Agência para a Modernização Administrativa I.P.

Sistema de Certificação de Atributos Profissionais

Documento de Integração - Consumidores de Atributos

Versão 2.0

AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA

Referências a outros Documentos

Ref.	Descrição	Autor
Ref1	Guia rápido de utilização do OAuth2 do FA	AMA

Registo de Revisões

Data	Versão	Descrição	Autor
23-06-2022	2.0	Novos serviços de pesquisa de atributos e de assinatura com múltiplos documentos	Tiago Brás

Índice

1 Introdução

O presente documento visa especificar o serviço a disponibilizar no **Sistema de Certificação de Atributos Profissionais (SCAP)** para a realização de Assinaturas na Qualidade com Atributos Profissionais de ficheiros com múltiplos formatos através da assinatura da hash da informação a assinar. A aplicação das normas PAdES e XAdES, entre outras, serão suportadas pelos clientes que efetuam a integração com o SCAP.

O processo de assinatura compreende uma fase de ativação inicial, efetuada no momento da pesquisa de atributos, e duas fases na execução da assinatura:

1. Pesquisa de Atributos – Associado à pesquisa de atributos, nesta fase, além de se obter a lista de atributos dos cidadãos, é gerada uma *secretkey* que ficará associada ao identificador do cidadão e ao identificador da aplicação cliente utilizada para a obtenção dos atributos. Esta *secretkey* será utilizado depois na geração e validação de TOTPs (Time-based One Time Password);
2. Autorização – A aplicação cliente envia para o SCAP o pedido de assinatura contendo os atributos a utilizar por cada fornecedor, as hashes dos documentos a assinar, certificado público do cidadão e 1 TOTP gerado a partir da *secretkey* previamente obtida. Após validação, o SCAP devolve à aplicação cliente uma lista de transações autorizados para assinatura. O número de transações desta lista corresponde ao número de fornecedores associados aos atributos a utilizar e a uma assinatura extra do SCAP (eSeal). Cada uma destas transações contém os atributos a utilizar por cada fornecedor, um identificador para a transação e um *Signature Activation Data* (SAD).
3. Assinatura – Para cada transação de assinatura obtida na fase anterior, a aplicação cliente invoca o SCAP com as hashes dos documentos, o identificador da transação, o SAD e o TOTP. No final, e após fazer pooling a um serviço de verificação de assinatura, o cliente obtém as hashes assinadas e deverá construir o documento assinado antes de utilizar a transação seguinte.

1.1 Pesquisa de Atributos

1.1.1 Pesquisa de fornecedores de atributos que integram com o SCAP (searchAttributeProviderInstitutionsRequest)

Este método permite obter informação sobre todos os fornecedores de atributos que integram com o SCAP. Contém informação que deverá ser utilizada na pesquisa de atributos.

1.1.2 Pesquisa de Atributos (searchCitizenAttributesRequest)

O momento da pesquisa de atributos irá despoletar o processo de criação de uma *secretkey* para o cidadão, associada a determinada aplicação cliente. No pedido de pesquisa de atributos, as aplicações cliente, deverão enviar para o SCAP o identificador de aplicação, a ser predefinido no momento da adesão. Para além disso, deve também ser enviado, no http header da mensagem, o certificado público do cidadão ou um token oauth resultante da autenticação do cartão de cidadão no Fornecedor de Autenticação da AMA (ver *Guia rápido de utilização do OAuth2 do FA*). Estes campos servem para confirmar a identidade do cidadão. Posteriormente nos pedidos de assinatura, a aplicação cliente deverá enviar sempre o identificador de aplicação e utilizar a *secretkey* para a geração do TOTP (Time-based One Time Password).

O SCAP recebe:

Headers:

- Authorization – credenciais de basic authentication
- *FAAuthorization* – token OAuth2 resultante da autenticação do cidadão no Fornecedor de Autenticação da AMA
- *X-SSL-Cert* – certificado público do Cartão de Cidadão

Body:

- *processId* – GUID gerado para cada pedido
- *citizenInfo* – informação do cidadão (ver secção "*Identificador Único do Cidadão*")
- *searchAllEnterpriseAttributes* – booleano que indica se a pesquisa é para todos os fornecedores de atributos empresariais
- *searchAllEmployeeAttributes* – booleano que indica se a pesquisa é para todos os fornecedores de atributos de funcionário

