Infraestrutura de Chaves Públicas Brasileira

PROCEDIMENTOS PARA

IDENTIFICAÇÃO BIOMÉTRICA

NA ICP-BRASIL

DOC-ICP-05.03

versão 1.4

13 de setembro de 2016

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	Item Alterado	Descrição da Alteração
Instrução Normativa nº nn, de 13.09.2016 (versão 1.4)	6.1	Define parâmetros para geração do IDN.
Instrução Normativa nº 04, de 07.06.2016 (versão 1.3)	2, 2.1 e 2.2	Altera os parâmetros mínimos para coleta das biometrias.
Instrução Normativa nº 01, de 31.03.2016 (versão 1.2)	3.2.1, 3.2.2, 3.2.2.1, 3.2.3, 3.3, 3.3.2, 3.3.3, 3.3.4, 3.3.7, 5 (novo), 5.1 e 6	Inclusão de Formatos e padrões das mensagens para os serviços de HUB, tratamento de erros e procedimentos para Autenticação e segurança.
Instrução Normativa nº 08, de 10.12.2015 (versão 1.1)	1.2, 2.2.1, 3, 5	Suplementa os procedimentos biométricos da ICP-Brasil.
Resolução nº 114, de 30.09.2015 (versão 1.0)		Aprova a versão 1.0 do Documento Procedimentos para Identificação Biométrica.

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC-RAIZ	Autoridade Certificadora Raiz da ICP-BRASIL
ANSI	American National Standards Institute
AGR	Agente de Registro
CPF	Cadastro de Pessoa Física
DOC-ICP	Documentos Principais da ICP-BRASIL
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDN	Identificador de registro biométrico
ITI	Instituto Nacional de Tecnologia da Informação
ISO	International Organization for Standardization
IEC	International Engineering Consortium
IV	Inicialization Vector
NIST	National Institute for Standards
NFIQ	NIST Fingerprint Image Quality
PKCS	Public Key Cryptography Standards
PSBio	Prestador de Serviço Biométrico credenciado pela ICP-BRASIL
PSS	Prestadores de Serviço de Suporte
SLA	Service Level Agreement
XML	EXtensible Markup Language
WSQ	Wavelet Scalar Quantization

1. INTRODUÇÃO

O Sistema Biométrico da ICP-Brasil tem por objetivo aumentar a segurança na identificação dos titulares e responsáveis por certificados digitais, reduzindo o risco de fraudes, e permitir a simplificação do processo de emissão de certificados digitais com verificação biométrica do requerente.

1.1. Conceitos

a) Dados biométricos: Dados biométricos da pessoa física que é titular e/ou responsável por um certificado digital, coletados de forma assistida por um agente de registro.
b) Dados biográficos: Dados biográficos utilizados para identificação da pessoa física titular e/ou responsável por um certificado digital, definidos nas Declarações de Práticas e Políticas de Certificação da ICP-Brasil.
c) AC/PSS: Autoridade Certificadora (AC) ou Prestador de Serviço de Suporte (PSS) responsável pela operação de sistemas de certificação digital devidamente credenciados na ICP-Brasil.
d) Identificador de registro biométrico (IDN): Os dados biométricos de cada pessoa física estarão relacionados a um único identificador em todo o sistema, chamado de IDN – Identificador de registro biométrico.
e) Base biométrica local: Base de dados biométricos de cada AC/PSS, que relaciona dados biográficos de cada pessoa ao seu respectivo IDN e, consequentemente, aos dados biométricos.
f) Transação biométrica: A transação biométrica é um conjunto de dados, em formato eletrônico, que tem um propósito, seja ele cadastramento, atualização ou consulta para fins de verificação de dados biométricos do requerente.
g) PSBio: Prestador de Serviço Biométrico credenciado pela ICP-Brasil. Cada AC/PSS deve contratar pelo menos um PSBio credenciado que será responsável por processar suas transações biométricas. Cada PSBio tem uma base biométrica, e essa base contém as biometrias e o identificador de registro biométrico (IDN), mas sem nenhum dado biográfico da pessoa.
h) Base biométrica ICP-Brasil: Conjunto das bases biométricas de cada PSBio da ICP-Brasil. Contém todas as biometrias e seus respectivos identificadores de registro biométrico (IDN).
i) HUB biométrico: Os PSBios são responsáveis por operar o serviço de HUB Biométrico, destinado à comunicação entre os PSBios para a execução das transações biométricas e replicação de dados biométricos.

1.2. Anonimato da base biométrica ICP-Brasil

A base biométrica ICP-Brasil, sob responsabilidade dos PSBios credenciados, será anônima. Esse anonimato é garantido pelo fato dos registros biométricos estarem associados ao identificador de registro biométrico (IDN) único para cada pessoa, não sendo possível ao PSBio relacionar esse identificador a nenhum dado biográfico da pessoa. É proibida a divulgação da chave simétrica, sendo que essa deve estar armazenada, com propriedade de não exportável, dentro dos HSM de cada AC recebedora da mesma.

1.3. Coleta de dados biométricos

A coleta de dados biométricos deve ser feita de forma assistida (acompanhada) por um agente de registro (AGR). Devem ser coletados, no mínimo, as biometrias da face e das impressões digitais.

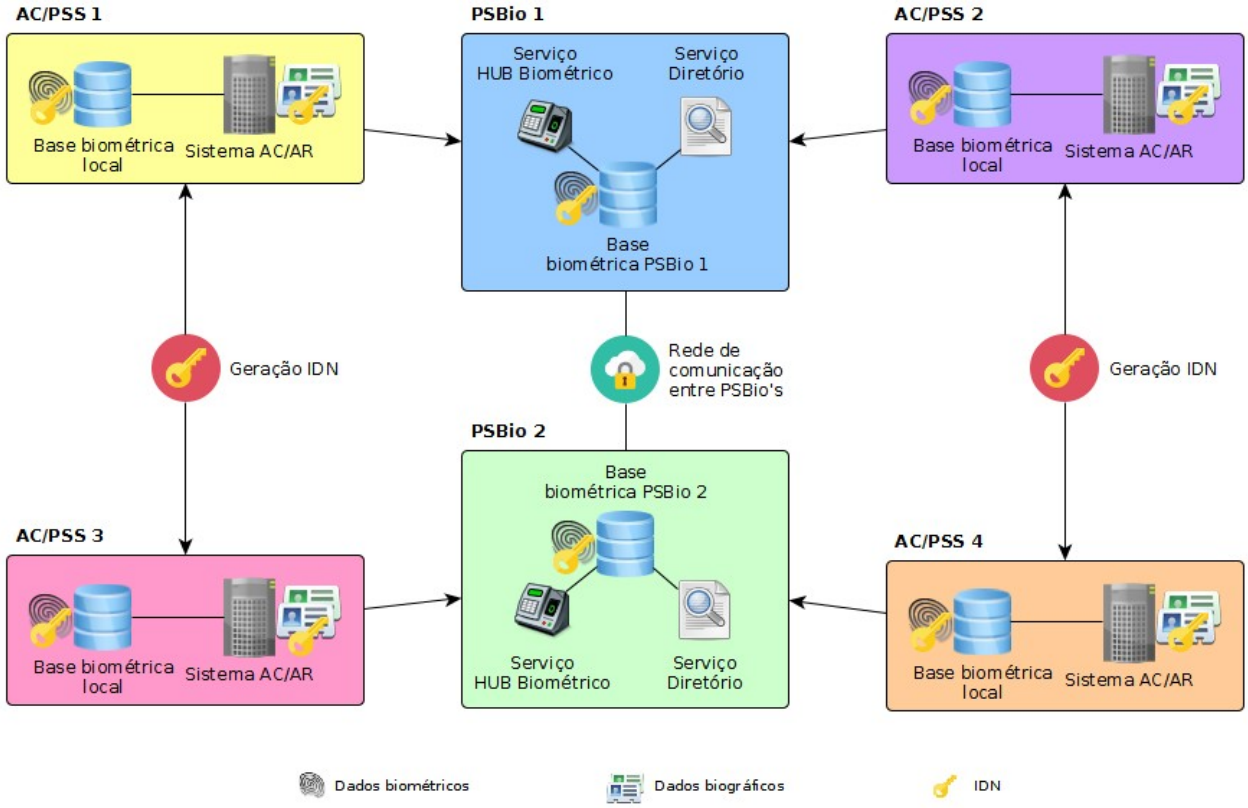
1.3.1. Responsável pela coleta

A coleta é de responsabilidade da AC/PSS e de sua rede de Autoridades de Registro. A AC/PSS pode utilizar tecnologia e sistemas próprios ou contratar de fornecedores no mercado à sua escolha, garantindo que os padrões estabelecidos neste documento sejam obedecidos.

1.3.2. PSBio na coleta

A AC/PSS pode utilizar os serviços de um PSBio credenciado para o fornecimento de tecnologia e sistemas. A AC/PSS também pode, por meio de uma empresa do mesmo grupo, operar um PSBio. Nesses dois casos, o PSBio deve garantir a segregação entre a base biométrica local da AC/PSS e a base biométrica do PSBio, mantendo o anonimato da base no PSBio.

1.4. Topologia do sistema



2. ESPECIFICAÇÃO DAS BIOMETRIAS

Todos os arquivos gerados pelas coletas das biometrias, determinadas nos itens subsequentes, devem conter trilha de auditoria em relação a data, horário e local da coleta e o registro do equipamento de coleta, conforme DOC-ICP-05.

