UNIVERSIDADE FEDERAL DE SANTA CATARINA
GABINETE DA REITORIA
Campus Universitário Reitor João David Ferreira Lima - Trindade
CEP: 88040-900 - Florianópolis - SC
Telefone: (48) 3721-9320 - Fax: (48) 3721-8422
E-mail: gr@contato.ufsc.br

TED 02 fls 15

Ofício nº 999 /2015/GR

Florianópolis, 18 de dezembro de 2015.

Ao Senhor
Ruy César Ramos Filho
Assessor Técnico do Instituto Nacional de Tecnologia da Informação – ITI
SSCN, Quadra 02, Bloco E – Edifício-sede ITI
70712-905 – Brasília – DF

Assunto: **Encaminhamento de documentos referente ao projeto "Suporte e Avaliação de Adequabilidade Tecnológica dos Sistemas de Gerenciamento de Certificados Digitais Ywapa e Ywyra"**

Senhor Assessor,

1. Encaminhamos o Termo de Execução Descentralizada (TED nº 02/2015), o Termo de Referência e o Plano de Trabalho referentes ao projeto "Suporte e Avaliação de Adequabilidade Tecnológica dos Sistemas de Gerenciamento de Certificados Digitais Ywapa e Ywyra".

2. A celebração desse Termo é de grande importância, visto que o Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina (UFSC) tem grande interesse em realizar o suporte e a avaliação de adequabilidade tecnológica dos Sistemas de Gerenciamento de Certificados Digitais, Ywapa e Ywyra, de propriedade do ITI.

3. A proposta do presente Plano de Trabalho e do referido TED compreende o valor total de recursos de R$ 128.400,00 (cento e vinte e oito mil e quatrocentos reais) para utilização em auxílio financeiro a estudantes no período de 27 de novembro de 2015 a 26 de novembro de 2016.

4. Colocamo-nos à disposição para quaisquer esclarecimentos adicionais, salientando que o projeto está sob a Coordenação do Prof. Ricardo Felipe Custódio, que pode ser contado pelo *e-mail* ricardo.custodio@ufsc.br ou pelos telefones (48) 3721-7546 e (48) 3721-6369.

Atenciosamente,

PROFª ROSELANE NECKEL
Reitora

Universidade Federal de Santa Catarina

PLANO DE TRABALHO

1 - OBJETO

1.1 Suporte e Avaliação de Adequabilidade Tecnológica dos Sistemas de Gerenciamento de Certificados Digitais Ywapa e Ywyra.

2 - JUSTIFICATIVA

2.1 O presente Termo de Execução Descentralizada apresenta uma proposta de manutenção e de estudos de diversas melhorias dos Sistemas de Gerenciamento de Certificados Digitais ICP-Brasil, chamados Ywapa e Ywyra. Essa proposta foi feita pelo Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina (UFSC) que foi responsável pelo desenvolvimento das versões atualmente em produção desses softwares. O conteúdo deste documento foi elaborado a partir de uma profunda análise do estado atual desses sistemas e tem como principal objetivo o suporte, o estudo das melhorias e atualizações nos softwares de forma que eles possam continuar sendo utilizados e se mantenham condizentes com as necessidades e novos requisitos da ICP-Brasil.

2.2 O LabSEC tem sido reconhecido como um dos maiores centros de pesquisa científica e tecnológica na área de certificação digital no país. Desde a sua criação em 1999, já foram desenvolvidos mais de 150 trabalhos de conclusão de curso de graduação, dissertações de mestrado e teses de doutorado em infraestrutura de chaves públicas e suas aplicações. Foram mais de 50 artigos científicos publicados nos mais renomados eventos e periódicos científicos, nacionais e internacionais. O LabSEC tem participado dos dois maiores esforços acadêmicos em atividade relacionados ao desenvolvimento de tecnologia nacional para a gestão do ciclo de vida de chaves criptográficas: projetos ICPEDU com finalidade de pesquisa e ensino e o João de Barro.

2.3 Para o projeto Infraestrutura de Chaves Públicas para Pesquisa e Ensino (ICPEDU) da Rede Nacional de Ensino e Pesquisa (RNP), desenvolveu e mantém um sistema acadêmico aberto de gerenciamento de certificados digitais e o software para a gestão de chaves criptográficas para módulo

de segurança criptográfica (ASIHSM). A solução desenvolvida está sendo usada por mais de 20 universidades de todo o país na implantação de um infraestrutura para fins de pesquisa e ensino em certificação digital.

2.4 O Programa João de Barro foi a iniciativa que possibilitou o desenvolvimento do Sistema de Gerenciamento do Ciclo de Vida de Certificados Digitais tanto para a Autoridade Certificadora Raiz Brasileira quanto para autoridades certificadoras intermediarias off-line. Nesse âmbito também foi desenvolvido o software para emissão de certificados digitais à usuários finais conhecido como Hawa. Estes sistemas estão hoje em uso por várias autoridades certificadoras no âmbito da Infraestrutura de Chaves Públicas Brasileira.

