AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
PRESIDÊNCIA DO CONSELHO DE MINISTROS

Sistema de Certificação de Atributos Profissionais do Cartão de Cidadão

SCAP – Manual de Integração de Fornecedores de Atributos

Versão 2.7

Nome do Documento: SCAP – Manual de Integração de Fornecedores de Atributos

Evolução do Documento			
Versão	**Autor**	**Data**	**Comentários**
0.1	MULTICERT	2013-04-04	Versão inicial
0.2	MULTICERT	2013-04-08	Adição de secções
0.3	AMA	2013-04-19	Revisão da estrutura; adição de informação adicional, nomeadamente sobre a integração com a PIAP; revisão do exemplo fornecido
0.4	AMA	2013-04-22	Revisão
0.5	Luís Felix	2013-07-03	Revisão e atualização de conteúdos
0.6	AMA	2013-07-05	Revisão
0.7	MULTICERT	2013-08-01	Atualização de funcionamento de Web Services. Revisão e atualização de s*chemas* e WSDL's.
0.8	AMA	2013-11-04	Revisão (aceitação de alterações, revisão de *schemas*)
0.9	MULTICERT	2014-03-20	Revisão dos *schemas* referentes aos pedidos e respostas de atributos
1.2	MULTICERT	2014-07-28	Uniformização das versões em conformidade com repositório
1.3	MULTICERT / AMA	2015-03-12	Comunicação entre PIAP e entidades fornecedoras de atributos passou de síncrona para assíncrona
1.4	AMA	2018-10-26	Atualização global ao documento
2.0	AMA	2019-06-28	Atualização de funcionamento de Web Services para validação TOTP
2.1	AMA	2019-10-11	Atualização de comunicação com fornecedores de atributos
2.2	AMA	2020-05-04	Atualização de comunicação com fornecedores de atributos
2.3	AMA	2020-10-08	Atualização de informação sobre integração
2.4	AMA	2021-10-26	Atualização de informação sobre integração (adição de guidelines)
2.5	AMA	2022-03-17	Atualização de informação sobre integração (adição de normalização de atributos)
2.6	AMA	2022-06-28	Atualização de informação sobre integração (adição de informação sobre atributos sem data de validade definida)
2.7	AMA	2023-03-16	Atualização de informação sobre integração (alteração de informação sobre headers da mensagem de validação de TOTP) e possibilidade de cartão na aplicação móvel *id.gov.pt*

Termos e Abreviaturas usadas	
Termo/Abreviatura	**Descrição**
AMA	Agência para a Modernização Administrativa, I.P.
SCAP	Sistema de Certificação de Atributos Profissionais

Índice

1. INTRODUÇÃO

O presente documento tem como objetivo descrever o processo de integração de Fornecedores de Atributos com o Sistema de Certificação de Atributos Profissionais (SCAP).

1.1. Público Alvo

Este documento deverá ser disponibilizado pela AMA aos Fornecedores de Atributos de forma a facilitar a sua integração no SCAP.

1.2. Estrutura do documento

Este documento é constituído por:

- Enquadramento - onde se apresenta o âmbito e estrutura deste documento;
- Visão geral da solução - onde é apresentada uma visão geral das funcionalidades relevantes para a integração, sendo apresentados os diferentes atores envolvidos no processo de certificação de atributos profissionais, bem como a forma como estes interagem entre si;
-
- Integração do SCAP com Fornecedores de Atributos - onde se apresenta em maior detalhe a integração de Fornecedores de Atributos com o SCAP, nomeadamente os requisitos e passos necessários para a integração de novos fornecedores de atributos no SCAP, assim como os serviços disponíveis para a comunicação entre o SCAP e os Fornecedores de Atributos;
- Informação a enviar à AMA para configuração aplicacional – Conjunto de dados para configuração do SCAP com a informação do Fornecedor de Atributos;

2. ENQUADRAMENTO

O SCAP foi desenvolvido com o objetivo de possibilitar a associação da identidade eletrónica de um cidadão (expressa nos certificados digitais no chip do Cartão do Cidadão e Chave Móvel Digital) aos papéis que o mesmo desempenha na sociedade, por exemplo, “Engenheiro”, “Presidente” de uma Instituição, “Administrador”, “Diretor”, entre outros. Este sistema permite que, através da autenticação ou assinatura eletrónica de documentos, sejam certificados um conjunto de atributos (qualidades) que o cidadão tem e lhe estão atribuídos por entidades fornecedoras de atributos. Este sistema assegura o não-repúdio de todas as assinaturas e autenticações realizadas na qualidade de determinado(s) atributo(s).

