AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
PRESIDÊNCIA DO CONSELHO DE MINISTROS

Sistema de Certificação de Atributos Profissionais: Especificação do Serviço de Assinatura

22 de fevereiro de 2021

Versão 1.4

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.

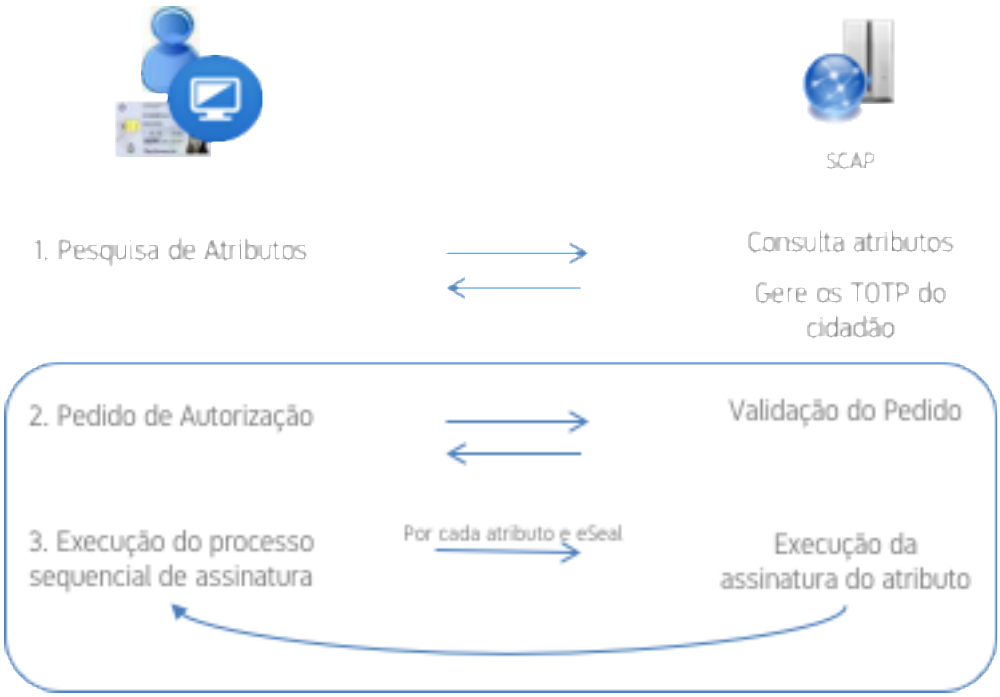


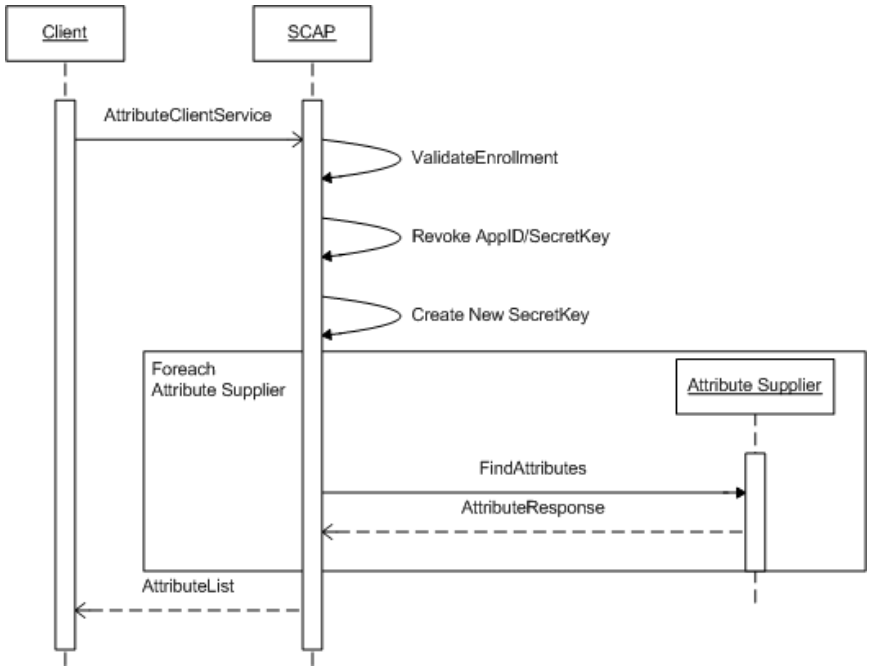
Figura 1. Diagrama ilustrativo do fluxo de assinatura na qualidade