2.1. Fotografia frontal da face. Parâmetros mínimos para biometria facial:

a. Preferencialmente fundo branco ou de cor clara e uniforme;

b. A fotografia deve estar focada (não borrada);

c. O requerente deve estar em posição frontal em relação à lente da câmera;

d. Os olhos do requerente devem estar abertos e na horizontal;

e. A distância mínima entre os centros dos olhos deve ser de 7,6 mm (equivalente a 90 pixels a 300 dpi);

f. Iluminação homogênea, sem sombras em partes da face;

g. Sem obstrução facial (cabelo sobre o rosto, chapéu, boné, etc);

h. Os requerentes que usam óculos devem, preferencialmente retirá-los; óculos só devem ser utilizados em casos de extrema necessidade e estes não podem ter armação grossa ou que obstrua parte dos olhos, as lentes devem ser transparentes (não coloridas ou escuras);

i. Sem reflexos nas lentes dos óculos eventualmente usados;

j. Expressão facial neutra (sem sorriso, franzimento etc);

k. Em hipótese alguma a fotografia pode conter objetos que atrapalhem a identificação da face ou outras pessoas além do requerente;

l. A fotografia deve ser gerada em formato de imagem (PNG, JPEG ISO/IEC 10918), com resolução mínima de 300 dpi, com cor, e o arquivo resultante deverá possuir tamanho máximo de 1 MB. Compressões sucessivas (salvamentos sucessivos do arquivo) da fotografia devem ser evitadas;

m. Para garantir que a face está inteiramente visível, as seguintes proporções devem ser respeitadas:
   i. a face deve ocupar entre 50% a 75% da largura da imagem;
   ii. a distância entre a ponta do queixo e o centro superior da face deve ocupar entre 60% e 90% da altura total da imagem.

2.2. Impressão digital. Parâmetros mínimos da impressão digital

a. resolução de 500 dpi e 8bit tons de cinza;

b. imagem de saída comprimida em WSQ;

c. área de leitura mínima de 294 mm²;

d. verificação de qualidade e quantidade de minúcias da impressão digital baseado no padrão NFIQ (aceitar notas 1, 2 ou 3). http://www.nist.gov/itl/iad/ig/bio_quality.cfm (sítio onde se encontra o algoritmo).

2.2.1. Parâmetros para coleta

a. A coleta da impressão digital deve ser, por padrão, dos 4 dedos indicadores e médios e deve possuir sistema para detecção de dedos repetidos. A falta destes deverá ser justificada e feito o registro através de outros dedos. No caso de indisponibilidade temporária de todos os dedos preferenciais, é necessária a identificação 1:N na biometria facial; (o serviço de diretório deve informar ao sistema da AC, no momento da verificação, quais dedos foram cadastrados);

b. coleta deve ser de forma batida (pousada sobre o leitor);

c. no caso do requerente não possuir qualquer impressão digital, ou da impossibilidade de validação (qualidade da impressão digital muito ruim, notas 4 e 5, baseado no padrão NFIQ), essa informação deve constar em seu registro (campo vazio do arquivo biométrico), visto que esse não poderá ser identificado pela biometria da impressão digital;

d. o AGR deve estar atento para evitar qualquer uso de simulações de impressões digitais por supostos fraudadores, como dedo de silicone, ou qualquer outro processo que simule uma impressão digital.

3. PSBIO – PRESTADOR DE SERVIÇO BIOMÉTRICO

Os PSBios deverão ser entidades devidamente credenciadas, fiscalizadas e auditadas pela ICP-Brasil, como descrito no DOC-ICP-03, DOC-ICP-08 e DOC-ICP-09. O PSBio opera uma base biométrica (que compõe a base biométrica ICP-Brasil) e o serviço de HUB biométrico e não pode utilizar os registros para outros fins diferentes dos especificados no rol de normas da ICP-Brasil.

Os PSBios credenciados devem tratar cada tipo de transação separadamente em fila única, por ordem cronológica de solicitação, independentemente de qual entidade (ACs ou outros PSBios), devendo preservar as trilhas de auditoria para comprovação de horário de chegada e saída das transações.

3.1. Base biométrica ICP-Brasil

O PSBio deve manter sua base de dados biométricos com as seguintes características:

a. armazenar os registros biométricos de impressão digital e face, tendo cada registro vinculado ao IDN (identificador de registro biométrico);

b. deve ser capaz de realizar a identificação (1:N) biométrico de impressão digital e face, garantindo a inexistência de outro registro com essas biometrias antes da inclusão de um novo registro;

c. deve ser capaz de fazer a verificação on-line (1:1) de um registro por meio de seu IDN durante o processo de emissão de um certificado digital; caso não seja possível ser realizado por meio das impressões digitais cadastradas para um IDN, deve ser feito por meio da face;

d. deve ser capaz de indexar, quando os requisitos da coleta forem cumpridos, quatro/quatro, três/três, duas/duasou uma/uma impressão digital e a face, se necessário;

e. quando não for possível a identificação (1:N) por impressão digital, o reconhecimento facial deve ser utilizado para garantir a unicidade do registro biométrico para aquele IDN;

f. deve ser capaz de identificar as irregularidades e duplicidades dos registros e prontamente realizar as comunicações para as entidades biométricas credenciadas, se for o caso, publicando essas informações para a AC/PSS que solicitou o cadastramento, para os devidos encaminhamentos;

g. deve possuir desempenho, escalabilidade e disponibilidade, com SLA mínimo de 99,5% (resguardadas as janelas programadas de manutenção) ao mês, para atender toda a demanda da ICP-Brasil.

h. deve manter um ambiente segregado de homologação para os testes, com as ACs e PSBios, de tecnologia e interconexão necessários para operação do sistema e atendimento as normas da ICP-Brasil, com SLA mínimo de 95,5% ao mês.

i. O sistema utilizado para realizar as identificações dos requerentes de um certificado digital deve, para um espaço amostral de 10 mil registros, ter, no mínimo, a seguinte acurácia:

- Impressão digital (NFIQ = 1 e indexando um dedo): para FAR (false accept rate) de 0,01%, TAR (true accept rate) de, no mínimo, 99,0%.
- Impressão digital (NFIQ = 1 e indexando dois dedos): para FAR de 0,01%, TAR de, no mínimo, 99,4%.
- Impressão digital (NFIQ = 1 e indexando três ou quatro dedos): para FAR de 0,01%, TAR de, no mínimo, 99,8%.
- Face: para FAR de 0,1%, TAR de, no mínimo, 90%.

3.2. HUB biométrico

O PSBio deve oferecer o serviço de HUB biométrico para processamento de transações biométricas às AC/PSS que o contratarem e aos demais PSBios credenciados pela ICP-Brasil. Esse serviço terá as seguintes características:

a. ter interface de comunicação que faça uso dos padrões especificados neste documento;

b. o tráfego de informações deve ocorrer por meio de transações biométricas especificadas neste documento e deve utilizar canal seguro de comunicação (HTTPS com dupla autenticação por certificado digital);

c. não é autorizado, por parte do HUB Biométrico, guardar qualquer tipo de informação biográfica de indivíduos que possam ser vinculados às biometrias cadastradas;

d. deve suportar as transações biométricas especificadas neste documento e a comunicação de irregularidades para as AC/PSS;

e. deve garantir a inexistência de dados biométricos divergentes para um mesmo IDN;

f. deve realizar a identificação (1:N) antes de efetuar um novo cadastro para garantir a inexistência de duplicidade de dados biométricos.

NOTA: Os PSBios devem enviar ao ITI a topologia de rede de comunicação com as AC/PSS e demais PSBios que compõe o Sistema Biométrico da ICP-Brasil.

3.2.1 Formatos e padrões das mensagens para os serviços de HUB

As requisições para os serviços de HUB devem seguir o padrão assíncrono, ou seja, todas as respostas devem ser retornadas pelo HUB que recebeu a solicitação quando o mesmo tiver a informação disponível. O modelo assíncrono implementado deve seguir o conceito “PULL”, ou seja, quem recebeu a requisição é responsável por gerar e entregar a requisição de resposta.

As requisições devem utilizar o método POST, e conter apenas o arquivo ANSI/NIST no corpo da requisição (de acordo com o padrão especificado neste documento), além de conter obrigatoriamente os seguintes cabeçalhos (headers):

a) NIST/XML:
Content-Type: application/xml

b) NIST/binary
Content-Type: application/octet-stream

3.2.2. Tratamento de erros

Em geral, pela sua característica assíncrona, o HUB retorna os erros de forma assíncrona com um arquivo ANSI/NIST de resposta conforme descrito neste documento. Em algumas situações específicas, o erro é gerado em tempo de execução da requisição. Nestes casos, o serviço deve

retornar um código de erro HTTP 500, seguidos de uma mensagem de erro no padrão descrito abaixo.

```
{
“error_code”:””””
  “error_message”:””””,
  “additional_data”:””””
}
```

3.2.2.1 Códigos de erro (em tempo de execução)

999 – Requisição mal formatada/arquivo ANSI/NIST inválido
102 – PSBio não encontrado
401 – Não autorizado / erro de autenticação

3.2.3. Autenticação e segurança

Como já mencionado, todas as requisições devem utilizar autenticação dupla, e a identificação do PSBio deve ser feita por meio do certificado enviado pelo lado cliente (quem originou a requisição). O identificador do PSBio deve estar presente no CN (Common name) do certificado e o certificado deve corresponder ao publicado para aquele PSBio.

