The described sequence will run from Client to RadiusProxy to IdentityProvider and back. The Client wants to connect to the IdentityProvider, and this will happen via the RadiusProxy. The Client will send an AccessRequest, coupled with a request for additional information inside the inner-tunnel. The RadiusProxy will inject its certificate in the AccessRequest’s outer-tunnel. The IdentityProvider will perform a check to see if the received certificate is legit, and if the inner-tunnel contains a request for additional information. If this is the case, an encrypted request will be added to the regular answer as an Attribute Value Pair back to the RadiusProxy. The RadiusProxy will in turn perform a check to see if this is the right Attribute Value Pair, and if the IdentityProvider accepted the credentials (if the answer is Reject or Challenge, the sequence will continue without any more intervention from our Radius Module, until the returned answer is Accept). If this is the case, the Attribute Value Pair will be decrypted, and the requested attributes injected in the answer. This answer, plus the encrypted requested attributes, are then sent back to the Client.