PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL
SCN QUADRA 02 BLOCO E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3945 - https://www.iti.gov.br

INSTRUÇÃO NORMATIVA Nº 07, DE 30 DE OUTUBRO DE 2019

Altera os itens 6.4 e 6.5.7 do DOC-ICP-17.01, que tratam dos requisitos para serviços de confiança de uso de chaves privadas e da Lista de Prestador de Serviço de Confiança.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 9º do anexo I do Decreto nº 8.985, de 8 de fevereiro de 2017, e pelo art. 1º da Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004,

RESOLVE:

Art. 1º O DOC-ICP-17.01, versão 2.1, passa a vigorar com as seguintes alterações:

"……..

6.4.3.1……

……..

i. Código de Autorização
ii. Token de Acesso
iii. Assinatura

Quando for necessário utilizar serviço de confiança destinado somente à autenticação do titular, ou seja, sem o uso de chave privada, deverá ser precedido de solicitação bem-sucedida, por parte de aplicações, dos seguintes serviços:

i. Código de Autorização
ii. Token de Acesso
iii. Recuperação de Certificado

6.4.3.2 Trânsito de Fatores de Autenticação

As aplicações não deverão coletar fatores de autenticação do titular. Para este fim, os PSC deverão se comunicar diretamente com equipamento do titular, previamente identificado e cadastrado junto ao PSC de forma segura.

Excetua-se desta regra o Serviço "Autorização com Credenciais do Titular".

……..

6.4.4……

a) ……..

……..

v. Listagem de Certificados do Titular

vi. Localização de Titular

vii. Recuperação de Certificado

b) ……..

……..

6.4.5.1. Serviços de Autorização

6.4.5.1.1 Código de Autorização (*Authorization Code Request*)

Serviço para obter do titular a autorização de uso da sua chave privada ou autorizar autenticação sem uso da chave privada.

Caso o titular possua mais de um certificado, o PSC deverá apresentá-los para que o titular faça a escolha no mesmo contexto de aplicação em que transitarem os fatores de autenticação.

Caberá ao PSC apresentar ao titular o escopo da solicitação (vide parâmetro "*scope*" abaixo), permitindo a diferenciação inequívoca de solicitações que envolvam assinaturas daquelas que tratam somente de autenticação. Esta apresentação deverá ser feita durante o trânsito de fatores de autenticação.

a) Solicitação

- Path : <URI-base>/oauth/authorize;
- Método HTTPS: GET;
- Parâmetros da requisição: concatenados após o Path como parâmetros http query, usando o formato "application/x-www-form-urlencoded":
  - response_type: obrigatório, valor "code";
  - client_id: obrigatório, deve conter a identificação da aplicação;
  - redirect_uri: opcional, deve ter a URI para redirecionar o usuário de volta para a aplicação de origem. A URI deve estar na lista de URI's autorizadas para a aplicação. Deve ser URL ENCODED. Se não informado, será considerada a primeira URI cadastrada para a aplicação;
  - state: opcional, é retornado sem modificações para aplicação de origem;

- Recomendado. Um valor opaco usado pela aplicação para manter o estado entre a requisição e a resposta. O serviço de autorização incluirá este valor ao redirecionar o módulo do usuário de volta ao endereço da aplicação. Este parâmetro deverá ser usado para prevenir ataques de falsificação de requisições entre sites (cross-site request forgery).

- lifetime: opcional, indica o tempo de vida desejado para o token a ser gerado. Inteiro, em segundos;
- scope: opcional, se não informado, será considerado "*authentication_session*". (ver lista de escopos abaixo). Possíveis valores para o parâmetro:
  - **single_signature**: token que permite a assinatura de apenas um conteúdo (hash), sendo invalidado apos a sua utilização;
  - **multi_signature**: token que permite a assinatura de múltiplos hashes em uma única requisição, sendo invalidado apos a sua utilização;
  - **signature_session**: token de sessão OAuth que permite várias assinaturas em várias chamadas a API, desde que o token esteja dentro do prazo de validade ou que não tenha sido revogado pela aplicação ou pelo usuário;
  - **authentication_session**: token de sessão OAuth para autenticação do titular, não permitindo a realização de assinaturas ou outras utilizações da chave privada.
- code_challenge: obrigatório, ver RFC 7636
- code_challenge_method: obrigatório, valor “S256” (ver RFC 7636).
- login_hint: opcional, valor de CPF ou CNPJ a ser informado como filtro para seleção do certificado a ser utilizado.

