ROTEIRO DE DEMONSTRAÇÃO DA SOLUÇÃO

Credenciamento de Gerenciadoras de Consentimento e Ciência – GCC
Secretaria Nacional de Trânsito – SENATRAN

MINISTÉRIO DOS TRANSPORTES

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

1. FINALIDADE E ESCOPO

O presente Roteiro estabelece as diretrizes técnicas, operacionais e procedimentais para a realização da Demonstração da Solução no âmbito do credenciamento de pessoas jurídicas interessadas em atuar como Gerenciadoras de Consentimento e Ciência – GCC.

A Demonstração possui natureza eliminatória e objetiva comprovar, de forma prática, mensurável e auditável, a capacidade da interessada de atender integralmente aos requisitos previstos no Estudo Técnico Preliminar e no Termo de Referência, especialmente quanto à interoperabilidade com os sistemas da SENATRAN e à entrega da solução como um todo.

2. PRINCÍPIOS E GOVERNANÇA

A Demonstração observará os princípios da legalidade, isonomia, impessoalidade, transparência, segurança da informação, rastreabilidade, governança e controle.

Todas as interessadas serão submetidas ao mesmo procedimento, critérios e condições técnicas, assegurando tratamento uniforme e vedação a qualquer favorecimento, salvo atualizações de versões deste documento técnico, que somente serão promovidas quando justificado operacionalmente, visando sempre o atingimento dos objetivos da demonstração exigidos no Termo de Referência.

3. ORGANIZAÇÃO DA SESSÃO DE DEMONSTRAÇÃO

A Demonstração será realizada presencialmente em Brasília/DF, na data e horário previamente informados por correio eletrônico.

A duração estimada da sessão será de aproximadamente 4 (quatro) horas, podendo ser concluída em prazo inferior, observado o limite máximo de 5 (cinco) horas.

Eventuais ocorrências que possam comprometer a participação deverão ser comunicadas previamente à Comissão de Contratação, inclusive por telefone indicado para situações urgentes.

A sessão será integralmente gravada, incluindo áudio, vídeo e compartilhamento de telas. Será coletada lista de presença dos participantes presenciais. O acompanhamento remoto poderá ocorrer por meio de plataforma de videoconferências indicada pela SENATRAN.

4. INFRAESTRUTURA E CONDIÇÕES TÉCNICAS

A interessada poderá utilizar equipamento próprio ou equipamento disponibilizado pela SENATRAN.

Caso utilize equipamento próprio, será responsável pela conectividade à internet ou pelo cumprimento das regras de segurança para acesso à rede institucional.

Deverão estar ativos: certificado digital válido, credenciais de acesso ao ambiente de homologação e todos os recursos técnicos necessários à execução integral da Demonstração.

5. AMBIENTE DE TESTES E MASSA DE DADOS

A Demonstração utilizará exclusivamente o ambiente oficial de homologação das APIs disponibilizado pela SENATRAN, por meio do Serviço Federal de Processamento de Dados – SERPRO.

A massa de dados será aquela existente no ambiente de homologação, podendo a SENATRAN gerar dados adicionais durante a sessão, conforme critérios técnicos.

É vedada a utilização de dados reais externos ao ambiente oficial.

BLOCO I – INTEROPERABILIDADE

O primeiro bloco da Demonstração visa comprovar a integração plena do ambiente tecnológico e da solução da interessada com o sistema Credencia e Plataforma de Gestão de Consentimento e Ciência – PGCC, mediante execução integral das 33 APIs previstas no roteiro oficial.

Para todas as API's deverá ser demonstrado resposta HTTP esperada, payload válido, persistência da operação, registro em log e rastreabilidade da transação. Os detalhes de execução das API's constam da documentação técnica disponibilizada em https://hom-pgcc.np.bsa.estaleiro.serpro.gov.br/manual/, mesmo link já utilizado para os testes iniciais de integração, e no Anexo I – Checklist Consolidado.