Todos os atributos profissionais de um determinado cidadão são validados e certificados pelos Fornecedores de Atributos com competência provada para tal. Por exemplo, um cidadão que queira realizar uma assinatura de um documento digital usando um atributo de Dirigente Público, só o poderá fazer se o atributo estiver devidamente publicado no DRE e disponível no respetivo fornecedor de atributos.

3. VISÃO GERAL DA SOLUÇÃO

Nesta secção do documento é apresentado o modelo conceptual do SCAP, com o intuito de demonstrar as relações entre as diversas entidades. Na figura 1, para além do SCAP, encontram-se representadas diversas entidades que integram com o mesmo, assim como a plataforma de Interoperabilidade da Administração Pública (iAP) responsável por garantir a comunicação entre o SCAP e os Fornecedores de Atributos.

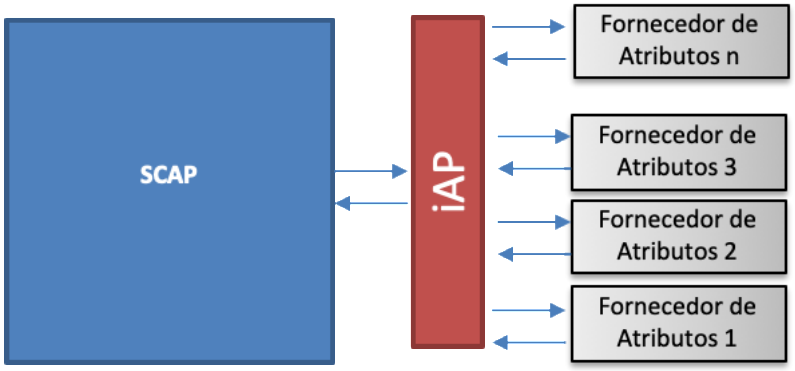

Figura 1: Modelo conceptual de integração com o SCAP

A comunicação entre o SCAP e os Fornecedores de Atributos é feita de forma assíncrona e é despoletada pelo SCAP. O SCAP envia um pedido de consulta de atributos ao Fornecedor de Atributos de um cidadão, o Fornecedor de Atributos efetua o processamento do pedido e invoca, sequencialmente, um serviço da iAP com a resposta ao pedido de atributos e outro serviço para validação da operação. Este último serviço só pode ser invocado se o cidadão tiver atributos ativos.

Cabe a cada um dos Fornecedores de Atributos a implementação de 1 *web service* para recepção dos pedidos de consulta de atributos, e de 2 clientes para invocar os serviços do SCAP que recebem, respetivamente, a resposta ao pedido de consulta de atributos e a validação dessa operação. Os Fornecedores de Atributos devem respeitar obrigatoriamente o contrato detalhado no WSDL referido no capítulo 4 deste documento,

3.1. Sistema de Certificação de Atributos Profissionais (SCAP)

É ao SCAP que compete disponibilizar aos utilizadores finais as funcionalidades de autenticação e assinatura digital com atributos profissionais. É também o SCAP que inicia a comunicação com os

fornecedores de atributos profissionais, para que estes certifiquem os respetivos atributos profissionais.

A gestão do SCAP está a cargo da AMA. Desta forma, a inclusão/integração de novos Fornecedores de Atributos no SCAP é da responsabilidade da AMA, mediante pedido direto a esta por parte dos fornecedores de atributos.

Para a configuração em ambiente de produção, os Fornecedores de Atributos, têm que efetuar a aquisição de um Certificado Qualificado Selo Eletrónico com o CSR (*Certificate Signing Request*) emitido aquando da criação da conta desse fornecedor no SCAP. Para além desse CSR, é também disponibilizado um ficheiro com a password encriptada da conta do Fornecedor de Atributos e uma *secret key* que será utilizada na validação das operações.

3.2. Plataforma de Interoperabilidade da Administração Pública (iAP)

A plataforma de Interoperabilidade da Administração Pública (iAP) atua como intermediária num universo de sistemas e tecnologias heterogéneas e é responsável pela interligação do SCAP com os fornecedores de atributos.

Esta plataforma é baseada numa arquitetura orientada aos serviços (SOA), em que as funcionalidades são disponibilizadas através de w*eb services* SOAP assíncronos. Atendendo aos requisitos de segurança, e sensibilidade das informações transacionadas, todas a comunicações entre o SCAP, iAP e os Fornecedores de Atributos é efetuada através do protocolo HTTPS.