3.3. Diretório de registros biométricos

O serviço de diretório deve ser oferecido por cada um dos HUBs/PSBio como um mecanismo rápido de consultas, e é crítico para manutenção da consistência das bases biométricas. O serviço de diretório deve prover cinco operações básicas:

a. Acusar a existência ou não de um IDN dentro no PSBio e a lista de biometrias cadastradas;

b. Lista de transações pendentes (transações de identificação 1:N e transações de atualização, notificações de atualização de status);

c. Solicitar reenvio de operações pendentes;

d. Listar os IDNs de seus registros (exceto os de seu cache);

e. Receber notificação de mudança de status de um IDN (notificação de fraude e finalização de processo de cadastramento ou atualização);

3.3.1. Operação de consulta de IDN

A operação de consulta de IDN deve ser feita ao diretório de um PSBio como mecanismo para confirmar a existência ou não de determinado IDN nos registros do PSBio, além de um indicador das biometrias capturadas.

3.3.2 Operação de listagem de operações pendentes

A operação de listagem de operações pendentes é utilizada quando um PSBio tiver seus serviços temporariamente indisponíveis e precisar restabelecer os serviços. Nesta situação, o PSBio deve

consultar o serviço de diretório dos demais PSBios para obter as pendências, que podem ser relativas a lista de cadastros pendentes de busca 1:N e atualizações de status pendentes. Nas duas situações, o PSBio que reestabeleceu as suas operações deve solicitar o reenvio da operação pendente.

NOTA 1: Para evitar excesso de tráfego de dados, a operação de listagem de buscas 1:N pendentes retornara no máximo 1000 registros. Caso o PSBio possua uma fila maior que 1000 registros para tratar, deve fazer o tratamento dos primeiros 1000 registros enviados (e assim sucessivamente até processar todas as transações pendentes).

3.3.3 Operação de requisição de reenvio de operações pendentes

Ao retornar de uma falha, o PSBio deve executar todas as operações que estiverem pendentes junto a outros PSBios, que podem ser buscas 1:N pendentes, finalizações de cadastro pendentes e notificações de fraude pendentes.

No caso das buscas 1:N pendentes, o processo terá as seguintes etapas:

a. A primeira etapa deste processo é consultar o serviço especificado no item 3.3.2 para saber a lista de IDNs pendentes em cada um dos PSBios.

b. A segunda etapa é enviar o pedido de reenvio da busca 1:N aos PSBios que aguardam uma resposta. Esse pedido é uma sinalização de que o PSBio que estava em falta voltou a operar, mas não é ainda o resultado da busca 1:N.

c. Os PSBios que forem notificados devem então repetir a solicitação de busca 1:N pendente ao PSBio que voltou a operar.

No caso de notificações de alteração de status, o processo terá as seguintes etapas:

a. A primeira etapa para o este processo é consultar o serviço especificado no item 3.3.2 para saber a lista de IDNs pendentes de alteração de status em cada um dos PSBios.

b. A segunda etapa é enviar o pedido de reenvio alterações de status.

c. Os PSBios que forem notificados, farão uma nova tentativa de notificação de alteração de status.

3.3.4 Receber notificação de alteração de status

O PSBio deve possuir uma interface para receber as notificações de fraude/irregularidade de um IDN e de notificação de finalização de um cadastro. Seguem as situações de uso previstas para a operação.

- Notificação de finalização de cadastro (STATUS 1): Sempre que um PSBio finalizar uma transação de cadastramento ou atualização de um determinado IDN. O PSBio responsável pelo IDN deve enviar esta notificação para todos os outros PSBios, identificando o novo status para aquele IDN.

- Notificação de fraude (STATUS 0): Sempre que uma AC responsável pelo IDN finalizar a análise de irregularidade. A operação permite remover um determinado registro da base. O IDN utilizado na irregularidade deve ser liberado, para que o seu real detentor possa executar o cadastro biométrico.

O PSBio que receber a notificação deve repassá-la aos demais PSBios para que estes possam remover o registro do cache, se for o caso.

3.3.5 Operação listagem de IDNs (para reconstrução de cache)

Quando o PSBio precisar criar, recompor ou atualizar seu cache, deverá consultar a lista de IDNs dos demais PSBios. A partir da data da última atualização do registro e do número único da transação (TCN) que originou ou atualizou o registro, o PSBio solicitante decidirá se precisa ou não inserir ou atualizar esse registro em seu cache. A consulta poderá indicar a data e hora iniciais para a pesquisa para que o PSBio indique apenas registros que foram inseridos ou atualizados a partir da data e hora solicitadas. Serão listados no máximo 1.000 registros a cada consulta. O PSBio requisitante deve repetir a solicitação com nova data e hora do último registro retornado até receber uma resposta com menos de 1.000 registros.

Para cada registro que necessitar de inserção ou atualização no cache, o PSBio deverá solicitar o reenvio da transação de cadastramento (1:N) ao PSBio que tem o registro desejado. Deve, no entanto, sinalizar no campo adequado que se trata de uma operação para recomposição do cache para que o PSBio que tem o registro saiba que não precisa aguardar resposta para essa transação.

NOTA 2: A operação de listagem de IDNs deve receber como parâmetro a data inicial e final para os IDNs desejados, em formato UNIX TIMESTAMP zona UTC. Caso o parâmetro não seja enviado, o PSBio retornara os primeiros 1.000 registros de sua base. A resposta da operação de listagem de IDNs deve conter o seguinte conteúdo: Código IDN, código TCN e data de última atualização.

NOTA 3: O resultado da operação, deve ser ordenado, de forma crescente, utilizando a data de última atualização como referência (registros mais antigos serão os primeiros).

NOTA 4: O serviço de listagem dos IDNs (3.3.5) e o reenvio com objetivo de recomposição de cache estarão disponíveis apenas no período noturno (entre 01:00 e 09:00 UTC).

***NOTA 5*:** O PSBio só informará os IDNs de registros sob sua responsabilidade, e não os registros que porventura tenha em seu cache. Para o PSBio manter o cache consistente, os demais PSBios devem ser consultados.

3.3.6 Formatos e padrões das mensagens para os serviços do diretório

3.3.6.1 Padrões de requisição

As requisições para os serviços de diretório devem seguir o padrão síncrono, ou seja, todas as respostas devem ser retornadas na mesma requisição/resposta. Deve-se utilizar a versão 1.1 ou superior do protocolo HTTP.

As requisições devem utilizar o método POST e conter obrigatoriamente os seguintes cabeçalhos (headers):

Accept: application/json
Content-Type: application/json

Os cabeçalhos (headers) de resposta devem conter obrigatoriamente os seguintes parâmetros:

Content-Type: application/json

NOTA 6: Os serviços relacionados a reenvio de pacotes padrão ANSI/NIST (reenvio de busca 1:N), devem retornar um valor positivo ou negativo relativo ao recebimento da operação, e a integração deve ser feita diretamente entre os pontos de comunicação dos HUBs biométricos.

3.3.6.2 Autenticação e segurança

Como já mencionado, todas as requisições devem utilizar autenticação dupla, e a identificação do PSBio deve ser feita por meio do certificado enviado pelo lado cliente (quem originou a requisição). O identificador do PSBio deve estar presente no CN (Common name) do certificado e o certificado deve corresponder ao publicado para aquele PSBio.

3.3.6.3 Tratamento de erros

Os erros devem ser retornados com um HTTP Status Code 200, seguidos de uma mensagem JSON descrevendo a ocorrência, seguindo o seguinte padrão:

```
{
“error_code”:””
  “error_message”:””,
  “additional_data”:””
}
```

3.3.6.3.1. Códigos de erro

999 – Requisição mal formatada
100 – Registro não encontrado
101 – Registro não pertence ao PSBio
102 – PSBio não encontrado
103 – Registro inválido
401 – Não autorizado / erro de autenticação

3.3.6.4 Operação de consulta de IDN

JSON

Requisição:

```
{
        “resquestType”:”idn_query”,
        “idn”:”Código alfanumérico do IDN”
}
```

Resposta:
{
“idn”:”Código alfanumérico do IDN”,
“t_14_013_1”:”TRUE|FALSE”,
“t_14_013_2”:”TRUE|FALSE”,
“t_14_013_3”:”TRUE|FALSE”,
“t_14_013_4”:”TRUE|FALSE”,
“t_14_013_5”:”TRUE|FALSE”,
“t_14_013_6”:”TRUE|FALSE”,
“t_14_013_7”:”TRUE|FALSE”,
“t_14_013_8”:”TRUE|FALSE”,
“t_14_013_9”:”TRUE|FALSE”,
“t_14_013_10”:”TRUE|FALSE”,
“t_10”:”TRUE|FALSE”
}

3.3.6.5 Operação de listagem de operações pendentes

JSON

Requisição:
{
“resquestType”:”pending_operations”,
}

Resposta:
{
“requestType”:”pending_operations”,
“pendingOperationsList”:
[
{“operationType”: “1_n_queue”,
“idnList”:[
“Código alfanumérico do TCN”,
(...)
“Código alfanumérico do TCN”
]},
{“operationType”: “changeStatus”,
“idnList”:[
“Código alfanumérico do TCN”,
(...)
“Código alfanumérico do TCN”
]}
]}

3.3.6.6 Operação de requisição de reenvio de operação pendente

JSON

Requisição:
{
“resquestType”:”operation_resend”,
“operationType”:”1_n_resend / status_change”,
“idn”:”Código alfanúmerico do IDN”,
“cacheRebuild”: “TRUE/FALSE” // Somente para reenvio de busca 1:N
}

Resposta:
{
“response”:”Mensagem de resultado da operação”,
“responseCode”:”código de retorno de resultado da operação”
}

3.3.6.7 Operação de notificação alteração de status

JSON

Requisição:
{
“resquestType”:”change_status”,
“statusCode”: “0|1”, // [NOVO_STATUS: 1- finalizado, 0 – notificação de fraude]
“idn”:”Código alfanúmerico do IDN”
}