2.5 O laboratório tem grande interesse em dar continuidade nas atividades suporte e estudos de aprimoramento dos softwares Ywapa e Ywyra. O interesse justifica-se tanto do ponto de vista da extensão universitária, quanto da pesquisa e do ensino. A extensão universitária é uma forma de aproximar a universidade da sociedade, dando oportunidade ao corpo discente e docente em aprender com um caso real, apesar de complexo, mas de extrema relevância para o entendimento da ciência e tecnologia da certificação digital. Há desafios tecnológicos interessantes, não só de aplicação da tecnologia da criptografia, mas também de engenharia de software, que propiciam aos alunos e professores uma experiência muito rica. No âmbito do ensino o projeto também visa a formação de recursos humanos capacitados em certificação digital.

2.6 Os softwares Ywapa e Ywyra já vem sendo utilizados por Autoridades Certificadoras dentro do escopo da ICP-Brasil de forma muito bem sucedida. Fruto de etapas anteriores do projeto, a ICP-Brasil conta nestes softwares com os mais modernos algoritmos criptográficos, bem como melhorias significativas em diversos subsistemas da solução. Destacamos a interoperabilidade com novos sistemas de banco de dados e a atualização das interfaces gráficas para a biblioteca QT4, o que também possibilitou melhorias de usabilidade no sistema, além do suportes a novos algoritimos como o Brainpool e novas garantias de integridade nos dados armazenados pelos sistemas.

3 – DA FORMA DE EXECUÇÃO

3.1 Mediante Termo de Execução Descentralizada (TED).

4 – DO QUANTITATIVO

4.1 Suporte e manutenção dos 5 (cinco) artefatos

6.3 Manutenção corretiva e de testes

6.3.1 Os sistemas de gestão de certificados Ywapa e Ywyra são testados desde a sua criação através de planos de testes elaborados através da análise de requisito funcionais. Estes testes foram suficientes por um longo período, mas devidos as mudanças da arquitetura, do suporte a novos algoritimos criptográficos e das alterações dos fluxos internos e de bibliotecas, este modelo tem sido exaurido dentro do projeto.

6.3.2 Outro quesito importante dos sistemas de gestão de certificados neste processo de constante manutenção e evolução é a de documentação do processo de desenvolvimento. Com a rápida adição de funcionalidades nos últimos anos, algumas porções do código tem documentação rudimentar e defasada. Isso acarreta em problemas para o preciso entendimento de algumas funções internas do código e para a geração da documentação de desenvolvimento.

6.3.3 Desta forma é necessário que de forma gradativa todo o código hoje presente nos sistemas de gestão de certificados seja adaptado para um padrão de consistência de documentação e de testes unitários e de integração. Sendo assim, o código das aplicações passará a contar além de uma documentação mais compreensiva, com um sistema de testes que visa garantir a integridade do sistema perante quaisquer modificações pontuais no código.

6.3.4 Por isso propomos que todas os trechos de códigos que forem modificados durante a execução do projeto tenham a sua documentação de código conferida e que sejam gerados para elas arquivos de testes unitários para a garantia das funcionalidades existentes hoje. Também propomos uma modificação no modelo de integração e testes, passando pelo uso de uma plataforma automatizada para a geração de releases com a introdução de compilações e testes periódicos em um servidor de integração.

6.3.5 Dessa forma, além de melhorarmos a documentação e as garantias de estabilidade ante a modificações pontuais no código dos sistemas, passaremos a contar com uma estrutura de geração de pacotes que nos permitirá gerar regularmente versões dos sistemas para a análise e demonstração de funcionalidades e também com um sistema de aplicação do plano de testes de forma automatizada e reprogramável. Estas modificações não afetarão diretamente as funcionalidades do sistemas de gestão de certificados, mas garantirá a estabilidade e qualidade de todo o processo de software no presente e no futuro.

6.3.6 Dessa forma esta atividade vai requerer que façamos as seguintes tarefas:

a) Suporte a execução e acompanhamento de implantação dos sistemas Ywapa/Ywyra;

b) Análise e atualização da documentação de código;

c) Devemos implantar um novo repositório de código que permita a verificação em tempo de commit de código de que as regras impostas estão sendo seguidas;

d) Devemos implantar um modelo de revisão de código, onde o processo de gerencia de qualidade seja verificado ativamente, fazendo com que a liberação de novas funcionalidades esteja também atrelada às garantias desta estratégia de documentação e testes;

e) Devemos criar um ambiente de integração e de pré-homologação.Estes ambientes permitirão a geração de versões do Ywapa/Ywyra devidamente testados, não somente com base nos testes unitários, mas também teste de pré-homologação, permitindo avaliar o sistema antes de ser disponibilizado ao ITI. O ITI deverá receber um relatório de todos os testes realizados, de forma a fazer seus próprios testes e verificar aqueles que foram feitos em ambiente e produção.

6.3.7 Do ponto de vista de risco, esta atividade pode ser classificada como de risco médio. Os desafios de documentação são relativamente fáceis de explicitar, mas laboriosos de cumprir. Já os desafios de testes são moderadamente difíceis de expressar e consideravelmente difíceis de implementar.

6.4 Atualização do sistema operacional

6.4.1 A plataforma de sistema operacional dos softwares Ywapa e Ywyra é hoje baseada no Red Hat Enterprise 5.5. Nos anos de 2006 e 2007, durante o desenvolvimento inicial do projeto a escolha por este sistema operacional se deu por causa do atendimento dos seguintes requisitos elencados pelo CASNAV:
a) Ser um sistema operacional baseado em código aberto;

b) Possuir a certificação common criteria EAL4+;

c) Ter a possibilidade de contratação de suporte por parte do distribuidor.