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. Ativação – 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 NIC do cidadão e ao identificador da aplicação cliente utilizada para a obtenção dos atributos;
2. Autorização – A aplicação cliente envia para o SCAP o pedido de assinatura contendo os atributos, a hash do documento assinada com CC ou CMD e respetiva assinatura, a chave pública e 1 TOTP (Time-based One Time Password) gerado a partir da *secretkey* previamente obtida. Após validação, o SCAP, devolve à aplicação cliente o estado da operação, um identificador para a transação e uma lista de identificadores de assinatura, equivalente ao número de pedidos atributos e eSeal, que a aplicação cliente deverá utilizar efetuar para o processo de assinatura;
3. Assinatura – Para cada identificador de assinatura obtido na fase anterior, a aplicação cliente invoca o SCAP com a hash do documento conjuntamente com o TOTP e obtém o valor da assinatura.

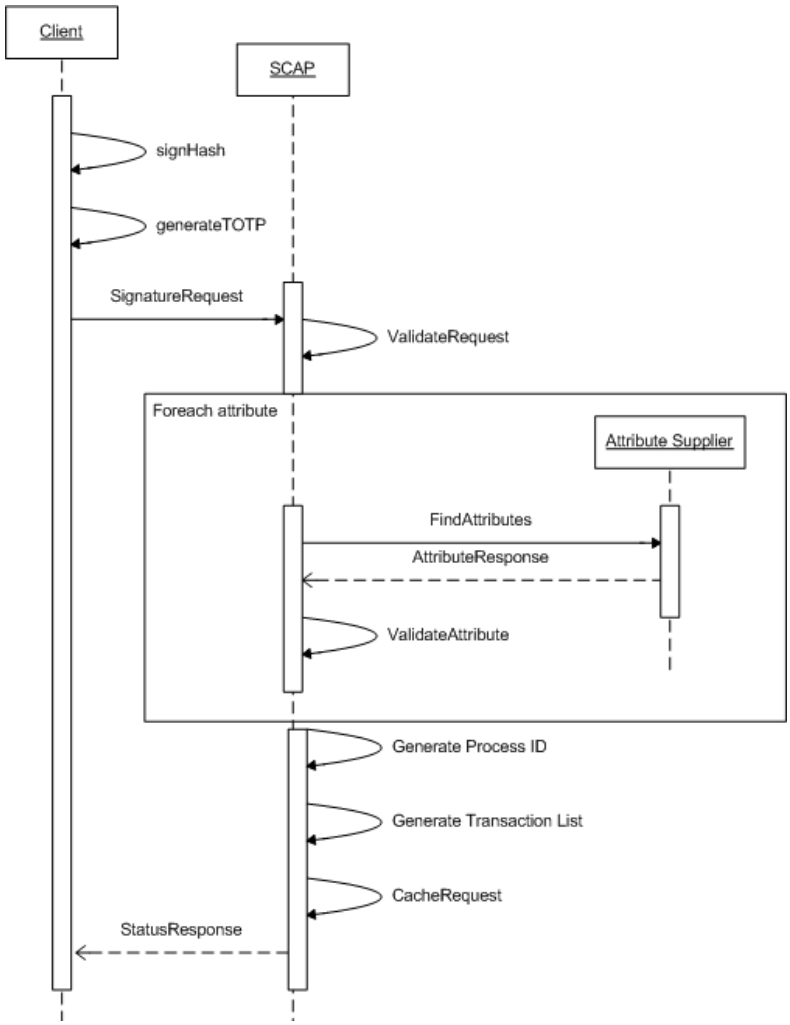
1.1 Ativação

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 digital do cidadão ou um token oauth resultante da autenticação do cidadão no Fornecedor de Autenticação da AMA. 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).



1.2 Autorização

A primeira fase no processo de execução de assinatura passa pelo pedido de autorização. As assinaturas na qualidade do SCAP implicam sempre a assinatura prévia pelo cidadão através da aposição da assinatura eletrónica qualificada através do cartão de cidadão ou CMD. Além do envio da assinatura, e de todos os seus elementos, realizada pelo cidadão no pedido de autorização, a aplicação cliente irá enviar também um TOTP gerado e a lista de atributos que serão utilizados para a assinatura na qualidade.