Resposta:
{
“response':”Mensagem de resultado da operação',
“responseCode':'código de retorno de resultado da operação”
}

3.3.6.8 Operação de reconstrução de cache

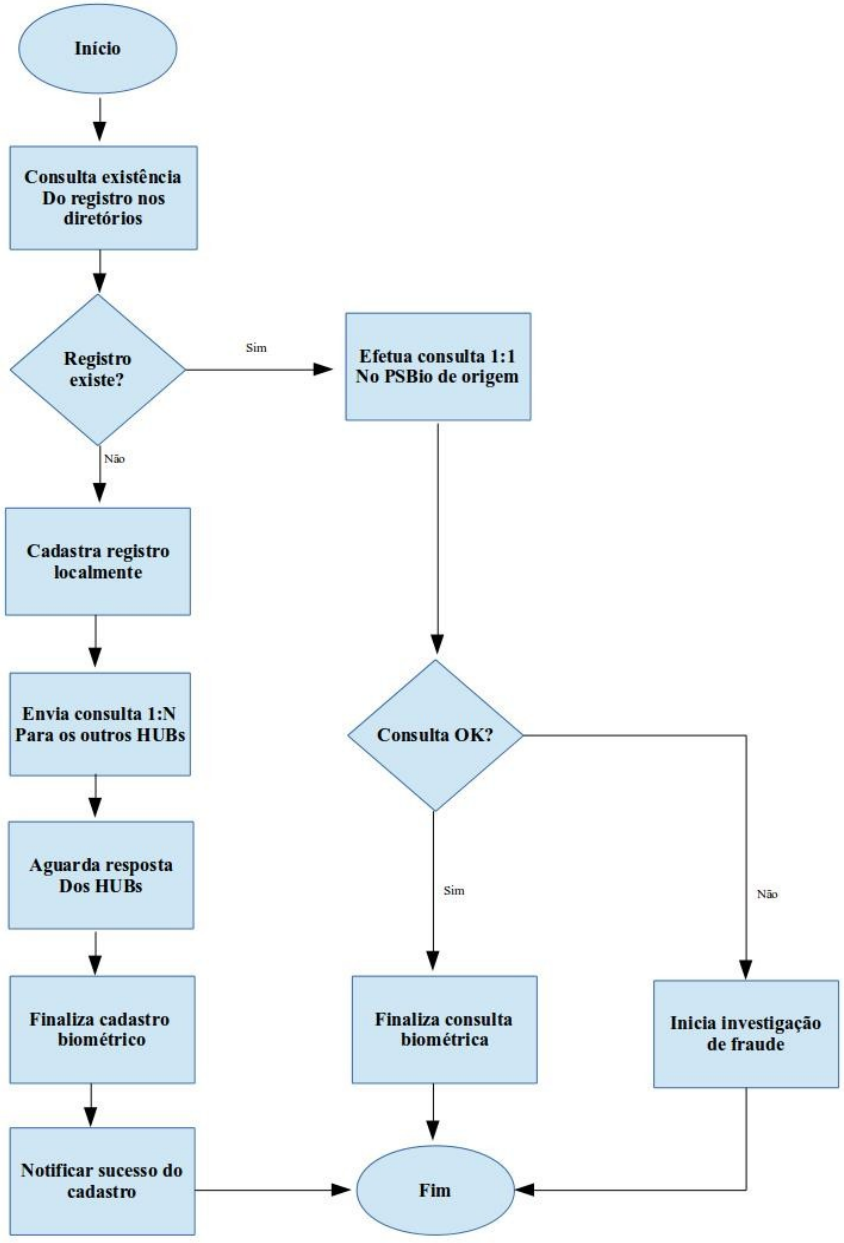
JSON

Requisição:
{
“resquestType”:”idn_list'”,
“startDate”, “UNIX_TIMESTAMP_UTC”,
“endDate”, “UNIX_TIMESTAMP_UTC”
}

Resposta:
{
“responseCode”:”código de retorno de resultado da operação”,
“idnList”:[
{ “idn”: “Código IDN”,
“tcn”:”Código TCN”,
“timestamp”: “timestamp da última atualização”},
...
{ “idn”: “Código IDN”,
“tcn”:”Código TCN”,
“timestamp”: “timestamp da última atualização”}
]
}

3.4. Fluxo padrão de cadastramento e consulta biométrica e consistência das bases biométricas

O fluxo padrão de uma consulta ou cadastramento de biometria exige que o PSBio consulte os diretórios em busca da existência do IDN em um dos PSBios, se o IDN for localizado, deve ser executada uma verificação biométrica 1:1 entre os PSBio.
Caso o registro não seja encontrado em nenhum dos PSBios, um novo cadastramento pode ser feito no PSBio. A execução desta operação exige que o PSBio execute uma busca 1:N em todos os outros PSBios antes de considerar o processo de cadastramento completo.



3.5. Garantia de consistência da base biométrica

Todo PSBio deve verificar em intervalos de hora em hora a lista de operações de consulta 1:N pendentes em todos os PSBios e executar, se necessário, as ações especificadas no item 3.3.3 deste documento.

Esse processo periódico tem por objetivo garantir que nenhuma operação de identificação (1:N) deixará de ser executada, reduzindo significativamente o risco de duplicidade de registro biométricos.

3.6. Operação de busca 1:N

A operação de 1:N deve ser separada em três etapas: busca 1:N em lista negativa, busca 1:N local, e busca remota.

3.6.1 Operação de busca 1:N em lista negativa

Consiste na operação de busca de biometrias em uma base restrita a biometrias de fraudadores. Esta busca deve ser realizada antes de prosseguir com qualquer transação de cadastramento ou atualização. Para otimizar a performance das transações, é sugerido que a busca em lista negativa seja executada em etapa anterior a busca 1:N local. Caso uma das biometrias seja encontrada em lista negativa, o processo deve ser interrompido com erro.

3.6.2 Operação de busca 1:N local

Ocorre antes de enviar a solicitação de busca para outros PSBio. O PSBio deve a efetuar uma busca 1:N das biometrias recebidas em uma transação de cadastramento, ou em uma transação de verificação. Se o resultado for negativo (as biometrias não existem em base local), o PSBio deve disparar o processo de consulta 1:N remoto (outros PSBios).

3.6.3 Operação de busca 1:N remota

A operação de busca 1:N remota é efetuada após a busca 1:N local, e consiste no envio da transação de cadastramento ou atualização para os demais PSBios. Caso o PSBio tenha um modelo de Cache, conforme descrito no item 3.7, o PSBio fica dispensado de aguardar o resultado das respostas 1:N dos demais PSBios, sendo que ele possui uma réplica completa de toda a base biométrica ICP-Brasil. Para os PSBios que não possuem a implementação de cache, é necessário aguardar a resposta de sucesso dos demais PSBios.

NOTA 7: O PSBio que possui implementação de Cache biométrico fica dispensado de aguardar o resultado das buscas 1:N remotas, mesmo assim continua obrigado de enviar os registros para os demais PSBios (afim de manter a consistência do cache dos demais PSBios).

3.7. Cache da base biométrica

O cache de base biométrica é uma funcionalidade opcional, que pode ou não ser implementada pelo PSBio. Sempre que uma transação de cadastramento ou de atualização é executada, as informações da transação são repassadas para todos os PSBios para que a busca 1:N seja executada. No término do cadastramento, o PSBio que recebeu a transação de cadastramento/atualização deve incluir em seu diretório o IDN com data e hora da inserção/atualização e número único da transação que o originou (TCN).

Os PSBios que implementarem o cache possuem dois mecanismos para garantir a sua consistência e manutenção do conteúdo de cache.

a) Construção de cache durante as transações e atualizações: sempre que uma transação de cadastramento ou de atualização é executada, as informações da transação são repassadas para todos os PSBios para que a busca 1:N seja executada. No término do cadastramento, o PSBio que recebeu a transação de cadastramento/atualização deve informar a todos os PSBios o sucesso da transação.

b) Reconstrução de cache / manutenção de cache: os PSBios que implementarem o cache podem consultar no diretório do PSBio que originou a busca 1:N e, ao verificar que o IDN está presente com o mesmo TCN que ele recebeu e poderá incluir esse registro em seu cache.

Com estes mecanismos, é possível que os PSBios que executaram a ação de busca 1:N possam utilizar estes dados para gerar um cache local das biometrias, afim de acelerar a execução futuras consultas.

3.8. Operação em contingência

Para que o Sistema Biométrico ICP-Brasil funcione em condições normais é preciso que todos os PSBios credenciados estejam disponíveis. A falha em um PSBio implica na paralisação das operações de cadastramento.

Para que todo o sistema não seja prejudicado, estão definidas a seguir condições para operação em contingência.

3.8.1. Situação operacional do sistema biométrico

3.8.1.1. Operação normal

Todos os PSBios estão operacionais e respondendo dentro dos parâmetros estabelecidos.

3.8.1.2. Alarme

Ocorre quando um ou mais PSBios estão inacessíveis, mas modo de operação em contingência ainda não foi ativado. Nesta situação os PSBios não enviarão o retorno positivo da operação para a AC, até que a operação seja reestabelecida ou o modo de contingência seja ativado.

As operações de verificação que não dependerem de registros biométricos dos PSBios afetados são executadas normalmente.

