Transferência de arquivos sobre os certificados digitais, biometrias, agentes de registro e outras informações

1 Acesso ao Serviço

Para fins de envio de documentos, o Instituto Nacional de Tecnologia da Informação - ITI disponibiliza, através de SFTP (*SSH File Transfer Protocol*), meio para transferência dos arquivos relativos ao envio dos certificados, biometrias e demais informações solicitadas pelo ITI. A transferência deve ser feita entre o equipamento da AC/PSS e o serviço disponibilizado pelo ITI.

Para acesso ao serviço, o responsável técnico da AC responsável pelo envio deve encaminhar e-mail para cgope@iti.gov.br, contendo:

- Endereço IP a partir do qual serão realizados os acessos ao serviço disponibilizado pelo ITI;
- Chave pública padrão RSA 2048 (se PSS, deve haver 1 chave para cada AC representada);
- Nome da AC (em caso de PSS, esse deve informar o nome de cada AC);
- Dados (nome e contatos) do(s) responsável(is) técnico(s) da AC ou Prestador de Serviço de Suporte (PSS).

Por ocasião da alteração de qualquer dos dados acima, a AC ou seu PSS deverá retificá-lo por meio do mesmo e-mail.

Após o recebimento e validação das informações acima, o ITI encaminhará, como resposta, e-mail com as seguintes informações:

- Url do canal de comunicação no qual será disponibilizado o serviço;
- Dados (nome, telefones e endereço de correio eletrônico) do responsável para suporte técnico;
- Informações/orientações para configuração de um serviço de autenticação ssh.

Qualquer alteração nas informações acima será comunicada por e-mail para os endereços informados pelas ACs.

Em caso de problema de acesso aos serviços disponibilizados pelo ITI, envie e-mail com a descrição do problema.

Eventuais indisponibilidades programadas serão informadas por e-mail para os responsáveis técnicos

devidamente cadastrados.

Toda e qualquer comunicação entre ITI e ACs ou vice-versa se dará por mensagem de correio eletrônico (e-mail) assinada digitalmente com certificado digital padrão ICP-Brasil.

2 Identificação dos arquivos biométricos

Os arquivos biométricos da face e das impressões digitais deverão ter os formatos conforme consta no DOC-ICP-05.02 e no DOC-ICP-05.03. O nome do arquivo biométrico deve ser formado pelo hash SHA1 do arquivo do certificado e a indicação do dedo, se for o caso, seguindo os seguintes padrões:

I – FACE

Arquivo de face (jpeg, jpg)

(i) Nome: “aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.jpeg”, onde as letras “a” representam o hash SHA1 do arquivo do certificado.

(ii) Tamanho: 1MB (max).

II – IMPRESSÃO DIGITAL

Arquivo de impressão digital (wsq)

(i) Nome: “aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa_1.wsq”, onde as letras “a” representam o hash SHA1 do arquivo do certificado e o número seguinte ao caractere *underscore* representa a indicação do dedo (um ou dois dígitos – no exemplo é o polegar esquerdo).

(ii) Tamanho: 50KB (max).

O hash SHA1 utilizado na identificação dos arquivos biométricos deve ser gerado a partir do correspondente arquivo do certificado que será encaminhado ao ITI. Esse mesmo hash deverá ser informado no conteúdo do arquivo “Anexo1.csv” associado ao local da emissão.

3 Identificação do arquivo compactado

O nome do arquivo compactado, contendo todos os arquivos elencados na Instrução Normativa ITI nº 31, de 14 de março de 2025, deve seguir o formato: AAAAMMDD_Nome-da-AC_Emissora.zip, em que AAAA=ano de referência, MM=mês de referência, DD=dia de referência, Nome-da-AC=nome que identifica a AC emissora.

O Nome-da-AC identifica a AC que emitiu o certificado, devendo ser enviado um arquivo compactado para cada AC que emite certificados para usuário final.

Esse arquivo deverá conter os certificados, as biometrias e o anexo (CSV) com os locais de emissão dos certificados referentes as emissões de certificados do período correspondente.

4 Definições do formato dos arquivos csv

4.1 Formato do arquivo

Para a transferência das informações ao Instituto Nacional de Tecnologia da Informação - ITI devem ser observados os dados solicitados para cada caso, devendo ser utilizados arquivos no formato CSV.