Em resumo, a articulação com a iAP é suportada através dos seguintes protocolos:

- Comunicação – HTTP/ HTTPS via VPN;
- Especificação de mensagens – SOAP;
- Extensões para garantir o assincronismo – WS-Addressing.

3.3. Fornecedores de Atributos

No âmbito do SCAP, os Fornecedores de Atributos representam as entidades certificadoras com competência para associar determinados atributos profissionais a cidadãos. Estas entidades certificam a associação de atributos profissionais a cidadãos. Os Fornecedores de Atributos são responsáveis pela gestão da relação atributos / cidadãos e pela implementação do w*eb service* e clientes definidos pelos contratos especificados nos WSDL em anexo (ver anexos na pasta da documentação).

4. INTEGRAÇÃO DO SCAP COM FORNECEDORES DE ATRIBUTOS

Aquando da integração de um novo Fornecedor de Atributos, existe um conjunto de requisitos que devem ser tidos em consideração:

- Suportar comunicações com a iAP através de VPN;
- Implementar o *web service* de pedido de consulta de atributos (*SCAPAttributeRequestService.wsdl*), e clientes para resposta ao pedido e validação da operação (*SCAPAttributeResponseService.wsdl*), segundo a especificação do W3C. O assincronismo será garantido pela utilização da extensão WS-Addressing. O WS-Addressing é necessário para enviar um *MessageId e* um *RelatesTo* no SOAP Header das mensagens;
- Identificar e devolver os atributos profissionais de um cidadão através do identificador do cidadão que é enviado ao Fornecedor de Atributos, na mensagem de pedido de atributos, juntamente com o ficheiro com a password encriptada da conta do Fornecedor de Atributos. Este identificador segue a norma *ETSI 319 412-1* para cidadãos estrangeiros. Para cidadãos portugueses, são utilizados os carateres “BI” em vez de “IDC” (ver ponto 4.3);
- Gerar e devolver um *Time-based One-time Password* (TOTP) de forma a validar a operação;
- Para os casos em que o pedido origina um erro, o Fornecedor de Atributos deverá retornar um código de erro (ver ponto 4.2);
- Disponibilizar à AMA os contactos técnicos para resolução de problemas de ligação/integração;
- Fornecer apoio presencial em todas as cerimónias e processos de inicialização no ambiente de produção.

4.1. *Web Service* e Clientes a implementar pelos Fornecedores de Atributos

Nesta secção do documento serão apresentados e explicados o *web service* e clientes que deverão ser implementados pelos Fornecedores de Atributos, de forma a responder aos pedidos efetuados pela iAP no âmbito da integração com o SCAP. Adicionalmente serão apresentados alguns exemplos dos objetos de *request / response* desse w*eb service* e clientes com o intuito de demonstrar a estrutura dos mesmos (exemplos em anexo a este documento).

4.1.1. *Web Service* de pedido de atributos associados a um cidadão

O SCAP efetua um pedido de atributos ao Fornecedor de Atributos, através da iAP, sendo essa comunicação realizada através de mensagens assíncronas. A iAP invoca o *web service* criado pelo Fornecedores de Atributos, enviando uma mensagem com o pedido. O *web service* implementado pelo fornecedor recebe o pedido e responde com um ACK e efetua o processamento do pedido. O serviço a implementar pelo Fornecedor de Atributos tem que cumprir obrigatoriamente o WSDL SCAPAttributeRequestService.wsdl (ver anexos a este documento). Neste WSDL estão definidos todos os campos, o seu tipo e quais são obrigatórios. Pode ser consultado um exemplo no anexo "*SCAPAttributeRequest.xml*" deste documento.

4.1.1.1. Notas sobre o serviço

- O campo *SignatureInfo* só é enviado se a pesquisa de atributos estiver associada a uma assinatura; nesse caso, o fornecedor deve apenas reenviar esse campo. Se se tratar apenas de uma pesquisa de atributos, este campo não é enviado. Este campo contém informação sobre as hashes que o cidadão pretende assinar;
- O campo *InfoFile* do *AttributeProvider* não é enviado neste serviço;
- O campo *RequestType* contém a descrição do âmbito para o qual o pedido de atributos está a ser feito. Pode ser utilizado para fazer distinção na informação que é enviada para o SCAP. Por exemplo, se este campo assumir o valor *IDGOVCARD* (ver ponto 4.4), significa que o pedido de atributos é feito no âmbito de uma criação/atualização de um cartão na aplicação móvel id.gov.pt, e o fornecedor pode enviar informação diferente para ser apresentada nesse cartão.