- *attributeProviderUriIds* – lista de fornecedores específicos para os quais se pretende efetuar a pesquisa de atributos. Esta lista contém os identificadores dos fornecedores de atributos
- *credentialId* – GUID identificador da aplicação/cidadão que está a efetuar o acesso ao SCAP
- *clientName* – nome da aplicação que efetua o pedido (obtido no processo de integração)

O SCAP retorna (informação relevante):

- ResponseResult – resultado da pesquisa para cada fornecedor

Notas:

Em relação ao serviço de pesquisa de atributos, importa referir que:

- o campo "*credentialId*" deve ser um GUID específico por cada instalação da aplicação;
- pode ser feita a pesquisa por "*attributeProviderUriIds*" e/ou pelos campos booleanos *searchAllEnterpriseAttributes* e *searchAllEmployeeAttributes*de;
- caso seja utilizado o mecanismo de oAuth2 para autenticação:
    - o cidadão deverá pedir obrigatoriamente os atributos http://interop.gov.pt/MDC/Cidadao/NIC e http://interop.gov.pt/MDC/Cidadao/NomeCompleto aquando da sua autenticação.

1.1.3 Obter resposta dos atributos (getCitizenAttributesResponse)

Após a pesquisa de atributos, será necessário invocar o método para obter a resposta dos atributos através do processId que foi passado na mesma. O pooling deve ser feito de 2 em 2 segundos até um máximo de 50 segundos.

O SCAP recebe:

- *processId* – GUID enviado no pedido de pesquisa de atributos

O SCAP retorna (informação relevante):

- *secretKey* – *secretkey* a utilizar na geração dos TOTPs
- *status* – estado da resposta ao pedido de atributo. Pode assumir os seguintes valores:
    - 200 - OK
    - 102 - Pedido de atributos em processamento
    - 204 - Cidadão não tem atributos ou encontram-se expirados. Verificar detalhes para cada fornecedor de atributos
    - 206 - Resposta não contém toda a informação pedida. Verificar detalhes para cada fornecedor de atributos
    - 500 - Erro interno
- *citizenAttributes* – lista de atributos por cada fornecedor
    - status – resultado da pesquisa para um fornecedor específico. Pode assumir os seguintes valores:
        - 200 - OK
        - 204 - Cidadão não tem atributos
        - 205 - Cidadão tem os atributos expirados
        - 500 - Erro interno
    - attributeProviderInfo – informação do fornecedor
        - certificate – certificado público associado ao fornecedor, e que será utilizado na construção de documentos assinados com atributos do fornecedor

- attributes – lista de atributos
  - Attribute – informação do atributo
    - id – identificador do atributo perante o SCAP
    - description – descrição do atributo
    - validity – validade do atributo
    - subAttributes – subatributos do atributo (opcional). Podem conter informação a ser adicionada nos detalhes da assinatura

1.2 Pedido de Autorização para Assinatura (signHashAuthorization)

A primeira fase no processo de execução de assinatura passa pelo pedido de autorização (ver Fluxo de utilização do SCAP). As assinaturas na qualidade do SCAP implicam sempre a assinatura prévia pelo cidadão através da aposição da assinatura eletrónica qualificada através do CC ou CMD.

O SCAP recebe:

- *processId* – GUID gerado para cada pedido
- *credentialId – GUID identificador da aplicação/cidadão que está a efetuar o acesso ao SCAP*
- *clientName – nome da aplicação que efetua o pedido (obtido no processo de integração)*
- *totp* – gerado com base na secretkey obtida na pesquisa de atributos
- *totp* – gerado com base na secretkey obtida na pesquisa de atributos
- *numSignatues* – número de hashes a assinar. Deve corresponder ao número de documentos a assinar e deverá ter o valor entre 1 e 10.
- *attributeProviderSignatures*
  - *attributesToSign* – lista de atributos a utilizar nas assinaturas, por fornecedor. A informação a constar nestes campos é obtida na pesquisa de atributos)
- *originalHashesInfo* – lista de hashes a assinar com os atributos do campo *attributesToSign*. Esta lista corresponde às hashes dos documentos já assinados com CC ou CMD

- *citizenInfo* – informação do cidadão (ver secção "*Identificador Único do Cidadão*")
- *citizenCertificates* – contém a cadeia de certificados públicos do cidadão, utilizados nas assinaturas com CC ou CMD