CSV é a abreviação do termo em inglês *Comma-Separated Values*, que pode ser traduzido para o português como "Valores separados por vírgulas", e é constituído de um arquivo de texto cujas informações contidas estão separadas por **ponto e vírgula**. Exemplo: Fulano de Tal;23/10/1983;Maria de Tal.

Normalmente, a extensão do arquivo utilizada nesses casos é ".csv" e refere-se a um formato de arquivo de dados definido na RFC 4180, sendo suportado pela maioria dos softwares de planilha eletrônica e Sistemas Gerenciadores de Banco de Dados - SGDB. Além disso, é recomendado pelo Padrão de Interoperabilidade de Governo Eletrônico - ePing e utilizado pelo Portal da Transparência do Governo Federal.

No caso dos arquivos CSV que devem ser encaminhados ao ITI, cada linha deve conter uma unidade de informação, com os campos separados por ponto e vírgula. A ordem dos campos deve seguir rigorosamente a ordem solicitada em cada caso.

O ponto e vírgula deverá constar mesmo quando o campo correspondente não for preenchido. Exemplo: 1234;5678;;;91011. Nesse caso, dois campos foram deixados sem preenchimento. Importante observar que a linha não pode terminar em ponto e vírgula, exceto se a informação do último campo estiver vazia.

Para evitar problemas de compatibilidade na codificação dos caracteres, os arquivos encaminhados ao ITI devem utilizar a codificação UTF-8 ISO/IEC 10646:2014, recomendada pelo ePing.

4.2 Formatação dos campos

Em cada caso, quando solicitado, devem ser observadas as orientações abaixo para o preenchimento dos campos.

Código IBGE: O código IBGE do município está disponível no site do IBGE e deve ser informado com sete dígitos, por exemplo, para Brasília deve ser informado o código 5300108. Excepcionalmente, para emissões realizadas no localidades fora do Brasil, fica estabelecido como código de Município o numeral 90 (noventa), acrescido da codificação numérica de país definida pela ISO 3166, com 3 (três) dígitos numéricos. Exemplos: EUA=90840; Portugal=90620.

CNPJ: O número do Cadastro Nacional de Pessoa Jurídica deve ser informado com 14 dígitos sem os separadores. Exemplo: o CNPJ 99.999.999/9999-99 deve ser informado 99999999999999.

Data: as informações de data devem ser preenchidas no formato Timestamp (“YYYY-MM-DDThh:mm:ssthh”). Exemplo (“2018-03-22T12:00:00-03”)

Ano: a informação de ano deve ser preenchida no formato aaaa, ou seja, sempre com os quatro números que compões essa informação, exemplos: 1999, 2000, 2021, 2022, etc.

Relação das não conformidades identificadas: código do controle (primeira coluna) constante do ADE_ICP 08.E, dois pontos e descrição da não conformidade conforme consta do relatório de auditoria. Ex: 20601002:Fragilidade nas atualizações do sistema operacional. Caso tenha uma não conformidade que envolva vários itens do ADE_ICP 08.E, deve ser lançado o código do item mais relevante ou principal.

Número do OID da DPC da AC: Os números de identificação de cada DPC das AC credenciadas na ICP-Brasil estão disponíveis no documento ADE-ICP-04.01, no arco 2.16.76.1.1 - Arco de OID para Declarações de Prática de Certificação na ICP-Brasil, primeira coluna. No preenchimento dos campos de OID no arquivo CVS devem ser retirados os pontos separadores, assim, o OID 2.16.76.1.1.0 deve ser informado como 21676110.

