

# INCM

## O VALOR DA SEGURANÇA

### CryptoSAF-T – Manual de Integração VERSÃO 1.0

REFERÊNCIA  
CRYPTOSAFTMANUALINTPUB  
DATA **07/01/2021**  
CryptoSAF-T  
**Manual de Integração**



**Imprensa nacional-casa da moeda, s. A.**  
Avenida de António José de Almeida  
1000-042 Lisboa | Portugal

T +351 21 781 07 00  
[www.incm.pt](http://www.incm.pt)

nipc 500 792 887 | crc lisboa

## Versões do Documento

<b>Versão</b>	<b>Data</b>	<b>Descrição</b>
0.1	20-11-2020	Versão inicial
0.2	01-01-2021	Versão pré-final
1.0	07-01-2021	Versão Final

## Índice

<b>1</b>	<b>Introdução .....</b>	<b>4</b>
<b>2</b>	<b>Enquadramento .....</b>	<b>5</b>
<b>3</b>	<b>Arquitetura .....</b>	<b>6</b>
<b>4</b>	<b>Fluxo .....</b>	<b>7</b>
<b>5</b>	<b>Requisitos .....</b>	<b>8</b>
<b>6</b>	<b>Integração.....</b>	<b>9</b>
6.1	<i>Web Services.....</i>	<i>9</i>
6.2	<i>Códigos de erro.....</i>	<i>10</i>
6.3	<i>Ambientes.....</i>	<i>11</i>

## 1. Introdução

Este documento descreve as condições técnicas de acesso ao serviço CryptoSAF-T e os procedimentos necessários à integração de aplicações com este serviço.

Tem como principal função instruir e orientar os fabricantes de aplicações a desenvolver programas que realizem a descaracterização de ficheiros SAF-T (PT) relativos à contabilidade nos termos do Decreto-Lei n.º 48/2020 e que, por isso, precisam de comunicar com o serviço de geração e armazenamento de chaves. Estes fabricantes, além de garantir a conformidade do processo de descaracterização com o referido Decreto-Lei, devem assegurar a conformidade com o Regulamento do serviço publicado no portal do CryptoSAF-T e com o este documento.

O processo de descaracterização envolve uma sequência de passos e cálculos que vão para além da obtenção das chaves criptográficas. No capítulo 2 é feito um enquadramento genérico e sem detalhes técnicos de todo o processo para ajudar a contextualizar a integração com o CryptoSAF-T. Nos portais da ASSOFT e da AT pode-se encontrar mais detalhes técnicos de todo o processo.

## 2. Enquadramento

O Decreto-Lei n.º 48/2020, de 3 de agosto, veio estabelecer o procedimento a adotar na descaracterização do ficheiro SAF-T (PT) (Standard Audit File for Tax Purposes) previamente à sua submissão à Autoridade Tributária e Aduaneira (AT). Este procedimento, além da descaracterização propriamente dita, necessita que seja calculada uma soma de verificação (checksum) e que o resultado seja submetido em conjunto com o ficheiro descaracterizado à AT.

Por forma a garantir a integridade dos dados originais, é efetuado o cálculo da soma de verificação sobre o ficheiro inicial sem nenhuma descaracterização. Este valor será depois submetido à AT juntamente com o ficheiro descaracterizado. O valor assim calculado permitirá, tanto a AT como ao sujeito passivo, comprovar a integridade dos dados após a reversão da descaracterização, obtendo os dados originais.

O processo de descaracterização permite o envio de um ficheiro SAF-T (PT) completo, no qual os campos relativos a descrições e dados pessoais constantes do anexo ao Decreto-Lei n.º 48/2020, de 03 de Agosto, são cifrados usando uma chave simétrica fornecida por uma terceira parte de confiança (INCM). A reversão deste processo só é possível recorrendo à chave simétrica que se encontra armazenada pelo serviço CryptoSAF-T durante o período legal de forma segura.

O serviço CryptoSAF-T foi desenhado usando as técnicas mais recentes consideradas seguras, gerando as chaves simétricas num dispositivo criptográfico e armazenando as mesmas num formato encriptado pelo referido dispositivo criptográfico. Toda a solução é gerida de forma independente e autónoma, garantindo apenas o acesso às chaves nos casos previstos na lei, como é o caso de um eventual procedimento inspetivo.

