INTEGRAÇÃO DA CERTIDÃO

AUTOMÁTICA

Operador Nacional
do Sistema de Registro
Eletrônico de Imóveis

Resumo

Este manual tem o objetivo de esclarecer o processo de resposta automática a pedidos de certidão tramitados pelo sistema, eliminando a necessidade de interação humana.

Neste documento, são especificados os parâmetros de entrada e saída necessários para o desenvolvimento interno por parte das empresas fornecedoras de sistemas para cartórios. Estes parâmetros visam garantir a criação de módulos de aplicação que possibilitem a comunicação e integração com o serviço de certidão digital.

Com essa integração, você poderá receber os pedidos através do WS Ofício, utilizando os métodos listados no capítulo 1. Após serem recepcionados, os documentos podem ser assinados utilizando o Assinador Web (Rest PKI Core), que inclui a adição de QR Code, marca d'água, hash de validação e carimbo de tempo. Por fim, para concluir e responder ao pedido, utilizamos o WS Ofício, que envia o documento assinado como resposta.

É crucial que o cartório siga as diretrizes descritas neste manual para assegurar a correta execução do processo de emissão automática.

Índice

CAPÍTULO 1

WS Ofício

Operador Nacional
do Sistema de Registro
Eletrônico de Imóveis

O que é o WS Ofício?

O WS OFÍCIO é um Web Service de comunicação e integração com os diversos serviços oferecidos pelo SAEC. Este serviço envia o documento assinado, respondendo assim o pedido.

Requisitos de Segurança

O modelo de segurança consiste em validação de hash entre as mensagens. Além disso, como acréscimo de segurança, o acesso aos serviços do ONR está restrito por IP. Um hash de autenticação é formado pela combinação da chave + token. O hash é então codificado no padrão SHA-1, codificação UTF-8.

A chave é uma string única que é de conhecimento somente do ONR e da instituição. Essa chave não é transmitida entre as mensagens. Para obter a chave única referente à sua instituição entre em contato com o ONR através do e-mail: oficioeletronico@onr.org.br. O token é uma string dinâmica criada para, em conjunto com a chave, gerar o hash de autenticação. Dessa forma o hash usado em cada mensagem será diferente e poderá ser usado apenas uma vez. Caso a mensagem seja interceptada, o mesmo hash não poderá ser reaproveitado impedindo assim o uso indevido da aplicação.

Esse modelo de autenticação é de gerenciamento simples e seguro, pois o token é gerado no momento da requisição, além da chave que precisa ser de conhecimento para cada entidade envolvida.

Login

Todos os serviços disponibilizados pelo ONR através de Web Services utilizam um sistema de validação por hash. Um hash válido é gerado através da combinação de uma chave + token (Para mais informações consulte o capítulo 2). O token necessário para gerar o hash é obtido através da validação de usuário, utilizando um serviço de "Login". O Web Service de Login tem o único propósito de retornar os tokens a serem utilizados para gerar o hash necessário para a troca das mensagens. Os tokens são apenas retornados após validação das credenciais de um usuário válido, previamente cadastrado no sistema OFÍCIO ELETRÔNICO. O serviço pode retornar vários tokens em uma única requisição, isso para que não seja necessário uma nova requisição de token sempre que for executado outro serviço. A quantidade padrão de tokens retornados pelo serviço em uma única requisição é 5, porém esse valor pode ser alterado.

Os tokens são strings dinâmicas, formadas por 6 caracteres. Ex.: JGX3QL LGO8A7 XUWR08 AG5K3U 1MLG7B Cada token poderá ser usado apenas uma vez. Depois de usado o sistema não permitirá que o mesmo token seja reutilizado. Além disso cada token tem uma validade de 8 horas a partir de sua geração. Segue diagrama que contempla uma visão geral referente à utilização dos serviços oferecidos pelo ONR através de Web Services.

Certidões a Emitir

• O ONR disponibiliza os serviços referentes à emissão de certidões através de web services contemplando as seguintes funcionalidades:

- Devolução
Responde uma solicitação com status "Devolvido"

- Envio de anexo
Anexa arquivos ao protocolo informado.

- Finalização
• Modifica o status de uma solicitação para "Respondido", após ao menos um arquivo ter sido anexado.

• Informação de Custas
Permite que o cartório informe as custas do pedido.

