Métodos de Interface do Serviço de Lista Negativa

Para fins de consulta para emissão de certificados, o ITI disponibiliza, por meio de serviços web, a Lista Negativa da ICP-Brasil, além do serviço para Comunicação de Fraude, de forma que a comunicação deve ser feita diretamente entre o sistema do ITI e os sistemas de AC.

Dentro da sua interface, o serviço web do ITI disponibilizará os seguintes métodos de acesso para Lista Negativa e Comunicação de Fraude:

Consulta Situação do Serviço: Informa ao computador cliente se o serviço está ou não ativo. Desta forma, evita-se erros de comunicação assim como reduz-se tráfego desnecessário de dados em situações em que o serviço não está disponível;

Envia Ocorrências: Recebe da AC uma lista de ocorrências novas e salva todas as ocorrências válidas, gerando um número único para cada uma delas. Como resposta, a AC recebe uma lista com os respectivos números das ocorrências ou com o código do erro ocorrido durante o processamento;

Sincroniza Ocorrências: Fornece para a AC uma lista de todas as ocorrências registradas a partir da data/hora da última consulta assim como as entradas da Lista Negativa. Desta forma, a AC mantém seu próprio banco de ocorrências para consultas offline;

Restaura Ocorrências: Fornece para a AC uma lista completa de todas as ocorrências desde o início da operação do sistema, assim como as entradas da Lista Negativa. Desta forma, a AC mantém seu próprio banco de ocorrências para consultas offline;

A descrição completa dos métodos, para fins de implementação da comunicação nos sistemas de AC, será encaminhada por e-mail paras as ACs de primeiro nível que solicitarem acesso ao serviço.

Para acesso ao serviço, os responsáveis técnicos das AC de primeiro nível devem encaminhar mensagem de correio eletrônico, assinada digitalmente com certificado padrão ICP-Brasil, para o endereço saf.suporte@iti.gov.br com as seguintes informações:

- Endereço(s) IP(s) a partir do(s) qual(is) será(ão) realizado(s) os acessos aos serviços disponibilizados pelo ITI;

- Certificado digital do(s) equipamento(s) que realizará(ão) os acessos aos serviços disponibilizados pelo ITI e respectiva cadeia no formato PKCS7 para fins de autenticação mútua entre as partes comunicantes;

- Dados (nome, telefones...) 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 endereço eletrônico.

Após o recebimento e validação das informações acima, o ITI encaminhará, como resposta, mensagem de correio eletrônico, assinada digitalmente com certificado padrão ICP-Brasil, com as seguintes informações:

- Endereços IPs nos quais serão disponibilizados os serviços;

- Certificados digitais dos equipamentos que responderão pelos serviços disponibilizados pelo ITI e respectiva cadeia no formato PKCS7 para fins de autenticação mútua entre as partes comunicantes;

- Dados (nome, telefones, endereço de correio eletrônico...) do responsável para suporte técnico.

Quaisquer alterações nas informações acima serão encaminhadas, por meio de mensagens de correio eletrônico, para os endereços informados pelas ACs.

Em caso de problema de acesso aos serviços disponibilizados pelo ITI, este deverá ser comunicado, por meio de mensagem de correio eletrônico para o endereço informado acima, assinada digitalmente com certificado padrão ICP-Brasil, pela AC, seu PSS ou um dos responsáveis técnicos devidamente cadastrados. Mensagens recebidas em desconformidade com as especificações serão descartadas automaticamente.

O serviço Restaura Ocorrências ficará indisponível de segunda-feira a sábado, das 8 h às 18 h. Os demais serviços web mencionados acima terão uma janela diária para manutenção da base de dados e backup no período de 01:00 a 02:00 horas com indisponibilidade total dos serviços.

Outras indisponibilidades programadas serão informadas por meio de mensagens de correio eletrônico, assinadas digitalmente com certificado padrão ICP-Brasil, para os responsáveis técnicos devidamente cadastrados.