Credencia – Gestão de Vínculos (9 APIs)

Total de verificações obrigatórias: 9

PGCC – Gestão de Chaves Criptográficas (4 APIs)

Total de verificações obrigatórias: 4

PGCC – Gestão de HASH (4 APIs)

Total de verificações obrigatórias: 4

PGCC – Gestão de Consentimento (4 APIs)

Total de verificações obrigatórias: 4

PGCC – Gestão de Webhooks (5 APIs)

Total de verificações obrigatórias: 5

PGCC – Gestão da Privacidade do Cidadão (7 APIs)

Total de verificações obrigatórias: 7

BLOCO II – DEMONSTRAÇÃO DA SOLUÇÃO COMO UM TODO

O segundo bloco da Demonstração visa aferir a solução desenvolvida pela GCC para prestação dos serviços objeto do Credenciamento, nos termos do item 9.27, do Termo de Referência, e do Estudo Técnico Preliminar.

Para tanto, a interessada deverá promover a integração plena do ambiente tecnológico e da solução da interessada com o sistema Credencia e Plataforma de Gestão de Consentimento e Ciência – PGCC, mediante execução integral das 33 APIs previstas no roteiro oficial, além dos 16 itens relacionados à solução.

Serão avaliados os seguintes itens:

- Mecanismo de autenticação do titular;
- Interface web responsiva ou aplicação mobile com observância à acessibilidade digital (WCAG 2.1);
- Visualização de todos os tratamentos realizados;
- Ferramentas de filtro e pesquisa;
- Módulo de concessão revogação de consentimento;
- Apresentação da identidade e contato do encarregado de dados pessoais, da política de privacidade e dos termos de uso;
- Área de comunicação de incidentes de segurança e de registro de denúncias ou queixas sobre tratamento de dados;
- Apoio na pré-autorização de usuários;
- Capacidade de produção de tutoriais e conteúdos explicativos voltados aos titulares de dados e de produção de treinamentos aos colaboradores da SENATRAN e do SERPRO;
- Capacidade de atendimento integrado (apresentação e discussão, conforme documentação apresentada na fase de habilitação);
- Desenvolvimento de painéis e relatórios gerenciais;
- Documentação técnica dos serviços;
- Geração de logs, trilhas de auditoria completas e relatórios gerenciais;
- Geração de arquivos batch (CSV, JSON ou XML);
- Plano de continuidade de negócios e gestão de incidentes (apresentação e discussão, conforme documentação apresentada na fase de habilitação).

6. CRITÉRIOS DE AVALIAÇÃO

Cada item do checklist será classificado como: Atendido, Atendido com Ressalva, Não Atendido ou Não Aplicável.

Para fins de credenciamento será exigido atendimento integral (100%) dos requisitos.

Caso a interessada alcance no mínimo 90% (noventa por cento) dos requisitos avaliados, será concedido prazo máximo de 5 (cinco) dias úteis para saneamento das pendências, mediante nova sessão restrita aos itens não atendidos.

Percentuais inferiores a 90% implicarão no indeferimento do pedido de credenciamento.

7. RELATÓRIO FINAL

Ao término da Demonstração serão consolidados o checklist preenchido, o registro de evidências, os logs apresentados e a gravação da sessão, que subsidiarão a elaboração de relatório circunstanciado contendo a conclusão fundamentada.

A interessada deverá disponibilizar todos os logs gerados durante a sessão antes do encerramento.

Aprovada a Demonstração, após a elaboração do relatório circunstanciado, com o resultado da avaliação, os autos serão encaminhados à autoridade competente para seguimento dos trâmites do Credenciamento.

ANEXO I – CHECKLIST CONSOLIDADO

Bloco I – APIs: 33 verificações obrigatórias.
Bloco II – Solução como um todo: 16 verificações obrigatórias.
Total mínimo de verificações: 49 itens avaliáveis.

Cada item será registrado em planilha específica contendo: descrição do requisito, evidência apresentada, classificação atribuída e observações técnicas.

ANEXO II – DETALHAMENTOS DAS API'S

Este Anexo apresenta a estrutura de demonstração para Gerenciadoras de Consentimento e Ciência (GCC) comprovarem a interoperabilidade com os sistemas da SENATRAN.

O Objetivo da Demonstração é comprovar a capacidade técnica da GCC de integrar-se completamente aos sistemas da SENATRAN, operando todos os serviços disponíveis nas plataformas Credencia e PGCC.

