Sistemas de Elevada Confiabilidade

Projecto - parte 2

Suporte de autenticação de smart card no sistema de ficheiros

Pedro Miguel Isaac Correia de Castro, nº58384
Ricardo Ângelo Costa Maia, nº70252
Luís Filipe Pookatham Ribeiro Gomes, nº72904

Novas funcionalidades no sistema de ficheiros

No projecto anterior era gerado um par de chaves públicas e privadas para assinar documentos e garantir desta forma integridade dos mesmos. Neste projecto, para criarmos um processo de autenticação, usámos a tecnologia do cartão de cidadão da república portuguesa. Assim criámos uma biblioteca chamada *CC_Auth* que permite retornar a chave pública do certificado do cartão, assinar documentos com o *PIN* de autenticação e validar assinaturas de documentos previamente assinados.

Para integrar uma fácil integração dos mecanismos de autenticação, criámos uma interface chamada IAuth que tem os métodos para obter a chave pública, assinar documentos e validar documentos e é implementada pelo *CC_Auth*. A biblioteca cliente (*FileSystem e FileSystemClient*) usa então os métodos do IAuth para autenticar e assinar documentos.

Para registar novos clientes criámos uma key store no *FileSystemServer*. O cliente comunica ao *FileSystemServer* o seu certificado (em *bytes*), que é retirado do cartão de cidadão, através da invocação remota do método *storePubKey* no método *FS_Init* da biblioteca do cliente. O *FileSystemServer* ao receber o pedido *storePubKey*, vai verificar se o certificado já foi previamente adicionado à java keyStore e caso contrário adiciona. Foi também criado o método remoto *readPubKeys* no *FileSystemServer* para retornar ao cliente todas as chaves públicas dos clientes registados no sistema. Este método é invocado pela biblioteca do cliente no método *FS_List*. O cliente agora pode fazer pedidos de leitura dos ficheiros de outros clientes, enviando a chave pública do cliente que tem direitos de escrita sobre o ficheiro pretendido.

Considerações sobre segurança

A autenticação no sistema é garantida pela confiabilidade dos certificados e chaves do cartão de cidadão. Para assegurarmos essa confiabilidade, verificamos a entidade que assinou o certificado de autenticação do cartão do cidadão com o certificado descarregado do portal oficial do cartão. Depois de verificarmos a origem do certificado de autenticação então validamos a chave pública do mesmo para termos a certeza que a chave ainda é válida e que não expirou.

A assinatura usada para assinar os documentos é do tipo *SHA-1* com *RSA* e é gerada através de funcionalidades da biblioteca *pteidlib* que usa a chave privada do cartão que é desbloqueada pela introdução do *PIN* de autenticação do cartão. Para validar esta assinatura é usado a chave pública do certificado de autenticação, com a qual é gerada uma nova assinatura que é usada para validar a assinatura que assinou os dados enviados. Desta forma conseguimos continuar a assegurar integridade dos dados porque se os dados forem perdidos ou modificados então a verificação da assinatura vai falhar.

Nos métodos FS_init, FS_write e FS_read fazemos a verificação dos argumentos, verificando se não existem argumentos a nulo (métodos *CheckFileSystemClientNullability*, *checkFileSystemClientNonNullability*, *checkArgumentsNonNullability* e *checkContentSize*).

Keystore