5 Modelo Informacional de Dados dos Certificados Emitidos

Item	Descrição	Tipo de Dado	Presença de conteúdo	Conceito/Observação (regra de negócio)
Hash_SHA1	Hash SHA1 da chave pública do certificado	Caracteres alfanuméricos	Obrigatória na emissão Presencial, Videoconferência, Certificado Digital e AR eletrônica	Representa o resumo criptográfico SHA1 da chave pública do certificado digital emitido. Texto variável máximo de 40 caracteres.
Codigo_IBGE	Código do município no cadastro do IBGE	Caracteres numéricos	Obrigatória na emissão Presencial e Videoconferência, nos demais casos preencher “0” (zero)	O identificador é o código do município onde ocorreu a identificação presencial. Tamanho variável máximo de sete caracteres. Deve ser informado com 7 caracteres, por exemplo, para Brasília deve ser informado o código 5300108. Excepcionalmente, para emissões realizadas no localidades fora do Brasil, fica estabelecido como código de Município o numeral 90 (noventa), acrescido da codificação numérica de país definida pela ISO 3166, com 3 (três) dígitos numéricos. Exemplos: EUA=90840; Portugal=90620
Modo_emissao	Modalidade de emissão (Presencial ou Videoconferência ou Certificado Digital ou AR eletrônica	Caracteres alfanuméricos	Obrigatória na emissão Presencial, Videoconferência, Certificado Digital e AR eletrônica	Indica a modalidade utilizada na identificação do titular no processo de emissão do certificado digital. Texto variável, máximo 16 caracteres
CNPJ_AR	CNPJ da AR que realizou a identificação do titular	Caracteres alfanuméricos	Obrigatória na emissão Presencial, Videoconferência e AR eletrônica, nos demais casos preencher “VAZIO”	O identificador é o número de inscrição no CNPJ – Cadastro Nacional de Pessoas Jurídicas da Autoridade de Registro - AR que realizou a identificação do titular. Texto variável, máximo de 14 caracteres sem separador. O campo dever ser preenchido com zeros a esquerda (exemplo: 00000000100. Regra Negocial: Caso a emissão tenha ocorrido sem a etapa de verificação (renovação com certificado digital valido, nos casos previstos em norma, deve conter o CNPJ da AR da AC emissora

Item	Descrição	Tipo de Dado	Presença de conteúdo	Conceito/Observação (regra de negócio)
CPF_AGR_i	CPF_AGR Identificação presencial ou videoconferência	Caracteres numéricos	Obrigatória na emissão Presencial e Videoconferência, nos demais casos preencher “0” (zero)	O identificador é o número de inscrição no CPF do(a) AGR que realizou a identificação presencial. Texto variável, máximo de 11 caracteres sem separadores. O campo dever ser preenchido com zeros a esquerda (Exemplo 11111111111)
CPF_AGR_v	CPF do AGR Verificação da solicitação de certificado	Caracteres numéricos	Obrigatória na emissão Presencial, nos demais casos preencher “0” (zero)	O identificador é o número de inscrição do(a) no CPF do AGR que realizou a identificação verificação. Texto variável, máximo de 11 caracteres sem separadores. O campo dever ser preenchido com zeros a esquerda (Exemplo 00111111111)
Data_i	Data e Hora da Identificação do titular	Timestamp	Obrigatória na emissão Presencial, Videoconferência e AR eletrônica, nos demais casos preencher “VAZIO”	Identifica a data e hora que foi realizada a IDENTIFICAÇÃO da Pessoa física requerente do certificado digital, conforme registrado no sistema de AR da AC, de acordo com o formato (“YYYY-MM-DDThh:mm:ssthh”) e ajustado o exemplo (“2018-03-22T12:00:00-03”)
Data_v	Data e hora da Validação do titular	Timestamp	Obrigatória na emissão Presencial, nos demais casos preencher “VAZIO”	Identifica a data e hora que foi realizada a VALIDAÇÃO dos dados da Pessoa física requerente do certificado digital, conforme registrado no sistema de AR da AC, de acordo com o formato (“YYYY-MM-DDThh:mm:ssthh”) e ajustado o exemplo (“2018-03-22T12:00:00-03”)
Data_em	Data e hora da Emissão do certificado	Timestamp	Obrigatória na emissão Presencial, Videoconferência, Certificado Digital e AR eletrônica	Identifica a data e hora que foi realizada a EMISSÃO DO CERTIFICADO ao titular do certificado digital, conforme registrado no sistema de AR da AC, de acordo com o formato (“YYYY-MM-DDThh:mm:ssthh”) e ajustado o exemplo (“2018-03-22T12:00:00-03”)
Data_PSBIO	Data hora da resposta do PSBIO	Timestamp	Obrigatória na emissão Presencial, Videoconferência e AR eletrônica, nos demais casos preencher “VAZIO”	Identifica a data e hora que foi realizada o batimento biométrico da Pessoa física requerente do certificado digital, conforme registrado no sistema de AR da AC, de acordo com o formato (“YYYY-MM-DDThh:mm:ssthh”) e ajustado o exemplo (“2018-03-22T12:00:00-03”)