6.4.2 Passados quase 10 anos do processo de avaliação inicial para a escolha da plataforma, o sistema operacional hoje apresenta um envelhecimento natural em termos do suporte e da atualidade dos pacotes presentes. Isso hoje é um fator que limita e dificulta a evolução tecnológica da plataforma.

6.4.3 Será feita uma avaliação e gerado novas versões do Ywapa e Ywyra para o novo sistema operacional.

6.5 Suporte a cartões javacard

6.5.1 Toda a segurança dos perfis de operação nos softwares Ywapa/Ywyra é hoje baseada em uma autenticação em dois fatores com o uso de smartcards. O suporte a smartcards no âmbito da plataforma de software é hoje bastante limitado, tendo sido ultimamente atualizado quando do projeto inicial da plataforma. Desta forma hoje, a compatibilidade com cartões pelos softwares é bastante restrita, sendo ultimamente suportados cartões que já tiveram sua fabricação terminada ou que estão em vias de terminação.

6.5.2 A evolução dos smartcards nestes últimos 10 anos foi bastante direcionada à plataforma global de javacard. Sendo assim, os fabricantes de cartões inteligentes pararam de fabricar cartões com fins específicos tais como Infraestrutura de Chaves Públicas (ICP), EMV e Telefonia e passara a fabricar um único cartão que roda um sistema java que é capaz de rodar inúmeros applets e atender os vários segmentos com uma personalização de software. Com esta tendência, para fins de longevidade da plataforma Ywapa/Ywyra é muito importante que estes sistemas dêem suporte a este novo formato de cartões no âmbito da sua autenticação de perfil.

6.5.3 A biblioteca de interfaceamento com smartcards hoje em uso pelos sistemas é a OpenSC. A biblioteca OpenSC além e dar suporte aos cartões em uso hoje, possui um applet chamado Muscle que foi desenvolvido pelo projeto que pode ser carregado em cartões compatíveis com GlobalPlatform Javacard. Assim sendo, nossa proposta é estudar as bibliotecas e os softwares Ywapa/Ywyra para a comunicação com javacards que estejam rodando o applet Muscle ou outros applets pertinentes. Essa tarefa independe de um cartão específico, mas necessita de cartões aderentes ao GlobalPlatform.

6.5.4 Uma vez que haverá a atualização do sistema operacional, o suporte aos smartcards serão também avaliados nesta nova plataforma.

6.6 Gestão de chaves simétricas

6.6.1 Será adicionada ao Ywapa a gestão do ciclo de vida de chaves simétricas. Através da criação de uma entidade AC Raiz no Ywapa, esta poderá gerar, armazenar e exportar chaves simétricas. Tais chaves poderão ser transportadas, através de arquivos cifrados, a outros sistemas que precisem de tais chaves. As chaves simétricas serão codificadas em formatos padrões (por exemplo, CMS) e poderão ser importados por quais sistemas ou equipamentos que suportarem esses padrões. Um dos padrões que poderão ser usados será o PKCS#11.

7 - DO LOCAL DE ENTREGA DOS PRODUTOS

7.1 Os produtos deverão ser entregues nos locais definidos pelo ITI.

8 - DA PRESTAÇÃO DE CONTAS

8.1 A prestação de contas deste TED será firmado e apurado em uma única etapa. A prestação de contas final tem o escopo de apurar as contas terminativas da contratação, momento em que será realizada em conformidade necessária ao encerramento da vigência do presente termo, devendo esta ser prestada no prazo máximo de 60 (sessenta) dias.

9 – VIGÊNCIA

9.1 O presente documento entra em vigor na data de sua assinatura e terá vigência pelo período de 12 (doze) meses, sendo possível a renovação por aditamento.

10 – CRONOGRAMA DE EXECUÇÃO

10.1 Propõe-se um prazo total de 12 meses para todas as atividades. Os prazos e recursos foram estimados com base nos históricos de atividades realizadas nos sistemas Ywapa, Ywyra, em desenvolvimento pelo LabSEC nos últimos 10 anos.

10.2 A Tabela 1 apresenta uma estimativa do prazo necessário à realização de cada uma das atividades previstas durante o os estudos das soluções Ywapa e Ywyra.

Tabela 1 - Lista de Atividades

	Atividades	Duração em meses
1	Atualização da biblioteca criptográfica.	16
2	Manutenção corretiva e de testes com atualização da documentação.	24
3	Atualização do sistema operacional.	36
4	Suporte a cartões Javacard	16
5	Adição da funcionalidade de gestão de chaves simétricas ao Ywapa.	10

10.3 Os prazos definidos não estendem-se necessariamente em períodos contínuos de tempo, uma vez que determinadas atividades dependem da realização de outras.

10 4 A Tabela 2 lista os entregáveis com as datas previstas para liberação de versões do sistema

Tabela 2 - Versões dos sistemas Ywapa / Ywyra

Item	Entregáveis	Data prevista para entrega
1	Duas versões do Ywapa / Ywyra: 1) estável com biblioteca criptográfica atual e 2) para avaliação com nova biblioteca criptográfica.	Fevereiro de 2016
2	Ywapa / Ywyra com gestão de chaves simétricas	Abril de 2016
3	Ywapa / Ywyra, beta, com atualização do sistema operacional	Agosto de 2016
4	Ywapa / Ywyra, avaliação de suporte a novos cartões	Outubro de 2016
5	Documentação final do projeto e versões finais	Dezembro de 2016

11 – ORÇAMENTO

A Tabela 3 mostra o orçamento em termos de recursos humanos para o projeto.