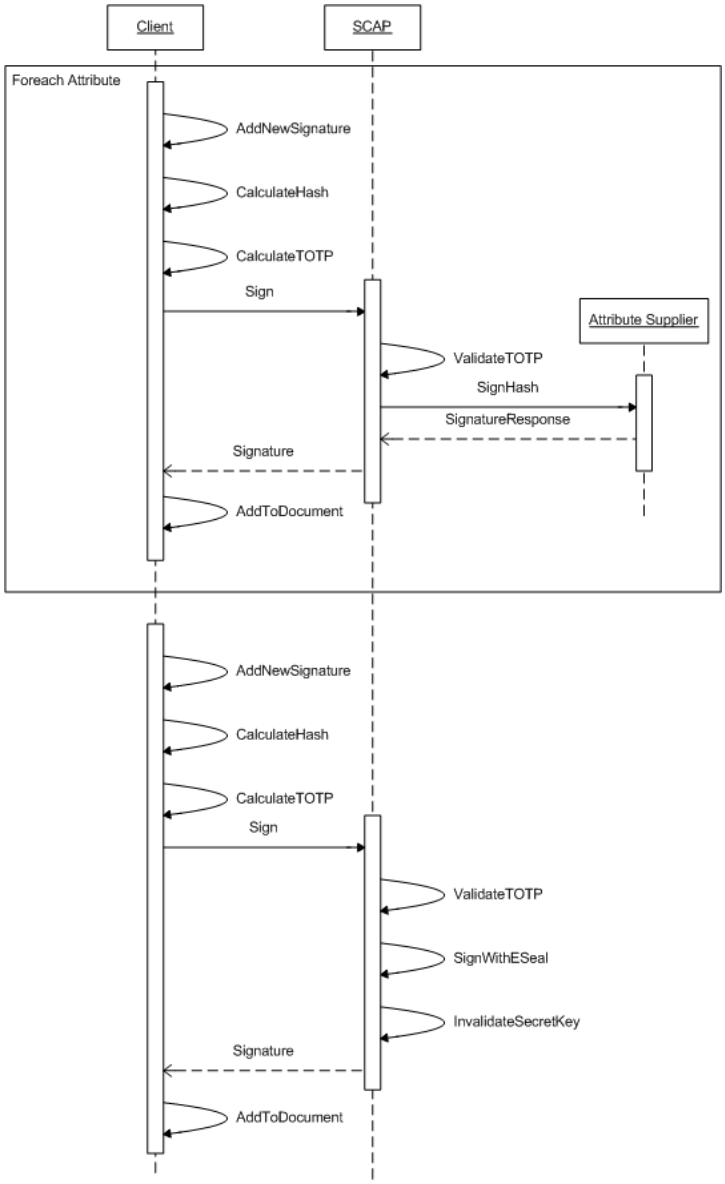


Ao receber o pedido de autorização, o SCAP efetuará a validação do TOTP e dos atributos que se encontram no pedido. Em caso de sucesso são gerados os seguintes elementos que permitirão a realização das assinaturas:

- Identificador do Processo – identificador único a ser utilizado em todos pedidos de assinatura;
- Lista de transações – Lista de identificadores equivalentes a cada pedido de assinatura a serem efetuados para completar o processo de assinatura de qualidade.

1.3 Assinatura

Após a realização do pedido de autorização, a aplicação cliente irá proceder ao pedido de assinatura por cada item da lista de transações. O número de transações irá equivaler ao número de atributos selecionados e a mais um pedido para aplicação de selo eletrónico do SCAP.