O SCAP retorna:

- *transactions* – lista de transações de assinatura a serem chamadas
    - *sad – Signature Activation Data* a ser utilizado na assinatura
    - *transactionId* – identificador da transação a ser utilizado na assinatura
    - *attributeProviderSignatures*
        - *attributesToSign* – lista de atributos a utilizar nas assinaturas, por fornecedor. A informação a constar nestes campos tem que ser exatamente igual à obtida na pesquisa de atributos
        - *originalHashesInfo* – lista de hashes a assinar com os atributos do campo anterior. Esta lista corresponde às hashes dos documentos já assinados com CC ou CMD

1.3 Pedido de Assinatura (signHash)

Após a realização do pedido de autorização, a aplicação cliente irá proceder ao pedido de assinatura por cada item da lista de transações (ver Fluxo de utilização do SCAP). O número de transações corresponde ao número de fornecedores associados aos atributos a utilizar e a uma assinatura extra do SCAP (eSeal).

O SCAP recebe:

- *processId* – GUID gerado para cada pedido
- *credentialId – GUID identificador da aplicação/cidadão que está a efetuar o acesso ao SCAP*
- *clientName – nome da aplicação que efetua o pedido (obtido no processo de integração)*

- *totp* – gerado com base na secretkey obtida na pesquisa de atributos
- *sad* – *Signature Activation Data* a ser utilizado na assinatura. Obtido na resposta da autorização
- *transactionId* – identificador da transação a ser utilizado na assinatura. Obtido na resposta da autorização
- *hashes* – lista de hashes a assinar na corrente transação. Na primeira transação serão as hashes dos documentos assinados apenas com CC ou CMD. A partir daí serão as hashes dos documentos assinados com as sucessivas hashes

1.4 Obter resposta ao pedido de assinatura (getSignHashResult)

Para obter a lista de hashes assinadas, o cliente deve fazer pooling ao serviço ***getSignatureResult*** de 2 em 2 segundos até um máximo de 50 segundos.

O SCAP recebe:

- *processId* – GUID enviado no pedido de assinatura
- *sad* – *Signature Activation Data* a ser utilizado na assinatura. O mesmo utilizado no pedido de assinatura
- *transactionId* – identificador da transação a ser utilizado na assinatura. O mesmo utilizado no pedido de assinatura

O SCAP retorna:

- *status* – estado da resposta ao pedido de atributo. Pode assumir os seguintes valores:
  - 200 - OK
  - 102 - Pedido de assinatura em processamento
  - 204 - Cidadão não tem atributos
  - 205 - Cidadão tem os atributos expirados
  - 401 - Transação de assinatura inválida

  - 401 - Transação de assinatura inválida - Informação não validada no fornecedor de atributos
  - 401 - TOTP Inválido - Cliente
  - 401 - TOTP Inválido - Fornecedor de Atributos
  - 500 - Erro interno
- *Signatures* – lista de hashes assinadas. A lista está ordenada de acordo com a lista de hashes que foram recebidas no pedido de autorização e de assinatura.

Depois de receber a lista de hashes assinadas, o cliente deve adicionar essas hashes aos documentos a assinar, antes de invocar a transação seguinte. O processo de assinatura considera-se finalizado quando todos os documentos tiverem a assinatura do eSeal SCAP.