3.8.1.3. Operação em contingência

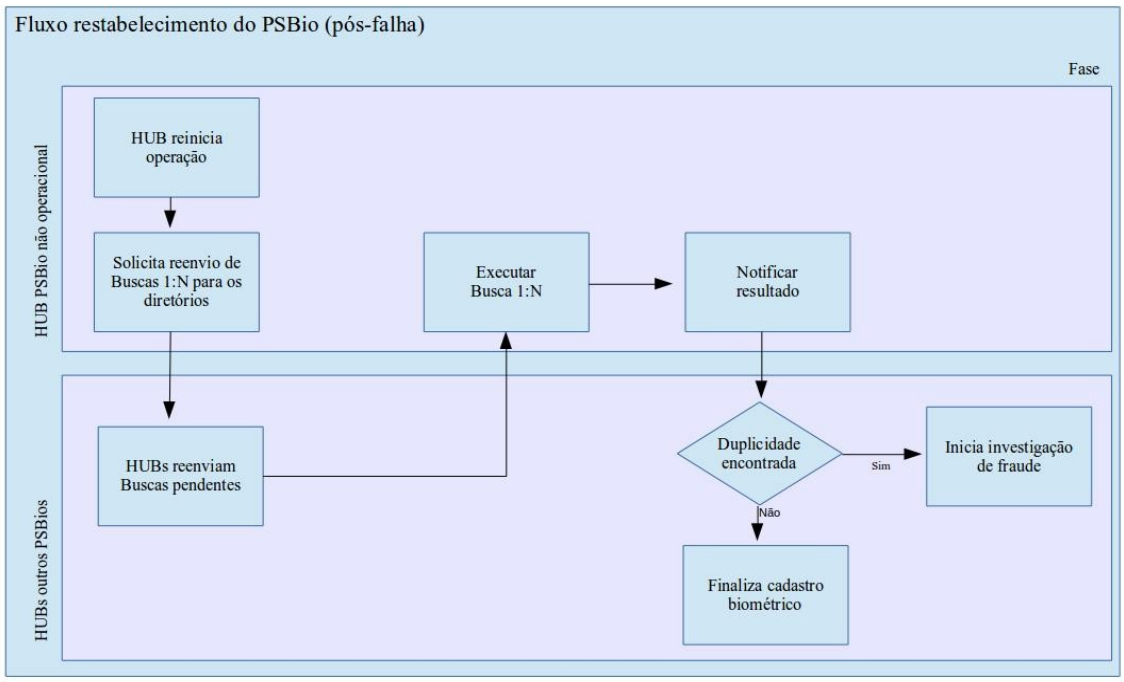
Após situação de alarme, o modo de contingência foi ativado.
Em modo de contingência, os PSBios inacessíveis são desconsiderados nas operações de cadastramento e de consulta, mas todas as operações de cadastramento são sinalizadas como "contingência", e mantendo para cada operação sinalizada a lista de PSBios inacessíveis no momento em que foram executadas.

3.8.1.4. Recuperação da operação

Após a operação em modo de contingência, quando o PSBio afetado reestabelecer seus serviços ele entrará em modo de "recuperação da operação".

Nesse modo, o PSBio deve procurar no diretório por transações de cadastramento sinalizadas como "contingência". Deve então executar a identificação (1:N) de cada transação e responder ao PSBio solicitante.
Se identificar duplicidade de IDN ou de biometria, o nó que executou a operação em modo de contingência deve tomar as providências para notificação de irregularidade/duplicidade.

O fluxo abaixo ilustra o fluxo para recuperação do modo de contingência:



3.8.2. Ativação do modo de contingência

Toda operação de cadastramento é anunciada com situação "pendente" no diretório até que todos os PSBios executem a identificação (1:N) da biometria que se pretende cadastrar. Quando todos os PSBios responderem, a operação é concluída e então é removida do diretório de transações pendentes.

Qualquer PSBio que demorar mais de 2 (duas) horas para responder a uma transação de cadastramento pendente será considerado inacessível pelos demais.

Quando houver três ou mais PSBios credenciados e em operação, o PSBio que não conseguir se comunicar com, pelo menos, um PSBio deve ser considerado inacessível, devendo entrar em modo "alarme" e suspender seus serviços de cadastramento até reestabelecer a comunicação.

Quando um ou mais PSBios forem considerados inacessíveis, os demais devem entrar em modo "contingência".

4. BASE BIOMÉTRICA LOCAL (AC/PSS)

A AC/PSS deve manter em base de dados a relação entre dados biográficos dos requerentes de certificados digitais e seus respectivos IDNs (identificador de registro biométrico).

A AC/PSS também deve manter as imagens das biometrias coletadas (impressão digital e face) em arquivo. Pode, a seu critério, manter sistema biométrico capaz de realizar operação de verificação (1:1) com o objetivo de fazer uma verificação prévia antes de submeter a transação ao PSBio, e nesse caso o sistema biométrico substitui a necessidade de manter as imagens das biometrias em arquivos.

A AC/PSS deve garantir a segregação entre dados biográficos e dados biométricos, além de tratar adequadamente a segurança contra acesso e divulgação não autorizadas.

NOTA: A verificação em base local da AC/PSS não dispensa a necessidade de submeter a transação ao PSBio durante o processo de emissão do certificado digital.

5. PUBLICAÇÃO DOS SERVIÇOS DE PSBIO

Serão publicados pela ICP-Brasil uma listagem de todos os PBios homologados, esta listagem deve conter a seguintes informações de cada PSBio:

- ID do PSBio
- Localização/URL do serviço de diretório
- Localização/URL do serviço de troca de arquivos ANSI/NIST (HUB biométrico)
- x509/certificado para fins de autenticação do PSBio

A publicação será feita em arquivo em formato JSON, seguindo o formato abaixo.

```
[
{
“PSBioId:”  “Certibio”,
“nist_endpoint”: “URL PARA ENVIO DE ARQUIVOS ANSI/NIST”,
“directory_endpoint”: “URL PARA SERVIÇO DE DIRETÓRIO”,
“x509”: “BASE64 X.509”
},
{...}
]
```

6. SERVIÇO DE GERAÇÃO DO IDN

O IDN (identificador de registro biométrico) será gerado a partir do CPF da pessoa física, de forma não a existir dois IDNs para um mesmo CPF e nem tão pouco dois CPFs com mesmo IDN.

O serviço de geração da chave simétrica do IDN será mantido pelo ITI, conforme descrito no DOC-ICP-05.04. Em hipótese alguma, uma AC/PSS deve transmitir a chave gerada para o PSBio contratado.

O serviço de geração do IDN estará disponível somente para as ACs devidamente credenciados pela ICP-Brasil, e o serviço terá as seguintes características:

a. o IDN deve ser uma sequência de caracteres do tipo alfanumérico, gerados a partir de função criptográfica simétrica, com tamanho de 64 caracteres;

b. ao gerar uma transação biométrica, o serviço deve ser consultado para gerar o IDN relacionado ao CPF na transação;

c. o acesso ao serviço de geração do IDN é feito diretamente pelas ACs, antes do envio das transações biométricas para os PSBios;

d. o acesso será feito com dupla autenticação com certificado digital.

e. As ACs devem guardar trilha de auditoria das operações de entrada e saída, do respectivo HSM, em relação a cada requisição para cálculo do IDN, pelo período mínimo de 6 anos, conforme DOC-ICP-05.

6.1. Geração do IDN

A geração do IDN utilizará criptografia simétrica com chave armazenada em HSM, da seguinte forma:

a. o CPF é criptografado utilizando algoritmo AES-256 (modo CBC[1]), como especificado no DOC-ICP-01.01;

1 Sendo iv=0; bloco de 128 bits; padding PKCS#7; CPF somente números, nas primeiras 11 (onze) posições (preenchimento com zeros à esquerda, se necessário).

b. em seguida o *hash* SHA256 (32 bytes) é calculado para o CPF criptografado no passo (a);
c. resultado de (b) é concatenado com o cálculo do *hash* SHA256(32 bytes) do resultado de (b);
d. por fim, o resultado do passo (c) é codificado em BASE64 (RFC 4648) para gerar o IDN.

IDN = BASE64 (SHA256(AES(CPF))||SHA256(SHA256(AES(CPF))))

A AC/PSS que utiliza o IDN pode verificar sua integridade antes de aceitá-lo.

7. NOTIFICAÇÃO DE IRREGULARIDADE E DUPLICIDADE

As ACs farão uso do item 3.1 do DOC-ICP-05.02 - PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL para encaminhar os dados biométricos do suposto fraudador.

A AC responsável pelo registro/IDN, ao receber uma notificação deve repassar ao seu PSBio, por meio do serviço de diretório, que o indexador relacionado a irregularidade deve ser desconsiderado. Nesta situação, o IDN deve ser removido da base biométrica de produção e procedimentos de fraude devem realizados conforme DOC-ICP-05.02 - PROCEDIMENTOS PARA IDENTIFICAÇÃO DO REQUERENTE E COMUNICAÇÃO DE IRREGULARIDADES NO PROCESSO DE EMISSÃO DE UM CERTIFICADO DIGITAL ICP-BRASIL.

8. TRANSAÇÕES BIOMÉTRICAS

8.1. Ciclo de vida da transação biométrica

O ciclo de vida de uma transação biométrica digital compreende os processos descritos na tabela a seguir.

Processo	Descrição
Coleta de dados biométricos	De forma assistida, os dados biométricos que serão utilizados na transação devem ser coletados, utilizando os equipamentos necessários.
Coleta de dados biográficos	Dados biográficos necessários para geração do IDN são coletados.
Criação	Dados biométricos e IDN são associados em um arquivo de transação biométrica.
Submissão	A transação é submetida ao destinatário.

Validação	O destinatário deve validar se o conteúdo enviado atende aos padrões estabelecidos.
Execução	O propósito da transação deve ser executado pelo servidor biométrico, seja ele uma verificação, armazenamento ou atualização. O resultado deve ser retornado ao remetente.
Validação da resposta	O remetente deve validar o conteúdo da resposta e finalizar a transação.