As estimativas são um valor médio daqueles que foram necessários à manutenção e aprimoramento das versões anteriores desses sistemas.

Tabela 3 - Orçamento

Item	Descrição	Valor [R$]
1	Bolsas para Gestão de Requisitos, Qualidade e de Configuração.	66 000,00
2	Bolsas para Auxiliares de programação júnior e sênior.	62.400,00
	Total R$	128.400,00

11 – DAS DISPOSIÇÕES GERAIS

11.1 A contratação a que se destina este Plano de Trabalho deverá ocorrer com base em Termo de Execução Descentralizada, com arrimo na Nota Técnica nº 301/2005/STN/CONED, datada de 23 de março de 2005, observadas as condições expressas neste instrumento.

11.2 O referido TED deverá ser emitido em favor da UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC, devendo ser observada a destinação da Nota de Crédito – NC, para a Unidade Gestora – UG nº 153.163 e a Programação Financeira – PF para a UG nº 160075.

11.3 O TED será emitido no valor de R$ 128.400,00 (Cento e vinte e oito mil e quatrocentos reais), destinados a fazer face ao objeto deste termo.

11.4 Nos termos da Portaria nº 01/2003, será designado o responsável pela fiscalização e gestão do TED.

12 – Cronograma de Desembolso Financeiro

12.1 O Cronograma de desembolso será feito em 2 (duas) parcelas sendo

- Primeira parcela no valor de R$ 64.200,00 em 27 de novembro de 2015
- Segunda parcela no valor de R$ 64.200,00 em 27 de maio de 2016

13 – DADOS CADASTRAIS DA PROPONENTE/ CONTRATADA

Órgão/ Entidade UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC	CNPJ 83.899.526/000182
Endereço Campus Universitário - Trindade	UG 153.163
Cidade UF CEP DDD/ Telefone Florianópolis SC 88.040-900 (48) 3721.9320	E.A Federal
Nome do Responsável Roselane Neckel	CPF 641.354.119/91
Posto REITORA	Matricula : SIAPE: 1193867
Endereço Campus Universitário - Trindade	CEP 88.040-900

Brasília/DF, 27 de novembro de 2015

ROSELANE NECKEL
REITORA DA UFSC

Aprovo o presente Plano de Trabalho, na forma proposta.

Brasília/DF, 11 de novembro de 2015

RENATO DA SILVEIRA MARTINI
Diretor Presidente
Instituto Nacional de Tecnologia da Informação (ITI)

TERMO DE EXECUÇÃO DESCENTRALIZADA	TED Nº 02/2015
Órgão Descentralizador: INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO – ITI.	
Nome do Órgão Proponente: UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC	
Código Orçamentário e Nome da Ação: 20.204 04.125.2038.49170001 – Operacionalização, manutenção, modernização da certificação digital	

1- DADOS CADASTRAIS DO ÓRGÃO PROPONENTE

Nome do Órgão Proponente: UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC				
Endereço: Campus Universitário - Trindade				
E-mails: gr@contato.ufsc.br	CNPJ: 83.899.526/000182		UG: 153.163	Gestão: 15.237
Cidade: Florianópolis	UF: SC	CEP: 88.040-900	DDD/Telefone: (48) 3721.9239	DDD/FAX: (48) 3721-9048

2- DADOS CADASTRAIS DO DIRIGENTE DO ÓRGÃO PROPONENTE

Nome do dirigente Máximo do Órgão: ROSELANE NECKEL			
Ato de Nomeação: Decreto	Data: 04/05/2012	Publicado no DOU: 07/05/2012	CPF: 641.354.119/91
RG/Órgão Expedidor: 1.812.211-6 SSP/SC	Cargo/Função: REITOR		Matrícula: SIAPE: 1193867

3- DESCRIÇÃO DO PROJETO/AÇÃO

Título: Suporte e Avaliação de Adequabilidade Tecnológica dos Sistemas de Gerenciamento de Certificados Digitais Ywapa e Ywyra	Vigência	
	Início 27/11/2015	Término 26/11/2016

4- CRONOGRAMA DE EXECUÇÃO

Entregas	Prazo de entrega
Duas versões do Ywapa / Ywyra: 1) estável com biblioteca	Fevereiro 2016

1	criptográfica atual e 2) para avaliação com nova biblioteca criptográfica.	
2	Ywapa / Ywyra com gestão de chaves simétricas	Abril de 2016
3	Ywapa / Ywyra, beta, com atualização do sistema operacional	Agosto de 2016
4	Ywapa / Ywyra, avaliação de suporte a novos cartões	Outubro de 2016
5	Documentação final do projeto e versões finais	Novembro de 2016

5 - DESCENTRALIZAÇÃO DO CRÉDITO

Natureza da Despesa	Valor em R$ 1,00
339000	128.400,00

6- CRONOGRAMA DE DESEMBOLSO

Data	Valor
27/11/2015	R$ 64.200,00
27/05/2016	R$ 64.200,00

7- JUSTIFICATIVA

7.1 O presente documento apresenta uma proposta de manutenção e de estudos de diversas melhorias dos Sistemas de Gerenciamento de Certificados Digitais ICP-Brasil, chamados Ywapa e Ywyra por um prazo de doze (12) meses.