1.4 TOTP Time-based One Time Password

Algoritmo de geração e validação baseado no IETF RFC 6238 (https://tools.ietf.org/html/rfc6238). Parâmetros de referência:

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

2 SERVIÇOS

Nesta secção são descritas as especificações dos serviços para assinatura na qualidade a disponibilizar pelo SCAP. Os sistemas externos que desejem efetuar a integração com este serviço devem implementar os seguintes protocolos para a comunicação:

- Comunicação HTTPS;
- Mensagem SOAP;

Endpoints

PPR	https://preprod.mw.autenticacao.gov.pt/DSS/ACService?wsdl https://preprod.mw.autenticacao.gov.pt/SCAPSignature/AuthorizationService?wsdl https://preprod.mw.autenticacao.gov.pt/SCAPSignature/SignatureService?wsdl
PRD	https://scap.autenticacao.gov.pt/DSS/ACService?wsdl https://scap.autenticacao.gov.pt/SCAPSignature/AuthorizationService?wsdl https://scap.autenticacao.gov.pt/SCAPSignature/SignatureService?wsdl

2.1 Serviço Pesquisa de Atributos (ACService)

Este serviço tem como objetivo a realização do pedido de atributos do cidadão num ou vários fornecedores de atributos.

Este serviço obriga a autenticação do cidadão, através do envio do certificado de autenticação ou encontrando-se previamente autenticado através de oAuth2 disponibilizado pelo Fornecedor de Autenticação.

A seguinte tabela descreve os campos relevantes para a invocação deste serviço.

Parâmetros	Tipo	Obrigatório?	Descrição
ProcessId	string	Sim	Identificador único do pedido (GUID)
Citizen			
Name	string	Sim	Nome do cidadão
NIC	string	Sim	NIC do cidadão
AttributeSuppliers	AttributeSupplierType[] (2.3.8)	Não	Lista de fornecedores de atributos
AllEnterprises	Boolean	Não	Flag para pesquisar em todos os fornecedores de atributos empresariais
appName	string	Sim	Nome da aplicação que efetua o pedido.
appID	string	Sim	Identificador único da aplicação cliente que está a efetuar o acesso ao SCAP.
secretKey	string	Não	Chave atual utilizada para o cálculo de TOTP no processo de assinatura. No primeiro pedido o valor deverá vir vazio.

2.1.1 Notas sobre o serviço

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

- o campo "*appID*" deve ser um GUID específico por cada instalação da aplicação;
- em ambiente de pré-produção, o campo "*appName*" deve conter o valor "TEST". Em ambiente de produção, será criado um "*appName*" específico para cada entidade;
- podem ser efetuados 2 tipos de pesquisa de atributos:
    - pedido de atributos para fornecedores de atributos específicos – deve ser introduzida uma lista de fornecedores de atributos ("*AttributeSupplierType*") dentro do campo "*AttributeSuppliers*", e o campo "*AllEnterprises*" deve conter o valor "falso" ou não ser enviado;
    - pedido de atributos para todos os fornecedores de atributos empresariais onde o cidadão tem atributos – o campo "*AttributeSuppliers*" não deve ser enviado ou ser vazio, e o campo "*AllEnterprises*" deve conter o valor "verdadeiro".
- 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.
    - no pedido de pesquisa de atributos, o header http deverá conter o campo "Authorization: *TOKEN*", onde *TOKEN* faz referência ao token obtido na autenticação via oAuth2 (ver exemplo do header http abaixo).

```
POST /DSS/ACService HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml;charset=UTF-8
Authorization: 11dd26e4-a1f4-4626-8834-001c00b9158
SOAPAction: ""
Content-Length: 324034
Host: preprod.scap.autenticacao.gov.pt

…
```

2.2 Serviço de Assinatura

Este serviço tem como objetivo que o cidadão possa efetuar uma assinatura com os atributos obtidos no serviço de Pesquisa de Atributos (ver ponto 2.1), e disponibiliza 2 operações, conforme é possível verificar na tabela abaixo.

Serviço	SCAPSignature	Serviço que disponibiliza as operações de assinatura;
Operação	Authorization	Operação para realização de autorização de assinatura na qualidade (2.2.1)
Operação	Signature	Operação para realização de assinatura na qualidade (2.2.2)

2.2.1 Autorização

Operação	Authorization
Parâmetro de Entrada	AuthorizationRequest (2.3.1)
Parâmetro de Saída	AuthorizationResponse (2.3.2)

2.2.2 Assinatura

Operação	Signature
Parâmetro de Entrada	SignatureRequest(2.3.3)
Parâmetro de Saída	SignatureResponse(2.3.4)