- **Etapa 1: APIs CREDENCIA**

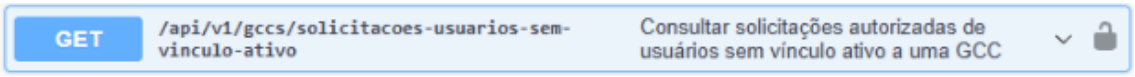
Foco: Credenciamento, Prospecção e Gestão de Vínculos

Pré-requisitos:

- Certificado digital e-CNPJ registrado no credencia de homologação.
- Ter solicitação de credenciamento autorizada e habilitada no ambiente de homologação do Credencia
- Ter ambiente de teste configurado com acesso à API Credencia
- Ter contrato de teste em formato PDF com no máximo 3MB preparado para upload

GESTÃO DE VÍNCULOS (9)

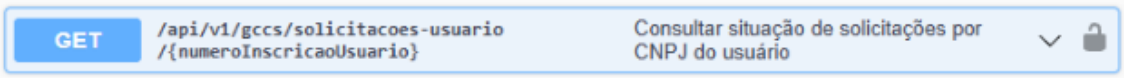
1- Consultar Usuários sem Vínculo Ativo:



Listar usuários autorizados que ainda não possuem vínculo ativo com a GCC:

Critério de sucesso: Retorno 200 com uma lista de usuários

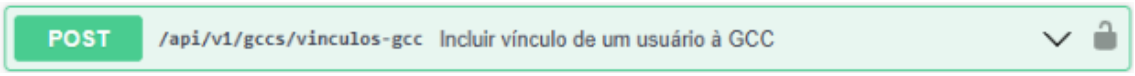
2 - Consultar situação de solicitações de um usuário:



Consultar detalhes das solicitações de um usuário específico fornecendo o CNPJ.

Critério de sucesso: Retorno 200 com as informações das solicitações do usuário informado.

3 - Incluir vínculo de usuário:



Realizar a vinculação de um usuário à GCC enviando o arquivo PDF do contrato.

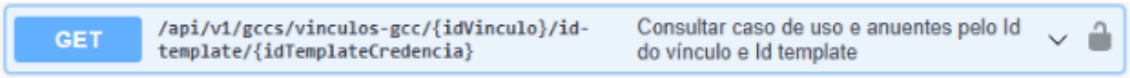
Critério de sucesso: Retorno 201 contendo ID do vínculo criado e dados do usuário. Anote o idVinculo para consultas posteriores. OBS: o Campo “deAcordo” estará com valor 0 (PENDENTE) aguardando confirmação do usuário.(Na demonstração essa confirmação será feita pela equipe do SERPRO)

4 - Consultar um vínculo específico fornecendo o ID do vínculo:

Permite consultar a situação do vínculo e saber se o usuário já confirmou a vinculação.

Critério de sucesso: Retorno 200 e informações do vínculo cujo ID foi informado.

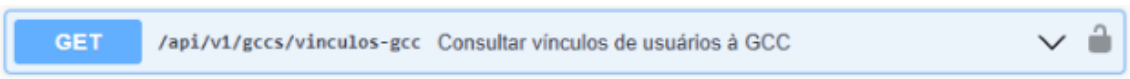
5 - Consultar casos de uso e anuentes pelo ID do vínculo e ID do template



Permite consultar casos de uso e anuentes de um usuário vinculado à GCC.

Critério de sucesso: Retorno 200 e informações de de caso de uso retornando metadados e anuentes.

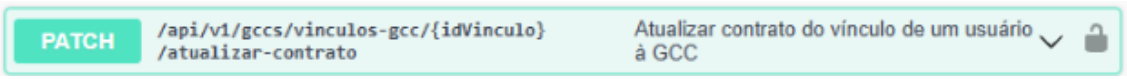
6 - Consultar usuários vinculados à GCC:



Listar todos os seus usuários vinculados. A GCC que está realizando a requisição é identificada pelo CNPJ contido no certificado digital;

Critério de sucesso: Retorno 200 e dados de todos os usuários vinculados à GCC requisitante.

