MULTICERT
Serviços de Certificação Electrónica, S.A.

Ano Lectivo 2006/2007
Proposta de Projecto
Opção III (LESI)

Assinatura Digital Avançada de Documentos XML

Desde a sua normalização pelo W3C, a linguagem XML tem vindo a ser adoptada por um número crescente de produtores de software como formato base para os documentos[1] utilizados pelas aplicações que desenvolvem.

O crescendo de utilização de documentos neste formato revelou o interesse em definir mecanismos que lhes permitissem aportar as características de segurança (origem, não-repúdio e integridade) adequadas a cenários de utilização mais exigentes. Para colmatar essa lacuna, o W3C definiu posteriormente a norma XMLDSIG[2].

Contudo, na sequência de imposições legislativas emanadas pela UE (nomeadamente através da directiva 1999/93/EC), surgiu a necessidade de uma norma que permitisse o armazenamento de assinaturas digitais ao longo de grandes períodos de tempo sem que pudesse ser questionada a sua validade[3], possibilitando a sua utilização para arbitragem de disputas entre assinante e verificador que, eventualmente, venham a ter lugar vários anos após a criação da referida assinatura digital. Nesse sentido, foi publicada a norma XAdES[4], com o objectivo de proporcionar o enquadramento necessário.

Objectivo:

Com este projecto pretende-se, aproveitando a experiência da **MULTICERT** na utilização de criptografia de chave pública e de assinatura de documentos **XML**, desenvolver uma aplicação em **Java** capaz de criar e validar assinaturas digitais avançadas no formato **XAdES**.

Considerandos:

- Em caso de dúvidas na implementação do projecto será possível ter o apoio de colaboradores da **MULTICERT** com vasta experiência em **Java** e na assinatura digital de documentos XML **(XMLDSIG)**

---

[1] Sejam estes mensagens, ficheiros de configuração, etc
[2] http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/
[3] Como cada assinatura digital se encontra associada a um certificado digital (que possui um determinado período de validade) é necessário comprovar se a assinatura digital foi gerada durante o período de validade do respectivo certificado
[4] http://www.w3.org/TR/2003/NOTE-XAdES-20030220/ e http://www.iaik.tu-graz.ac.at/teaching/11_diplomarbeiten/archive/mcentner.pdf

Notas:

1. A plataforma preferencial para testes e funcionamento é **Java**
2. A **MULTICERT** pretende adaptar e utilizar os resultados deste projecto.

Acompanhamento:

Este projecto será acompanhado tecnicamente por um elemento do DIUM e por um elemento da MULTICERT, a designar. O acompanhamento será efectuado através de ajuda na concretização do trabalho, assim como através de reuniões com periodicidade mensal (embora possa haver fases do projecto em que a periodicidade seja quinzenal).