2.3 Estruturas de Dados

2.3.1 AuthorizationRequest

Parâmetros	Tipo	Obrigatório?	Descrição
appId	string	Sim	Identificador da aplicação cliente
TOTP	string	Sim	Código TOTP
documentSignature	Byte[]	Sim	Assinatura do documento efetuada com CC ou CMD
documentHash	Byte[]	Sim	Hash do documento a que a o campo documentSignature diz respeito
signatureCertificate	string	Sim	Certificado público utilizado para a geração do campo documentSignature
PersonalData	PersonalDataType (2.3.5)	Sim	Informação do cidadão
AttributeList	AttributeListType[] (2.3.7)	Sim	Informação sobre o fornecedor de atributos e atributos

2.3.2 *AuthorizationResponse*

Parâmetros	Tipo	Obrigatório?	Descrição
status	Status (2.3.13)	Sim	Estado do Pedido
processId		Não	Número de processo de assinatura
transactionList	TransactionType[] (2.3.6)	Não	Lista de transações

2.3.3 *SignatureRequest*

Parâmetros	Tipo	Obrigatório?	Descrição
appId	string	Sim	Identificador da aplicação cliente
processId	string	sim	Identificador do processo de assinatura
TOTP	string	Sim	Código TOTP
Hash	Byte[]	Sim	Hash do documento a que a o campo documentSignature diz respeito
transaction	TransactionType (2.3.6)	Sim	Informação sobre o fornecedor de atributos e atributos

2.3.4 *SignatureResponse*

Parâmetros	Tipo	Obrigatório?	Descrição
status	Status (2.3.13)	Sim	Estado do Pedido
processId		Não	Número de processo de assinatura
documentSignature	Byte[]	Não	Assinatura da Hash

2.3.5 *PersonalData*

Parâmetros	Tipo	Obrigatório?	Descrição
Name	string	Sim	Nome do Cidadão
NIC	string	Sim	Número de identificação do Cidadão

2.3.6 *TransactionType*

Parâmetros	Tipo	Obrigatório?	Descrição
transationId	String	Sim	
AttributeSupplier	AttributeSupplierType (2.3.8)	Sim	Indentificador do fornecedor de atributos
MainAttribute	MainAttributeType (2.3.9)	Sim	identificador dos atributos
AttributeSupplierCertificateChain	string	sim	Certificado e respetiva

Parâmetros	Tipo	Obrigatório?	Descrição
			cadeia do fornecedor de atributos

2.3.7 AttributeListType

Parâmetros	Tipo	Obrigatório?	Descrição
AttributeSupplier	AttributeSupplierType (2.3.8)	Sim	Indentificador do fornecedor de atributos
MainAttribute	MainAttributeType (2.3.9)	Sim	identificador dos atributos

2.3.8 AttributeSupplierType

Parâmetros	Tipo	Obrigatório?	Descrição
Id	string	Sim	Indentificador do fornecedor de atributos
Name	string	Sim	Nome do fornecedor de atributos
Type	string	Não	Tipo do fornecedor de atributos

2.3.9 MainAttributeType

Parâmetros	Tipo	Obrigatório?	Descrição
AttributeID	string	Sim	Identificador do Atributo

Parâmetros	Tipo	Obrigatório?	Descrição
Description	string	Não	Descrição do Atributo
LegalActList	LegalActListType (2.3.11)	Não	Lista dos atos legais
SubAttributeList	SubAttributeListType (2.3.12)	Não	Lista de Subatributos

2.3.10 SubAttributeType

Parâmetros	Tipo	Obrigatório?	Descrição
AttributeID	string	Sim	Identificador do Subatributo
Description	string	Não	Descrição do subatributo
LegalActList	LegalActListType (2.3.11)	Não	Lista dos atos legais
Type	String	Não	Tipo do Subatributo

2.3.11 LegalActListType

Parâmetros	Tipo	Obrigatório?	Descrição
LegalAct	String	Sim	Descrição do ato legal

2.3.12 SubAttributeListType

Parâmetros	Tipo	Obrigatório?	Descrição
SubAttribute	SubAttributeType[] (2.3.10)	Sim	Lista de subatributos

2.3.13 Status

Parâmetros	Tipo	Obrigatório?	Descrição
Code	string	Sim	Código de Erro
Message	string	Sim	Mensagem do erro
Field	String	Não	Campo que provocou o erro
FieldValue	String	Não	Valor do campo que causo o erro