4.1.2. *Cliente* de resposta ao pedido de atributos e de validação de operação

O Fornecedor de Atributos deverá implementar um cliente de forma a invocar a iAP com a resposta aos pedidos de atributos e outro com a validação dessa resposta. Os clientes têm que implementar o WSDL SCAPAttributeResponseService.wsdl (ver anexos a este documento) que define todos os campos, tipos e quais são obrigatórios. Este serviço contém uma operação de resposta ao pedido de consulta de atributos e uma operação de validação dessa resposta. Podem ser consultados exemplo nos anexos "*SCAPAttributeResponse.xml*" e "*ValidateOperationWithTOTPRequest.xml*" deste documento.

4.1.2.1. Notas sobre a resposta aos pedidos de consulta de atributos

- O campo *ProcessId* deve ser o mesmo que foi recebido no pedido de atributos (ver ponto 4.1.1);
- Os campos *Id* e *Name* do *AttributeProvider* devem sem os mesmos que foram recebidos no pedido de atributos (ver ponto 4.1.1);
- O campo *ResponseStatus* deve ser preenchido de acordo com os códigos descritos no ponto 4.2.;
- O campo *InfoFile* do *AttributeProvider* deve conter o ficheiro com a password encriptada da conta do Fornecedor de Atributos, disponibilizado aquando da cerimónia de inicialização no ambiente de produção;
- O campo *ExtraInfo* pode conter informação complementar sobre o cidadão que fez o pedido de atributos ou sobre o fornecedor de atributos. A utilização principal da informação que consta deste campo é para a criação/atualização de um cartão na aplicação móvel id.gov.pt (ver ponto 4.4). No entanto, poderá no futuro ser utilizado em outros âmbitos;
- No SOAP Header da mensagem devem ser enviados os campos:
  - *MessageID* – GUID gerado a cada nova mensagem;
  - *RelatesTo* – *MessageID* recebido no pedido de atributos (ver ponto 4.1.1);

4.1.2.2. Notas sobre a validação da resposta aos pedidos de consulta de atributos

- Esta validação só deve ser invocada se o cidadão tiver atributos configurados no fornecedor. Caso contrário, a validação não deve ser invocada;
- Esta validação tem que ser enviada com, pelo menos, 2 segundos de diferença para a resposta ao pedido de atributos (ver ponto 4.1.2.1);
- O campo *ProcessId* deve ser o mesmo que foi recebido no pedido de atributos (ver ponto 4.1.1);
- Os campos *Id* e *Name* do *AttributeProvider* devem sem os mesmos que foram recebidos no pedido de atributos (ver ponto 4.1.1);
- No SOAP Header da mensagem deve ser enviado o campo:
  - *MessageID* – GUID gerado a cada nova mensagem;
- O campo *TOTP* é calculado com base na *secret key* 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 gerada
- **time** = timestamp da hora atual
- **returnDigits** = 6
- **crypto** = HmacSHA1

4.2. Tipos de respostas e sua codificação

No envio da resposta com os atributos, é sempre enviado um código e uma mensagem. A tabela seguinte lista os códigos e respetivas mensagens que devem ser enviadas para que o cidadão seja corretamente informado.

Código	Mensagem
200	OK
204	Cidadão não tem atributos
205	Cidadão tem atributos expirados
500	Erro Aplicacional

Pode ser consultado um exemplo de reposta que o Fornecedor de Atributos deve enviar quando recebe um pedido de um cidadão que não tem atributos no anexo "*SCAPAttributeResponse_noAttributes.xml*" deste documento. Nesse caso, não deve ser invocada a mensagem de validação de atributos.

4.3. 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

4.3.1. 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

4.3.2. Exemplos de Identificadores Únicos de cidadãos

1. Exemplo para cidadão português
    1. Tipo do documento – **BI**
    2. País do documento – **PT**
    3. Identificação do documento – **12345678**

2. Exemplo para cidadão estrangeiro com passaporte
    1. Tipo do documento – **PAS**
    2. País do documento – **BR**
    3. Identificação do documento – **12345678**

3. 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**

4.4. Cartão de entidade na aplicação móvel id.gov

Ao integrar como fornecedor de atributos do SCAP, a entidade tem a possibilidade de ver disponibilizado na aplicação móvel *id.gov.pt* um cartão específico da sua entidade. Para isso, basta dar indicação à AMA de que o pretende fazer e ter em consideração os seguintes pontos:

- O campo *RequestType* do pedido de atributos (ver ponto 4.1.1), assume o valor *IDGOVCARD* quando o pedido de atributos é feito no âmbito de uma criação/atualização de um cartão na aplicação móvel id.gov.pt. Ao receber esta indicação, o fornecedor deve adaptar a informação da resposta, para ir ao encontro do que pretende apresentar no cartão da aplicação móvel *id.gov.pt*;
- Na resposta ao pedido de atributos (ver ponto 4.1.2.1), o fornecedor de atributos deve preencher o campo *ExtraInfo* com informação complementar sobre o cidadão que fez o pedido de atributos (CitizenExtraInfo) e/ou sobre o próprio fornecedor de atributos (EntityExtraInfo). Para além da existência de alguns campos já definidos, existe também a possibilidade de ser adicionada mais informação no campo *ExtraFields*. Os parâmetros com o nome *Visible* são booleanos que identificam se um determinado campo deve estar visível no cartão da aplicação móvel *id.gov.pt* ou se apenas aparece quando o cartão é exportado para PDF (funcionalidade de exportação de cartões da aplicação móvel *id.gov.pt*). Os parâmetros com o nome *AdditionalInfo* identificam se um determinado campo deve conter informação adicional a ser mostrada nos detalhes de um cartão da aplicação móvel *id.gov.pt*.

5. GUIDELINES PARA DEFINIÇÃO DE ATRIBUTOS E SUBATRIBUTOS

O fornecedor de atributos é responsável pela criação e gestão da relação atributos / cidadãos, e devem ser tidos em conta os seguintes pontos:

- O campo *id* de um atributo deve ter o formato *"http://interop.gov.pt/SCAP/**<NomeFornecedor>**/**<IdentificadorUnicoAtributo***"* e o campo *id* de um subatributo deve ter o formato "*http://interop.gov.pt/SCAP/**<NomeFornecedor>**/**<IdentificadorUnicoAtributo>**/**<IdentificadorUnicoSubAtributo>***"*, onde:
    - <*NomeFornecedor*> é definido aquando da configuração aplicacional do fornecedor (normalmente o CommonName que ficará associado ao certificado do fornecedor);
    - <*IdentificadorUnicoAtributo*> é uma string definida pelo fornecedor que permita identificar univocamente o atributo nesse fornecedor;
    - <*IdentificadorUnicoSubAtributo*> é uma string definida pelo fornecedor que permita identificar univocamente o subatributo nesse fornecedor;
- O campo *Description* de um atributo deve conter uma string a ser mostrado ao cidadão aquando da utilização do atributo, e que permita ao cidadão reconhecer o seu cargo ou papel que desempenha no fornecedor;
- Cada atributo pode ter vários subatributos, que poderão ser utilizados nas seguintes vertentes:
    - *Subatributos de assinatura*: subatributos que serão utilizados no contexto de uma assinatura (constarão nos detalhes de assinatura de um documento);
    - *Subatributos de autenticação*: subatributos que serão utilizados no contexto de uma autenticação no Fornecedor de Autenticação. De forma a ser possível normalizar estes subatributos de autenticação, os fornecedores devem disponibilizar (**no mínimo, e se aplicável**) os seguintes subatributos:
        - NúmeroMecanograficoCidadao – identificador do cidadão no fornecedor (*"http://interop.gov.pt/SCAP/**<NomeFornecedor>**/**<IdentificadorUnicoAtributo/NumeroMecanograficoCidadao***")*
        - NomeCidadao – nome do cidadão no fornecedor (*http://interop.gov.pt/SCAP/**<NomeFornecedor>**/**<IdentificadorUnicoAtributo/NomeCidadao***)*
        - *Telefone*Cidadao – contacto telefónico do cidadão no fornecedor

(*"http://interop.gov.pt/SCAP/**<NomeFornecedor>**/**<IdentificadorUnicoAtributo/TelefoneCidadao**"*)

- *Email*Cidadao – contacto eletrónico do cidadão no fornecedor (*"http://interop.gov.pt/SCAP/**<NomeFornecedor>**/**<IdentificadorUnicoAtributo/EmailCidadao**"*)

- No caso de o atributo não ter uma data de validade definida, deve ser enviada a data **9999-12-31**

Não obstante o fornecedor fazer a gestão dos subatributos a enviar em cada pedido de atributos, o SCAP garantirá que os subatributos de assinatura só serão enviados aquando de uma assinatura, e que os subatributos de autenticação só serão enviados aquando de uma autenticação.