8.2. Padrões para transação biométrica

Na ICP-Brasil podem ser usados dois formatos equivalentes para Transações Biométricas Digitais:

a. Transação biométrica ANSI/NIST-ITL 1-2011 binário;

b. Transação biométrica ANSI/NIST-ITL 1-2011 XML.

A versão do ANSI/NIST-ITL utilizada neste documento é a descrita nas referências 1-2011 no sítio eletrônico do NIST, descritos a seguir. O padrão ANSI/NIST-ITL descreve uma estrutura para armazenamento de conteúdos (dados) biométricos de face, impressões digitais, palma da mão assinaturas, voz, íris, entre outras.

Este documento trata especificamente de biometrias de face e impressões digitais, relevante para o contexto ICP-Brasil. Este padrão ANSI/NIST-ITL 1-2011 dispõe de ampla documentação e variada gama de bibliotecas de software disponíveis.
Referências:

http://www.nist.gov/itl/iad/ig/ansi_standard.cfm
http://biometrics.nist.gov/cs_links/standard/AN_ANSI_1-2011_standard.pdf
http://www.nist.gov/itl/csd/biometrics/ansi-nist.cfm

8.3. Formatos das transações biométricas

Existem três propósitos de Transação Biométrica na ICP-Brasil: Operação de cadastramento; Operação de consulta de dados biométricos; e Operação de atualização de dados biométricos.

Os formatos das requisições e respostas de cada operação são descritos a seguir. O formato da resposta em caso de erro é descrito ao final e é usado sempre que uma transação falhar em sua execução.

8.3.1. Operação de cadastramento

Transações biométricas de cadastramento são utilizadas com o propósito de cadastrar um indivíduo em um banco de dados biométricos (PSBio), estabelecendo qual o padrão de

formatação e do conteúdo do cadastro. Uma transação biométrica de cadastramento deve ser composta, no mínimo, pelos seguintes dados:

a. IDN associado ao requerente a ser cadastrado;

b. Destinatário da transação;

c. Responsável pela coleta dos dados;

d. Data de coleta dos dados;

e. Local de coleta dos dados;

f. Imagens de impressões digitais dos dedos (de um a quatro);

g. Imagem frontal de face do cidadão a ser cadastrado.

Uma transação biométrica de cadastramento deve formatar os dados mencionados em formato ANSI/NIST conforme descrito a seguir.

8.3.1.1. Requisição

8.3.1.1.1. Conteúdo dos Registros do Tipo 1 da transação (Type 1)

Identificador	Índice campo	Nome do campo	Tipo de caracter e	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	1.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
VER	1.002	Versão do ANSI/NIST	Ver NIST ITL 1-2011					0500 = NIST ITL 1-2011
CNT	1.003	Conteúdo do arquivo	Ver NIST ITL 1-2011					
TOT	1.004	Tipo de transação	Ver NIST ITL 1-2011					ENR – requisição de cadastramento
DAT	1.005	Data	Ver NIST ITL 1-2011					
DAI	1.007	Agência de destino	AN	1	10	1	1	Código da agência de destino

ORI	1.008	Agência de origem	ANS	1	10	1	1	Código da agência de origem
TCN	1.009	Número de controle da transação	AN	1	40	1	1	Identificador único global (UUID / RFC 4122)
NSR	1.011	Resolução de captura	Ver NIST ITL 1-2011					19.69 – Fingerprint no type 14
NTR	1.012	Resolução de transmissão	Ver NIST ITL 1-2011					19.69 – Fingerprint no type 14

8.3.1.1.2. Conteúdo dos Registros do Tipo 2 da transação (Type 2)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	2.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	2.002	ID para informações	Ver NIST ITL 1-2011					
IDN	2.901	Identificador da identidade	AN	1	20	1	1	Ver seção 5 deste documento
IAG	2.902	Agência de emissão	AN	1	20	1	1	RFB - Agência responsável pelo documento de identificação
TOD	2.903	Tipo de documento	N	1	20	1	1	99 – CPF HASH

8.3.1.1.3. Conteúdo dos Registros do Tipo 10 da transação (Type 10)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	10.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	10.002	ID para informações	Ver NIST ITL 1-2011					
IMT	10.003	Tipo de Imagem	AS	4	11	1	1	FACE
SRC	10.004	Local de captura da imagem						
PHD	10.005	Data da foto	N	8	8	1	1	AAAAMMDD
HLL	10.006	Número de linhas horizontais	Ver NIST ITL 1-2011					
VLL	10.007	Número de linhas verticais	Ver NIST ITL 1-2011					
SLC	10.008	Escala de densidade de pixels	Ver NIST ITL 1-2011					

THPS	10.009	Densidade de pixels em direção horizontal	Ver NIST ITL 1-2011					
TVPS	10.010	Densidade de pixels em direção vertical	Ver NIST ITL 1-2011					
CGA	10.011	Algoritmo de Compressão	AN	3	5	1	1	JPEGB:JPEG ISO/IEC 10918 (Lossy) JPEGL:JPEG ISO/IEC 10918 (Lossless) JP2:JPEG 2000 ISO/IEC 15444-1 (Lossy) JP2L:JPEG 2000 ISO/IEC 15444-1 (Lossless) PNG:Portable Network Graphics
CSP	10.012	Escala de cor	Ver NIST ITL 1-2011					SRGB
DATA	10.999	Imagem da face	Ver NIST ITL 1-2011					

8.3.1.1.4. Conteúdo dos Registros do Tipo 14 da transação (Type 14)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	14.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	14.002	ID para informações	Ver NIST ITL 1-2011					

IMP	14.003	Tipo de impressão	N	1	2	1	1	
SRC	14.004	Agência de origem	UC	1	X			RFB - Agência responsável pelo documento de identificação
FCD	14.005	Data de captura da imagem	Ver NIST ITL 1-2011					
HLL	14.006	Tamanho Horizontal em pixels	Ver NIST ITL 1-2011					
VLL	14.007	Tamaho Vertical em pixels	Ver NIST ITL 1-2011					
SLC	14.008	Unidade de escala para densidade de pixels	Ver NIST ITL 1-2011					
THPS	14.009	Densidade de pixels em direção horizontal	Ver NIST ITL 1-2011					
TVPS	14.010	Densidade de pixels em direção vertical	Ver NIST ITL 1-2011					
CGA	14.011	Algorítimo de compressão						WSQ20: WSQ 3.1 ou superior
BPX	14.012	Bits por pixel	Ver NIST ITL 1-2011					

FGP	14.013	Número indexador do dedo	Josita	1: Polegar esquerdo 2: Indicador esquerdo 3: Dedo médio esquerdo 4: Anelar esquerdo 5: Dedo mínimo esquerdo 6: Polegar direito 7: Indicador direito 8: Dedo médio direito 9: Anelar direito 10: Dedo mínimo direito
AMP	14.018	Indisponível ou amputado	Ver NIST ITL 1-2011 Um único subcampo com dois itens de informação: FRAP e ABC.	FRAP (Posição de dedo): 1: Polegar esquerdo 2: Indicador esquerdo 3: Dedo médio esquerdo 4: Anelar esquerdo 5: Dedo mínimo esquerdo 6: Polegar direito 7: Indicador direito 8: Dedo médio direito 9: Anelar direito 10: Dedo mínimo direito ABC (Código do motivo): XX: Leitura parcial ou indisponível por amputação UP: Dedo temporariamente não disponível
DATA	14.999	Imagem da impressão digital	Ver NIST ITL 1-2011	Opcional, se AMP estiver presente

8.3.1.2. Resposta

8.3.1.2.1. Conteúdo dos Registros do Tipo 1 da transação (Type 1)

Identificador	Índice campo	Nome do campo	Tipo de caractere	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	1.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
VER	1.002	Versão do ANSI/NIST	Ver NIST ITL 1-2011					0500 = NIST ITL 1-2011
CNT	1.003	Conteúdo do arquivo	Ver NIST ITL 1-2011					
TOT	1.004	Tipo de transação	Ver NIST ITL 1-2011					ERE – retorno de cadastramento
DAT	1.005	Data	Ver NIST ITL 1-2011					
DAI	1.007	Agência de destino	AN	1	10	1	1	Código da agência de destino
ORI	1.008	Agência de origem	ANS	1	10	1	1	Código da agência de origem
TCN	1.009	Número de controle da transação	AN	1	40	1	1	Identificador único global (UUID / RFC 4122)
TCR	1.010	Número de controle de referência da transação	NA	1	40	1	1	Deve conter o TCN da requisição ao qual a resposta se refere
NSR	1.011	Resolução de captura	Ver NIST ITL 1-2011					00.00
NTR	1.012	Resolução de transmissão	Ver NIST ITL 1-2011					00.00

8.3.1.2.2. Conteúdo dos Registros do Tipo 2 da transação (Type 2)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	2.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	2.002	ID para informações	Ver NIST ITL 1-2011					
IDN	2.901	Identificador da identidade	AN	1	20	1	1	Ver seção 5 deste documento
IAG	2.902	Agência de emissão	AN	1	20	1	1	RFB - Agência responsável pelo documento de identificação
TOD	2.903	Tipo de documento	N	1	20	1	1	99 – CPF HASH

8.3.2. Operação de consulta

Transações biométricas de verificação são utilizadas com o propósito de verificar se determinada característica biométrica associada a um indivíduo é compatível com a biometria existente dentro de um Sistema Biométrico da ICP-Brasil (processo de verificação 1:1); ou para identificar se determinada característica biométrica já está associada a um indivíduo (processo de identificação 1:N).