Envelope de Entrada - ObterXMLSolicitacoes_v4

Os parâmetros de entrada são:

- Hash - Hash para validação da mensagem (tipo string).
- Protocolo - Filtro opcional para um protocolo específico (tipo string)
- Solicitante - Filtro opcional para o nome do solicitante (tipo string)

- **TipoCertidao - Filtro opcional para o tipo de certidão, baseado na seginte tabela:**
- 1 - PROPRIEDADE/NEGATIVA DE PROPRIEDADE
- 2 - VINTENÁRIA
- 3 - MATRÍCULA DO IMÓVEL
- 4 - TRANSCRIÇÃO
- 5 - PACTO ANTENUPCIAL
- 6 - ONUS
- 7 - DOCUMENTO ARQUIVADO
- 8 - CONVENÇÃO DE CONDOMÍNIO
- 9 - LIVRO3-Garantias
- 10 - OUTROS REGISTROS LIVRO3-Auxiliar
- 12- INTEIRO TEOR, ÔNUS E AÇÕES
- 13 - POR QUESITO
- 14 - NEGATIVA DE PENHOR
- 15 - ONUS REAIS E AÇÕES REIPERSECUTÓRIAS
- 16 - USUCAPIÃO
- 17 - PROPRIEDADE, ONUS E ALIENAÇOES
- 18 - CADEIA DOMINIAL (FILIAÇÃO ATÉ ORIGEM)
- 19 - AÇÕES REIPERSECUTÓRIAS
- 20 - ONUS REAIS
- 21 - CERTIDÃO DA SITUAÇÃO JURÍDICA ATUALIZADA DO IMÓVEL

• **PesquisaPor - Filtro opcional para o tipo de pesquisa, baseado na seguinte tabela:**
- 4 - MATRICULA
- 5 - TRANSCRIÇÃO
- 6 - PESSOA
- 7 - NUMERO REGISTRO
- 8 - NOME DOS PACTUANTES
- 9 - ENDEREÇO
- 10 - PROTOCOLO
- 11 - N° DO REGISTRO LIVRO3
- 12 - NOME CONDOMINIO
- 13 - N° DE MATRICULA COM COMPLEMENTO
- 14 - N° DE TRANSCRIÇÃO COM COMPLEMENTO

• **Status - Filtro opcional baseado na seguinte tabela:**
- 1 - Em Aberto:
- 2 - Processando
- 3 - Respondido
- 10 - Informar Valor dos Emolumentos
- 11 - Aguardando Pagamento
- 12 - Cancelado
- 13 - Pendente de Resposta
- 23 - Cancelado pelo Solicitante

• **TipoResposta - Filtro opcional, somente aplicável quando o filtro "Status = 3 (Respondido)".**
Baseia-se na seguinte tabela:
- ""(vazio) - Todos os respondidos
- "D" - Somente os respondidos com devolução (devolvidos)
- "C" - Somente respondidos com certidão.

- DataPedidoDe - Filtro opcional no formato: aaaa-mm-dd (tipo string), com a data inicial do período de solicitações
- Filtro opcional no formato: aaaa-mm-dd (tipo string), com a data final do período de solicitações
- DataConferenciaDe - Filtro opcional no formato: aaaa-mm-dd (tipo string), com a data inicial do período de respostas

Observação

Para os filtros não desejados, basta deixar o campo sem preenchimento. Para por exemplo uma filtragem de todos os pedidos solicitados no dia 2021-04-19, o envelope ficaria equivalente a:

<soapenv:Envelope xmins:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:wsof="http://tempuri.org/WSOficio">
<soapenv:Header/>
<soapenv:Body>
<wsof:ObterXMLSolicitacoes_v4>
<wsof:oRequest>
<wsof:Hash>... Hash obtido na autenticação ...</wsof:Hash>
<wsof:Protocolo></wsof:Protocolo>
<wsof:Solicitante></wsof:Solicitante>
<wsof: TipoCertidao></wsof: TipoCertidao>
<wsof:PesquisaPor> </wsof:PesquisaPor>
< wsof:Status></wsof:Status>
<wsof: TipoResposta></wsof:TipoResposta>
<wsof:DataPedidoDe>2021-04-19</wsof:DataPedidoDe>
<wsof:DataPedidoAte>2021-04-19</wsof:DataPedidoAte>
<wsof:DataConferenciaDe></wsof:DataConferenciaDe>
<wsof:DataConferenciaAte></wsof:DataConferenciaAte>
</wsof:oRequest>
</wsof:ObterXMLSolicitacoes_v4>
</soapenv:Body>
</soapenv:Envelope>

