## Environment

**Client**

The “user with end system” who wants to obtain extra services from the IdP. It sends data to the Radius proxy which forwards it to the IdP.

**Radius proxy**

The “middleman” who obtains data from the client and forwards it to the IdP and vice versa. The Radius proxy is able to “inject” additional information when requested by the IdP to the data which have to be forwarded.

**IdP**

The “end point” which receives authentication requests from the client encrypted and forwarded by the Radius proxy. It validates and approves the request from the client and request if necessary additional information from the Radius proxy to be sends to the client.

## Supported Algorithms

**Encryption**

The IdP will send messages encrypted with RSA to the Radius proxy. The Radius proxy will respond by signing the message with RSA and send the message to the client.

**Hashing**

The Radius proxy will hash the message received from the IdP with RSA and send the message encrypted to the client.

**Encoding**

The mime body’s will be encoded Base64, the headers will be constructed with US ASCI.

**Certificate format**

For the certificate formats the PKCS#7 format will be used according to the SMIME standard.