Anexo III

Procedimentos para obter o código *hash*

A função criptográfica *hash* é um algoritmo utilizado para garantir a integridade de um documento eletrônico, de modo que, um perito técnico possa comprovar que não houve alteração neste documento desde a época em que este foi transformado. Assim, uma simples alteração neste documento acarretará em uma alteração do resumo *hash* original, desconstituindo assim a prova de integridade do depósito do programa de computador.

Para realizar o pedido de registro de programa de computador é necessário promover a transformação, em resumo digital *hash*, dos trechos do programa de computador e de outros dados que considerar suficientes e relevantes para identificá-lo, ficando a responsabilidade da guarda do *objeto* com o titular do direito (UFSM) e o autor responsável pelo pedido junto à AGITTEC, pois esta é a propriedade intelectual que pertence a este e deve ser preservada na sua forma original e em ambiente seguro.

A apresentação da informação do resumo *hash* no formulário, no ato do pedido de registro, garantirá que o objeto não foi alterado ao longo do tempo desta guarda. Esta documentação técnica é fundamental para caracterizar a originalidade do programa de computador junto ao Poder Judiciário, quando for o caso.

IMPORTANTE

O *hash* de uma prova eletrônica pode ser obtido através de um único arquivo de entrada (PDF, TXT, etc.) ou de vários arquivos, todos "zipados" (.zip ou .rar), a ser(em) transformado(s) em um único resumo digital *hash* (texto de comprimento fixo) de saída. É fundamental que este resumo digital *hash* gerado possa ser

* e-RPC - Registro Eletrônico de Programa de Computador
13 http://www.bouncycastle.org/

conferido com o resumo digital *hash* a ser gerado pelo perito do juiz (em caso de processo judicial de comprovação de autoria/titularidade, por exemplo) tendo como base o código-fonte guardado em sigilo pelo titular do direito.

A geração do resumo digital *hash* a partir da documentação técnica (código-fonte) pode se dar tanto sobre um único arquivo de entrada (PDF, DOC, TXT, etc), como sobre uma coletânea de arquivos compactados em um único arquivo ZIP ou RAR. Em qualquer um dos casos, é de vital importância que este mesmo arquivo utilizado para gerar o *hash* seja mantido íntegro pelo interessado, preferencialmente em mais de um meio digital de armazenamento (*backup*).

A transformação do programa de computador em resumo digital *hash* será feita pelo autor do programa de computador, utilizando algoritmos públicos *hash* e esta informação irá compor o formulário eletrônico e-RPC* quando do pedido de registro. Recomenda-se o uso de algoritmo **SHA-512** ou algoritmo mais recente para a obtenção do resumo digital *hash*.

1- Na internet, podem ser encontrados artigos e sites dedicados à explicação e uso de tais algoritmos, por exemplo, "MD5", "SHA-1", "SHA-224", "SHA-256", "SHA-512", etc. Existem bibliotecas na internet, como a "*BouncyCastle*[13]", por exemplo, que disponibilizam este recurso.

Alguns destes algoritmos também são encontrados em ambiente Linux. Por exemplo, para rodar o algoritmo **SHA-512** no Linux, basta executar a seguinte linha de comando:

```
sha512sum nome_do_arquivo
```

Substitua a expressão nome_do_arquivo pelo nome do arquivo de origem, incluindo a extensão (ex.: código_fonte.pdf).

2- Outra possibilidade para gerar o *hash* é utilizando um comando nativo do **Microsoft Windows**. Para o Windows 7, siga os passos abaixo:

1) Copie o arquivo a partir do qual deseja gerar o resumo hash para a Área de Trabalho -(Desktop);

* e-RPC - Registro Eletrônico de Programa de Computador
13 http://www.bouncycastle.org/

2) Clique no botão “Iniciar” no canto inferior esquerdo da tela;

3) No campo de pesquisa, digite a palavra “cmd” e tecle “Enter”;

4) Na janela aberta (Prompt de comando), digite o seguinte comando: `cd Desktop`

5) Tecle “Enter”;

6) Insira, agora, a linha de comando abaixo:

```
CertUtil -hashfile nome SHA512 | find /i /v "sha512" | find
/i /v "certutil" > temp.txt
```

Substitua a palavra nome pelo nome do arquivo de origem, incluindo a extensão (ex.:código_fonte.pdf), e tecle “Enter”;

7) Por fim, copie e cole no prompt de comando as linhas abaixo:

```
powershell -Command "(gc temp.txt) -replace ' ', '' | Out-
File resumo_hash.txt"

taskkill /IM notepad.exe
```

8) Abra o arquivo-texto gerado na Área de Trabalho (Desktop), nomeado “resumo_hash.txt”. O resumo hash contido neste arquivo é exatamente o trecho que deve ser copiado e colado no formulário *e-RPC.

Cabe ressaltar que as opções apresentadas acima devem ser avaliadas pelos autores, a fim de escolher a opção considerada mais adequada.

Os autores devem armazenar o código-fonte ou objeto em qualquer meio de sua confiança e segurança (CD-ROM, DVD, Hard Disk, na nuvem, em pendrive) e guardá-lo por cinquenta anos, já que a validade do direito é de 50 anos a partir do dia 1° de janeiro do ano subsequente à sua publicação ou, na ausência desta, da sua criação.

* e-RPC - Registro Eletrônico de Programa de Computador
13 http://www.bouncycastle.org/

O resumo *hash* é um texto de tamanho fixo e deve conter apenas informação numérica na base hexadecimal (números de 0 a 9 e letras de A até F). Na tabela 1, são apresentados exemplos de resumo digital *hash* (texto de saída) do arquivo PDF disponível em https://goo.gl/e7WkNV

Função	**Resumo hash**
SHA-512	D4956a6bb548d996fa245318e150944a8789b3e10034d1d2325986ef03e3a40bb269d52caa1c18cce67ccc40 b5f3193cc0aac2813313163a9022694a4ec6dcea

Tabela 1 - Exemplo de resumos *hash* do arquivo PDF disponível em https://goo.gl/e7WkNV

Informações: 79 3194-7082 ou através do e-mail: cinttec.ufs.@gmail.com

* e-RPC - Registro Eletrônico de Programa de Computador
13 http://www.bouncycastle.org/