DTI
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

UFMG

Regras de Uso:

Certificado Digital – e-CPF – ICP-Brasil

DTI – Diretoria de Tecnologia da Informação

Dados Gerais

Identificação do documento:	Regras de Uso – Serviço de Certificado Digital – e-CPF – ICP-Brasil	
	Regras de Uso: Serviço de Certificado Digital – e-CPF – ICP-Brasil	
Histórico de Revisão:	**Atividade:**	**Responsável:**
	1.0 – Criação do Documento (02/07/2021)	Sadallo Andere Neto – DPS Karina Flaviana Ribeiro – ATC
	1.0 – Revisão do Documento (12/07/2021)	Carlos Alfeu Furtado da Fonseca – DTI
	1.1 – Alterações no Documento (07/04/2022)	Sadallo Andere Neto – DPS
	1.2 – Alterações no Documento (11/07/2022)	Sadallo Andere Neto – DPS
	1.3 – Alterações no Documento (03/03/2023)	Sadallo Andere Neto – DPS
	2.0 – Reestruturação do serviço devido à mudança de fornecedor (11/04/2023)	Lucilene Miranda da Silva – DPS Sadallo Andere Neto – DPS
	2.1 – Alterações no documento 08/05/2023	Lucilene Miranda da Silva – DPS Sadallo Andere Neto – DPS

Sumário

1. Apresentação

Este documento descreve as **Regras de Uso do Serviço de Certificado Digital – e-CPF – ICP-Brasil** da UFMG.

Este serviço tem como finalidade disponibilizar a certificação digital e-CPF, da infraestrutura ICP-Brasil, tipo A3, aos membros da comunidade UFMG cujas tarefas em sistemas de informação exijam tal mecanismo de segurança para autenticação.

O certificado digital é de uso individual e intransferível, possui prazo de validade de 3 (três) anos e se presta à realização de atividades de trabalho.

O certificado digital assegura que os usuários realizem atividades essenciais e rotineiras de forma segura e inequívoca.

Para a utilização deste serviço, o solicitante deve cumprir as etapas de **requerimento**, **justificativa** e **instalação** da solicitação do certificado digital.

Não está previsto, até o momento, o repasse de custos para a utilização deste serviço.

2. Termos e Definições

TERMO	DEFINIÇÃO
ATC	Assessoria Técnica
Certificado digital	Conjunto de dados de computador, gerados por uma Autoridade Certificadora que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação.
DAP	Departamento de Administração de Pessoal da Pró-Reitoria de Recursos Humanos
DCF	Departamento de Contabilidade e Finanças da Pró-Reitoria de Planejamento
DLO	Departamento de Logística de Suprimentos e de Serviços Operacionais da Pró-Reitoria de Administração
DPS	Divisão de Processos e Segurança da Diretoria de Tecnologia da Informação
DTI	Diretoria de Tecnologia da Informação
DRCA	Departamento de Registro e Controle Acadêmico
Fornecedor	Empresa contratada pela Diretoria de Tecnologia da Informação para a prestação dos serviços de certificação digital e do fornecimento de dispositivo eletrônico de armazenamento de certificado digital ICP-Brasil.
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira. Cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Essa infraestrutura é um conjunto elaborado de práticas, técnicas e procedimentos que serve para suportar um sistema criptográfico baseado em certificados digitais. O modelo adotado no Brasil para a infraestrutura de chaves públicas é chamado de certificação com raiz única, em que existe uma Autoridade Certificadora Raiz (AC-Raiz). Além de desempenhar esse papel, a AC-Raiz credencia os demais participantes da cadeia, além de supervisionar e auditar os processos. Foi criada pela MP 2002-2/2001 e está regulamentada pelas resoluções do Comitê-Gestor da ICP-Brasil.
Órgão Aprovador	Órgão da UFMG responsável por analisar e aprovar as solicitações deste serviço
SERPRO	Serviço Federal de Processamento de Dados, empresa contratada pela DTI para fornecer o serviço de certificação digital
UFMG	Universidade Federal de Minas Gerais
Usuário	Servidor da UFMG que necessite de certificado digital para o exercício das suas tarefas administrativas, cuja solicitação tenha sido devidamente justificada e aprovada.

3. Público-alvo

O serviço é oferecido exclusivamente aos servidores federais ativos da UFMG que sejam detentores de cargos efetivos ou de carreira cujas atividades exijam uso de certificado digital para fins de segurança e autenticação nos sistemas estruturantes do governo federal, assinatura de diploma digital dentre outras atividades.