Envelope de Saída - ObterXMLSolicitacoes_v4

Os parâmetros de saída são:

- RETORNO - Indica se houve erro ou não na execução do método (tipo boolean);
- CODIGOERRO - (se RETORNO = false) Código do erro (tipo int);
- ERRODESCRICAO - (se RETORNO = false) Descrição do erro (tipo string);
- XML - (se RETORNO = true), irá conter uma string com todo conteúdo XML equivalente ao obtido na opção do portal Ofício Eletrônico em Cartórios / Certidões a Emitir / Exportar

Listagem de erros possíveis retornados no envelope de saída:

Codigoerro	Errodescricao
0	Erro de sistema.
10	Request inválido.
11	O Hash de validação não foi informado.
18	Status Inválido.
19	Data inválida em "DataPedidoDe"
20	Data inválida em "DataPedidoAte"
21	Data inválida em "DataConferenciaDe"
22	Data inválida em "DataConferenciaAte"
23	Campo "TipoCertidao" deve estar em branco ou entre 1 e 10.
24	Campo "PesquisaPor" deve estar em branco ou entre 4 e 12.
26	Campo "TipoResposta" inválido. Valores permitidos: *''(vazio), "D" ou "C". Os valores "D" e "C" somente são permitidos se o campo "Sttatus" estiver preenchido com "3" (Respondido)

Codigoerro	Errodescricao
45	Hash inválido.
46	Hash inválido: Hash já utilizado.
47	Hash inválido: Hash expirado.
200	Não foram localizados registros para exportação

Envelope de Entrada – DevolverCertidao

Os parâmetros de entrada são:

- Hash - Hash para validação da mensagem (tipo string).
- Protocolo - Identifica a solicitação a ser devolvida (tipo string)
- Motivo - Razão da devolução (tipo string)

Envelope de Saída – DevolverCertidao

Os parâmetros de saída são:

- RETORNO - Indica se houve erro ou não na execução do método (tipo boolean);
- CODIGOERRO - (se RETORNO = false) Código do erro (tipo int);
- ERRODESCRICAO - (se RETORNO = false) Descrição do erro (tipo string);

Listagem de erros possíveis retornados no envelope de saída:

Codigoerro	Errodescricao
0	Erro de sistema.
10	Request inválido.
11	O Hash de validação não foi informado.
13	O motivo da devolução não foi informado.
45	Hash inválido.
46	Hash inválido: Hash já utilizado.
47	Hash inválido: Hash expirado.
200	Não foram localizados registros para exportação.

Envelope de Entrada – EnviarAnexoCertidao_DocID

precisa seguir os seguintes parâmetros:

- Hash – Hash para validação da mensagem (tipo string);
- Protocolo - Identifica a solicitação a ser anexado o arquivo (tipo string);
- DocumentID - Identifica o anexo no AssinadorWeb - Rest PKI Core (tipo string).

Envelope de Saída – EnviarAnexoCertidao_DocID

O Envelope de Saída– EnviarAnexoCertidao_DocID precisa seguir os seguintes parâmetros:

- RETORNO – Indica se houve erro ou não na execução do método (tipo boolean);
- CODIGOERRO – (se RETORNO = false) Código do erro (tipo int);
- ERRODESCRICAO – (se RETORNO = false) Descrição do erro (tipo string).

Listagem de erros possíveis retornados no envelope de saída:

Codigoerro	Errodescricao
0	Erro de sistema.
10	Request inválido.
11	O DocumentID não foi informado.
14	O nome do arquivo não foi informado.
15	O campo ArquivoBase64 deve ser preenchido com o conteúdo do arquivo.
26	Somente são permitidos arquivos com extensão .PDF ouo .P7S.
45	Hash inválido.
46	Hash inválido: Hash já utilizado.
47	Hash inválido: Hash expirado.
200	Não foram localizados registros para exportação.

Envelope de Entrada - EnviarAnexosListCertidao_DocID

Os parâmetros de entrada são:

- Hash – Hash para validação da mensagem (tipo string).
- Protocolo - Identifica a solicitação a ser devolvida (tipo string)
- AnexoList – Identifica a lista de anexos (tipo List)
- AnexoListCertidao_DocID_WSReq - Identifica o objeto que contém o DocId
- DocID- Identifica o anexo no AssinadorWeb (tipo string)

Envelope de Saída - EnviarAnexosListCertidao_DocID

Os parâmetros de saída são:

- RETORNO – Indica se houve erro ou não na execução do método (tipo boolean);
- CODIGOERRO – (se RETORNO = false) Código do erro (tipo int);
- ERRODESCRICAO – (se RETORNO = false) Descrição do erro (tipo string);

Listagem de erros possíveis retornados no envelope de saída:

Codigoerro	Errodescricao
0	Erro de sistema.
10	Request inválido.
11	O DocumentID não foi informado.
14	O nome do arquivo não foi informado.
15	O campo ArquivoBase64 deve ser preenchido com o conteúdo do arquivo.
25	Somente são permitidos arquivos com extensão .PDF ouo .P7S.
45	Hash inválido.
46	Hash inválido: Hash já utilizado.
47	Hash inválido: Hash expirado.
200	Não foram localizados registros para exportação.

Envelope de Entrada - FinalizarRespostaCertidao

Os parâmetros de entrada são:

- Hash – Hash para validação da mensagem (tipo string);
- Protocolo - Identifica a solicitação a ser finalizada (tipo string);
- Matrículas - Opcional (tipo string) com a lista de matrículas adicionais, exclusiva para o tipo de pesquisa por PESSOA (PesquisaPor = 6);
- InteresseSocial - Obrigatório: True ou False (tipo Boolean).

Envelope de Entrada - FinalizarRespostaCertidao

Os parâmetros de saída são:

- RETORNO – Indica se houve erro ou não na execução do método (tipo boolean);
- CODIGOERRO – (se RETORNO = false) Código do erro (tipo int);
- ERRODESCRICAO – (se RETORNO = false) Descrição do erro (tipo string).

Listagem de erros possíveis retornados no envelope de saída:

Codigoerro	Errodescricao
0	Erro de sistema.
10	Request inválido.
11	O DocumentID não foi informado.
16	O campo "Matriculas" só deve ser preenchido quando o tipo de pesquisa for por "Pessoa".
17	É necessário anexar ao menos um arquivo para finalizar a solicitação.
45	Hash inválido.
46	Hash inválido: Hash já utilizado.
47	Hash inválido: Hash expirado.
200	Não foram localizados registros para exportação.

Envelope de Entrada – InformarCustasCertidao

Os parâmetros são:

- Hash – Hash para validação da mensagem (tipo string);
- Protocolo - Identifica a solicitação a ser finalizada (tipo string);
- ValorCustar - Valor das custas informado pelo cartório (tipo valor).

Envelope de Saída – InformarCustasCertidao

Os parâmetros de saída são:

- RETORNO - Indica se houve erro ou não na execução do método (tipo boolean);
- CODIGOERRO - (se RETORNO = false) Código do erro (tipo int);
- ERRODESCRICAO - (se RETORNO = false) Descrição do erro (tipo string);

Listagem de erros possíveis retornados no envelope de saída:

Codigoerro	Errodescricao
0	Erro de sistema.
10	Request inválido.
11	O Hash de validação não foi informado.
14	Valor Inválido.
45	Hash inválido.
46	Hash inválido: Hash já utilizado.
47	Hash inválido: Hash expirado.
200	Não foram localizados registros para exportação.

CAPÍTULO 2

Assinando a Certidão Digital

Operador Nacional
do Sistema de Registro
Eletrônico de Imóveis

O que é o Rest PKI Core?

Rest PKI Core é responsável por realizar a assinatura do documento, e que inclui a adição de um QR Code, marca d'água, hash de validação e carimbo de tempo. Rest PKI Core é a nova versão do Rest PKI com compatibilidade estendida com ambientes e SGBDs.

O Assinador Web (Rest PKI Core) permite assinar outros pedidos realizados via sistema SREI e balcão do cartório, inserindo QR Code, marca d'água, hash de validação e carimbo de tempo.

Além de Windows Server (já suportado pelo Rest PKI), o Rest PKI Core é compatível com **Linux** (distribuições baseadas em Debian e RedHat) e também com **Docker**. Com relação a SGBDs, são suportados SQL Server e PostgreSQL.

Documentação completa

Acesse a documentação completa do Rest PKI Core aqui:

https://docs.lacunasoftware.com/pt-br/articles/rest-pki/core/index.html

Confira exemplo na Github da Lacuna:

https://github.com/LacunaSoftware

Operador Nacional
do Sistema de Registro
Eletrônico de Imóveis

Sede do ONR: SCS, Quadra 9, Bloco A - Torre C
Sala 1.104 - Edifício Parque Cidade Corporate
CEP: 70308-200 Brasília-DF
E-mail: contato@onr.org.br - www.onr.org.br