SAS - ESPECIFICAÇÃO PARA DOCUMENTO ASSINADO

Existem padrões para o armazenamento de mensagens assinadas, tal como o PKCS#7 (RSA), assim como padrões para documentos assinados, tal como o PAdES – Padrão Brasileiro de Assinatura Digital (DOC-ICP-15.X). Porém, por simplificação, será especificado um formato básico, contendo as características mínimas de um documento assinado.

Deve ser produzido um arquivo de extensão .txt cujo conteúdo contém apenas caracteres imprimíveis e que pode ser aberto por editores de texto comuns.

Especificação do documento

As linhas abaixo devem ser inseridas no documento exatamente como estão, substituindo apenas as partes delimitadas por < >, onde deve conter a informação ou orientação correspondente.

-----BEGIN DOCSIGNED-----
doc:<nome do documento com extensão para ser extraído e salvo, por exemplo teste.pdf>
alg:RSA
hash:SHA1
assinante:<campo CN do certificado para localização do certificado do assinante e verificação da assinatura>
<pule uma linha>
-----BEGIN DOC-----
<bytes do documento no formato BASE64, ver classe no package útil>
-----END DOC-----
-----BEGIN SIGNATURE-----
<bytes da assinatura no formato BASE64, ver classe no package útil>
-----END SIGNATURE-----
-----END DOCSIGNED-----

Atividade

Deve ser implementado dois códigos (preferencialmente em Java ou C) separados:

1. Código que produza um documento assinado no formato especificado acima.

   O código entregue deve ter como entrada o **nome do documento a ser assinado** e o **nome de um arquivo do tipo PKCS#12**, o qual contém a chave privada e certificado do assinante.

2. Código que verifique a assinatura de um documento no formato acima, extraia o documento e salve-o com o nome definido. A saída deve indicar “Documento íntegro e assinado por XXX” caso tenha sucesso, ou informação de erro, caso contrário.

   O código entregue deve ter como entrada o **nome do documento assinado** e o **nome de um arquivo do tipo .crt**, o qual contém os bytes do certificado do tipo X509.

Foi fornecido um arquivo modelo (DocSignedTeste.txt) gerado a partir das chaves em SAS_Yeda.p12, cuja senha é “Seguranca”, e o documento DocTeste.txt. Também foi fornecido um arquivo contendo o certificado no formato .crt para a verificação da assinatura. O certificado também está armazenado no keystore (p12) junto com a chave privada.

Entrega

Grupo: 2 alunos
Data: 14/01/2021
Conteúdo: código fonte, executável (ou jar), documento com orientações de execução (se necessário) e um arquivo assinado gerado com o certificado de um dos membros do grupo. O documento assinado deve ser um txt pequeno cujo conteúdo contenha o nome dos membros do grupo.