class Auth::SCRAM

Authentication using SCRAM

Table of Contents

```
unit package Auth;
class SCRAM { ... }
```

Synopsis

```
class MyClient {

  method client-first ( Str:D $client-first-message --> Str ) {

    # Send $client-first-message to server;

    # Return server response as server first message
  }

  method client-final ( Str:D $client-final-message --> Str ) {

    # Send $client-final-message to server.

    # Return server response as server final message
  }

  method error ( Str:D $message --> Str ) {
    # Errors? nah ... (Famous last words!)
  }
}

my Auth::SCRAM $sc .= new(
  :username<user>,
  :password<pencil>,
  :client-side(MyClient.new),
);

$sc.skip-sasl-prep(:skip);
my Str $error = $sc.start-scram;
```

While a client authentication is shown above Auth::SCRAM itself does not do any of this. The user of the Auth::SCRAM class provides a client-side or a server-side object with which the initialization phase will upgrade the object to a Auth::SCRAM object with a Auth::SCRAM::Client or

Auth::SCRAM::Server role.

Specific details are shown in the pods for these role modules.

Methods

Auth::SCRAM has some methods which are mostly used by the client or server roles and have not much use by the caller directly and are therefore not explained.

new

Defined as

```
submethod BUILD (
  Str :$username,
  Str :$password,
  Str :$authzid,

  Callable :$CGH = &sha1,
  :$client-side,
  :$server-side,
)
```

Initialize the process. The Cryptographic Hash function $CGH is by default set to SHA1. The authorization id($authzid) is needed when you want things done with the privileges of someone else. The client-side and server-side are objects with methods called by the SCRAM methods. Only one of the client or server objects can be defined.

skip-sasl-prep

Defined as

```
method skip-sasl-prep ( Bool:D :$skip )
```

Call this before starting authentication with start-scram. start-scram is explained in the other modules. The username, authorization id and password must be processed before authention is started. When old fashion ASCII letters and digits are used, no conversion is needed but it is when utf characters are used. The preparation is performed by default.