Uma transação biométrica de consulta deve ser composta pelos seguintes dados:

a. IDN associado ao requerente a ser verificado;
b. Destinatário da transação;
c. Responsável pela coleta dos dados;
d. Data de coleta dos dados;
e. Local de coleta dos dados;
f. Imagem frontal da face ou imagem de impressão digital de um dos dedos cadastrados.

O uso da biometria da face só deve ser utilizada caso o indivíduo não tenha qualidade de comparação ou tenha sua impressão digital temporariamente ou definitivamente comprometida.

Uma transação biométrica de verificação deve formatar os dados mencionados em formato ANSI/NIST conforme descrito a seguir.

8.3.2.1. Requisição – Impressão digital

8.3.2.1.1. Conteúdo dos Registros do Tipo 1 da transação (Type 1)

Identificador	Índice campo	Nome do campo	Tipo de caractere	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	1.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
VER	1.002	Versão do ANSI/NIST	Ver NIST ITL 1-2011					0500 = NIST ITL 1-2011
CNT	1.003	Conteúdo do arquivo	Ver NIST ITL 1-2011					
TOT	1.004	Tipo de transação	Ver NIST ITL 1-2011					VER – requisição de verificação (1:1) IDE – requisição de identificação (1:N)
DAT	1.005	Data	Ver NIST ITL 1-2011					
DAI	1.007	Agência de destino	AN	1	10	1	1	Código da agência de destino
ORI	1.008	Agência de origem	ANS	1	10	1	1	Código da agência de origem
TCN	1.009	Número de controle da transação	AN	1	40	1	1	Identificador único global (UUID / RFC 4122)
NSR	1.011	Resolução de captura	Ver NIST ITL 1-2011					19.69 – Fingerprint no type 14
NTR	1.012	Resolução de transmissão	Ver NIST ITL 1-2011					19.69 – Fingerprint no type 14

8.3.2.1.2. Conteúdo dos Registros do Tipo 2 da transação (Type 2)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	2.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	2.002	ID para informações	Ver NIST ITL 1-2011					
IDN	2.901	Identificador da identidade	AN	1	20	1	1	Ver seção 5 deste documento
IAG	2.902	Agência de emissão	AN	1	20	1	1	RFB - Agência responsável pelo documento de identificação
TOD	2.903	Tipo de documento	N	1	20	1	1	99 – CPF HASH

8.3.2.1.3. Conteúdo dos Registros do Tipo 14 da transação (Type 14)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	14.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					

IDC	14.002	ID para informaçõe s	Ver NIST ITL 1-2011					
IMP	14.003	Tipo de impressã o	N	1	2	1	1	
SRC	14.004	Agência de origem	UC	1	X			RFB - Agência responsável pelo documento de identificação
FCD	14.005	Data de captura da imagem	Ver NIST ITL 1-2011					
HLL	14.006	Tamanho Horizont al em pixels	Ver NIST ITL 1-2011					
VLL	14.007	Tamaho Vertical em pixels	Ver NIST ITL 1-2011					
SLC	14.008	Unidade de escala para densidade de pixels	Ver NIST ITL 1-2011					
TH P S	14.009	Densidad e de pixels em direção horizontal	Ver NIST ITL 1-2011					
TV P S	14.010	Densidad e de pixels em direção vertical	Ver NIST ITL 1-2011					
CGA	14.011	Algorítim o de compress ão						WSQ20: WSQ 3.1 ou superior

BPX	14.012	Bits por pixel	Ver NIST ITL 1-2011	
FGP	14.013	Número indexador do dedo		1: Polegar esquerdo 2: Indicador esquerdo 3: Dedo médio esquerdo 4: Anelar esquerdo 5: Dedo mínimo esquerdo 6: Polegar direito 7: Indicador direito 8: Dedo médio direito 9: Anelar direito 10: Dedo mínimo direito
DATA	14.999	Imagem da impressão digital	Ver NIST ITL 1-2011	

8.3.2.2. Requisição – Face

8.3.2.2.1. Conteúdo dos Registros do Tipo 1 da transação (Type 1)

Identificador	Índice campo	Nome do campo	Tipo de caractere	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	1.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
VER	1.002	Versão do ANSI/NIST	Ver NIST ITL 1-2011					0500 = NIST ITL 1-2011
CNT	1.003	Conteúdo do arquivo	Ver NIST ITL 1-2011					
TOT	1.004	Tipo de transação	Ver NIST ITL 1-2011					VER – requisição de verificação

DAT	1.005	Data	Ver NIST ITL 1-2011					
DAI	1.007	Agência de destino	AN	1	10	1	1	Código da agência de destino
ORI	1.008	Agência de origem	AN S	1	10	1	1	Código da agência de origem
TCN	1.009	Número de controle da transação	AN	1	40	1	1	Identificador único global (UUID / RFC 4122)
NSR	1.011	Resolução de captura	Ver NIST ITL 1-2011					19.69 – Fingerprint no *type* 14
NTR	1.012	Resolução de transmissão	Ver NIST ITL 1-2011					19.69 – Fingerprint no *type* 14

8.3.2.2.2. Conteúdo dos Registros do Tipo 2 da transação (Type 2)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	2.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	2.002	ID para informações	Ver NIST ITL 1-2011					
IDN	2.901	Identificador da identidade	AN	1	20	1	1	Ver seção 5 deste documento
IAG	2.902	Agência de emissão	AN	1	20	1	1	RFB - Agência responsável pelo documento de identificação
TOD	2.903	Tipo de documento	N	1	20	1	1	99 – CPF HASH

8.3.2.2.3. Conteúdo dos Registros do Tipo 10 da transação (Type 10)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	10.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	10.002	ID para informações	Ver NIST ITL 1-2011					
IMT	10.003	Tipo de Imagem	AS	4	11	1	1	FACE
SRC	10.004	Local de captura da imagem						
PHD	10.005	Data da foto	N	8	8	1	1	AAAAMMDD
HLL	10.006	Número de linhas horizontais	Ver NIST ITL 1-2011					
VLL	10.007	Número de linhas verticais	Ver NIST ITL 1-2011					
SLC	10.008	Escala de densidade de pixels	Ver NIST ITL 1-2011					
THPS	10.009	Densidade de pixels em direção horizontal	Ver NIST ITL 1-2011					
TVPS	10.010	Densidade de pixels em direção vertical	Ver NIST ITL 1-2011					

CGA	10.011	Algoritimo de Compressão	AN	3	5	1	1	JPEGB:JPEG ISO/IEC 10918 (Lossy) JPEGL:JPEG ISO/IEC 10918 (Lossless) JP2:JPEG 2000 ISO/IEC 15444-1 (Lossy) JP2L:JPEG 2000 ISO/IEC 15444-1 (Lossless) PNG:Portable Network Graphics
CSP	10.012	Escala de cor	Ver NIST ITL 1-2011					SRGB
DATA	10.999	Imagem da face	Ver NIST ITL 1-2011					

8.3.2.3. Resposta

As respostas de transação biométrica de verificação, de impressão digital ou face, devem formatar os dados mencionados em formato ANSI/NIST conforme descrito a seguir.

8.3.2.3.1. Conteúdo dos Registros do Tipo 1 da transação (Type 1)

Identificador	Índice campo	Nome do campo	Tipo de caractere	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	1.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
VER	1.002	Versão do ANSI/NIST	Ver NIST ITL 1-2011					0500 = NIST ITL 1-2011
CNT	1.003	Conteúdo do arquivo	Ver NIST ITL 1-2011					
TOT	1.004	Tipo de transação	Ver NIST ITL 1-2011					VRE – Resultado de consulta
DAT	1.005	Data	Ver NIST ITL 1-2011					
DAI	1.007	Agência de destino	AN	1	10	1	1	Código da agência de destino
ORI	1.008	Agência de origem	ANS	1	10	1	1	Código da agência de origem

TCN	1.009	Número de controle da transação	AN	1	40	1	1	Identificador único global (UUID / RFC 4122)
TCR	1.010	Número de controle de referência da transação	NA	1	40	1	1	Deve conter o TCN da requisição ao qual a resposta se refere
NSR	1.011	Resolução de captura	Ver NIST ITL 1-2011					00.00
NTR	1.012	Resolução de transmissão	Ver NIST ITL 1-2011					00.00

8.3.2.3.2. Conteúdo dos Registros do Tipo 2 da transação (Type 2)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	2.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	2.002	ID para informações	Ver NIST ITL 1-2011					
IDN	2.901	Identificador da identidade	AN	1	20	1	1	Ver seção 5 deste documento
IAG	2.902	Agência de emissão	AN	1	20	1	1	RFB - Agência responsável pelo documento de identificação
TOD	2.903	Tipo de documento	N	1	20	1	1	99 – CPF HASH
SRF	2.907	Resultado da busca	A	1	1	1	1	M – Resultado positivo para as biometrias enviadas X – Resultado negativo para as biometrias enviadas

8.3.3. Operação de atualização

Transações biométricas de atualização são utilizadas com o propósito de atualizar as informações biométricas de um indivíduo em um banco de dados biométricos (PSBio). Uma operação de atualização biométrica deve conter no mínimo as informações listadas abaixo:

a. IDN associado ao requerente a ser cadastrado;
b. Destinatário da transação;

c. Responsável pela coleta dos dados;
d. Data de coleta dos dados;
e. Local de coleta dos dados;

Além das informações listadas acima, deve conter no mínimo uma (ou mais) biometrias listadas abaixo:

f. Imagem de impressão digital frontal do dedo indicador direito;
g. Imagem de impressão digital frontal do dedo indicador esquerdo;
h. Imagem de impressão digital frontal do dedo médio direito;
i. Imagem de impressão digital frontal do dedo médio esquerdo;
j. Imagem frontal de face do cidadão a ser cadastrado.

