

Agência para a Modernização Administrativa I.P.

**Sistema de Certificação de Atributos  
Profissionais**

**Documento de Integração - Consumidores de  
Atributos**

Versão 2.1



### 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
20-07-2022	2.1	Correção de serviços e esclarecimento sobre <i>client certificate authentication</i>	Tiago Brás

## Índice

---

<b>1</b>	<b>INTRODUÇÃO .....</b>	<b>4</b>
1.1	PESQUISA DE ATRIBUTOS .....	5
1.1.1	Pesquisa de fornecedores de atributos que integram com o SCAP (searchAttributeProviderInstitutionsRequest) .....	5
1.1.2	Pesquisa de Atributos (searchCitizenAttributesRequest) .....	6
1.1.3	Obter resposta dos atributos (getCitizenAttributesResponse) .....	8
1.2	PEDIDO DE AUTORIZAÇÃO PARA ASSINATURA (SIGNHASHAUTHORIZATION) .....	10
1.3	PEDIDO DE ASSINATURA (SIGNHASH) .....	12
1.4	OBTER RESPOSTA AO PEDIDO DE ASSINATURA (GETSIGNHASHRESULT) .....	13
<b>2</b>	<b>FLUXO DE UTILIZAÇÃO DO SCAP .....</b>	<b>14</b>
<b>3</b>	<b>GERAÇÃO DE HASHES .....</b>	<b>15</b>
<b>4</b>	<b>ESPECIFICAÇÃO DE SERVIÇOS .....</b>	<b>16</b>
4.1	AMBIENTES .....	16
<b>5</b>	<b>APRESENTAÇÃO DE ASSINATURA .....</b>	<b>17</b>
5.1	ASSINATURA VISÍVEL .....	17
5.2	DETALHES DA ASSINATURA .....	18
<b>6</b>	<b>IDENTIFICADOR ÚNICO DO CIDADÃO .....</b>	<b>19</b>
6.1	TIPOS DE DOCUMENTOS ACEITES .....	19
6.2	EXEMPLOS DE IDENTIFICADORES ÚNICOS DE CIDADÃOS .....	19
<b>7</b>	<b>TOTP TIME-BASED ONE TIME PASSWORD .....</b>	<b>20</b>
<b>8</b>	<b>PROCEDIMENTO DE INTEGRAÇÃO .....</b>	<b>21</b>
<b>9</b>	<b>GUIDELINES DE INTEGRAÇÃO .....</b>	<b>22</b>

# 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 TOTP's (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 originais dos documentos a assinar, as assinaturas dos documentos originais, o 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). Para além disso, são também enviados os certificados públicos associados aos fornecedores de atributos, necessários para a construção de documentos assinados com atributos do fornecedor;
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.

O SCAP recebe (informação relevante):

- *processId* – GUID gerado para cada pedido

O SCAP retorna (informação relevante):

- *processId* – GUID enviado para o SCAP no pedido
- *status* – resultado da operação. Pode assumir os seguintes valores:
  - 200 - OK
  - 500 - Erro interno
- *attributeProviders* – lista de fornecedores 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. 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).

A aplicação cliente deverá também garantir que o cidadão está devidamente autenticado. A autenticação do cidadão pode ser efetuada através do Fornecedor de Autenticação da AMA (com CC ou CMD) ou interagindo diretamente com o cartão de cidadão. No caso de a autenticação ser feita através do Fornecedor de Autenticação da AMA, deve ser enviado no http header da mensagem *searchCitizenAttributesRequest* um token oauth resultante da autenticação (ver *Guia rápido de utilização do OAuth2 do FA*). Se a autenticação do cidadão for realizada diretamente através da leitura do cartão de cidadão, deverá ser efetuada *client certificate authentication*, utilizando o certificado público do cartão do cidadão.

Para acesso ao certificado do cartão de cidadão, pode ser utilizado, por exemplo, PKCS#11 (java). Mais informação em [https://amagovpt.github.io/docs.autenticacao.gov/manual\\_sdk.html#api-pkcs11](https://amagovpt.github.io/docs.autenticacao.gov/manual_sdk.html#api-pkcs11).