7 - Atualizar o contrato de um vínculo de usuário à GCC



Permite manter o cadastro atualizado em casos de alterações contratuais.

Critério de sucesso: Retorno 200 e dados do novo arquivo cadastrado no sistema.

8 - Desativar vínculo de usuário à GCC

Permite encerrar o contrato do usuário com a GCC.

Critério de sucesso: Retorno 200 com motivo do término do contrato com o usuário registrado.

9 - Reativar vínculo de usuário à GCC

Permite reativar o vínculo do usuário à GCC desde que haja contrato vigente.

Critério de sucesso: Retorno 200 e vínculo restabelecido ("ativo": true).

- **Etapa 2: APIs PGCC**

Foco: Chaves públicas, webhooks, HASHes e tratamento de dados (consentimento/ciência)

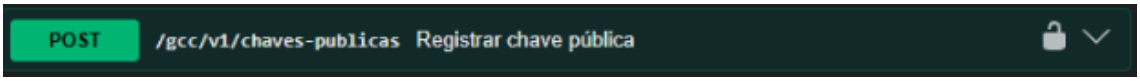
Pré-requisitos:

- Certificado digital e-CNPJ registrado no Credencia de homologação;

- Ter concluído a autorização e habilitação do credenciamento no Credencia;
- Ter vínculo ativo com ao menos um Usuário confirmado no Credencia;
- Capacidade de gerar chaves assimétricas RSA e mantê-las em segurança para a assinatura de JWTs;
- Prover um serviço web em domínio público acessível para o recebimento de mensagens via webhooks

GESTÃO DE CHAVES CRIPTOGRÁFICAS (4)

1 - Registrar chave pública



Permite registrar uma nova chave pública da GCC que será utilizada pela PGCC para manipular os HASHEs enviados pela GCC.

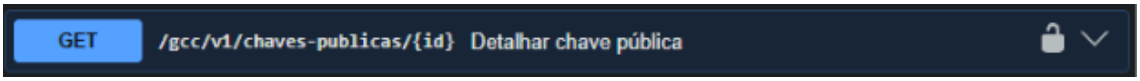
Critério de sucesso: retorno 201 com a confirmação da chave pública inserida.

2 - Consultar chaves públicas registradas

Permite consultar todas as chaves públicas já registradas pela GCC.

Critério de sucesso: retorno 200 e informações das chaves públicas registradas.

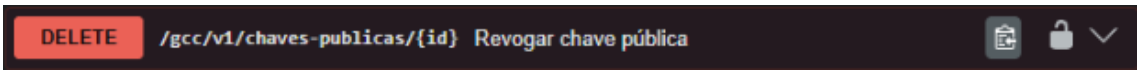
3 - Detalhar chave pública específica



Permite obter detalhes de uma determinada chave pública previamente registrada informando o ID.

Critério de sucesso: retorno 200 com as informações da chave pública especificada no ID.

4 - Revogar uma chave pública



Permite revogar uma chave pública específica informando seu ID

Critério de sucesso: retorno 200 com informações da revogação da chave pública especificada.

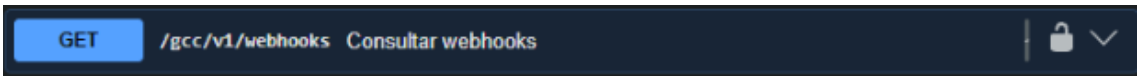
GESTÃO DE WEBHOOKS (5)

1 - Registrar Webhook

Registrar um novo webhook para receber as comunicações da PGCC

Critério de sucesso: Retorno 201 e dados do webhook inserido

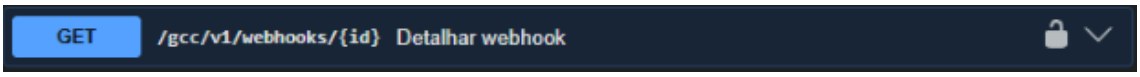
2 - Consultar webhooks



Resgatar os webhooks previamente registrados pela GCC

Critério de sucesso: Retorno 200 e receber informações dos webhooks registrados.

