Qpid Interoperability Documentation

Qpid Interoperability Documentation

This page documents the various interoperable features of the Qpid clients.

SASL

Standard Mechanisms

SASL Mechanisms

This table list the various SASL mechanisms that each component supports. The version listed shows when this functionality was added to the product.

Component	ANONYMOUS	CRAM-MD5	DIGEST-MD5	EXTERNAL	GSSAPI /Kerberos	PLAIN
C++ Broker	M3[#1]	M3[#1,#2]			M3[#1,#2]	M1
C++ Client	M3[#1]					M1
Java Broker		M1				M1
Java Client		M1				M1
.Net Client	M2	M2	M2	M2		M2
Python Client						?
Ruby Client						?

1: Support for these will be in M3 (currently available on trunk).

2: C++ Broker uses Cyrus Sasl which supports CRAM-MD5 and GSSAPI but these have not been tested yet

Custom Mechanisms

There have been some custom mechanisms added to our implementations.

Component	AMQPLAIN	CRAM-MD5-HASHED
C++ Broker		
C++ Client		
Java Broker	M1	M2
Java Client	M1	M2
.Net Client		
Python Client	M2	
Ruby Client	M2	

AMQPLAIN

CRAM-MD5-HASHED

The Java SASL implementations require that you have the password of the user to validate the incoming request. This then means that the user's password must be stored on disk. For this to be secure either the broker must encrypt the password file or the need for the password being stored must be removed.

The CRAM-MD5-HASHED SASL plugin removes the need for the plain text password to be stored on disk. The mechanism defers all functionality to the build in CRAM-MD5 module the only change is on the client side where it generates the hash of the password and uses that value as the password. This means that the Java Broker only need store the password hash on the file system. While a one way hash is not very secure compared to other forms of encryption in environments where the having the password in plain text is unacceptable this will provide and additional layer to protect the password. In particular this offers some protection where the same password may be shared amongst many systems. It offers no real extra protection against attacks on the broker (the secret is now the hash rather than the password).