b) Resposta da Requisição de Código de Autorização:

Se o usuário autorizar a solicitação, o PSC emite um código de autorização com tempo de validade curto e retorna para aplicação cliente com uma URI de redirecionamento contendo os seguintes parâmetros no componente http query, usando o formato "application/x-www-form-urlencoded":

- code: obrigatório, código de autorização gerado pelo PSC, a ser usado na solicitação do token de acesso.
- state: obrigatório caso tenha sido informado na requisição, deverá conter o que foi enviado na requisição.

Se o usuário não autorizar a solicitação, o PSC retorna para aplicação cliente através de sua redirect_uri os seguintes parâmetros via http query, usando o formato "application/x-www-form-urlencoded":

- error: obrigatório, com o valor “user_denied”;
- state: obrigatório caso tenha sido informado na requisição, deverá conter o que foi enviado na requisição.

6.4.5.1.2 ……..

.....

6.4.5.2 Assinatura

Os parâmetros com conteúdo a ser assinado e assinaturas deverão conter valores em Base64.

As assinaturas RAW estarão em Base64.
Assinaturas CMS estarão em formato CMS PEM de acordo com RFC 7468: o cabeçalho e rodapé CMS são obrigatórios; quebra de linha e espaços no conteúdo são opcionais; e as aplicações devem estar preparadas para lidar com diferentes formas de espaços e quebra de linhas no conteúdo, ou com a ausência destes.

Se o escopo do token permitir apenas uma assinatura (single_signature) e for informado mais de um conteúdo, uma mensagem de erro deve ser retornada.

Se o escopo for omitido ou assinalado para autenticação (authentication_session) uma mensagem de erro deve ser retornada.

a) Solicitação

- Path: <URI-base>/oauth/signature
- Método HTTPS: POST
- Cabeçalho
  - Content-type: application/json;
  - Accept : application/json;
  - Authorization: Bearer access_token;
- Parâmetros: formato "application/json;charset=UTF-8" :
  - certificate_alias: opcional, identificador do certificado correspondente à chave utilizada na assinatura;
  - hashes: conjunto com valores obrigatórios a serem assinados. Cada elemento do conjunto conterá:
    - id: identificador do conteúdo a ser assinado;
    - alias: forma legível do identificador do conteúdo;
    - hash: conteúdo a ser assinado;
    - hash_algorithm: Object Identifier (OID) do algoritmo de hash. Por exemplo, para SHA256 utilize o OID 2.16.840.1.101.3.4.2.1;
    - signature_format: deverá conter um dos valores:
      - RAW,
      - CMS.

Exemplo

……..

.....

b) Resposta da Requisição de Assinatura:

O PSC retornará a requisição com sucesso, via HTTP Status Code 200.

- Parâmetros: formato "application/json;charset=UTF-8":
  - certificate_alias: obrigatório, identificador do certificado correspondente à chave utilizada na assinatura;
  - signatures: obrigatório, conjunto com identificadores dos conteúdos assinados e valores assinados. Cada elemento do conjunto conterá:
    - id: identificador do conteúdo assinado;
    - Um dos formatos abaixo:
      - caso a solicitação tenha sido feita com “signature_format : RAW”

◦ raw_signature: valor numérico em base64 da assinatura produzida.

- caso a solicitação tenha sido feita com “signature_format : CMS”

◦ CMS detached (PKCS#7), contendo os seguintes atributos assinados:

- contentType

- signingTime (hora do PSC)

- messageDigest (hash informado pela aplicação na requisição)

- signingCertificateV2 (certificado do assinante)

Obs.: Os valores de assinatura deverão produzidos de acordo com a suíte de assinatura, se esta for informada.