Os sistemas de AC deverão consultar o serviço disponibilizado pelo ITI, para fins de atualização da base de dados local referente à Lista Negativa da ICP-Brasil, em intervalos de tempo não superior a 30 minutos, quando deverão ser realizados os seguintes passos:

1) Consultar a disponibilidade do serviço por meio do método Consulta Situação do Serviço;

2) Atualizar a base de dados da AC por meio do método Sincroniza Ocorrências, caso já exista uma base de dados disponível localmente para uso da AC, ou por meio do método Restaura Ocorrências, no caso da não existência de uma base de dados disponível localmente na AC.

Para fins de comunicação de fraude, os sistemas de AC deverão utilizar os serviços disponibilizados pelo ITI da seguinte maneira:

1) Consultar a disponibilidade por meio do método Consulta Situação do Serviço;

2) Enviar comunicações de fraude por meio do método Envia Ocorrências.

Para os casos mencionados acima, caso a consulta à disponibilidade do serviço obtenha a resposta 'não ativo', a AC deverá realizar novas consultas dentro de intervalos de tempo não superiores a 10 (dez) minutos até conseguir realizar a operação desejada.

Os sistemas de AC devem, com relação às atividades de acesso aos serviços disponibilizados pelo ITI e descritos neste ADE, registrar, armazenar, tratar e auditar os registros (logs) em conformidade com o DOC-ICP 02 e DOC-ICP-05. Além disso, deve-se armazenar registros das consultas realizadas à Lista Negativa armazenada localmente de forma a manter a sua correlação

com os respectivos certificados emitidos quando for o caso.

Informações na interface do sistema de comunicação de fraude

1 - A comunicação de fraude ou tentativa de fraude deve ser realizada por meio do preenchimento dos seguintes campos na interface do sistema de comunicação de fraude da AC:

a) A AC e AR onde ocorreu a fraude ou tentativa (tabela pré-determinada) – obrigatório (lembrando que essas informações não serão replicadas no método de atualização de base da AC, somente serão armazenadas no servidor ITI);

b) Nome do Informante: quem está cadastrando a fraude – opcional;

c) CPF do Informante: CPF de quem está cadastrando a fraude – opcional;

d) UF: escolha da UF onde ocorreu a fraude/indício (tabela pré-determinada) – obrigatório;

e) Município: escolha do município onde ocorreu a fraude/indício (tabela pré-determinada por UF) – obrigatório;

f) Tipo de Ocorrência: indício ou fraude – obrigatório;

g) Número do certificado: número de série do certificado se for fraude – obrigatório;

h) Ocorrência: breve relato do modo de operação do estelionatário, data, tipo de documento apresentado, tipo de certificado fraudado, como foi detectada a fraude/indício (2000 caracteres no máximo) – obrigatório;

i) Data da ocorrência: data da identificação do indivíduo – obrigatório;

j) Diligência de investigação: como foi detectada a fraude. Caso alguma forma de detecção tenha dado como válido o documento, marcar “válido”. Caso a forma de detecção tenha constatado a fraude no documento, marcar como “inválido”. Clicar em “Adicionar” para inclusão – opcional;

k) Nome: nome conforme aparece no documento apresentado – obrigatório;

l) CPF: número do CPF conforme apresentado no documento – obrigatório;

m) Data de nascimento: data conforme apresentado no documento – obrigatório;

n) Correio eletrônico: correio eletrônico fornecido do suposto fraudador – opcional;

o) Telefone: telefone fornecido do suposto cliente – opcional;

p) Documento de identidade: deverá ser informado o número e a data de expedição do respectivo documento e, sempre que constante do documento, o número do RG – obrigatório, se for o caso;

q) Certidão: certidões depois de 2009 apresentam uma matrícula (número único), que deve ser colocada no campo “número”. Fornecer as seguintes informações, quando constantes da certidão: (i) número; (ii) naturalidade ; (iii) livro; (iv) folha; (v) número de RG, CTPS, quando presentes – opcional;

r) CNH: caso seja CNH apresentada, fornecer as seguintes informações: (i) número; (ii) data de emissão; (iii) 1ª habilitação; (iv) UF expedição; (v) data de validade; (vi). formulário; (vii) número de identidade – obrigatório, se for o caso;