4. Requisitos

O servidor da UFMG que deseja utilizar e se tornar Usuário deste serviço, deverá satisfazer as seguintes exigências:

1. possuir cadastro ativo no minhaUFMG (portal de acesso aos serviços disponibilizados pela UFMG);
2. estar em exercício na UFMG, com os dados cadastrais atualizados no SouGov, incluindo sua lotação e aqueles relativos às chefias imediata e superior;
3. manter atualizados os e-mails cadastrados na plataforma SouGov (*Meu Perfil* > *Meus Contatos* > *Institucional e Pessoal*).

   O e-mail institucional cadastrado no SouGov deverá possuir o padrão **loginMinhaUFMG@ufmg.br** (ver seção 8.1.1)
4. desempenhar atividades laborais que exijam uso de certificado digital para fins de segurança e autenticação nos sistemas estruturantes do governo federal, assinatura de diploma digital dentre outras que justifiquem a necessidade do certificado digital custeado pela UFMG; e
5. estar de acordo com estas Regras de Uso e com os Termos de Uso de Recursos de TI, encontrados no portal minhaUFMG.

Caso o solicitante possua certificado digital vigente, ou seja, cuja validade não tenha expirado, nova solicitação de certificado deve ser realizada apenas **15 (quinze) dias antes** do vencimento.

5. Tipo de certificado

5.1 Certificado A3 em nuvem – NeoID

O certificado digital em nuvem (NeoID) é indicado para servidores que precisam de maior mobilidade, com uso em diversos dispositivos.

Sua utilização requer celular com acesso à internet e aplicativo NeoID instalado. *A DTI não disponibilizará celular institucional exclusivamente para este fim.*

Caso o certificado seja necessário para uso em sistema que não esteja apto à certificação em nuvem, o usuário deverá ter instalado no computador de trabalho o software *NeoID Desktop*.

Caso o servidor opte pelo NeoID e possua certificado digital **anterior** em token (pendrive), o dispositivo deverá ser entregue na DTI após o vencimento (salas 8010 ou 8011).

5.2 Certificado A3 com token – A3_TOKEN

O certificado A3 **com** fornecimento de token (pendrive) é indicado para servidores que estão solicitando pela primeira vez e optem pelo uso do token para armazenar o certificado.

Caso o servidor opte pelo A3 com token deverá retirar o token na DTI conforme contato pela Diretoria por e-mail, após a aprovação do certificado.

5.3 Certificado A3

O certificado digital A3 **sem** fornecimento de token é indicado para servidores que já possuem o token e desejam continuar utilizando-o.

O token deve ser de um dos modelos indicados no site do fornecedor contratado. Caso contrário, recomenda-se a solicitação de NeoID ou de A3 com token.

6. Identificação do Órgão Aprovador

Cabe ao solicitante identificar o órgão responsável por analisar sua solicitação de certificado, de acordo com a tabela a seguir, e informá-lo no Formulário de Justificativa.

Sistemas	**Órgão Aprovador**
Diploma Digital	DRCA
Sistemas de recursos humanos e de pessoal	DAP
Sistemas de passagens, diárias, contabilidade e controle de produtos químicos.	DCF
Sistemas de compras	DLO

Quadro 1 – *Relação de órgãos aprovadores por tipo de sistema*

Caso sejam identificadas dúvidas ou inconsistências na solicitação, o servidor poderá ser contatado pela DTI ou pelo Órgão Aprovador para os devidos esclarecimentos.

7. Fluxo do Serviço

1. **Regras de uso:** o servidor acessa o site da DTI para conhecer sobre o serviço e ler este documento;
2. **Requerimento:** o servidor solicita o certificado digital via SouGov, indicando o Tipo de Certificado (vide seção 5);
3. **Justificativa:** o servidor envia o formulário de justificativa, disponível no site da DTI, indicando o Órgão Aprovador responsável por analisar a solicitação (vide ***Quadro 1***);
4. **Aprovação:** o Órgão Aprovador, após ser notificado no e-mail do setor, segue as instruções da mensagem e:
    a. acessa o Módulo Aprovador SERPRO, autoriza ou indefere a solicitação;
    b. em caso de aprovação, notifica a DTI pelo link indicado no e-mail, clicando no botão ***Enviar***.
5. **Instalação:**
    a. em caso de aprovação, o servidor solicitante recebe um e-mail com instruções e prossegue com a instalação e uso do certificado;
    b. em caso de indeferimento, o servidor recebe um e-mail com o motivo do indeferimento.