2.3.14 Códigos de Erro

Código	Descrição
00	OK
10	Erro de sistema
20	Parâmetro inválido
21	Invalid request - fields don't match or the transaction order was not followed
401	Atributo(s) do Cidadão expirado(s)
402	Cidadão não tem atributo(s) ativos
403	Atributo(s) do pedido não corresponde(m) ao(s) atributo(s) do cidadão

SCAP: Serviço de Assinatura

3 APRESENTAÇÃO DE ASSINATURA

3.1 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

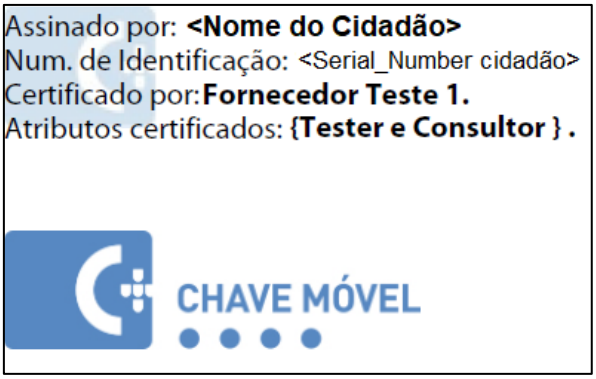


Figura 3. Assinatura com vários atributos de 1 entidade

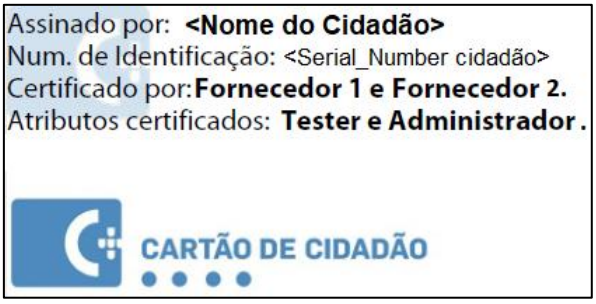


Figura 4. Assinatura com 1 atributo de várias entidades

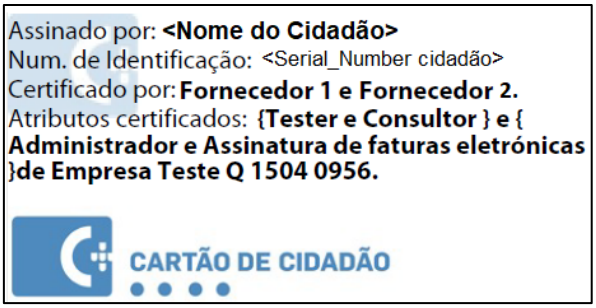


Figura 5. Assinatura com vários atributos de várias entidades

Figura 6. Logotipo do Cartão de Cidadão

Figura 7. Logotipo da Chave Móvel Digital

3.2 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>*

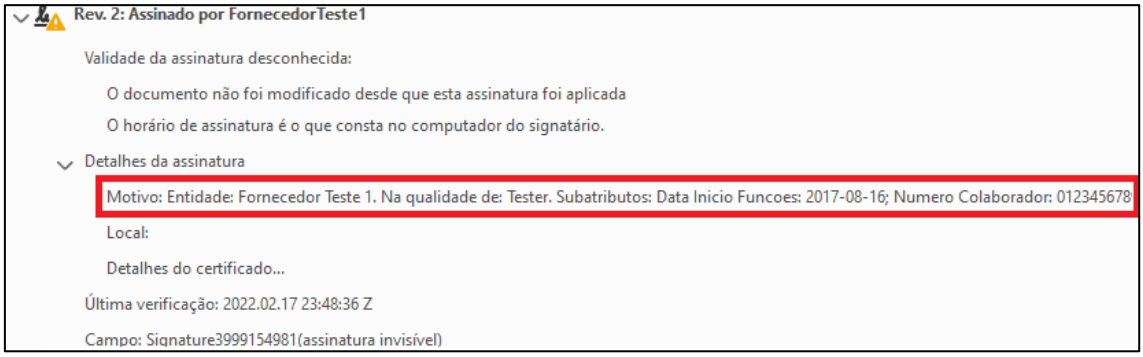


Figura 8. Exemplo de detalhe de assinatura