7.2 O Laboratório de Segurança em Computação (LabSEC) tem grande interesse em realizar esse projeto de manutenção e de estudos de diversas melhorias dos Sistemas suporte e manutenção, dando assim continuidade às pesquisas que vem sendo desenvolvidas no laboratório em assinatura digital.

7.3 Será realizado o suporte e o estudo das melhorias e atualizações nos softwares de forma que eles possam continuar sendo utilizados e se mantenham condizentes com as necessidades e novos requisitos da ICP-Brasil.

7.4 Com a execução deste projeto espera-se contribuir para com a sociedade realizando pesquisas, visando melhorias para os Sistemas de Gerenciamento de Certificados Digitais e formando especialistas nessa tecnologia.

8 - DECLARAÇÃO

8.1 A UFSC se compromete a:

8.1.1. Utilizar os créditos objeto da descentralização na execução do Projeto/Ação conforme a legislação vigente.

8.1.2 Pela execução orçamentária dos créditos recebidos, devendo ser respeitado fielmente o previsto no plano de ação.

8.1.3 A permitir a verificação da execução do objeto da Ação pelo descentralizador do crédito em qualquer momento das etapas previstas.

8.1.4 Os direitos relativos ao projeto pertencerão exclusivamente ao ITI, na forma do disposto no Art. 4º da Lei 9.609/1998.

8.1.5 Aplicar os recursos orçamentarios e fiannceiros transferidos em rígida consonância com a Lei nº 13.080/2015, obervando ainda a vedação para pagamentos a servidores por serviços de consultoria.

Brasília/DF, 21 de novembro de 2015.	RENATO DA SILVEIRA MARTINI Diretor-Presidente do ITI
Florianópolis/SC, 21 de novembro de 2015.	ROSELANE NECKEL REITOR DA UFSC

9- DA PRESTAÇÃO DE CONTAS

9.1 A prestação de contas deste Termo será firmado e apurado em uma única etapa. A prestação de contas final tem o escopo de apurar as contas terminativas da contratação, momento em que será realizada em conformidade necessária ao encerramento da vigência do presente termo, devendo esta ser prestada no prazo máximo de 60 (sessenta) dias.

10 - APROVAÇÃO DO RESPONSÁVEL PELO ÓRGÃO DESCENTRALIZADOR

10.1 AUTORIZO a celebração do Termo de Execução Descentralizada nº 02/2015, nas condições propostas.	
Brasília/DF, 17 de novembro de 2015	RENATO DA SILVEIRA MARTINI Diretor-Presidente do ITI

PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL
INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

UNIVERSIDADE FEDERAL DE SANTA CATARINA

TERMO DE REFERÊNCIA

1 – OBJETO, MOTIVAÇÃO E JUSTIFICATIVA - Suporte e Avaliação de Adequabilidade Tecnológica dos Sistemas de Gerenciamento de Certificados Digitais Ywapa e Ywyra. O ITI na qualidade de Ac-raiz da ICP-Brasil, não pode dispensar manutenção e estudos de diversas melhorias dos Sistemas de Gerenciamento de Certificados Digitais ICP-Brasil, chamados Ywapa e Ywyra. A execução dessa proposta consta apresentada pelo Laboratório de Segurança em Computação (LabSEC) da Universidade Federal de Santa Catarina (UFSC) que foi responsável pelo desenvolvimento das versões atualmente em produção desses softwares. O conteúdo deste documento foi elaborado a partir de uma profunda análise do estado atual desses sistemas e tem como principal objetivo o suporte, o estudo das melhorias e atualizações nos softwares de forma que eles possam continuar sendo utilizados e se mantenham condizentes com as necessidades e novos requisitos da ICP-Brasil. O LabSEC tem sido reconhecido como um dos maiores centros de pesquisa científica e tecnológica na área de certificação digital no país. Desde a sua criação em 1999, já foram desenvolvidos mais de 150 trabalhos de conclusão de curso de graduação, dissertações de mestrado e teses de doutorado em infraestrutura de chaves públicas e suas aplicações. Foram mais de 50 artigos científicos publicados nos mais renomados eventos e periódicos científicos, nacionais e internacionais. O LabSEC tem participado dos dois maiores esforços acadêmicos em atividade relacionados ao desenvolvimento de tecnologia nacional para a gestão do ciclo de vida de chaves criptográficas: projetos ICPEDU com finalidade de pesquisa e ensino e o João de Barro. Para o projeto Infraestrutura de Chaves Públicas para Pesquisa e Ensino (ICPEDU) da Rede Nacional de Ensino e Pesquisa (RNP), desenvolveu e mantém um sistema acadêmico aberto de gerenciamento de certificados digitais e o software para a gestão de chaves criptográficas para módulo de segurança criptográfica (ASI-HSM). A solução desenvolvida está sendo usada por mais de 20 universidades de todo o país na implantação de um infraestrutura para fins de pesquisa e ensino em certificação digital. O