2 Fluxo de utilização do SCAP

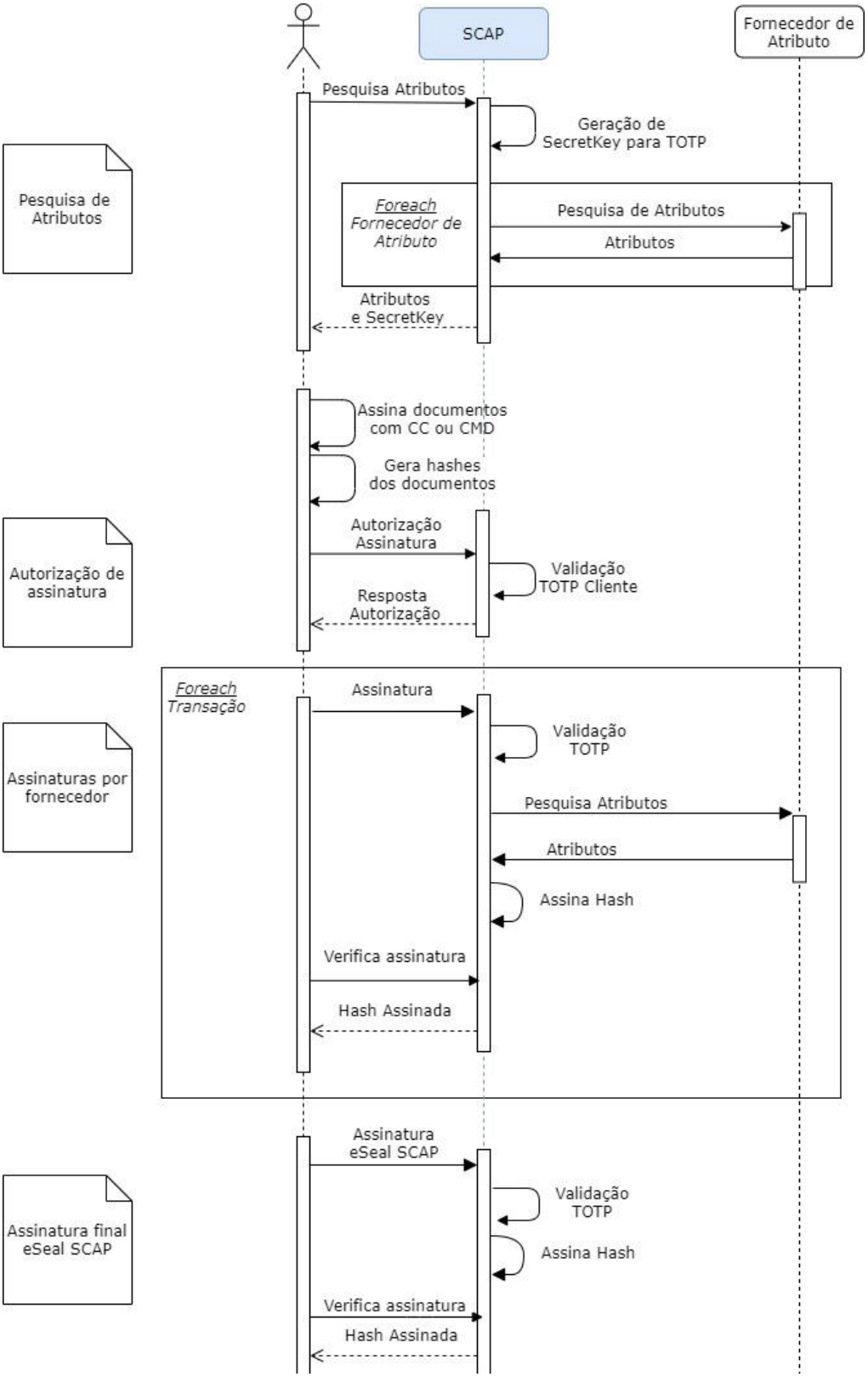

Figura 1. Fluxo de pesquisa de atributos e assinatura

3 Geração de hashes

A geração da hash deve ser feita segundo os passos 1 e 2 do ponto 9.2 da especificação "*PKCS #1: RSA Cryptography Specifications Version 2.2*" (disponível em https://tools.ietf.org/html/rfc8017#page-45).

Ou seja, após ser gerada a hash (com o algoritmo SHA-256) de um documento, deve ser adicionado o prefixo correspondente ao algoritmo SHA-256:

```
byte[] sha256SigPrefix =
        { 0x30, 0x31, 0x30, 0x0d, 0x06, 0x09, 0x60, (byte) 0x86, 0x48, 0x01, 0x65,
        0x03, 0x04, 0x02, 0x01, 0x05, 0x00, 0x04, 0x20 };
```

A hash enviada para assinatura deve ser a concatenação do *sha256SigPrefix* com a hash do documento.

4 Especificação de Serviços

Em anexo a este documento, são partilhados também os ficheiros que contêm as especificações dos serviços do SCAP. Estes documentos estão formatados segundo a especificação da OpenAPI (https://swagger.io/specification) e podem ser lidos por qualquer ferramenta de leitura de especificações OpenAPI (e.g. https://editor.swagger.io).

A comunicação entre os clientes e o SCAP deve ser feita através do protocolo HTTPS com basic authentication.