O processo de autenticação para obtenção da chave simétrica será efetuado com o envio de um código de levantamento enviado através do serviço ViaCTT para a conta associada ao sujeito passivo evitando assim a utilização de outras formas ou serviços de registo de identidade.

### 3. Arquitetura

O procedimento de descaracterização do ficheiro SAF-T (PT) obriga à adaptação das aplicações de contabilidade para integrarem com o serviço CryptoSAF-T e implementarem as rotinas de cálculo do checksum e descaracterização..

A solução global tipicamente envolve os seguintes elementos:

- › **Aplicação de descaraterização** – Aplicação que realiza a operação de cálculo do checksum e descaracterização do ficheiro SAF-T. Pode ser parte integrante da aplicação de contabilidade ou ser uma aplicação autónoma;
- › **CryptoSAF-T** – O serviço de geração e armazenamento de chaves criptográficas simétricas que servem de base ao algoritmo de cifra a realizar;
- › **Caixa Postal Eletrónica (ViaCTT)** – Sistema usado pelo CyptoSAF-T para envio do código de segurança e notificações de acesso à sua chave;
- › **Autoridade Tributária e Aduaneira (AT)** – entidade destinatária do ficheiro SAF-T (PT) descaracterizado juntamente com a soma de verificação.

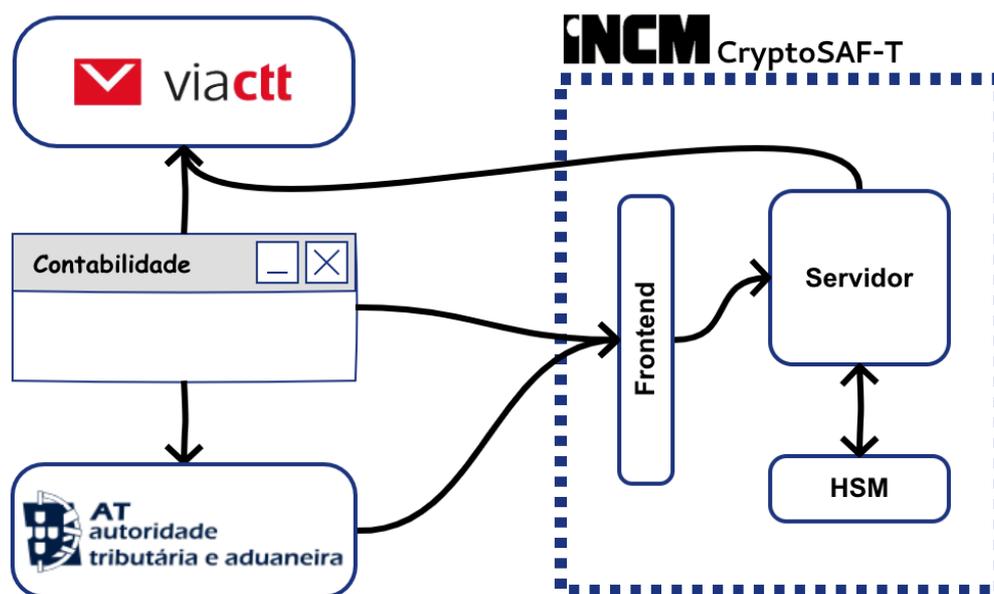


Figura 1 - Arquitetura Geral da Solução

## 4. Fluxo

O processo de descaracterização do ficheiro SAF-T é feito com recurso a uma chave criptográfica simétrica que será obtida do serviço CryptoSAF-T.