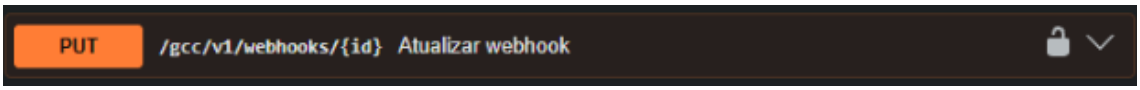
3 - Detalhar webhook



Resgatar informações de um webhook específico.

Critério de sucesso: Retorno 200 e receber informações do webhook pesquisado.

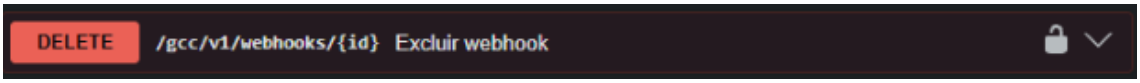
4 - Atualizar webhook



Permite alterar informações de um webhook previamente registrado.

Critério de sucesso: Retorno 200 e exibir as novas informações do webhook com data de atualização.

5 - Excluir webhook

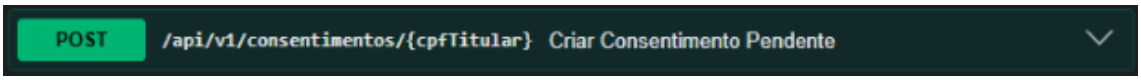


Permite excluir um webhook específico

Critério de sucesso: Retorno 200 e exibir as informações do webhook com a data de exclusão.

GESTÃO DE CONSENTIMENTO (4)

1 - Criar consentimento pendente



Permite criar um consentimento que vai ficar aguardando a aprovação do titular.

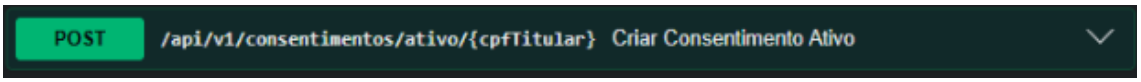
Critério de sucesso: Retorno 201 e log criado aguardando autorização do titular.

2 - Consultar consentimento

Consultar a situação de um consentimento

Critério de sucesso: Retorno 200 e receber dados do consentimento pesquisado.

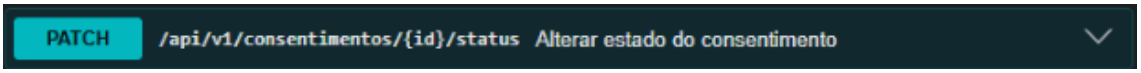
3 - Criar consentimento ativo



Criar na PGCC um consentimento previamente solicitado e já aprovado pelo titular.

Critério de sucesso: Retorno 201 e confirmação de consentimento criado na PGCC.

4 - Alterar estado do consentimento

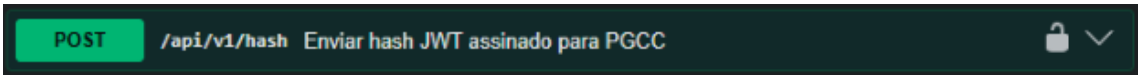


Alterar o estado de um consentimento existente

Critério de sucesso: Retorno 200 e status do consentimento alterado com sucesso.

Gestão de HASH (4)

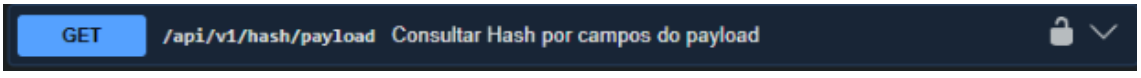
1 - Enviar um HASH para PGCC



Geração e envio de HASHs de consulta para a PGCC.

Critério de sucesso: PGCC receber e validar o HASH com a chave pública previamente registrada.

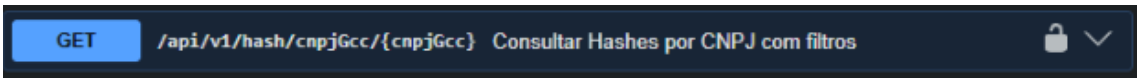
2 - Consultar HASHs por campos do payload



Consultar hash específico utilizando campos do payload (não pelo JWT completo).

Critério de sucesso: Retorno 200 e receber dados do HASH pesquisado.