O SCAP recebe (informação relevante):

Headers:

- Authorization – credenciais de basic authentication
- *FAAuthorization* – token OAuth2 resultante da autenticação do cidadão no Fornecedor de Autenticação da AMA (não enviar se tiver sido usado *client certificate authentication*)

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
- *attributeProviderUrlds* – 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)

**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 “*attributeProviderUrilds*” e/ou pelos campos booleanos *searchAllEnterpriseAttributes* e *searchAllEmployeeAttributes*;
- caso seja utilizado o mecanismo de OAuth2 para autenticação:
  - o cidadão deverá pedir obrigatoriamente os atributos <http://interop.gov.pt/MDC/Cidadao/NIC> aquando da sua autenticação.
- no caso de a *secretKey* estar expirada, o SCAP devolverá um código de erro 401 – *SecretKey Expirada* no campo *status* da resposta dos vários serviços. Nesse caso, o cliente deverá invocar novamente o serviço *searchCitizenAttributesRequest* de modo a obter uma nova *secretKey*.

### 1.1.3 Obter resposta dos atributos (getCitizenAttributesResponse)

Após a pesquisa de atributos, será necessário invocar o método para obter a resposta à pesquisa de atributos através do `processId` que foi passado na mesma. O pooling deve ser iniciado após **5 segundos, e feito de 2 em 2 segundos até um máximo de 50 segundos.**

O SCAP recebe (informação relevante):

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

O SCAP retorna (informação relevante):

- *secretKey* – *secretkey* a utilizar na geração dos TOTP's
- *completed* – booleano que indica se a pesquisa de atributos está ou não concluída
- *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
  - 404 - `ProcessId` não encontrado ou já utilizado
  - 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 de atributos



- *attributes* – lista de atributos
  - *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

**Notas:**

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

- O pooling deve ser iniciado após 5 segundos, e feito de 2 em 2 segundos até um máximo de 50 segundos.

## 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 eletrônica qualificada através do CC ou CMD.

O SCAP recebe (informação relevante):

- *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
- *numSignatures* – 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
- *documentHashesInfo* – lista que contém informação sobre as hashes a serem assinadas
  - *originalDocumentHash* – hash do documento original a ser assinado. Esta hash corresponde à hash gerada a partir do documento original (antes do cidadão efetuar assinatura com CC ou CMD)
  - *originalDocumentCitizenSignature* – assinatura do documento original feita com CC ou CMD
  - *documentName* – nome do documento a assinar
- *citizenInfo* – informação do cidadão (ver secção “Identificador Único do Cidadão”)
- *citizenCertificate* – contém o certificado público do cidadão, utilizado na assinatura com CC ou CMD

O SCAP retorna (informação relevante):

- *processId* – GUID enviado para o SCAP no pedido
- *status* – resultado da operação. 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 – Alguma das hashes assinadas pelo cidadão não foi corretamente validada
  - 401 - TOTP Inválido - Cliente
  - 404 - ProcessId não encontrado ou já utilizado
  - 500 - Erro interno
- *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.
      - *attributeProviderInfo* – informação do fornecedor de atributos
        - *certificates* – certificados públicos associados ao fornecedor, e que serão utilizados na construção de documentos assinados com atributos do fornecedor
    - *documentHashesInfo* – lista que contém informação sobre as hashes a serem assinadas (a mesma informação que a enviada no pedido)

### **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 mais uma assinatura extra do SCAP (eSeal).

O SCAP recebe (informação relevante):

- *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
- *hashesToSign* – 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 nas sucessivas transações

### 1.4 Obter resposta ao pedido de assinatura (*getSignHashResult*)

Para obter a lista de hashes assinadas, o cliente deve fazer pooling ao serviço *getSignatureResult*. O pooling deve ser iniciado após **5 segundos, e feito de 2 em 2 segundos até um máximo de 50 segundos**. 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.

O SCAP recebe (informação relevante):

- *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 (informação relevante):

- *status* – estado da resposta ao pedido de atributo. Pode assumir os seguintes valores:
  - 200 - OK
  - 401 - TOTP Inválido
  - 404 - ProcessId não encontrado ou já utilizado
  - 500 - Erro interno
- *signatures* – lista de hashes assinadas. A lista está ordenada de acordo com a ordem da lista de hashes que foram recebidas no pedido de autorização e de assinatura.