s) Passaporte: caso seja Passaporte apresentado, fornecer as seguintes informações: (i) número; (ii) data de expedição; (iii) data de validade; (iv) país (tabela pré-determinada) – obrigatório, se for o caso;

t) CTPS: caso seja CTPS apresentada, fornecer as seguintes informações: (i) número; (ii) data de emissão; (iii) PIS/PASEP; (iv) UF (tabela pré-determinada) – obrigatório, se for o caso;

u) Outro documento: qualquer outro documento de natureza civil, como, por exemplo, carteira de entidade de classe, que têm por força legal a presunção de identificação, fornecer as seguintes informações: (i) número; (ii) data de emissão; (iii) nome; (iv) UF (tabela pré-determinada) – obrigatório, se for o caso;

v) Características físicas: devem ser selecionadas as características físicas perceptíveis do suposto fraudador, tais quais: (i) cor da pele (seleção: amarelo; branco; indígena; negro; pardo); (ii) cor dos olhos (seleção: claros; escuros); (iii) cor predominante do cabelo (seleção: branco; escuro; grisalho; loiro; ruivo); (iv) deficiências físicas perceptíveis (seleção: cadeirante; cego; manco; mudo; surdo); (v) idade aparente (seleção: A – menor que 30 anos; B – entre 30 e 50 anos; C – mais de 50 anos); (vi). sexo (seleção: masculino; feminino); (vii) sinais corporais perceptíveis (seleção: falta de dedos nas mãos; mancha na pele; marcas como cicatrizes; tatuagem ou sinais em membros superiores; tatuagem ou sinais no rosto ou pescoço); (viii) tipo de cabelo (seleção: calvo; curto; longo; médio) – opcional;

w) Informações da empresa: fornecer as seguintes informações: (i) CNPJ; (ii) razão social; (iii) endereço; (iv) telefone; (v) CEP; (vi) CNAE; (vii) UF (tabela pré-determinada); (vii) Município (tabela pré-determinada por UF) – obrigatório, se for o caso;

x) Upload da imagem do documento de identificação e da face: deve ser enviada a imagem do documento de identificação (escolher tipos: RG, CNH, CTPS, PASSAPORTE, OUTROS) e da face (escolher o tipo FOTO) disposta em pé do suposto fraudador no comunicado – obrigatório.

1.1 - No campo “outros”, do Sistema de Comunicação de Fraude, deve-se, também, realizar o upload das imagens em formato WSQ das impressões digitais dos supostos fraudadores, conforme especificações contidas na Instrução Normativa ITI nº 09, de 22 de outubro de 2020. Os arquivos de impressões digitais devem estar nomeados da seguinte forma:

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; e
10. dedo mínimo direito.

1.1.1 - Essas impressões digitais, assim como a face, devem ser submetidas/enviadas pela AC/PSS ao seu respectivo Sistema Biométrico para inserção dessas biometrias no repositório de Lista Negativa biométrica deste.

1.2 - Deve-se ter certeza da informação antes de adicionar as características físicas do fraudador, ou, em caso de dúvida, deve-se deixar uma ou mais informações físicas sem serem adicionadas. Essas informações serão utilizadas posteriormente por todas as ACs para as pesquisas por características físicas na Lista Negativa da AC, sendo fundamental que estejam corretas para que se tornem eficientes.

1.3 - A imagem do documento de identificação deve ser juntada em formato JPG ou JPEG, com a face do requerente disposta em pé, nomeado com o CPF do mesmo (exemplo: 11122233344.jpeg), com no mínimo 300 dpi de resolução, com cor, tamanho máximo de 1 MB, em que se possa ler nitidamente todas as informações biográficas apresentadas no documento.

1.4 - A imagem da face deve estar em formato (JPG ou JPEG), com a face do requerente disposta em pé, nomeado com o CPF “FACE” do mesmo (exemplo: 11122233344FACE.jpeg), com no mínimo 300 dpi de resolução, com cor, tamanho máximo de 1 MB, podendo ser recortada do próprio documento de identificação.

1.5 - Após o preenchimento dos campos do comunicado e upload das imagens, deve ser realizada a verificação de todas as informações inseridas e, caso estejam corretas, deve ser enviado o comunicado ao ITI.