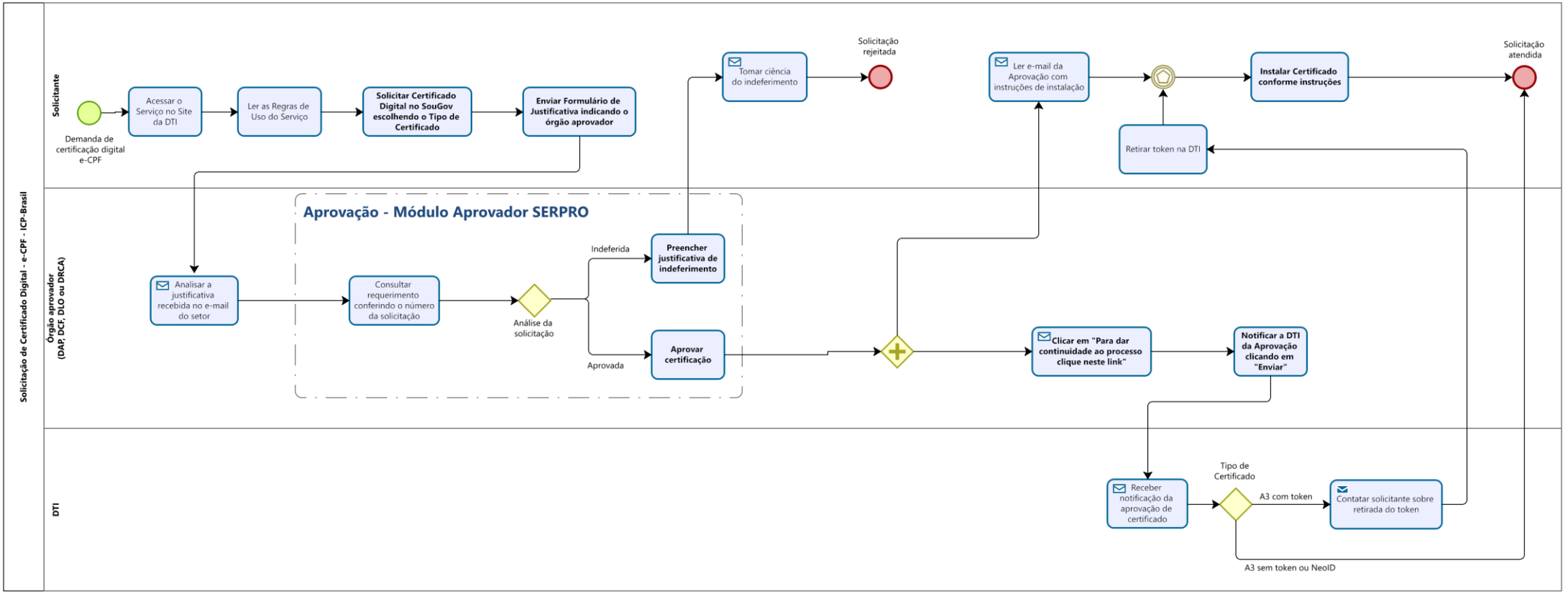

Figura 1 – *Fluxo do serviço*

8. Responsabilidades

8.1 Requerimento

8.1.1 E-mail institucional

Cabe ao solicitante realizar o requerimento do certificado digital na plataforma SouGov (*Solicitações* > *Realizar Solicitação*), em sua versão Web ou aplicativo.

É imprescindível que o solicitante mantenha atualizados os e-mails cadastrados no SouGov (*Meu Perfil* > *Meus Contatos* > *Institucional e Pessoal*). O e-mail institucional deverá obrigatoriamente seguir o padrão ***loginMinhaUFMG*@ufmg.br**. Caso contrário, não será possível realizar a solicitação.

> *Por exemplo, caso o e-mail institucional cadastrado no SouGov seja josedasilva@**farmacia.ufmg.br**, a solicitação será inválida.*

Caso o servidor não receba o código de confirmação, não possua acesso ao e-mail previamente cadastrado ou o SouGov apresente algum erro que impossibilite a atualização do e-mail, deve-se entrar em contato com a seção de pessoal local para que seja providenciada a atualização junto ao DAP.

8.1.2 Compatibilidade do token

É responsabilidade do usuário que opte por certificado A3 (sem token) verificar a compatibilidade do seu dispositivo conforme o especificado na seção 5.3. Caso contrário, recomenda-se a escolha por outro tipo de certificado.