Programa João de Barro foi a iniciativa que possibilitou o desenvolvimento do Sistema de Gerenciamento do Ciclo de Vida de Certificados Digitais tanto para a Autoridade Certificadora Raiz Brasileira quanto para autoridades certificadoras intermediarias off-line. Nesse âmbito também foi desenvolvido o software para emissão de certificados digitais à usuários finais conhecido como Hawa. Estes sistemas estão hoje em uso por várias autoridades certificadoras no âmbito da Infraestrutura de Chaves Públicas Brasileira. O laboratório tem grande interesse em dar continuidade nas atividades suporte e estudos de aprimoramento dos softwares Ywapa e Ywyra. O interesse justifica-se tanto do ponto de vista da extensão universitária, quanto da pesquisa e do ensino. A extensão universitária é uma forma de aproximar a universidade da sociedade, dando oportunidade ao corpo discente e docente em aprender com um caso real, apesar de complexo, mas de extrema relevância para o entendimento da ciência e tecnologia da certificação digital. Há desafios tecnológicos interessantes, não só de aplicação da tecnologia da criptografia, mas também de engenharia de software, que propiciam aos alunos e professores uma experiência muito rica. No âmbito do ensino o projeto também visa a formação de recursos humanos capacitados em certificação digital. Os softwares Ywapa e Ywyra já vem sendo utilizados por Autoridades Certificadoras dentro do escopo da ICP-Brasil de forma muito bem sucedida. Fruto de etapas anteriores do projeto, a ICI-Brasil conta nestes softwares com os mais modernos algoritmos criptográficos, bem como melhorias significativas em diversos subsistemas da solução. Destacamos a interoperabilidade com novos sistemas de banco de dados e a atualização das interfaces gráficas para a biblioteca QT4, o que também possibilitou melhorias de usabilidade no sistema, além do suportes a novos algorítimos como o Brainpool e novas garantias de integridade nos dados armazenados pelos sistemas.

2 – DA VANTAGEM DA EXECUÇÃO - Com a execução deste projeto espera-se contribuir para o mais efetivo suporte, além de propor estudo das melhorias e atualizações nos softwares de forma que eles possam continuar sendo utilizados e se mantenham condizentes com as necessidades e novos requisitos da ICP-Brasil.

3 – DA FORMA DE EXECUÇÃO – A execução do ajuste ocorerá mediante Termo de Execução Descentralizada (TED), assistido por Plano de Trabalho e TED, constantes os respectivos cronograma físico-financeiro e obrigaçẽos recíprocas dos partícipes.

4 – DOS RECURSOS ORÇAMENTÁRIOS - Os recursos orçamentários para execução deste Plano de Trabalho serão repassados por TED entre a Universidade Federal de Santa Catarina (UFSC) e o

Instituto Nacional de Tecnologia da Informação (ITI), consoante ao **Código Orçamentário e Nome da Ação:**

20.204 04.125.2038.49170001 – Operacionalização, manutenção, modernização da certificação digital.

5 – DO ESCOPO DO OBJETO - O escopo dos serviços compreende suporte e manutenção aos 2 (dois) artefatos assim denominados, observadas as diretrizes definidas nas etapas de desenvolvimento. Para os fins a que se destina este Plano de Trabalho apresenta-se propostas para a manutenção e de estudos de diversas melhorias dos Sistemas de Gerenciamento de Certificados Digitais ICP-Brasil: Ywapa e Ywyra.

6 - DA ATUALIZAÇÃO DA BIBLIOTECA CRIPTOGRAFICA - Durante o ultimo projeto de atualização e manutenção da plataforma Ywapa/Ywyra foi acrescido o suporte a assinaturas em curvas elípticas e em especial as curvas do padrão Brainpool, hoje usada no AC Raiz v4 e nas ACs credenciadas desta cadeia. O suporte foi colocado no Ywapa 2.5.4, que foi escolhido em virtude da sua estabilidade. Isso foi feito através do uso de um patch que dava o suporte a estas curvas no OpenSSL 1.0.1. Este patch foi desenvolvido por terceiros e foi verificado e integrado pelas equipes do LabSEC no lado do software e pela equipe da Kryptus no lado do HSM. Entretanto, algum tempo depois, foi lançado o Openssl 1.0.2 que trás suporte nativo às curvas elípticas Brainpool, tornando a solução por patch obsoleta e trazendo problemas de compatibilidade futura com o OpenSSL. Desta forma, uma solução importante para a longevidade dos software Ywapa/Ywyra é a adoção da implementação das curvas elípticas Brainpool através da implementação padrão do OpenSSL. Isso com certeza garantirá todo o suporte de segurança da biblioteca e consequentemente do software. Trata-se, portanto, de uma atividade prioritária. Salienta-se que esta atividade precisa ser coordenada junto a empresa Kryptus, uma vez que o ASI-HSM deve prover as funcionalidades e suporte à mesma versão do OpenSSL.