As credenciais de basic authentication, assim como o valor do campo *clientName* e do *clientId* para autenticação OAuth serão facultadas aos Softwares de Faturação, aquando da sua integração com o SCAP. Todos os métodos expostos pelo SCAP têm um parâmetro *processId*, que espera um novo *Globally Unique Identifier* (GUID) para cada invocação.

Em ambiente de pré-produção, podem ser utilizadas, as seguintes credenciais:

- basic authentication - *user: clientTest; password: Test*
- clientName – *clientTest*

4.1 Ambientes

Os métodos que constam na especificação estão publicados nos ambientes que constam da Tabela 1.

Ambiente	Domínio
Pré-Produção	https://preprod.mw.autenticacao.gov.pt
Produção	https://scap.autenticacao.gov.pt

Tabela 1. Ambientes

5 Apresentação de Assinatura

5.1 Assinatura Visível

Recomendamos que a construção da assinatura visível siga a mesma estrutura que a utilizada pela aplicação Autenticação.Gov (download em https://www.autenticacao.gov.pt/web/guest/cc-aplicacao). Apresentam-se abaixo exemplos dessa estrutura:

Figura 2. Assinatura com 1 atributo de 1 entidade

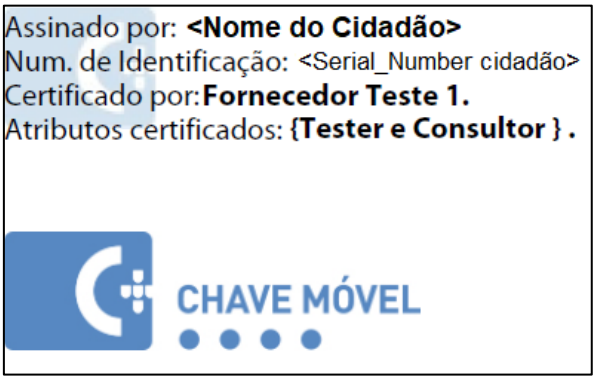

Figura 3. Assinatura com vários atributos de 1 entidade

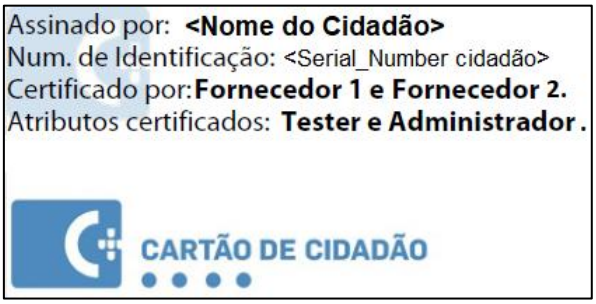

Figura 4. Assinatura com 1 atributo de várias entidades

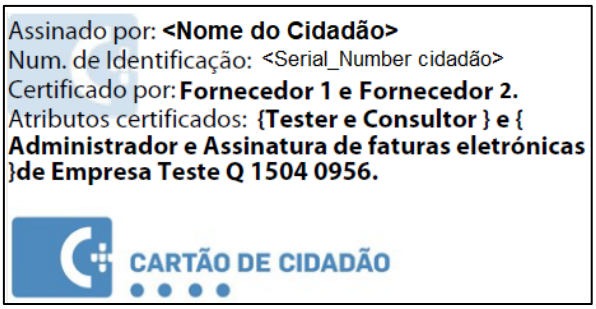

Figura 5. Assinatura com vários atributos de várias entidades

Figura 6. Logotipo do Cartão de Cidadão

Figura 7. Logotipo da Chave Móvel Digital

5.2 Detalhes da assinatura

Recomendamos que, associada a cada assinatura, seja colocado no campo *Reason/Razão/Motivo* a mesma estrutura que a utilizada pela aplicação Autenticação.Gov (download em https://www.autenticacao.gov.pt/web/guest/cc-aplicacao). Essa estrutura define-se da seguinte forma:

"**Entidade:**" + *<Nome da entidade que fornece o atributo>* + "**. Na qualidade de:**" + *<Descrição do atributo utilizado na assinatura>* + "**.Subatributos:**" *<Descrição Subatributo_1>* + "**:**" + *<Valor Subatributo_1>* + "**;**" + *<Descrição Subatributo_N>* + "**:**" + *<Valor Subatributo_N>*