No caso da autenticação estar associada à criação de um cartão na aplicação id.gov.pt será utilizada por *default* a informação que consta nos subatributos do primeiro atributo enviado pelo fornecedor.

6. PROCEDIMENTO DE INTEGRAÇÃO

1. Fornecedor – Enviar email para eid@ama.pt a formalizar a intenção de integrar com o SCAP enquanto fornecedor de atributos;
2. AMA + Fornecedor – Celebrar protocolo.

6.1. Ambiente de pré-produção

1. Fornecedor – Envio de informação para configuração aplicacional da entidade (ver ponto 8);
2. AMA + Fornecedor – Configuração de VPN para comunicação entre Fornecedor e iAP;
3. AMA – Configuração aplicacional da entidade, e envio dos seguintes ficheiros ao fornecedor:
    - *SCAP_<Fornecedor>_UriId* – contém identificador da entidade perante o SCAP;
    - *SCAP_<Fornecedor>_TotpSecreyKey* – contém secretKey para geração de TOTPs;
    - *SCAP_<Fornecedor>_InfoFile* – contém informação da conta do Fornecedor de Atributos;
4. Fornecedor – Desenvolvimento e configuração de atributos de testes pedidos pela AMA;
5. AMA – Validação do desenvolvimento;
6. Integração concluída.

6.2. Ambiente de produção

1. Fornecedor – Produção de relatório assinado com evidências de cumprimento de *Guidelines de Integração do SCAP* (ver documento anexo);
2. Fornecedor – Envio de informação para configuração aplicacional da entidade;
3. AMA + Fornecedor – Configuração de VPN para comunicação entre Fornecedor e iAP;
4. AMA – Configuração aplicacional da entidade, e envio dos seguintes ficheiros ao fornecedor:
    - *SCAP_<Fornecedor>_UriId* – contém identificador da entidade perante o SCAP;
    - *SCAP_<Fornecedor>_TotpSecreyKey* – contém secretKey para geração de TOTPs;
    - *SCAP_<Fornecedor>_InfoFile* – contém informação da conta do Fornecedor de Atributos;

- *SCAP_<Fornecedor>_CSR* – contém CSR para pedir emissão de certificado;

5. Fornecedor – Aquisição de *certificado qualificado de selo eletrónico* com base no CSR gerado no passo anterior, e envio do certificado adquirido;
6. AMA – Atualização da configuração aplicacional da entidade, com o certificado adquirido pelo fornecedor;
7. Fornecedor – Configuração de atributos de testes pedidos pela AMA;
8. AMA – Validação;
9. Integração concluída.

7. TESTE DE PEDIDO DE ATRIBUTOS

De forma a poderem testar os pedidos de atributos, os fornecedores podem recorrer aos seguintes meios:

- Obtenção de atributos via Aplicação do Cartão de Cidadão

  1. Instalar Aplicação do Cartão de Cidadão (disponível em https://www.autenticacao.gov.pt/cc-aplicacao);
  2. Se o teste for realizado no ambiente de pré-produção, editar registo do Windows, de forma a apontar para esse ambiente:
     a. Abrir regedit.exe;
     b. Aceder a "*Computador\HKEY_CURRENT_USER\Software\PTEID\general"*;
     c. Adicionar a propriedade "*scap_host"* com o valor "*preprod.mw.autenticacao.gov.pt*";
  3. Aceder ao menu "*Definições -> Atributos Profissionais*", e efetuar uma pesquisa de atributos para o fornecedor pretendido.

- Obtenção de atributos via portal Autenticacao.Gov (*ainda não disponível*);

  1. Aceder e fazer autenticação em https://www.autenticacao.gov.pt (ambiente de produção) ou https://pprwww.autenticacao.gov.pt (ambiente de pré-produção);
  2. Aceder ao menu "*Área Reservada -> Os Meus Atributos Profissionais -> Consulta de Atributos*", e efetuar uma pesquisa de atributos para o fornecedor pretendido.

8. INFORMAÇÃO A ENVIAR À AMA PARA CONFIGURAÇÃO APLICACIONAL

- Nome completo da entidade;
- NIPC/NIF;
- CAE (Código da Classificação Portuguesa de Atividades Económicas), se aplicável;
- Contacto telefónico;
- Email;
- CommonName (que ficará associado ao certificado) - e.g. iniciais da entidade;
- Localidade (que ficará associada ao certificado).