O processo pode ser descrito de forma genérica na seguinte sequência de passos:

1. **Pedido de Chave** - A aplicação inicia processo de obtenção de chave criptográfica fazendo uma chamada ao *web service* do CryptoSAF-T com indicação do número fiscal e o ano contabilístico;
2. **Envio de Código de Segurança** - CryptoSAF-T envia código de segurança para a caixa postal ViaCTT do sujeito passivo;
3. **Receção de Código de Segurança** - Sujeito passivo obtém o código de segurança a partir da sua caixa postal ViaCTT e introduz na aplicação – em alternativa, este passo pode ser efetuado automaticamente pela aplicação;
4. **Levantamento de Chave** - Aplicação invoca o *web service* de levantamento de chave criptográfica indicando o número fiscal, o ano contabilístico e o código de segurança obtendo a chave simétrica;
5. **Produção do Ficheiro SAF-T** - É produzido um ficheiro SAF-T (PT) relativo à contabilidade;
6. **Cálculo do checksum** - A aplicação efetua o cálculo do checksum sobre o ficheiro produzido no passo anterior;
7. **Descaracterização** - Aplicação descaracteriza (i.e., cifra) os dados do ficheiro SAF-T;
8. **Envio para a AT** - Aplicação submete ficheiro descaracterizado à AT, bem como o checksum previamente calculado.

Numa fase posterior, no âmbito de um eventual procedimento inspetivo, a AT poderá solicitar ao CryptoSAF-T a disponibilização da chave criptográfica indicando o número fiscal e ano. Neste caso, o sujeito passivo receberá uma notificação deste acontecimento na sua caixa postal ViaCTT.

## 5. Requisitos

Para utilizar o CryptoSAF-T com sucesso é necessário ter:

- ▶ **Rotina de descaracterização**

Para realizar estas operações, é necessária uma rotina aplicacional devidamente integrada com o CryptoSAF-T. Esta rotina pode estar embebida na aplicação de geração do ficheiro SAF-T (PT) (e.g. aplicação de contabilidade) ou ser uma aplicação autónoma que trabalha sobre ficheiros SAF-T (PT), gerados pela aplicação de contabilidade, em formato não-descaracterizado.

- ▶ **ViaCTT ativo para o sujeito passivo**

Apesar de não ser necessário nenhum pré-registo para se conseguir obter o código de segurança que permite o levantamento da chave criptográfica, é necessário que o sujeito passivo tenha a sua conta criada e ativa na Caixa Postal ViaCTT.

- ▶ **Acesso à internet**

Antes de iniciar a descaracterização do ficheiro, a aplicação necessita de obter uma chave criptográfica a partir do CryptoSAF-T que servirá de base ao processo cifra dos dados. Este serviço só está acessível através da internet.

## 6. Integração

A aplicação de descaracterização precisa de comunicar com o CryptoSAF-T para obter a chave criptográfica para o par: sujeito passivo (NIF), ano fiscal. Este processo é dividido em duas etapas:

- › **Pedido de Chave para o par NIF/ano** - despoleta o envio de uma notificação para a conta associada ao NIF indicado no ViaCTT com o respetivo código de segurança.
- › **Levantamento de Chave** - devolve a chave associada a um par Ano fiscal/NIF, validando o código de segurança.

O CryptoSAF-T disponibiliza uma interface aplicacional baseada em *web services* SOAP<sup>1</sup> para cada uma das etapas, sobre https e sem necessidade de pré-registo.

### 6.1. Web Services

Este *web service* estará exposto ao público sem qualquer autenticação e permitirá invocar as operações de pedido e levantamento de chave. Estão, no entanto, sujeitos a limites de utilização documentados no Regulamento do Serviço. Os fabricantes, sujeitos passivos e contabilistas, devem assegurar que estes limites são respeitados

#### 6.1.1. Pedido de Chave (KeyRequest)

Serviço de pedido de chave que associa uma chave a um par Ano fiscal/NIF e despoleta o envio de uma notificação ViaCTT para o contribuinte com o respetivo código de segurança. Este pedido só deve ser efetuado uma vez para cada par Ano fiscal/NIF sendo recomendável que o código de segurança seja mantido na conta do ViaCTT ou noutra local seguro.

Após o 1º pedido efetuado com sucesso (notificação enviada) para um dado par Ano fiscal/NIF o serviço bloqueia os pedidos seguintes respondendo com o erro 6 - Código de segurança já enviado. Só será possível o desbloqueio do serviço pelas equipas de Helpdesk.

