Atbash Key Server

Rudy De Busscher

Version 0.5, 09/01/2019

Table of Contents

Release notes

0.5

Initial release - POC

Content

Code related to using the Diffie Hellman Algorithm.

- impl\diffieHellman
  Code related to creating a shared symmetric Key from Public/private Key pairs. see **be.atbash.keys.diffiehellman.DHKeyExchangeManager**

- impl\keymanager-sign
  Code for exchanging/creating keys behind the scene.
  be.atbash.keys.manager.sign.ProxyKeyManager which caches a Key from the Key Server for a certain time.
  be.atbash.keys.manager.sign.KeyRequester Retrieves a Key fro mthe server using the Diffie Hellman Algortihm
  ...

- examples
  app1 retrieves a private Key from the Key server (encrypted with a symmetric Key) and pass a signed message to app2. App2 retrieves the public key from the Key Server.

In future releases important changes in classes and project structure can occur.