for the receiver to extract (parse) the new XML formatted data from the transmission and provide it to the application that will work with it.

XML uses "tags" to identify the specific type of data being sent as well as the beginning and ending of the sections of data within the larger transmission (which includes security and transport information). Tags also use "attributes" to specify the identification and characteristics of the data.

- 1) tags are case sensitive
- 2) attribute values are always quoted

Base64 (RFC 1341 part 5.2),

A file format using 64 ASCII characters to encode the six bit Binary Data values 0-63.

To convert data to base 64, the first byte is placed in the most significant eight bits of a 24-bit buffer, the next in the middle eight, and the third in the least significant eight bits. If there are fewer than three bytes to encode, the corresponding buffer bits will be zero. The buffer is then used, six bits at a time, most significant first, as indices into the string "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/" and the indicated character output. If there were only one or two input bytes, the output is padded with two or one "=" characters respectively. This prevents extra bits being added to the reconstructed data. The process then repeats on the remaining input data.

Base 64 is used when transmitting binary data through text-only media such as electronic mail.