#### Notas:

Em relação ao serviço de obtenção de resposta ao pedido de assinatura, importa referir que:

- O pooling deve ser iniciado após **5 segundos, e feito de 2 em 2 segundos até um máximo de 50 segundos**.
- 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

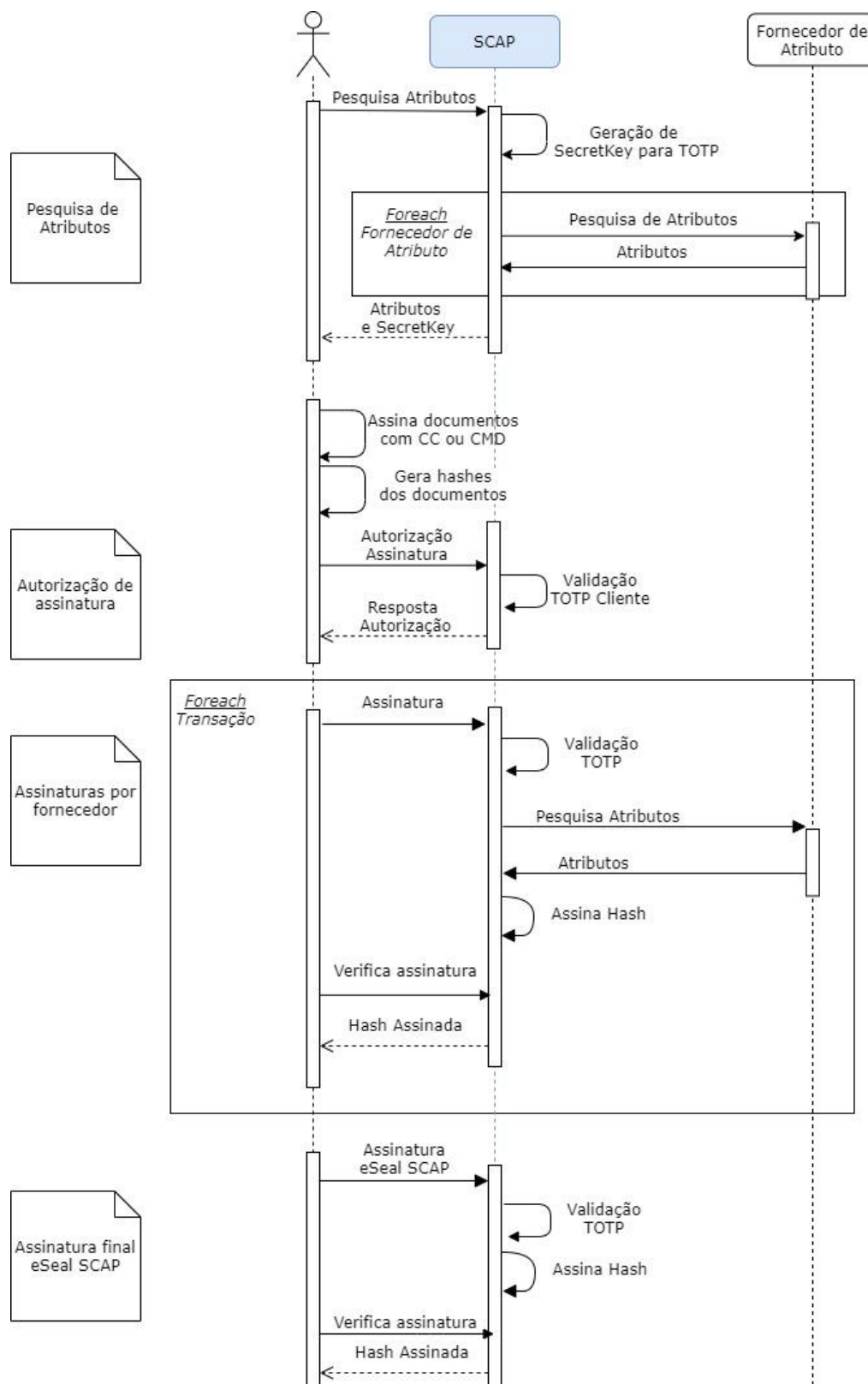


Figura 1. Fluxo de pesquisa de atributos e assinatura

### 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	<a href="https://preprod.mw.autenticacao.gov.pt">https://preprod.mw.autenticacao.gov.pt</a>
Produção	<a href="https://scap.autenticacao.gov.pt">https://scap.autenticacao.gov.pt</a>

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:

