(UFG) Universidade Federal de Goiás
Aluno: Geovane Alves de Oliveira
Curso: Engenharia de Software
Disciplina: Desenvolvimento de Software para Web

# Relatório Assinatura Digital de Arquivo

Este trabalho tinha como proposito criar uma página usando html, javascript e css, por meio da qual se seleciona um documento e ao pressionar o botão correspondente o mesmo é assinado digitalmente. Nela também deveria conter a checagem da assinatura, onde um documento seria carregado e ao pressionar o botão correspondente, seria verificada se a assinatura corresponde a do documento assinado inicialmente.

Para o desenvolvimento do trabalho utilizei a IDE NetBeans 8.0 a qual possui suporte a html 5, pois é uma IDE que já trabalho a algum tempo e já tenho uma maior facilidade, além de ser bem conhecida e usada por muitos desenvolvedores, facilitando assim a busca por tutorias e páginas de suporte quando surgem duvidas relacionadas a utilização de algum dos seus recursos.

Para a criação desta página tive que fazer muitas pesquisas em diversos sites, mais teve dois que se destacaram, o primeiro foi o http://kjur.github.io/jsrsasign/, site fundamental para a criação da estrutura da página, pois nos DEMOS encontrados nele tem um (Sample Application for RSA signing in JavaScript) que era praticamente o que estava sendo pedido no trabalho, precisava apenas de algumas modificações, pois nele a assinatura era de texto e não de arquivo e a sua estrutura era um pouco confusa. O segundo foi o http://www.html5rocks.com/pt/tutorials/file/dndfiles/ , um tutorial que mostra exatamente o que deve ser feito para transformar um arquivo em uma sequência binária / string para que a mesma seja assinada, esta é uma particularidade do javascript. No código abaixo é mostrado como fazer isso:

```
$(document).ready(function(){

	priv_key = $("#priv_key").val();

	if(window.File && window.FileReader && window.FileList && window.Blob)
	{
		$("input[name='doc']").bind("change", function(evt){

			var files = evt.target.files;

			for(var i=0, f; i<files.length; ++i)
			{
				f = files[i];
				var reader = new FileReader();

				reader.onload = (function(theFile){
					return function(e)
					{
```

```
                    text = reader.result;
                    alert("Documento carregado!");
                };
            })(f);

            reader.onloadstart = (function(theFile){
                return function(e)
                {
                    text = undefined;

                };
            })(f);

            reader.onabort = (function(theFile){
                return function(e)
                {
                    text = undefined;
                    alert("Erro ao ler documento!");
                };
            })(f);

            reader.onerror = (function(theFile){
                return function(e)
                {
                    text = undefined;
                    alert("Erro ao ler documento!");
                };
            })(f);

            reader.readAsBinaryString(f); /*a propriedade result conterá os dados do arquivo/blob como uma sequência binária. */
        }
    });
```

## Referências:


http://kjur.github.io/jsrsasign/
http://www.html5rocks.com/pt/tutorials/file/dndfiles/