8.2 Justificativa

O preenchimento do Formulário de Justificativa deve ser realizado pelo solicitante **imediatamente** após o Requerimento do certificado digital no SouGov, em link disponibilizado no site da DTI.

8.3 Aprovação do certificado digital

A aprovação do certificado digital é responsabilidade de servidor lotado em Órgão Aprovador que tenha sido designado para a função, através da ferramenta disponibilizada pelo fornecedor. Cabe ao servidor analisar o e-mail com a Justificativa enviada pelo solicitante e notificar a DTI após a aprovação, conforme instruções da DTI contidas na referida mensagem.

8.4 Instalação do certificado digital

Durante a instalação, pode ser solicitado ao usuário que faça *download* e instale software indicado pelo fornecedor. Caso o computador de trabalho possua restrições de instalação, a equipe de TI local deve ser acionada.

8.5 Armazenamento do certificado digital

É de responsabilidade exclusiva do usuário titular do certificado armazená-lo em local seguro. O acesso do certificado individual por terceiros pode resultar em acessos, autenticações e assinaturas indevidas.

8.6 Senha

A senha (pin) do certificado é pessoal, única e intransferível. Após definição da senha, o usuário não poderá recuperá-la.

8.7 Token (*pendrive)*

Caso o certificado digital escolhido acompanhe token, é dever do usuário prezar pela sua integridade e segurança, sendo proibida sua utilização por terceiros.

A DTI entrará em contato com o solicitante por e-mail para tratar da entrega do token.

8.8 Problemas no uso inicial do certificado

Após a instalação, caso o certificado apresente algum problema, o usuário deverá entrar em contato com o fornecedor contratado, pelo canal informado na seção seguinte.

Caso o usuário não obtenha sucesso no contato ou na resolução do problema, deve contatar a DTI através do canal indicado na seção seguinte.

9. Suporte

Para suporte ao certificado digital, o usuário deve contatar o SERPRO, fornecedor contratado para a emissão do certificado, pelo site indicado pela empresa, informando seus dados e o CNPJ 17.217.985/0054-16.

Caso haja restrição para instalação de *software* no computador, favor contatar a equipe de TI local.

10. Proteção dos Dados Pessoais

A DTI realizará tratamento de dados pessoais do usuário logado e responsável pela requisição via formulário de justificativa e do requisitante dos serviços. As Disposições Gerais sobre o Tratamento de Dados Pessoais nos Serviços Fornecidos pela DTI podem ser encontradas no site da DTI, sendo essas informações complementares a estas Regras de Uso e sua leitura obrigatória pelo requisitante.

Os dados pessoais coletados do requisitante do serviço são:

- Nome completo;
- Número do Cadastro de Pessoas Físicas (CPF);
- E-mail; e
- Telefone.

Os dados pessoais coletados do usuário logado e responsável pela requisição:

- Nome completo;
- Login;
- E-mail do Usuário logado;
- Telefone;
- Matrícula UFMG;

É altamente recomendável que o próprio usuário requisitante do certificado digital preencha o formulário de justificativa.

Os dados são coletados para as seguintes finalidades:

- Permitir que a DTI identifique e entre em contato com o Requisitante do serviço;
- Permitir que a DTI identifique as solicitações de certificação com token e ajuste a entrega com o requisitante;
- Permitir que a DTI ateste os serviços prestados pela contratada para posterior pagamento;
- Permitir que a DTI conheça a demanda por certificação digital na universidade, defina a média de consumo a fim de garantir a continuidade do serviço e selecionar as melhores tecnologias para promover a melhoria contínua na prestação do serviço.

11. Contato

Dúvidas relacionadas a estas Regras de Uso deverão ser enviadas para o setor de suporte no endereço suporte@dti.ufmg.br.

Ficam estabelecidos o correio eletrônico da UFMG e o site da DTI como meios de comunicação oficiais entre os usuários e a DTI. Outras formas de comunicação não serão aceitas.

12. Considerações Gerais

A DTI considera-se no direito de modificar ou atualizar este documento sem prévio aviso ou consentimento de seus usuários.

A versão atualizada estará disponível no site da DTI (www.ufmg.br/dti).

A DTI entende que todos que solicitarem o serviço estão de acordo com as Regras de Uso descritas neste documento.

Caberá à Diretoria da DTI julgar os casos omissos neste documento.