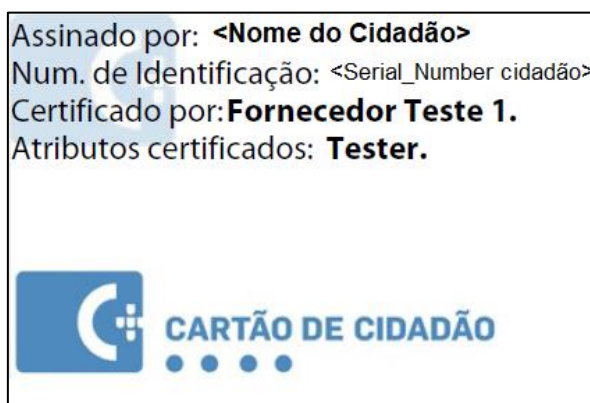


Figura 2. Assinatura com 1 atributo de 1 entidade

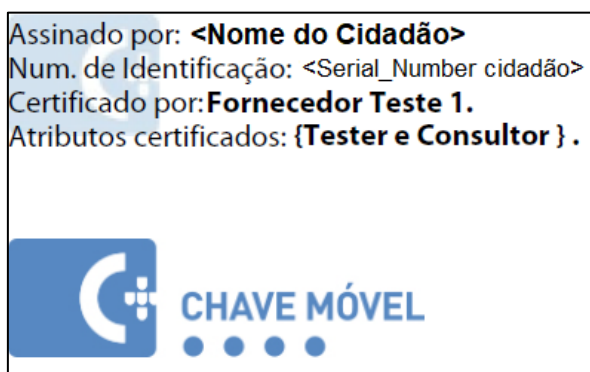


Figura 3. Assinatura com vários atributos de 1 entidade

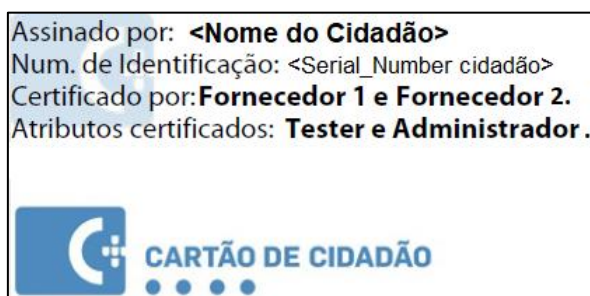


Figura 4. Assinatura com 1 atributo de várias entidades

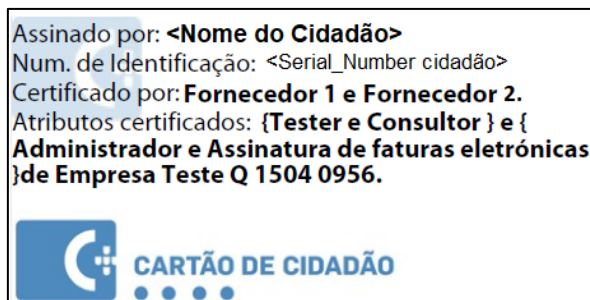


Figura 5. Assinatura com vários atributos de várias entidades



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>

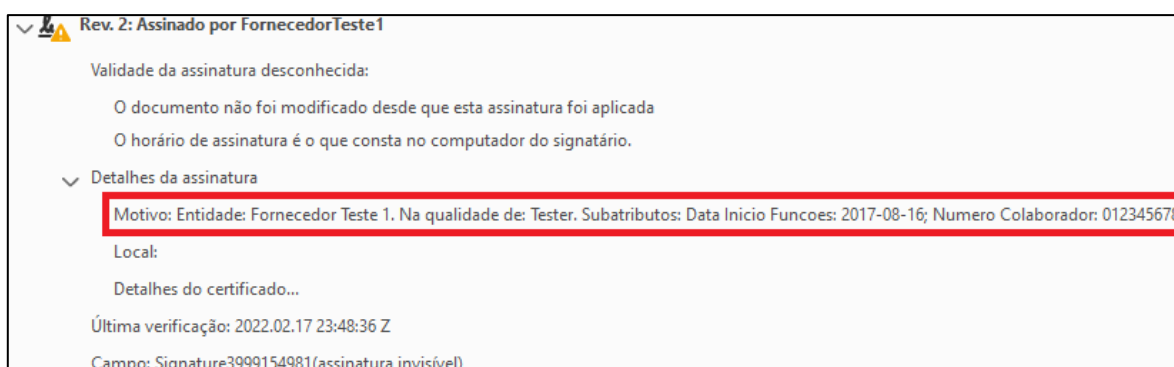


Figura 8. Exemplo de detalhe de assinatura

## 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 caracteres “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](mailto: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.