6.1 Da Manutenção Corretiva e Testes - Os sistemas de gestão de certificados Ywapa e Ywyra são testados desde a sua criação através de planos de testes elaborados através da análise de requisito funcionais. Estes testes foram suficientes por um longo período, mas devidos as mudanças da arquitetura, do suporte a novos algoritimos criptográficos e das alterações dos fluxos internos e de bibliotecas, este modelo tem sido exaurido dentro do projeto. Outro quesito importante dos sistemas de gestão de certificados neste processo de constante manutenção e evolução é a de documentação do processo de desenvolvimento. Com a rápida adição de funcionalidades nos últimos anos, algumas porções do código tem documentação rudimentar e defasada. Isso acarreta em problemas para o preciso entendimento de algumas funções internas do código e para a geração da documentação de desenvolvimento. Desta forma é necessário que de forma gradativa todo o código hoje presente nos

sistemas de gestão de certificados seja adaptado para um padrão de consistência de documentação e de testes unitários e de integração. Sendo assim, o código das aplicações passará a contar além de uma documentação mais compreensiva, com um sistema de testes que visa garantir a integridade do sistema perante quaisquer modificações pontuais no código. Por isso propomos que todas os trechos de códigos que forem modificados durante a execução do projeto tenham a sua documentação de código conferida e que sejam gerados para elas arquivos de testes unitários para a garantia das funcionalidades existentes hoje. Também propomos uma modificação no modelo de integração e testes, passando pelo uso de uma plataforma automatizada para a geração de releases com a introdução de compilações e testes periódicos em um servidor de integração. Dessa forma, além de melhorarmos a documentação e as garantias de estabilidade ante a modificações pontuais no código dos sistemas, passaremos a contar com uma estrutura de geração de pacotes que nos permitirá gerar regularmente versões dos sistemas para a análise e demonstração de funcionalidades e também com um sistema de aplicação do plano de testes de forma automatizada e reprogramável. Estas modificações não afetarão diretamente as funcionalidades do sistemas de gestão de certificados, mas garantirá a estabilidade e qualidade de todo o processo de software no presente e no futuro. Dessa forma esta atividade vai requerer que façamos as seguintes tarefas: a) Suporte a execução e acompanhamento de implantação dos sistemas Ywapa/Ywyra. b) Análise e atualização da documentação de código. c) Devemos implantar um novo repositório de código que permita a verificação em tempo de commit de código de que as regras impostas estão sendo seguidas. d) Devemos implantar um modelo de revisão de código, onde o processo de gerencia de qualidade seja verificado ativamente, fazendo com que a liberação de novas funcionalidades esteja também atrelada às garantias desta estratégia de documentação e testes e) Devemos criar um ambiente de integração e de pré-homologação.Estes ambientes permitirão a geração de versões do Ywapa/Ywyra devidamente testados, não somente com base nos testes unitários, mas também teste de pré-homologação, permitindo avaliar o sistema antes de ser disponibilizado ao ITI. O ITI deverá receber um relatório de todos os testes realizados, de forma a fazer seus próprios testes e verificar aqueles que foram feitos em ambiente e produção. Do ponto de vista de risco, esta atividade pode ser classificada como de risco médio. Os desafios de documentação são relativamente fáceis de explicitar, mas laboriosos de cumprir. Já os desafios de testes são moderadamente difíceis de expressar e consideravelmente difíceis de implementar.

6.2 Da Atualização do Sistema Operacional - A plataforma de sistema operacional dos softwares Ywapa e Ywyra é hoje baseada no Red Hat Enterprise 5.5. Nos anos de 2006 e 2007, durante o desenvolvimento inicial do projeto a escolha por este sistema operacional se deu por causa do atendimento dos seguintes requisitos elencados pelo CASNAV: a) Ser um sistema operacional baseado em código aberto. b) Possuir a certificação common criteria EAL4+ c) Ter a possibilidade de contratação de suporte por parte do distribuidor. Passados quase 10 anos do processo de avaliação inicial para a escolha da plataforma, o sistema operacional hoje apresenta um envelhecimento natural em termos do suporte e da atualidade dos pacotes presentes. Isso hoje é um fator que limita e dificulta a evolução tecnológica da plataforma. Será feita uma avaliação e gerado novas versões do Ywapa e Ywyra para o novo sistema operacional.

6.3 Do Suporte a Cartões Javacard - Toda a segurança dos perfis de operação nos softwares Ywapa/Ywyra é hoje baseada em uma autenticação em dois fatores com o uso de smartcards. O suporte a smartcards no âmbito da plataforma de software é hoje bastante limitado, tendo sido ultimamente atualizado quando do projeto inicial da plataforma. Desta forma hoje, a compatibilidade com cartões pelos softwares é bastante restrita, sendo ultimamente suportados cartões que já tiveram sua fabricação terminada ou que estão em vias de terminação. A evolução dos smartcards nestes últimos 10 anos foi bastante direcionada à plataforma global de javacard. Sendo assim, os fabricantes de cartões inteligentes pararam de fabricar cartões com fins específicos tais como Infraestrutura de Chaves Públicas (ICP), EMV e Telefonia e passara a fabricar um único cartão que roda um sistema java que é capaz de rodar inúmeros applets e atender os vários segmentos com uma personalização de software. Com esta tendência, para fins de longevidade da plataforma Ywapa/Ywyra é muito importante que estes sistemas dêem suporte a este novo formato de cartões no âmbito da sua autenticação de perfil. A biblioteca de interfaceamento com smartcards hoje em uso pelos sistemas é a OpenSC. A biblioteca OpenSC além e dar suporte aos cartões em uso hoje, possui um applet chamado Muscle que foi desenvolvido pelo projeto que pode ser carregado em cartões compatíveis com GlobalPlatform Javacard. Assim sendo, nossa proposta é estudar as bibliotecas e os softwares Ywapa/Ywyra para a comunicação com javacards que estejam rodando o applet Muscle ou outros applets pertinentes. Essa tarefa independe de um cartão específico, mas necessita de cartões aderentes ao GlobalPlatform. Uma vez que haverá a atualização do sistema operacional, o suporte aos smartcards serão também avaliados nesta nova plataforma.