#### 6.1.2. Parâmetros de entrada:

- › **KeyRequest.FiscalYear** (*Obrigatório, Valor numérico entre 2020 e 9999*) - Ano fiscal a que se refere o pedido de chave
- › **KeyRequest.VatNumber** (*Obrigatório, Valor numérico entre 100000000 e 999999999*) - Número de identificação fiscal (NIF) válido a que se refere o pedido de chave

#### 6.1.3. Parâmetros de saída:

- › **KeyRequestResponse.Response** (*Obrigatório*) - Ver secção 6.1.7-Resonse mais abaixo

<sup>1</sup> Ver: <https://www.w3.org/TR/soap/>

#### 6.1.4. Levantamento de Chave (KeyRetrieve)

Serviço de levantamento de chave que devolve a chave associada a um par Ano fiscal/NIF, validando o código de segurança.

Este serviço permite um máximo de 3 pedidos por hora para um dado par Ano fiscal/NIF após os quais será necessário esperar 1 hora para repetir o pedido. Os pedidos bloqueados serão respondidos com o erro 4-Ano fiscal/NIF bloqueado.

#### 6.1.5. Parâmetros de entrada:

- › **KeyRetrieve.FiscalYear** (*Obrigatório, Valor numérico entre 2020 e 9999*) - Ano fiscal a que se refere o levantamento de chave
- › **KeyRetrieve.VatNumber** (*Obrigatório, Valor numérico entre 100000000 e 999999999*) - Número de identificação fiscal válido a que se refere o levantamento de chave
- › **KeyRetrieve.RetrieveCode** (*Obrigatório, Valor alfanumérico com tamanho 10*) - Código de segurança enviado ao contribuinte pelo ViaCTT.

#### 6.1.6. Parâmetros de saída:

- › **KeyRetrieveResponse.Key** - (*Opcional*) Chave produzida pelo serviço correspondente ao Ano Fiscal/NIF (Base64)
- › **KeyRetrieveResponse.IV** - (*Opcional*) Vector de inicialização (IV) produzida pelo serviço correspondente ao Ano Fiscal/NIF (Base64)
- › **KeyRetrieveResponse.Response** (*Obrigatório*) - Ver secção Response mais abaixo

#### 6.1.7. Response

- › **Response.ResponseCode** (*Obrigatório, Valor numérico*) - Código de resposta que indica o sucesso ou erro da mesma (ver tabela de *Códigos de erro*)
- › **Response.Error** (*Opcional, Valor alfanumérico*) - Breve descrição do erro

## 6.2. Códigos de erro

ResponseCode	Descrição
0	Sucesso
1	Ano fiscal inválido
2	NIF inválido
3	Código de segurança inválido
4	Ano fiscal/NIF bloqueado
5	Aviso - Canal ViaCtt não ativo

<b>ResponseCode</b>	<b>Descrição</b>
6	Código de segurança já enviado

### 6.3. Ambientes

Existem dois ambientes de funcionamento do serviço disponíveis: produção e testes.

O ambiente de produção é real. É onde as operações realizadas têm resultado efetivo nos termos da Lei. É, assim, destinado ao uso exclusivo dos sujeitos passivos.

O ambiente de teste destina-se a fornecer um meio para o desenvolvimento da integração de aplicações de descaracterização. É de acesso exclusivo a fabricantes de aplicações que desenvolvam este tipo de aplicações. Durante o processo de integração é necessário o acesso a uma conta no ambiente de testes do ViaCTT, sendo recomendável contactar a linha de apoio previamente ao início do processo de integração.

Endereços dos ambientes:

<b>Ambiente</b>	<b>Tipo</b>	<b>Endereço</b>
Produção	Serviço	<a href="https://keys.cryptosaft.incm.pt/service/public">https://keys.cryptosaft.incm.pt/service/public</a>
	WSDL	<a href="https://keys.cryptosaft.incm.pt/service/public?wsdl">https://keys.cryptosaft.incm.pt/service/public?wsdl</a>
Teste	Serviço	<a href="https://keys-tst.cryptosaft.incm.pt/service/public">https://keys-tst.cryptosaft.incm.pt/service/public</a>
	WSDL	<a href="https://keys-tst.cryptosaft.incm.pt/service/public?wsdl">https://keys-tst.cryptosaft.incm.pt/service/public?wsdl</a>

\*FIM\*