Item	Descrição	Tipo de Dado	Presença de conteúdo	Conceito/Observação (regra de negócio)
TCN	TCN - transação biométrica	Caracteres alfanuméricos	Obrigatória na emissão Presencial, Videoconferência e AR eletrônica, nos demais casos preencher “VAZIO”	O Número de controle da Transação - TCN é o número único que originou a transação biométrica do requerente de certificado digital. Texto variável, máximo de 36 caracteres
IDN	IDN do Titular ou do Responsável pelo certificado de PJ	Caracteres alfanuméricos	Obrigatória na emissão Presencial, Videoconferência e AR eletrônica, nos demais casos preencher “VAZIO”	O identificador de registro biométrico - IDN correspondente ao número de inscrição do CPF do requerente do certificado que realizou a identificação presencial. Texto variável, máximo de 88 caracteres
CPF_RESP_SELO	CPF do Responsável Legal pela Pessoa Jurídica solicitante do Selo Eletrônico ou certificado de PJ	Caracteres numéricos	Obrigatória na emissão Presencial e Videoconferência, para certificados de SELO, nos demais casos preencher “VAZIO”	O identificador é o número de inscrição no CPF do(a) representante legal da Pessoa Jurídica, identificado presencialmente ou por videoconferência que solicitou o certificado digital de Selo Eletrônico ou de Pessoa Jurídica. Texto variável, máximo de 11 caracteres sem separadores. O campo dever ser preenchido com zeros a esquerda (Exemplo 11111111111)
CNPJ_titular	CNPJ do titular de certificado de pessoa jurídica	Caracteres alfanuméricos	Obrigatório na emissão de certificado de pessoa jurídica e SSL. Certificados de pessoa física preencher “VAZIO”	O identificador é o número de inscrição no Cadastro Nacional de Pessoas Jurídicas do Titular do certificado. Texto variável, máximo de 14 caracteres sem separador. Regra negocial: Caso o certificado digital emitido seja de Pessoa Física o campo deve ser preenchido com ZEROS (Exemplo 00000000000000)
Resposta_DATAVALID	Resposta DATAVALID (MATCH ou NO_MATCH ou NAO_LOCALIZADO)	Caracteres alfanuméricos	Obrigatória na emissão presencial e videoconferência, nos demais casos preencher “VAZIO”	Identifica a resposta recebida pela AC durante o procedimento de batimento biométrico com a base do DATAVALID (CNH). Texto codificado máximo de 14 caracteres
Resposta_PSBIO	Resposta do PSBIO (menagem recebida do PSBIO que autoriza a emissão)	Caracteres alfanuméricos	Obrigatória na emissão Presencial, Videoconferência e AR eletrônica, nos demais casos preencher “VAZIO”	Identifica a resposta recebida pela AC que sustentou a emissão do certificado, durante o procedimento de batimento biométrico com o PSBIO. Texto codificado máximo de 14 caracteres

Item	Descrição	Tipo de Dado	Presença de conteúdo	Conceito/Observação (regra de negócio)
Forma_pagto	Forma de Pagamento	Texto Codificado	Obrigatória na emissão Presencial, Videoconferência, nos demais casos preencher "VAZIO"	Indica a modalidade utilizada no pagamento efetuado pelo solicitante do certificado digital. Texto variável, máximo 20 caracteres (: Cartao_de_credito; Credito pre-pago; Faturamento por AR; Voucher; PIX; Dinheiro; Outros)
ID_MAQ_AGR	ID da Máquina utilizada pelo AGR (identificação unívoca do equipamento)	Caracteres alfanuméricos	Obrigatória na emissão Presencial e Videoconferência, nos demais casos preencher “VAZIO”	Indica a identificação unívoca do equipamento do AGR constante no cadastro da AC (notebook ou desktop) utilizado no procedimento de identificação do solicitante do certificado. Texto variável, máximo 64 caracteres
ID_MAQ_cliente	ID da Máquina utilizada para instalação do certificado (identificação do equipamento) podendo ser o IP, endereço MAC ou nome do host.	Caracteres alfanuméricos	Obrigatória na emissão Presencial, Videoconferência e AR eletrônica, nos demais casos preencher “VAZIO”	Indica a identificação do equipamento do solicitante do certificado utilizado no momento da emissão do certificado digital (geração das chaves criptográficas). Texto variável, máximo 64 caracteres, separados por ponto.