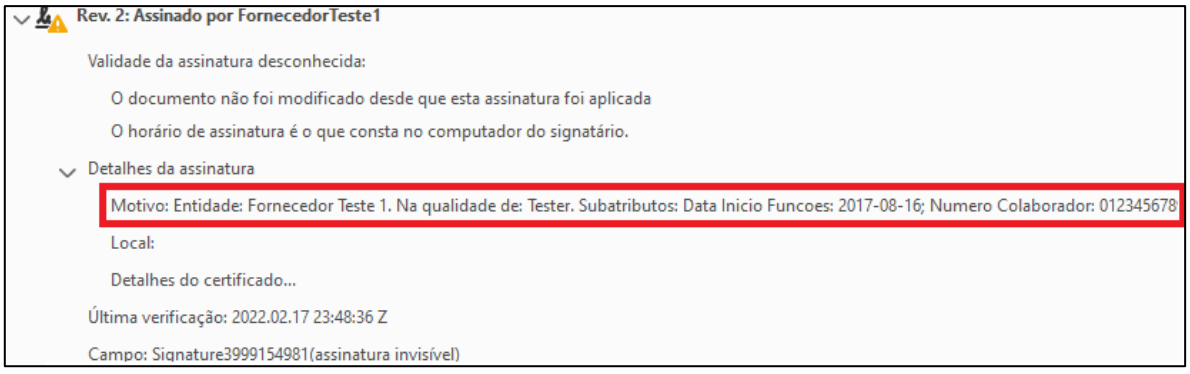

Figura 8. Exemplo de detalhe de assinatura

6 Identificador Único do Cidadão

O identificador único do cidadão segue a norma *ETSI 319 412-1* para cidadãos estrangeiros. Para cidadãos portugueses, são utilizados os carateres "BI" em vez de "IDC". Esta norma identifica o cidadão através dos seguintes elementos:

1. Tipo do documento;
2. País do documento;
3. Identificação do documento.

6.1 Tipos de documentos aceites

Os tipos de documentos aceites pelo SCAP são:

- **BI** – Cartão de Cidadão / Bilhete de Identidade
- **PAS** – Passaporte
- **TR:** – Título de Residência
- **CR:** – Cartão de Residência

6.2 Exemplos de Identificadores Únicos de cidadãos

Exemplo para cidadão português

1. Tipo do documento – **BI**
2. País do documento – **PT**
3. Identificação do documento – **12345678**

Exemplo para cidadão estrangeiro com passaporte

1. Tipo do documento – **PAS**
2. País do documento – **BR**
3. Identificação do documento – **12345678**

Exemplo para cidadão estrangeiro com título de residência (TR:) / cartão de residência (CR:)

1. Tipo do documento – **TR:**
2. País do documento – **BR**
3. Identificação do documento – **12345678**

7 TOTP Time-based One Time Password

O campo TOTP é calculado com base na *secretkey* gerada aquando da cerimónia de inicialização no ambiente de produção (ver exemplo de geração de TOTP no anexo "TOTPGeneratorExample.java" deste documento), e deve ser enviado em base64. O algoritmo de geração e validação é baseado no IETF RFC 6238 (https://tools.ietf.org/html/rfc6238), e tem os seguintes parâmetros de referência:

- ***keyBytes*** = *secretKey* devolvida na pesquisa de atributos;
- ***time*** = *timestamp* da hora atual;
- ***returnDigits*** = 6;
- ***crypto*** = HmacSHA1

8 Procedimento de Integração

De modo a poder integrar com o SCAP enquanto consumidor de atributos, a entidade responsável pelo software tem de:

1. Enviar email para eid@ama.pt a formalizar a intenção de integrar com o SCAP enquanto consumidor de atributos;
2. Celebrar protocolo com a AMA;
3. Produzir relatório assinado com evidências de cumprimento de Guidelines de Integração (ver 9);
4. Realizar processo de certificação da solução, enviando:
    - Vídeo demonstrativo da solução;
    - 5 exemplares de documentos assinados;
    - Código fonte da aplicação para certificação por parte da AMA. Como alternativa, pode também ser pedida a certificação da aplicação a uma entidade externa independente e credenciada para auditorias eIDAS.
5. Receber credenciais de Basic Authentication e ClientName para integração com o SCAP;
6. Receber ClientId para integração OAuth.

9 Guidelines de Integração

O software cliente deve cumprir as guidelines que constam no ficheiro em anexo.