6.4 Da Gestão de Chaves Simétricas - Será adicionada ao Ywapa a gestão do ciclo de vida de chaves simétricas. Através da criação de uma entidade AC Raiz no Ywapa, esta poderá gerar, armazenar e exportar chaves simétricas. Tais chaves poderão ser transportadas, através de arquivos cifrados, a outros sistemas que precisem de tais chaves. As chaves simétricas serão codificadas em formatos padrões (por exemplo, CMS) e poderão ser importados por quais sistemas ou equipamentos que suportarem esses padrões. Um dos padrões que poderão ser usados será o PKCS#11.

7 - DO LOCAL DE ENTREGA DOS PRODUTOS - Os produtos deverão ser entregues na sede do ITI

8 – DA PRESTAÇÃO DE CONTAS - A prestação de contas deste TED será firmado e apurado em uma única etapa. A prestação de contas final tem o escopo de apurar as contas terminativas da contratação, momento em que será realizada em conformidade necessária ao encerramento da vigência do presente termo, devendo esta ser prestada no prazo máximo de 60 (sessenta) dias.

9 – DA VIGÊNCIA - O presente documento entra em vigor na data de sua assinatura e terá vigência pelo período de 12 (doze) meses, sendo possível a renovação por aditamento.

10 – DO CRONOGRAMA DE EXECUÇÃO - Propõe-se um prazo total de 12 meses para todas as atividades. Os prazos e recursos foram estimados com base nos históricos de atividades realizadas nos sistemas Ywapa, Ywyra, em desenvolvimento pelo LabSEC nos últimos 10 anos.

Tabela 1 - Lista de Atividades

	Atividades	Duração em meses
1	Atualização da biblioteca criptográfica.	16
2	Manutenção corretiva e de testes com atualização da documentação	24
3	Atualização do sistema operacional.	36
4	Suporte a cartões Javacard	16
5	Adição da funcionalidade de gestão de chaves simétricas ao Ywapa	10

- Os prazos definidos não estendem-se necessariamente em períodos contínuos de tempo, uma vez que determinadas atividades dependem da realização de outras.

Tabela 2 - Versões dos sistemas Ywapa / Ywyra

Item	Entregáveis	Data prevista para entrega
1	Duas versões do Ywapa / Ywyra: 1) estável com biblioteca criptográfica atual e 2) para avaliação com nova biblioteca criptográfica.	Fevereiro de 2016
2	Ywapa / Ywyra com gestão de chaves simétricas	Abril de 2016
3	Ywapa / Ywyra, beta, com atualização do sistema operacional	Agosto de 2016
4	Ywapa / Ywyra, avaliação de suporte a novos cartões	Outubro de 2016
5	Documentação final do projeto e versões finais	Dezembro de 2016

- **A Tabela 1** apresenta uma estimativa do prazo necessário à realização de cada uma das atividades previstas durante o os estudos das soluções Ywapa e Ywyra.

- **A Tabela 2** lista os entregáveis com as datas previstas para liberação de versões do sistema

- **A Tabela 3** demonstra o orçamento em termos de recursos humanos para o projeto

11 – DO ORÇAMENTO - As estimativas são um valor médio daqueles que foram necessários à manutenção e aprimoramento das versões anteriores desses sistemas.

Tabela 3 - Orçamento

Item	Descrição	Valor [R$]
1	Bolsas para Gestão de Requisitos, Qualidade e de Configuração.	66.000,00
2	Bolsas para Auxiliares de programação júnior e sênior	62.400,00

- Primeira parcela no valor de R$ 64.200,00 em 27 de novembro de 2015.
- Segunda parcela no valor de R$ 64.200,00 em 27 de maio de 2016.

13 – DA VANTAJOSIDADE DE CONTRATAÇÕES - Cumpre a UFSC certificar-se no mercado e por meio dos mecanismos de licitação, a partir de detalhamento orçamento dos preços praticados e demais elementos formadores da almejada vantagem em prol do interesse público, a teor do que consta recomendado pela douta Procuradoria do ITI, ex vi subitem 20 do Parecer nº 202/2015/DSB/PFE-ITI/PGF/AGU.

14 – DADOS CADASTRAIS DA PROPONENTE/PARTÍCIPE

Órgão/Entidade UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC	**CNPJ** 83.899.526/000182
Endereço Campus Universitário - Trindade	**UG** 153.163
Cidade UF CEP DDD/Telefone Florianópolis SC 88.040-900 (48) 3721.9320	**E.A** Federal
Nome do Responsável Roselane Neckel	**CPF** **641.354.119/91**
Posto REITORA	**Matricula :** SIAPE: 1193867
Endereço Campus Universitário - Trindade	**CEP** 88.040-900

Brasília-DF, 27 de novembro de 2015

ROSELANE NECKEL
Reitora
Universidade Federal de Santa Catarina

RENATO DA SILVEIRA MARTINI
Diretor-Presidente
Instituto Nacional de Tecnologia da Informação - ITI