As transações de atualização, devem ser precedidas de uma transação de verificação (VER), que valide pelo menos uma das biometrias do registro existente.

Durante o processo de atualização, os dados biométricos enviados na transação devem sobrepor os já existentes, e caso alguma biometria não seja enviada, os dados anteriores devem ser mantidos. Deve ser realizado o processo de busca 1:N em todas as novas biometrias enviadas na transação.

Uma transação biométrica de atualização deve formatar os dados mencionados em formato ANSI/NIST conforme descrito a seguir.

8.3.3.1. Requisição

8.3.3.1.1. Conteúdo dos Registros do Tipo 1 da transação (Type 1)

Identificador	Índice campo	Nome do campo	Tipo de caractere	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	1.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
VER	1.002	Versão do ANSI/NIST	Ver NIST ITL 1-2011					0500 = NIST ITL 1-2011
CNT	1.003	Conteúdo do arquivo	Ver NIST ITL 1-2011					

TOT	1.004	Tipo de transação	Ver NIST ITL 1-2011					UPR – requisição de atualização
DAT	1.005	Data	Ver NIST ITL 1-2011					
DAI	1.007	Agência de destino	AN	1	10	1	1	Código da agência de destino
ORI	1.008	Agência de origem	ANS	1	10	1	1	Código da agência de origem
TCN	1.009	Número de controle da transação	AN	1	40	1	1	Identificador único global (UUID / RFC 4122)
NSR	1.011	Resolução de captura	Ver NIST ITL 1-2011					19.69 – Fingerprint no type 14
NTR	1.012	Resolução de transmissão	Ver NIST ITL 1-2011					19.69 – Fingerprint no type 14

8.3.3.1.2. Conteúdo dos Registros do Tipo 2 da transação (Type 2)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	2.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	2.002	ID para informações	Ver NIST ITL 1-2011					
IDN	2.901	Identificador da identidade	AN	1	20	1	1	Ver seção 5 deste documento

IAG	2.902	Agência de emissão	AN	1	20	1	1	RFB - Agência responsável pelo documento de identificação
TOD	2.903	Tipo de documento	N	1	20	1	1	99 – CPF HASH

8.3.3.1.3. Conteúdo dos Registros do Tipo 10 da transação (Type 10)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	10.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	10.002	ID para informações	Ver NIST ITL 1-2011					
IMT	10.003	Tipo de Imagem	AS	4	11	1	1	FACE
SRC	10.004	Local de captura da imagem						
PHD	10.005	Data da foto	N	8	8	1	1	AAAAMMDD
HLL	10.006	Número de linhas horizontais	Ver NIST ITL 1-2011					

VLL	10.007	Número de linhas verticais	Ver NIST ITL 1-2011	
SLC	10.008	Escala de densidade de pixels	Ver NIST ITL 1-2011	
THPS	10.009	Densidade de pixels em direção horizontal	Ver NIST ITL 1-2011	
TVPS	10.010	Densidade de pixels em direção vertical	Ver NIST ITL 1-2011	
CGA	10.011	Algoritimo de Compressão	AN 3 5 1 1	JPEGB:JPEG ISO/IEC 10918 (Lossy) JPEGL:JPEG ISO/IEC 10918 (Lossless) JP2:JPEG 2000 ISO/IEC 15444-1 (Lossy) JP2L:JPEG 2000 ISO/IEC 15444-1 (Lossless) PNG:Portable Network Graphics
CSP	10.012	Escala de cor	Ver NIST ITL 1-2011	SRGB
DATA	10.999	Imagem da face	Ver NIST ITL 1-2011	

8.3.3.1.4. Conteúdo dos Registros do Tipo 14 da transação (Type 14)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	14.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	14.002	ID para informações	Ver NIST ITL 1-2011					
IMP	14.003	Tipo de impressão	N	1	2	1	1	
SRC	14.004	Agência de origem	UC	1	X			RFB - Agência responsável pelo documento de identificação
FCD	14.005	Data de captura da imagem	Ver NIST ITL 1-2011					
HLL	14.006	Tamanho Horizontal em pixels	Ver NIST ITL 1-2011					
VLL	14.007	Tamaho Vertical em pixels	Ver NIST ITL 1-2011					
SLC	14.008	Unidade de escala para densidade de pixels	Ver NIST ITL 1-2011					

THPS	14.009	Densidade de pixels em direção horizontal	Ver NIST ITL 1-2011	
TVPS	14.010	Densidade de pixels em direção vertical	Ver NIST ITL 1-2011	
CGA	14.011	Algorítimo de compressão		WSQ20: WSQ 3.1 ou superior
BPX	14.012	Bits por pixel	Ver NIST ITL 1-2011	
FGP	14.013	Número indexador do dedo		2: Indicador esquerdo 3: Dedo médio esquerdo 7: Indicador direito 8: Dedo médio direito
AMP	14.018	Indisponível ou amputado	Ver NIST ITL 1-2011 Um único subcampo com dois itens de informação: FRAP e ABC.	FRAP (Posição de dedo): 2: Indicador esquerdo 3: Dedo médio esquerdo 7: Indicador direito 8: Dedo médio direito ABC (Código do motivo): XX: Leitura parcial ou indisponível por amputação UP: Dedo temporariamente não disponível
DATA	14.999	Imagem da impressão digital	Ver NIST ITL 1-2011	Opcional, se AMP estiver presente

8.3.3.1.5. Conteúdo dos Registros do Tipo 1 da transação (Type 1)

Identificador	Índice campo	Nome do campo	Tipo de caractere	Tamano por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	1.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
VER	1.002	Versão do ANSI/NIST	Ver NIST ITL 1-2011					0500 = NIST ITL 1-2011
CNT	1.003	Conteúdo do arquivo	Ver NIST ITL 1-2011					
TOT	1.004	Tipo de transação	Ver NIST ITL 1-2011					ERE – retorno de cadastramento
DAT	1.005	Data	Ver NIST ITL 1-2011					
DAI	1.007	Agência de destino	AN	1	10	1	1	Código da agência de destino
ORI	1.008	Agência de origem	ANS	1	10	1	1	Código da agência de origem
TCN	1.009	Número de controle da transação	AN	1	40	1	1	Identificador único global (UUID / RFC 4122)
TCR	1.010	Número de controle de referência da transação	NA	1	40	1	1	Deve conter o TCN da requisição ao qual a resposta se refere
NSR	1.011	Resolução de captura	Ver NIST ITL 1-2011					00.00
NTR	1.012	Resolução de transmissão	Ver NIST ITL 1-2011					00.00

8.3.3.1.6. Conteúdo dos Registros do Tipo 2 da transação (Type 2)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamano por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	2.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	2.002	ID para informações	Ver NIST ITL 1-2011					
IDN	2.901	Identificador da identidade	AN	1	20	1	1	Ver seção 5 deste documento

IAG	2.902	Agência de emissão	AN	1	20	1	1	RFB - Agência responsável pelo documento de identificação
T/OD	2.903	Tipo de documento	N	1	20	1	1	99 – CPF HASH

8.3.4. Falha em operação biométrica

Qualquer transação biométrica que falhar em sua execução deve enviar uma resposta de erro em formato ANSI/NIST conforme descrito a seguir.

8.3.4.1. Conteúdo dos Registros do Tipo 1 da transação (Type 1)

Identificador	Índice campo	Nome do campo	Tipo de caracter	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	1.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
VER	1.002	Versão do ANSI/NIST	Ver NIST ITL 1-2011					0500 = NIST ITL 1-2011
CNT	1.003	Conteúdo do arquivo	Ver NIST ITL 1-2011					
TOT	1.004	Tipo de transação	Ver NIST ITL 1-2011					ERR – retorno de erro na operação
DAT	1.005	Data	Ver NIST ITL 1-2011					
DAI	1.007	Agência de destino	AN	1	10	1	1	Código da agência de destino
ORI	1.008	Agência de origem	ANS	1	10	1	1	Código da agência de origem
TCN	1.009	Número de controle da transação	AN	1	40	1	1	Identificador único global (UUID / RFC 4122)
TCR	1.010	Número de controle de referência da transação	NA	1	40	1	1	Deve conter o TCN da requisição ao qual a resposta se refere
NSR	1.011	Resolução de captura	Ver NIST ITL 1-2011					00.00
NTR	1.012	Resolução de transmissão	Ver NIST ITL 1-2011					00.00

8.3.4.2. Conteúdo dos Registros do Tipo 2 da transação (Type 2)

Identificador	Índice do campo	Nome do campo	Tipo de caracteres	Tamanho por ocorrência		Ocorrências		Observações
				Min	Max	Min	Max	
LEN	2.001	Tamanho do registro lógico	Ver NIST ITL 1-2011					
IDC	2.002	ID para informações	Ver NIST ITL 1-2011					
MSG	2.060	Mensagem de erro	AN	1	300	1	1	Mensagem de erro da operação
COD	2.061	Código de erro	NA	1	3	1	1	Código identificador de erro da operação.

8.3.4.2.1. Códigos de erro (COD 2.061)

Os possíveis erros estão especificados a seguir:

Código	Descrição do erro
101	IDN informado já existe na base biométrica
102	Biometria informada foi encontrada associada a outro IDN
190	Dados informados são inválidos para transação de cadastramento
201	IDN informado não existe na base biométrica
202	Impressão digital para dedo informado não existe na base biométrica
290	Dados informados são inválidos para transação de consulta
901	TCN duplicado
990	Dados inválidos