Exemplo

.....

.....

6.4.5.3. Cadastro de Aplicação com Certificado

.....

.....

6.4.5.4 Recuperação de Certificado

Serviço para recuperar certificado armazenado no PSC.
A aplicação deverá ter um Access Token válido.

a) Solicitação

- Path : <URI-base>/oauth/certificate-discovery;
- Método HTTPS: GET
- Cabecalho
  - Content-type: application/json;
  - Accept: application/json;
  - Authorization: Bearer access_token;
- Parâmetros da requisição: concatenados após o *Path* como parâmetros *http query*, utilizando o formato “*application/x-form/urlencoded*”
  - certificate_alias: opcional, é o identificador do certificado a ser recuperado.

.....

.....

6.4.5.5. Localização de Titular

.....

.....

6.4.6.3 . .....

.....

a) Solicitação

- Path: <URI-base>/oauth/pwd_authorize ;
- Método HTTPS: POST;
- Cabeçalho:
  - Content-type: application/json;
  - Accept: application/json;
- Parâmetros: formato "application/json;charset=UTF-8" :
  - grant_type, obrigatório, valor "password”;
  - client_id, obrigatório, identificação da aplicação;
  - client_secret, opcional, sendo obrigatório apenas quando a aplicação não utilizar certificado ICP-Brasil;
  - username, obrigatório, identificação do usuário por meio de CPF ou CNPJ;
  - password, obrigatório, valor da concatenação de fatores de autenticação informadas pelo usuário;
  - lifetime, opcional, valor inteiro, indica o tempo de vida desejado para o token a ser gerado em segundos. Para acesso a objeto de pessoas físicas não deve ultrapassar 7 (sete) dias, sendo que para pessoas jurídicas este limite será de 30 (trinta) dias;
  - scope, opcional, se não informado será considerado "*authentication_session*". (ver lista de escopos para Serviço de Código de Autorização).
  - slot_alias: opcional, indica o slot do usuário no qual a autenticação deve ser feita. Se não informado, o PSC decidirá em qual slot tentar a autenticação.

Exemplo

.....

.....

b) Resposta da Requisição de Autorização com Credenciais do Titular

- Parâmetros de retorno para os demais valores de "*scope*": formato "application/json;charset=UTF-8":
  - access_token, obrigatório, valor do token de acesso;
  - token_type, obrigatório, valor "Bearer";
  - expires_in, obrigatório, valor inteiro com validade do token em segundos. Para acesso a objeto de pessoas físicas, não deve ultrapassar 7 (sete) dias, sendo que para pessoas jurídicas, esse limite será de 30 (trinta) dias;
  - scope, opcional, informado apenas se o escopo retornado for diferente do solicitado pela aplicação.
  - slot_alias: obrigatório, indica o slot do usuário no qual a autenticação foi feita (sem middleware).

Exemplo

.....

.....

6.5.7 A LPSC conterá na URI de base que define o serviço (*SchemeServiceDefinitionURI*) a versão da API correspondente, podendo apresentar mais de uma instância de versão para minimizar comprometimento das aplicações integradas.

....." (NR)

Art. 2º Aprovar a versão 2.2 do documento DOC-ICP-17.01 - PROCEDIMENTOS OPERACIONAIS MÍNIMOS PARA OS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL.

§ 1º As demais cláusulas do referido documento, na sua versão imediatamente anterior, integram a presente versão e mantêm-se válidas.

§ 2º O documento referido no caput encontra-se disponibilizado, em sua totalidade, no sítio http:// www.iti.gov.br.

Art. 3º Esta Instrução Normativa entra em vigor na data de sua publicação.

MARCELO AMARO BUZ

Diretor-Presidente

Documento assinado eletronicamente por **Marcelo Amaro Buz**, **Presidente**, em 30/10/2019, às 11:37, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.
Nº de Série do Certificado: 22449

A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0383150** e o código CRC **9436CBF8**.