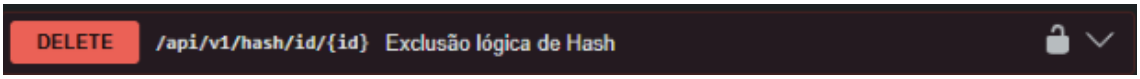
3 - Consultar HASH por CNPJ



Consultar HASH específico filtrando por CNPJ e outros filtros

Critério de sucesso: Retorno 200 e receber dados do HASH pesquisado.

4 - Exclusão lógica do HASH

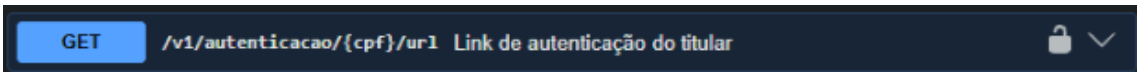


Exclusão lógica um determinado HASH

Critério de sucesso: Retorno 200 e HASH marcado como excluído com sucesso.

GESTÃO DA PRIVACIDADE DO CIDADÃO (7)

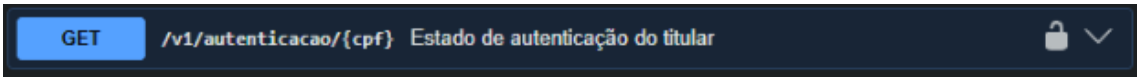
1 - Link de autenticação do titular



Gera um endereço de autenticação para o titular cujo CPF foi informado no parâmetro.

Critério de sucesso: Retorno 200 e a url criada para o usuário

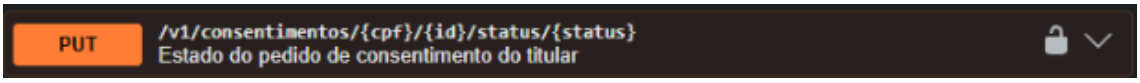
2 – Estado de autenticação do titular



Traz informação do estado de autenticação do titular logado na plataforma.

Critério de sucesso: Retorno 200 e informações de autenticação do titular logado na plataforma.

3 - Alterar o estado de um consentimento



Permite alterar o estado de um consentimento a pedido do titular.

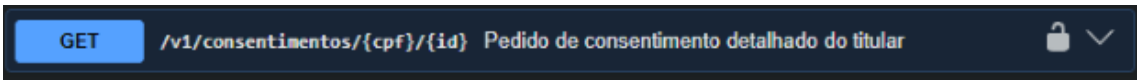
Critério de sucesso: Retorno 200 e receber informações do consentimento com o novo status de acordo com a alteração.

4 - Pedidos de consentimento do titular

Exibe todos os consentimentos do titular solicitante e logado na plataforma.

Critério de sucesso: Retorno 200 e relação dos consentimentos do titular solicitante e logado na plataforma.

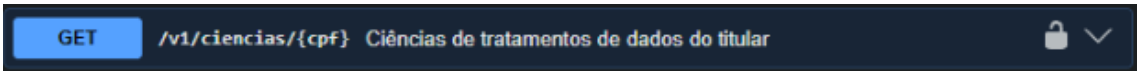
5 - Detalhes de um pedido de consentimento específico



Traz mais informações de um consentimento especificado na busca que seja do titular logado na plataforma

Critério de sucesso: Retorno 200 e detalhes do consentimento buscado.

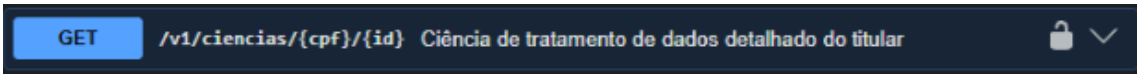
6 - Ciências de tratamento de dados



Traz todas as ciências de tratamento de dados do titular logado na plataforma.

Critério de sucesso: Retorno 200 e relação das ciências de tratamento de dados do titular logado na plataforma.

7 - Detalhe de uma ciência de tratamento de dados



Traz informações de uma ciência de tratamento de dados especificada pelo ID

Critério de sucesso: Retorno 200 e todas as informações referentes à ciência de dados especificada na consulta.