IUESO – INSTITUTO UNIFICADO DE ENSINO SUPERIOR OBJETIVO

ALUNOS: JEAN BRUNO SOUTO VILLETE – 452345-8

PROFESSOR: DAVY

MATÉRIA: ORIENTAÇÃO TCC

**Objetivo deste documento: Definição do Tema, Objetivo, Roteiro e Cronograma de Desenvolvimento do TCC.**

**Tema**: Certificação Digital

**Objetivo**: Após a segunda guerra mundial, a tecnologia do computador extrapolou os limites do uso militar, e começou uma expansão pelas instituições públicas e privadas dos países do capitalismo central. No início eram máquinas difíceis de serem manuseadas, e só especialistas é que tinham esta honra. Os anos de 1980 trouxeram duas grandes novidades; os computadores pessoais e as redes de trabalho; As redes evoluíram rapidamente e de forma a espantosa de pequenas redes locais (Local Area Network-LAN) para redes metropolitanas (Metropolitan Area Network-MAN) até chegar a uma nuvem que ***interliga*** todas as redes, recebendo o nome de Internet, a grande rede mundial de computadores.

O avanço da Tecnologia da Informação e Comunicação (TIC), ocorrido a partir dos anos de 1990 mudou radicalmente os mecanismos de registro e de comunicação da informação nas instituições públicas e privadas. Os documentos gerados no decorrer das atividades dessas instituições, até então em meio convencional, assumem novas características, isto é, passam a ser gerados em ambientes eletrônicos, armazenados em suportes magnéticos e ópticos, em formato digital, e deixam de ser apenas entidades físicas para se tornarem entidades lógicas.

Dado um ambiente sem limites geográficos e facilidade em criar e tramitar mensagens e informações, nasce também uma outra necessidade, a Certificação Digital, onde através desta é possível garantir a segurança das informações que tramitam no vasto mundo Digital. A Internet faz uso de certificação digital, garantindo que determinado site que está sendo visitado é seguro, as mais diversas empresas que precisam tramitar informações sigilosas fazem uso da certificação digital.

Diante deste ambiente, este trabalho vem apresentar a história da certificação digital, a regulamentação dos diferentes países que a adotam, a infra-estrutura necessária e existente por detrás desta tecnologia, o Brasil e a ICPBrasil (Infra-Estrutura de chaves públicas brasileiras), chaves públicas e chaves privadas, cadeias de certificações, a necessidade e os tipos disponíveis de criptografia das mensagens, os mais diversos e atuais suportes e dispositivos de certificação de uma mensagem, a necessidade da popularidade desta tecnologia, a camada segura do protocolo Http (SSL, troca de informações pela web), enfim, o mundo que a Certificação Digital abrange. Adicionalmente uma API para certificação digital será desenvolvida, e uma simples aplicação mostrando a utilização desta API. Atualmente o desenvolvimento de aplicativos com a utilização da certificação digital são onerosos e caros, isto por que empresas que desenvolvem soluções para certificação digital cobram altos valores por suas poderosas APIs. Este trabalho tem o objetivo de fazer com que tal API desenvolvida aqui seja continuada por desenvolvedores da comunidade livre, por tanto um projeto open-source será criado e disponibilizado, tanto o binário quanto o fonte.

A API será desenvolvida fazendo utilização da linguagem Java pela sua robustez e portabilidade, tanto para web quanto para aplicativos desktop. A API aqui desenvolvida é a continuidade de um trabalho do Mestre em Ciências da Computação Nakov ([www.nakov.com](http://www.nakov.com)), um búlgaro que desenvolveu o uma simples API para apresentar a certificação digital e assinaturas digitais de documentos. O objetivo é dar continuidade ao trabalho, no que ficou faltando, e lançar o projeto para comunidade livre para o aperfeiçoamento desta API. O texto da monografia será desenvolvido de acordo com que as etapas do roteiro são desenvolvidas e/ou alcançadas.

**Roteiro**:

1-Estudo e captação de informação da história da Certificação Digital;

2-Captação de informação da normas técnicas práticas e legais (livro Assinatura Digital, aspecto técnicos, práticos e legais. De: Volpi, Marlon Marcelo)

3-Captação e conceitos básicos de chaves públicas, privadas, cadeias de certificações, requisitos da API para Assinaturas digitais (Artigo Nakov, <http://www.nakov.com/documents-signing/docs/Digital-Document-Signing-in-Java-based-Web-Applications-En.html>)

4-Documentar requisitos implementados e não implementados por Nakov.

5-Desenvolvimento de um desenho UML mostrando os principais componentes da API.

6-Implementar requisitos ainda não implementados por Nakov.

7-Implementar uma pequena aplicação “X”para apresentar a API em utilização. Possivelmente, esta aplicação estará dentro de padrões de projetos como, por exemplo, o MVC.

8-Alocar um espaço na internet para o lançamento do projeto open-source para comunidade livre.

**Nota**:

Quanto ao desenrolar do trabalho escrito (monografia) é válido notar que boa parte da mesma estará sendo desenvolvida enquanto cada etapa (item/marco) do roteiro é concluído.

**Cronograma**:

Obs.: É de suma importância que o trabalho seja concluído no mês Setembro, tanto aplicação implementada quanto o trabalho escrito (monografia). O motivo é que “o todo” deve ser entregue em Novembro, logo dentro deste prazo de dois meses, a aplicação será submetida a testes e aperfeiçoamento, e o trabalho escrito será colocado em revisão de texto, normas técnicas ABNT, etc.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Atividade | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Março | Abril | Maio | Junho | Julho | Agosto | Setembro | |
|  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | |
| 1 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
| 2 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
| 3 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
| 4 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
| 5 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
| 6 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
| 7 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
| 8 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |