AT autoridade tributária e aduaneira

MANUAL DE INTEGRAÇÃO DE SOFTWARE

Comunicação de contratos de arrendamento e emissão de recibos de renda à AT

HISTÓRICO DE ALTERAÇÕES

VERSÃO	DATA	ALTERAÇÕES
1.0	31/07/2015	Criação do documento
1.1	18/11/2015	Inclusão do endereço de testes Melhoria dos códigos de resposta
1.2	26/11/2015	Inclusão do endereço de produção
1.3	16/03/2016	Inclusão dos herdeiros e da data de recebimento na emissão do recibo, a entrar em vigor no dia 18/04/2016.
1.4	23/03/2017	Atualização do Glossário

ÍNDICE

1 Introdução

O presente documento descreve os procedimentos e requisitos necessários à comunicação de início de contratos e à emissão de recibos à Autoridade Tributária e Aduaneira (AT).

Este documento destina-se a apoiar as entidades ou indivíduos, doravante designados por produtores de software, que desenvolvam e/ou comercializem software para as associações de proprietários e empresas (seus clientes utilizadores do software produzido).

Os produtores de software são responsáveis por desenvolver programas que cumpram com os requisitos legais da comunicação de contratos e emissão de recibos e para este efeito devem guiar-se pelas especificações produzidas pela AT.

As associações de proprietários e empresas são responsáveis pelo envio de dados do pedido (credenciais, contratos e recibos), uma vez que utiliza as suas credenciais no Portal das Finanças (Utilizador e Senha). Estas credenciais só podem ser conhecidas pelos emitentes devendo o software produzido estar preparado para solicitar estas credenciais, sempre que necessário à comunicação dos dados.

Complementarmente às credenciais solicitadas, o software deve também estar preparado para solicitar as credenciais do Contribuinte no Portal das Finanças (Utilizador e Senha).

Cada software é identificado perante a AT através de um Certificado SSL emitido pelo produtor de software e assinado digitalmente pela AT através de processo de adesão disponível no site e-fatura [6.1].

A AT só aceita estabelecimento de comunicação de dados se for enviado no processo de comunicação, o Certificado SSL emitido para este efeito. Este certificado apenas garante o estabelecimento da comunicação sendo responsabilidade do produtor de software transmitir corretamente os dados dos seus clientes.

1.1 Namespaces usados

Por uma questão de síntese, a declaração dos namespaces foi omitida dos exemplos e da referência nos capítulos seguintes.

São listados na seguinte tabela, para referência, todos os prefixos de namespaces utilizados.

Prefixo	Namespace	Descrição
at	http://at.pt/wsp/auth	AT Authentication Extension
S	http://schemas.xmlsoap.org/soap/envelope/	SOAP Envelope Specification
wss	http://schemas.xmlsoap.org/ws/2002/12/secext	Web Services Security Policy Language

2 Enquadramento

A solução apresentada permite a submissão de contratos de arrendamento e a emissão e obtenção de recibos através de webservice.

O cumprimento desta obrigação fica ao encargo do próprio Contribuinte.

2.1 Comunicação de contratos de arrendamento e emissão de recibos de renda por Webservice

Para efetuar a comunicação por Webservice os programas informáticos tem que estar adaptados de forma a:

1. Respeitar o modelo de dados tal como definido em formato WSDL.
2. Utilizar os protocolos de comunicação definidos para a transmissão de dados utilizando este serviço, designadamente o protocolo SOAP.
3. Implementar os mecanismos de segurança na transmissão de dados que visam garantir a confidencialidade dos dados, designadamente:
    a) Comunicação de dados através de canal HTTPS, com utilização de certificado SSL que identifica o produtor de software e que foi previamente assinado pela AT;
    b) Encriptação da senha dos utilizadores no Portal das Finanças recorrendo a chave pública (RSA) do Sistema de Autenticação;
    c) Demais mecanismos, definidos em detalhe neste documento para garantir a segurança da transmissão dos dados para a AT.

3 Adaptação do software

Nesta secção a AT apresenta as suas recomendações aos produtores de software de forma a alterarem os seus programas informáticos para incluírem a comunicação de contratos, emissão de recibos e obtenção de recibo emitido, via Webservice.

3.1 Comunicação por Webservice

Cada produtor de software é responsável por implementar o módulo que vai enviar dados dos contratos, emitir recibos e obter recibos emitidos, que deverá respeitar os seguintes passos:

1. Se ainda não tiver efetuado a adesão ao serviço, deverá realizar o processo de adesão à comunicação de contratos e à emissão e consulta de recibos:
    a) É necessário utilizar o certificado SSL e submetê-lo para ser assinado pela AT, através do processo de adesão por parte dos produtores de software.
2. O utilizador preenche a declaração no programa informático próprio;
    a) O programa informático solicita as credenciais dos intervenientes nesta submissão tal como definidas no Portal das Finanças.
3. Com base nos dados da declaração criada no passo n.º 1 e nas credenciais solicitadas no passo n.º 2 deve construir o pedido SOAP:
    a) Seguindo o WSDL;
    b) Estes pedidos SOAP (Webservice) são compostos pelas seguinte secções, descritas no capítulo 4 - Estrutura do serviço de comunicação de contratos e emissão de recibos à AT (SOAP), e que se resumem a:
        - SOAP:Header – onde se incluem os campos de autenticação dos utilizadores que vão ser responsáveis pela invocação do Webservice (as senhas que vão nesta secção têm que ser cifradas recorrendo à chave pública do sistema de autenticação do portal das finanças);
        - SOAP:Body – contém os dados do contrato ou recibo;
        - SOAP:Fault – contém a exceção de autenticação ocorrida ao efetuar o pedido.
4. Estabelecer uma ligação segura em HTTPS com o portal das finanças.
5. Processar corretamente o código de resposta devolvido pelo Webservice, que pode ser de três tipos:
    a) Mensagens de autenticação inválida;
    b) Mensagens de processamento inválido do contrato ou recibo;

c) Registo com sucesso do contrato ou recibo.

Para adaptar os programas informáticos é recomendada execução das seguintes fases de implementação:

- Desenvolvimento
- Testes
- Distribuição
- Produção

Fase de Desenvolvimento

Para poder iniciar o desenvolvimento, cada produtor de software deve obter junto da AT os elementos necessários para o efeito, designadamente:

1. Obter a chave pública do Sistema de Autenticação do Portal das Finanças para cifrar a senha do utilizador e certificado SSL assinado para comunicação com o endereço de testes:

   É necessário enviar um email à AT a solicitar o envio dos mesmos. A mensagem a enviar por email deve respeitar o seguinte *template*:

TO:	asi-cd@at.gov.pt
Subject:	Obtenção do certificado SSL para testes e chave pública do sistema de Autenticação - NIF <NIF>

Exmos. Senhores,

O Produtor de Software <NOME> (NIF <NIF>) vem por este meio solicitar o envio dos seguintes elementos para desenvolvimento e testes da comunicação de contratos e emissão de recibos via Webservice:

- Chave pública do Sistema de Autenticação do PF;
- Certificado SSL para comunicação com o endereço de testes de Webservices.

Estes elementos serão utilizados por este produtor de software para incluir nos seguintes programas:

Designação Software	**Certificado AT / DGCI**
<SOFTWARE 1>	<CERTIFICADO 1>

...	...
<SOFTWARE N>	<CERTIFICADO N>

Aguardamos a vossa resposta.

No *template* anterior, cada produtor de software deve substituir os seguintes elementos pelos seus dados:

<NIF> - Substituir pelo NIF do produtor de software;

<NOME> - Substituir pelo Nome do produtor de software.

<SOFTWARE N> - Designação do software N

<CERTIFICADO N> - Nº de certificado da AT (DGCI se ainda for o caso)

2. Obter o WSDL que define a estrutura do pedido SOAP a construir para enviar os contratos e emitir os recidos.

   Para a correta construção do pedido SOAP (invocação do Webservice) deve utilizar a informação complementar disponível no capítulo 4 - Estrutura do serviço de comunicação de contratos e emissão de recibos à AT (SOAP), onde se detalha a informação que deve constar dos campos do pedido SOAP bem como a sua forma de construção.

Fase de Testes

A AT disponibiliza um endereço de testes para verificação da comunicação de dados à AT de forma a apoiar cada produtor de software na correta disponibilização dos seus programas aos Contribuintes, seus clientes.

Para este efeito, a aplicação desenvolvida para a submissão de contratos e emissão de recibos deverá seguir o seguinte procedimento:

1. Solicitar as credenciais de utilizador e senha criada para os testes de comunicação de contratos e emissão de recibos (e.g., 555555555 + SENHA);
2. Construir o SOAP:Body de acordo com o definido no capítulo 4.1 - Pedido SOAP;
3. Cifrar a senha e compor o SOAP:Header de acordo com o definido na secção SOAP:Header do capítulo 4.1 - Pedido SOAP;
4. Estabelecer uma ligação HTTPS com o seguinte endereço disponibilizado apenas para testes;
5. Submeter o pedido SOAP construído no ponto 3;

6. Processar a resposta que o serviço lhe devolve de acordo com as várias hipóteses definidas no capítulo 4.2 - Resposta ao pedido SOAP. As respostas são dos seguintes tipos:
    a) Código de sucesso;
    b) Erros de autenticação referentes aos campos do SOAP:Header;
    c) Erros nos dados referentes aos campos preenchidos no SOAP:Body.

Para efeitos de despiste, é disponibilizada uma página de testes de conectividade e exemplos de pedido e resposta SOAP para comparação com o programa do produtor de software.

Tendo em consideração que se trata do ambiente de testes, existe a possibilidade dos dados existentes neste ambiente poderem ser apagados periodicamente.

Fase de Distribuição

Depois de confirmarem a correta adaptação do programa informático e antes de distribuir os vossos programas aos vossos clientes é necessário proceder da seguinte forma:

1. Efetuar a adesão ao envio de dados através do formulário disponível em:

    Site e-fatura » página Produtores de Software » opção Aderir ao Serviço

    É necessário aceitar os termos e condições do serviço, disponíveis para consulta no formulário;

    a) Para completar o pedido de adesão é necessário gerar um certificado SSL de acordo com as instruções disponíveis no capítulo 5 - Assinatura certificado SSL (CSR);
    b) A AT responde a este pedido por mensagem de e-mail contendo o certificado SSL assinado digitalmente pela AT.
2. Alterar o endereço de comunicação para o endereço de comunicação de dados à AT em ambiente de produção.
3. Substituir o certificado SSL utilizado em testes (ponto 4 da Fase de Testes) pelo certificado SSL de produção emitido no ponto 1 alínea c) desta fase.

Depois de concluído este procedimento o(s) vosso(s) programas informáticos estão prontos para serem distribuídos aos vossos clientes.

Fase de produção

Depois de instalado o programa informático nos computadores dos vossos clientes (Contribuintes) estão em condições para iniciar o envio de contratos e emissão de recibos via Webservice.

Por regra, o envio procede da seguinte forma:

1. O utilizador preenche os dados no programa informático;
2. São obtidas as credenciais dos intervenientes na submissão do pedido, configuradas no programa informático;
3. É construído o pedido SOAP e invocado o Webservice, em produção, com os dados do ponto 1 e ponto 2;
4. Programa processa a resposta do serviço e informa o utilizador do sucesso ou solicita ação do utilizador para o caso de erro no envio.

4 Estrutura do serviço de comunicação de contratos e emissão de recibos à AT (SOAP)

Nesta secção descreve-se informação complementar ao definido no WSDL do serviço de comunicação de contratos e emissão de recibos.

O pedido é efetuado segundo o protocolo SOAP e é constituído por duas secções:

a) SOAP:Header;

b) SOAP:Body

A primeira secção, o Header, inclui todos os campos de autenticação dos utilizadores que vão ser responsáveis pela invocação do Webservice. Estes utilizadores podem ser o NIF do contribuinte declarante com as respetivas permissões.

A segunda secção contém os dados da comunicação de contratos e emissão de recibos, os quais se detalham no tópico SOAP:Body.

O serviço prevê três operações:

a) **registarDadosContrato**, que permite a comunicação dos dados de um contrato de arrendamento à AT;

b) **emitirRecibo**, que permite a emissão de um recibo;

c) **obterRecibo**, que permite obter um recibo emitido.

Mais à frente neste capítulo serão explicados os campos envolvidos na invocação de cada uma das operações deste serviço.

4.1 Pedido SOAP

SOAP:Header

O desenho do Header tem como requisito garantir a confidencialidade dos dados de autenticação e a impossibilidade de reutilização dos mesmos em ataques Man-in-the-middle (MITM). Por este motivo, só serão aceites invocações que respeitem os seguintes procedimentos de encriptação.

O SOAP:Header é construído de acordo com o standard WS-Security, definido pela OASIS e recorrendo à definição do Username Token Profile 1.1, também definido pela mesma organização.

Na seguinte tabela, detalha-se a forma de construção de cada campo do WS-Security, e de acordo com as necessidades de segurança específicas do sistema de autenticação do portal das finanças.

Parâmetro	Descrição	Obrig.[1]	Tipo Dados[2]
H.1 - Utilizador (Username)	Identificação do utilizador que vai submeter os dados, composto da seguinte forma e de acordo com a autenticação do portal das finanças: <NIF do emitente>/<UserId> Exemplos possíveis: 1. 555555555/0000 (utilizador principal) 2. 555555555/1 (subutilizador n.º 1) 3. 555555555/0002 (subutilizador n.º 2) 4. 555555555/1234 (subutilizador n.º 1234)	S	string
H.2 - Nonce	Chave simétrica gerada por autenticação para cifrar o conteúdo dos campos H.3 - Password e H.4 - Created. Cada autenticação deverá conter esta chave gerada aleatoriamente e a qual não pode ser repetida entre headers de autenticação (wss:Security) e entre pedidos. Para garantir a confidencialidade, a chave simétrica tem de ser cifrada com a chave pública do Sistema de Autenticação de acordo com o algoritmo RSA e codificada em Base 64. A chave pública do sistema de autenticação do portal das finanças deve ser obtida por solicitação própria e através do endereço de e-mail asi-cd@at.gov.pt conforme o descrito na secção Fase de Desenvolvimento do capítulo 3.1.	S	string (base64)

[1] Obrigatório: S – Sim; N – Não.
[2] A validar na especificação WSDL (*Web Service Definition Language*) do serviço

	O campo é construído de acordo com o seguinte procedimento $$Nonce := Base64(C_{RSA,Kpub_{SA}}(K_s))$$ **K_S** := array de bytes com a chave simétrica de 128 bits, produzida de acordo com a norma AES. **$C_{RSA,KpubSA}$** := Função de cifra da chave simétrica com o algoritmo RSA utilizando a chave pública do sistema de autenticação (K_{pubSA}). **Base64** := Codificação em Base 64 do resultado.		
H.3 - Password	O campo Password deverá conter a senha do utilizador / subutilizador, a mesma que é utilizada para entrar no Portal das Finanças. Esta senha tem de ser cifrada através da chave simétrica do pedido (ver campo Nonce) e codificado em Base64. $$Password := Base64(C_{K_s}^{AES,ECB,PKCS5Padding}(SenhaPF))$$ **SenhaPF** := Senha do utilizador definido no campo H.1 - Username; $C_{K_s}^{AES,ECB,PKCS5Padding}$:= Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado. Adicionalmente este campo deverá conter o atributo Digest. Este atributo deverá conter um digest da password, seguindo a seguinte fórmula: $$Digest := Base64(C_{K_s}^{AES,ECB,PKCS5Padding}(SHA-1(K_s + Created + SenhaPF)))$$ **K_s+Created+SenhaPF** := São os bytes dos três campos concatenados; **SHA**-1 := Função de cáluculo de digest usando o algoritmo SHA-1; $C_{K_s}^{AES,ECB,PKCS5Padding}$:= Função de cifra utilizando o algoritmo AES, Modelo ECB, PKCS5Padding e a chave simétrica do pedido (K_S). **Base64** := Codificação em Base 64 do resultado.	S	string (base64)
H.4 - Data de sistema (Created)	O campo Created deverá conter a data e hora de sistema da aplicação que está a invocar o webservice. Esta data é usada para validação temporal do pedido, pelo que é		string (base64)

	crucial que o sistema da aplicação cliente tenha o seu relógio de acordo com a hora legal. Sugere-se a sincronização com o Observatório Astronómico de Lisboa: http://www.oal.ul.pt/index.php?link=acerto A zona temporal deste campo deverá estar definida para UTC e formatado de acordo com a norma ISO 8601 tal como é definido pelo W3C: http://www.w3.org/QA/Tips/iso-date http://www.w3.org/TR/NOTE-datetime e.g.: 2013-01-01T19:20:30.45Z Este campo não deve ser cifrado. $Created := Timestamp$ **Timestamp** := data hora do sistema (UTC).		

Autenticação

O sistema de autenticação do Portal das Finanças estendeu o protocolo de autenticação atual para permitir a autenticação de mais de um contribuinte. Esta nova versão, versão "2", é compatível com o uso da versão anterior. Isto é, existindo a necessidade de autenticação de apenas um utilizador, é aceite o uso de qualquer uma das versões de autenticação.

Para a utilização desta versão deverá ser utilizado o atributo */wss:Security/@Version* com o valor "2", tal como os exemplos que se seguem o demonstram.

Exemplos SOAP:Header

Como resultado da aplicação das regras de construção anteriores será produzido um header de pedido SOAP tal como o seguinte exemplo:

```
<S:Header>
   <wss:Security xmlns:wss="http://schemas.xmlsoap.org/ws/2002/12/secext"
      at:Version="2">
      <wss:UsernameToken>
         <wss:Username>111111111</wss:Username>
         <wss:Password Digest="AAAAAA==">AAAAAAAAAAAAAAAA=</wss:Password>
         <wss:Nonce>
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
            AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
         </wss:Nonce>
         <wss:Created>2015-03-09T20:45:05.424Z</wss:Created>
      </wss:UsernameToken>
   </wss:Security>
</S:Header>
```

SOAP:Body

O corpo do pedido é distinto conforma a operação que foi solicitada. As secções seguintes apresentam os diferentes SOAP:Body.

Operação *registarDadosContrato* - elemento *registarDadosContratoRequest*

De seguida são apresentados os campos para a operação de registo dos dados de um contrato de arrendamento, e que compõem o elemento *registarDadosContratoRequest*.

Parâmetro	Descrição	Obrig.[3]	Tipo Dados[4]
1.1 – NIF declarante do contrato (nifDeclarante)	NIF declarante • Preencher com o NIF do declarante dos dados de um contrato.	S	int
1.2 – Referência (*referencia*)	Referência • Utilize este campo para atribuir uma identificação pessoal ao contrato.	S	string
1.3 – Tipo (tipo)	Tipo • Indica o tipo do contrato. Valores possíveis: 1. ARREND (Arrendamento) 2. SUBARR (Subarrendamento) 3. PROMES (Promessa de arrendamento com entrega do bem locado) 4. CEDENC (Cedência de uso do prédio ou de parte dele, que não arrendamento) 5. ALUGUE (Aluguer de maquinismos e mobiliário instalados no imóvel locado)	S	string
1.4 – Finalidade (finalidade)	Finalidade • Indica a finalidade do contrato. Valores possíveis: 1. H_PERM (Habitacional permanente) 2. H_NPER (Habitacional não permanente) 3. N_HABI (Não habitacional)	S	string

[3] Obrigatório: S – Sim; N – Não.
[4] A validar na especificação WSDL (*Web Service Definition Language*) do serviço.

1.5 – Data de início (dataInicio)	Data de início • Indica a data de início do contrato	S	date
1.6 – Data de termo (dataTermo)	Data de termo • Preencher nos casos em que o contrato prevê uma data de fim.	N	date
1.7 – Renovável (renovavel)	Renovável • Assinalar nos casos em que no contrato esteja prevista a possibilidade de renovação.	N	boolean
1.8 – Lista de imóveis (imoveis)		S	
1.8.1 – Imóvel (imovel)		S	
1.8.1.1 – Código do distrito (distrito)	Distrito • Indicar o código do distrito do imóvel. Exemplos possíveis: 1. 12 2. 01	S	string
1.8.1.2 – Código do concelho (concelho)	Concelho • Indicar o código do concelho do imóvel . Exemplos possíveis: 1. 12 2. 01	S	string
1.8.1.3 – Código da freguesia (freguesia)	Freguesia • Indicar o código da freguesia do imóvel. Exemplos possíveis: 1. 12 2. 01	S	string
1.8.1.4 – Tipo (tipo)	Tipo do imóvel • Indicar se o tipo de imóvel é urbano ou rústico. Valores possíveis: 1. U (Urbano) 2. R (Rústico)	S	string

1.8.1.5 – Secção (seccao)	Secção do imóvel • Indicar a secção do imóvel.	N	string
1.8.1.6 – Artigo (artigo)	Artigo do imóvel • Indicar o artigo do imóvel. Exemplos possíveis: 1. 2321 (Artigo nº 2321) 2. P123 (Artigo provisório nº 123)	N	string
1.8.1.7 – Fração ou parte (fracao)	Fração ou parte do imóvel • Indicar a fração/parte do imóvel.	N	string
1.8.1.8 – Árvore colonia (arvCol)	Árvore colonia do imóvel • Indicar a árvore colonia do imóvel.	N	string
1.8.1.9 – Código postal (codigoPostal)	Código postal • Indicar o código postal do imóvel. Exemplos possíveis: 1. 2321 2. 0012	N	short
1.8.1.10 – Unidade funcional (unidadeFuncional)	Unidade funcional • Indicar a unidade funcional do imóvel. Exemplos possíveis: 1. 232 2. 001	N	short
1.8.1.11 – Localidade (localidade)	Localidade • Indicar a localidade do imóvel.	N	string
1.8.1.12 – Morada (morada)	Morada • Indicar a morada ou localização do imóvel.	N	string
1.8.1.13 – Número/lote (numeroLote)	Número/Lote • Indicar o número/lote do imóvel.	N	string

1.8.1.14 – Andar (andar)	Andar • Indicar o andar do imóvel.	N	string
1.8.1.15 – Parte arrendada (parteArrendada)	Parte arrendada • Indicar a parte arrendada do imóvel.	N	string
1.8.1.16 – Parte comum (parteComum)	Parte comum • Assinalar quando o contrato é relativo a uma parte comum do imóvel em propriedade horizontal.	N	boolean
1.8.1.17 – Bem omisso (bemOmisso)	Bem omisso • Assinalar quando o imóvel não está inscrito na matriz predial.	N	boolean
1.9 – Lista de locadores (locadores)		S	
1.9.1 – Locador (locador)		S	
1.9.1.1 – NIF (nif)	NIF • Indicar o NIF do locador.	S	int
1.9.1.2 – Quota Parte (quotaParte)	Quota parte • Indicar a quota parte do locador. Exemplos possíveis: 1. 1 2. 0 3. 2/3	S	string
1.9.1.3 – Regime de casamento (regimeCasamento)	Regime de casamento • Indicar o regime de casamento do locador. Valores possíveis: 1. CO_GER (Comunhão geral) 2. CO_ADQ (Comunhão de adquiridos)	N	string
1.9.1.4 – NIF cônjuge (nifConjuge)	NIF cônjuge • Indicar o NIF cônjuge do locador.	N	int

1.9.1.5 – Benefício (beneficio)	Benefício • Indicar o benefício do locador. Valores possíveis: 1. BNF001 (O Estado, as Regiões Autónomas, as autarquias locais e as associações e federações de municípios de direito público, e seus serviços, estabelecimentos e organismos, compreendidos os institutos públicos, que não tenham carácter empresarial) 2. BNF002 (Pessoas colectivas de utilidade pública administrativa e de mera utilidade pública) 3. BNF003 (As instituições particulares de solidariedade social e entidades a estas legalmente equiparadas) 4. BNF004 (As instituições de segurança social) 5. BNF005 (Zona Franca da Madeira e de Santa Maria - Entidades licenciadas nas Zonas ou concessionárias da exploração da Zona) 6. BNF006 (Sociedades de agricultura de grupo) 7. BNF007 (Universidade Católica Portuguesa) 8. BNF008 (Observatório europeu da droga e da toxicodependência) 9. BNF009 (Banco Inter Americano de Desenvolvimento) 10. BNF010 (Programa Polis) 11. BNF011 (Partidos políticos) 12. BNF012 (Código da Insolvência e da Recuperação de Empresas - Transmissões integradas em Planos de insolvência ou de pagamentos ou no âmbito da liquidação da massa insolvente) 13. BNF013 (Instituições de ensino superior público) 14. BNF014 (FIIAH / SIIAH - Artigo 8 - aquisição pelo FIIAH / SIIAH) 15. BNF015 (Cooperativas) 16. BNF016 (Arrendamento Rural)	N	string
1.10 – Lista de locatários (locatarios)		S	
1.10.1 – Locatário (locatario)		S	
1.10.1.1 – NIF (nif)	NIF • Indicar o NIF do locatário, caso português.	N	int
1.10.1.2 – Documento de Identificação (docIdentificacao)	Documento de Identificação • Indicar o documento de identificação do locatário, caso estrangeiro.	N	string

1.10.1.3 – Nome (nomeEstrangeiro)	Nome • Indicar o nome do locatário, caso estrangeiro.	N	string
1.10.1.4 – País (pais)	Pais • Indicar o código ISO de 2 letras do país do locatário.	S	string
1.10.1.5 – Retenção na fonte (retencaoFonte)	Retenção na fonte • Indicar a retenção na fonte caso se trate de um locatário português. Valores possíveis: 1. RIRS01 (À taxa de 25% - artigo 101.º, n.º 1, al. e) do CIRS) 2. RIRS02 (À taxa de 20% (Açores DLR n.º 2/99/A, de 20/01, após 1-01-2014)) 3. RIRS03 (Dispensa de retenção - artigo 101.º-B, n.º 1, do CIRS) 4. RIRS04 (Sem retenção - artigo 101.º, n.º 1, do CIRS)	N	string
1.11 – Valor da renda (valorRenda)	Valor da renda • Indicar a renda atual. Se o arrendamento tiver duração superior a um mês, indicar o valor da renda mensal. Se o arrendamento tiver duração inferior a mês, indicar o valor da renda desse período	S	decimal
1.12 – Valor das despesas (valorDespesas)	Valor das despesas • Indicar as despesas que são da responsabilidade do locador mas que por acordo contratual são suportadas pelo locatário, acrescendo ao valor da renda. Exemplo: Mensalidade do condomínio.	N	decimal
1.13 – Valor da renda máxima (valorRendaMaxima)	Valor da renda máxima • Indicar a renda mais elevada, quando prevista no contrato.	N	decimal
1.14 – Período de renda (periodoRenda)	Período de renda • Indicar se o período da renda é mensal ou inferior a um mês. Exemplos possíveis: 1. MENSAL (Mensal) 2. MENORM (Inferior a um mês)	S	string

1.15 – Lista de locadores do contrato anterior (locadoresPrevios)		N	
1.15.1 – Locador do contrato anterior (locadorPrevio)		N	
1.15.1.1 – NIF (nif)	NIF • Indicar o NIF do locatário.	S	int
1.16 – Observações (observacoes)	Observações • Indicar informações ou comentários relevantes sobre o contrato para além das indicadas previamente.	N	string
1.17 – NIF autorizado (nifautorizado)	NIF autorizado • Indicar o NIF do terceiro autorizado a cumprir as obrigações decorrentes do contrato.	N	int

Operação *emitirRecibo* – elemento *emitirReciboRequest*

Nesta secção são definidos os campos para a operação de emissão de recibos, e que compõem o elemento *emitirReciboRequest*.

Parâmetro	Descrição	Obrig.[5]	Tipo Dados[6]
1.1 – Número do contrato (*numeroContrato*)	Número do contrato • Preencher com o número do contrato.	S	long
1.2 – NIF emitente (nifEmitente)	NIF emitente • Indicar o NIF emitente do recibo.	S	int
1.3 – Lista de locadores (locadores)		S	
1.3.1 – Locador (locador)		S	
1.3.1.1 – NIF (nif)	NIF • Indicar o NIF do locador.	S	int
1.4 – Lista de locatários (locatarios)		S	

[5] Obrigatório: S – Sim; N – Não.
[6] A validar na especificação WSDL (*Web Service Definition Language*) do serviço

1.4.1 – Locatário (locatario)		S	
1.4.1.1 – NIF (nif)	NIF • Indicar o NIF do locatário, caso português.	N	int
1.4.1.2 – Documento de Identificação (docIdentificacao)	Documento de Identificação • Indicar o documento de identificação do locatário, caso estrangeiro.	N	string
1.4.1.3 – País (pais)	País • Indicar o código ISO de 2 letras do país do locatário.	S	string
1.4.1.5 – Retenção na fonte (retencaoFonte)	Retenção na fonte • Indicar a retenção na fonte caso se trate de um locatário português. Valores possíveis: 5. RIRS01 (À taxa de 25% - artigo 101.º, n.º 1, al. e) do CIRS) 6. RIRS02 (À taxa de 20% (Açores DLR n.º 2/99/A, de 20/01, após 1-01-2014)) 7. RIRS03 (Dispensa de retenção - artigo 101.º-B, n.º 1, do CIRS) 8. RIRS04 (Sem retenção - artigo 101.º, n.º 1, do CIRS)	N	string
1.5 – Tipo (tipo)	Tipo • Indica o tipo do recibo. Valores possíveis: 1. ARREND (Arrendamento) 2. SUBARR (Subarrendamento) 3. CEDENC (Cedência de uso do prédio ou de parte dele, que não arrendamento) 4. ALUGUE (Aluguer de maquinismos e mobiliário instalados no imóvel locado)	S	string
1.6 – Data de início (dataInicio)	Data de início • Indicar a data de início do período a que respeita a renda.	S	date

1.7 – Data de fim (dataFim)	Data de fim • Indicar a data de fim do período a que respeita a renda.	S	date
1.8 – Tipo de importância (tipoImportancia)	Tipo de importância • Indicar se a importância recebida é referente a uma renda, caução ou adiantamento. Valores possíveis: 1. RENDAC (Renda) 2. CAUCAO (Caução) 3. ADIANT (Adiantamento)	S	string
1.9 – Valor (valor)	Valor • Indicar o valor.	S	Decimal
1.10 – Lista de herdeiros (herdeiros)		N	
1.10.1 – Herdeiro (herdeiro)		S	
1.10.1.1 – NIF (nif)	NIF • Indicar o NIF do herdeiro.	S	int
1.10.1.2 – Quota-Parte (quotaParte)	Quota parte • Indicar a quota parte do herdeiro na renda. Exemplos possíveis: 1. 1 2. 1/6	S	string
1.10.1.3 – NIF da Herança Indivisa (nifHeranca)	NIF Herança • Indicar o NIF da Herança Indivisa registado como locador a que pertence o herdeiro.	S	int
1.11 – Data de recebimento (dataRecebimento)	Data de recebimento • Indicar a data de recebimento da importância do recibo.	S	date

Operação *obterRecibo* – elemento *obterReciboRequest*

Nesta secção são definidos os campos para a operação de obtenção de recibos, e que compõem o elemento *obterReciboRequest*.

Parâmetro	Descrição	Obrig.[7]	Tipo Dados[8]
1.1 – Número do contrato (*numeroContrato*)	Número do contrato • Preencher com o número do contrato.	S	long
1.2 – Número do recibo (numeroRecibo)	Número do recibo • Preencher com o número do recibo.	S	long

[7] Obrigatório: S – Sim; N – Não.
[8] A validar na especificação WSDL (*Web Service Definition Language*) do serviço

4.2 Resposta ao pedido SOAP

SOAP:Body

O corpo da resposta ao pedido é distinto conforma a operação que foi solicitada. As secções seguintes apresentam os diferentes SOAP:Body.

Operação *registarDadosContrato* – dados do elemento r*egistarDadosContratoResponse*

Nesta secção são apresentados os campos que compõem o elemento *registarDadosContratoResponse*. Este campo define a resposta ao pedido de comunicação dos dados de um contrato.

Parâmetro	Descrição	Obrig.[9]	Tipo Dados[10]
1.1 - Código de resposta (*codigo*)	Código do resultado da invocação desta interface. Se a resposta for zero, a operação foi bem sucedida. Se for um número diferente de zero, significa que a operação não foi bem-sucedida. Código de sucesso: 0 – Documento registado com sucesso. Códigos de resposta (autenticação): 1 - Utilizador não preenchido; 2 - Tamanho do utilizador incorreto; 3 - NIF inválido; 4 - Utilizador com formato inválido; 5 - Subutilizador com formato inválido; 6 - Senha não preenchida; 7 - Codificação Base64 inválida; 8 - Cifra da chave pública inválida; 9 - Formato do campo Created inválido; 10 - Validade da credencial expirada; 11 - Chave simétrica inválida; 12 - Chave simétrica repetida; 13 - Estrutura da senha inválida; 16 - Chave de sessão inválida. Não foi possível decifrar o campo Created; 17 - Chave de sessão inválida. Não foi possível decifrar o campo Password; 19 - Data de criação do pedido não preenchida; 20 - Chave do pedido não preenchida;	S	int

[9] Obrigatório: S – Sim; N – Não.
[10] A validar na especificação WSDL (*Web Service Definition Language*) do serviço

	33 - Pedido SOAP inválido; 99 - Erro na validação da senha (Senha errada, acesso suspenso, etc.). Códigos de resposta (serviço): -1 – O contrato apresenta um ou mais erros; -99 – Erro interno;		
1.2 – Mensagem de resposta (mensagem)	Mensagem do resultado da invocação desta interface.	S	string
1.3 – Número de contrato (numeroContrato)	Número do contrato, caso criado.	N	long
1.4 – Erros no registo (erros)		N	
1.4.1 – Erro (erro)			
1.4.1.1 – Campo com erro (*campo*)	Campo do formulário que deu origem ao erro.	N	string
1.4.1.2 – Mensagem de erro (mensagem)	Mensagem de erro.	S	string

Operação *emitirRecibo* – dados do elemento *emitirReciboResponse*

De seguida são apresentados os campos que compõem o elemento *emitirReciboResponse*. Este campo define a resposta ao pedido à operação de emissão de um recibo.

Parâmetro	Descrição	Obrig.[11]	Tipo Dados[12]
1.1 - Código de resposta (*codigo*)	Código do resultado da invocação desta interface. Se a resposta for zero, a operação foi bem sucedida. Se for um número diferente de zero, significa que a operação não foi bem-sucedida.	S	int

[11] Obrigatório: S – Sim; N – Não.
[12] A validar na especificação WSDL (*Web Service Definition Language*) do serviço

	Código de sucesso: 0 – Documento registado com sucesso. Códigos de resposta (autenticação): 1 - Utilizador não preenchido; 2 - Tamanho do utilizador incorreto; 3 - NIF inválido; 4 - Utilizador com formato inválido; 5 - Subutilizador com formato inválido; 6 - Senha não preenchida; 7 - Codificação Base64 inválida; 8 - Cifra da chave pública inválida; 9 - Formato do campo Created inválido; 10 - Validade da credencial expirada; 11 - Chave simétrica inválida; 12 - Chave simétrica repetida; 13 - Estrutura da senha inválida; 16 - Chave de sessão inválida. Não foi possível decifrar o campo Created; 17 - Chave de sessão inválida. Não foi possível decifrar o campo Password; 19 - Data de criação do pedido não preenchida; 20 - Chave do pedido não preenchida; 33 - Pedido SOAP inválido; 99 - Erro na validação da senha (Senha errada, acesso suspenso, etc.). Códigos de resposta (serviço): -1 – O recibo apresenta um ou mais erros e/ou alertas; -99 – Erro interno;		
1.2 – Mensagem de resposta (mensagem)	Mensagem do resultado da invocação desta interface.	S	string
1.3 – Número de recibo (numeroRecibo)	Número do recibo, caso criado.	N	long
1.4 – Erros na emissão do recibo (erros)		N	
1.4.1 – Erro (erro)			
1.4.1.1 – Campo com erro (*campo*)	Campo do formulário que deu origem ao erro.	N	string

1.4.1.2 – Mensagem de erro (mensagem)	Mensagem de erro.	S	string

Operação *obterRecibo* – dados do elemento *obterReciboResponse*

De seguida são apresentados os campos que compõem o elemento *obterReciboResponse*. Este campo define a resposta ao pedido à operação de obtenção de recibos.

Parâmetro	Descrição	Obrig.[13]	Tipo Dados[14]
1.1 - Código de resposta (*codigo*)	Código do resultado da invocação desta interface. Se a resposta for zero, a operação foi bem sucedida. Se for um número diferente de zero, significa que a operação não foi bem-sucedida. Código de sucesso: 0 – Documento registado com sucesso. Códigos de resposta (autenticação): 1 - Utilizador não preenchido; 2 - Tamanho do utilizador incorreto; 3 - NIF inválido; 4 - Utilizador com formato inválido; 5 - Subutilizador com formato inválido; 6 - Senha não preenchida; 7 - Codificação Base64 inválida; 8 - Cifra da chave pública inválida; 9 - Formato do campo Created inválido; 10 - Validade da credencial expirada; 11 - Chave simétrica inválida; 12 - Chave simétrica repetida; 13 - Estrutura da senha inválida; 16 - Chave de sessão inválida. Não foi possível decifrar o campo Created; 17 - Chave de sessão inválida. Não foi possível decifrar o campo Password; 19 - Data de criação do pedido não preenchida;	S	int

[13] Obrigatório: S – Sim; N – Não.
[14] A validar na especificação WSDL (*Web Service Definition Language*) do serviço

	20 - Chave do pedido não preenchida; 33 - Pedido SOAP inválido; 99 - Erro na validação da senha (Senha errada, acesso suspenso, etc.). Códigos de resposta (serviço): -1 – Não foi possível obter o recibo; -99 – Erro interno;		
1.2 – Mensagem de resposta (mensagem)	Mensagem do resultado da invocação desta interface.	S	string
1.3 – Recibo (recibo)	Recibo em formato pdf	N	base64Binary
1.4 – Erros na impressão do recibo (erros)		N	
1.4.1 – Erro (erro)			
1.4.1.1 – Mensagem de erro (mensagem)	Mensagem de erro.	S	string

5 Assinatura certificado SSL (CSR)

A invocação dos serviços web pressupõe um processo de autenticação mediante a validação da chave privada da aplicação, do conhecimento exclusivo do produtor de software (entidade aderente), sendo a respetiva chave pública comunicada e assinada pela AT.

O certificado SSL a ser utilizado na operação é assinado pela AT, a pedido da entidade aderente. Para este efeito, a empresa aderente deve efetuar um pedido de certificado SSL (CSR – Certificate Signing Request).

O CSR é um pequeno ficheiro de texto cifrado que contém o certificado SSL e toda a informação necessária para que a AT possa assinar digitalmente esse certificado. Posto isto, o certificado SSL assinado é devolvido para que possa ser utilizado no processo de autenticação na invocação do serviço web.

Os procedimentos para geração do CSR são simples mas variam de acordo com a tecnologia web utilizada pela entidade aderente, razão pela qual devem ser consultados os respetivos manuais de apoio de cada ferramenta.

A informação que o CSR deve conter é a seguinte, não podendo ultrapassar os tamanhos máximos indicados pois vai ultrapassar o tamanho total aceite para o campo CSR e onde todos os campos têm de estar preenchidos com informação relevante ou de acordo com a descrição abaixo:

Campo CSR	Descrição	Tamanho Máximo
C = Country	O código ISO de 2 letras referente ao local da sede. Por exemplo, no caso de Portugal é “PT”.	2 (chars)
ST = Province, Region, County or State	Distrito da sede.	32 (chars)
L = Town/City	Local da sede.	32 (chars)
CN = Common Name	Neste campo deve ser indicado o número de identificação fiscal da entidade aderente.	9 (chars)
O = Business Name / Organisation	Designação legal da empresa.	180 (chars)
OU = Department Name /Organizational Unit	Departamento para contacto.	180 (chars)

E = An email address	O endereço de correio eletrónico para contacto, geralmente do responsável pela emissão do CSR ou do departamento de informática. Tem que ser um endereço de email válido.	80 (chars)
Key bit length	Chave pública do certificado SSL gerado pelo produtor de software tem de ser gerado com 2048 bits.	2048 (bits)

A utilização de carateres especiais (e.g., portugueses, línguas latinas, etc.) não é aceite em nenhum dos campos acima indicados, uma vez que a utilização desses carateres vai invalidar a assinatura digital do certificado SSL.

Como resultado deste processo a AT procederá à assinatura do certificado SSL e remete em resposta ao pedido o certificado SSL assinado para integração na chave privada do produtor de software.

O certificado SSL terá a validade de 12 meses a contar da data da assinatura.

5.1 Gerar um certificado SSL

Um certificado SSL é uma chave RSA composta por duas partes: chave privada e chave pública.

Como a chave privada deve ser apenas do conhecimento do produtor de software a emissão da mesma tem sempre de ser efetuada pelo próprio, em computador próprio e nunca num site ou serviço web que encontre para o efeito.

Existem diversas ferramentas para geração de certificados SSL, proprietárias e Opensource. Para efeitos de exemplo a AT utiliza a ferramenta OpenSSL, que é a ferramenta Opensource de referência, livre de custos de utilização.

Para gerar um certificado SSL cada produtor de software deve fazê-lo no seu próprio computador utilizando o seguinte comando:

- **openssl req -new -subj** "**/C=**PT**/ST=**Distrito da Sede**/L=**Local da Sede**/O=**Empresa **/OU=**Departamento de Informatica**/CN=**555555555**/emailAddress=**informatica@empresa.pt" **-newkey rsa:2048 -nodes -out** 555555555.csr **-keyout** 555555555.key

Cada produtor de software deve substituir a informação especifica no comando anterior pelos seus dados, uma vez que os apresentados são apenas exemplificativos e não deve alterar a informação indicada a **BOLD**.

Como resultado o comando anterior será gerado o certificado SSL e serão produzidos dois ficheiros:

- 555555555.csr - Ficheiro com o pedido CSR a enviar à AT;
- 555555555.key - Ficheiro com a chave privada gerada.

5.2 Verificar conteúdo do CSR gerado

Antes de enviar o CSR para assinatura digita pela AT pode e deve ser verificado o conteúdo do ficheiro para garantir que toda a informação está como pretendido. Para tal deve ser usado o seguinte comando:

- **openssl req -text -noout -in** 555555555.csr

Onde cada produtor de software deve substituir os parâmetros que não estão a **BOLD** pelos nomes dos ficheiros corretos.

5.3 Integrar certificado SSL com a chave privada

Depois de receber o certificado SSL assinado pela chave digital da AT é necessário integrar esse certificado com a chave privada gerada no passo anterior (555555555.key). Para tal deve ser usado o seguinte comando:

- **openssl pkcs12 -export -in** 555555555.crt **-inkey** 555555555.key **-out** 555555555.pfx

Onde cada produtor de software deve substituir os parâmetros que não estão a BOLD pelos nomes dos ficheiros corretos.

Como resultado, o certificado SSL assinado pela AT é integrado com a chave privada e gravada com uma password de acesso que cada produtor de software deve definir na execução do comando.

6 Endereços Úteis

6.1 Página de produtores de software

Adesão ao serviço:

https://faturas.portaldasfinancas.gov.pt/consultarPedidosAdesao.action

Testar webservice:

https://faturas.portaldasfinancas.gov.pt/testarLigacaoWebService.action

6.2 Página de apoio ao contribuinte

http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/

6.3 Página de gestão de utilizadores

https://www.portaldasfinancas.gov.pt/pt/listAuthorizedUsers.action

6.4 Endereços para envio de dados à AT por Webservice

Ambiente de testes

https://servicos.portaldasfinancas.gov.pt:709/ws/arrendamento

Ambiente de produção

https://servicos.portaldasfinancas.gov.pt:409/ws/arrendamento

7 Glossário

Tabela de acrónimos, abreviaturas e definições de conceitos utilizados neste documento, ordenados alfabeticamente por termo.

Termo	Definição
AES	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
ECB	Referência do ECB:http://www.itl.nist.gov/fipspubs/fip81.htm Explicação do ECB:http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
OAL	Observatório Astronómico de Lisboa: http://www.oal.ul.pt/ Para acertar a hora do computador seguindo as instruções do Observatório: http://www.oal.ul.pt/index.php?link=acerto
OpenSSL	http://www.openssl.org/
PF	Portal das Finanças: www.portaldasfinancas.gov.pt
PKCS#5	Referência do PKCS #5: http://tools.ietf.org/html/rfc2898 Explicação do PKCS #5: http://en.wikipedia.org/wiki/PKCS
SA	Sistema de autenticação do Portal das Finanças: www.acesso.gov.pt. Sistema responsável por validar as credenciais de um utilizador registado no Portal das Finanças.
SOAP	http://www.w3.org/TR/soap/
Standard Date Format ISO 8601	http://www.w3.org/TR/NOTE-datetime http://www.w3.org/QA/Tips/iso-date
Username Token Profile	https://www.oasis-open.org/committees/download.php/16782/wss-v1.1-spec-os-UsernameTokenProfile.pdf
Webservice	http://www.w3.org/TR/ws-arch/
WS-Security	https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf
WSDL	http://www.w3.org/TR/wsdl