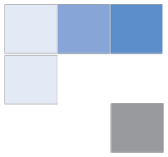
AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA
PRESIDÊNCIA DO CONSELHO DE MINISTROS



AUTENTICAÇÃO.GOV

FORNECEDOR DE AUTENTICAÇÃO DA ADMINISTRAÇÃO PÚBLICA PORTUGUESA

VERSÃO 1.5.1

DEZEMBRO DE 2018

Sumário

1 Introdução

1.1 Enquadramento

Este documento tem como objetivo apresentar as principais funcionalidades e benefícios do Autenticação.Gov.

O Autenticação.Gov surge da necessidade de identificação unívoca de um utilizador perante sítios na Web. Cabe a esta solução o processo de autenticação e o fornecimento dos atributos do utilizador necessários a que cada entidade possa efetuar a identificação do utilizador.

O Autenticação.Gov, em conjunto com o Cartão de Cidadão, também permite fazer uso da funcionalidade de Federação de Identidades da Plataforma de Interoperabilidade da Administração Pública para a identificação sectorial de um Cidadão, *id est,* a obtenção dos seus identificadores junto das entidades participantes da iniciativa do Cartão de Cidadão. É também responsável pela gestão dos vários fornecedores de atributos disponíveis e possui uma estreita ligação com a infraestrutura de chave pública do Cartão de Cidadão (PKI), com o intuito de manter elevados níveis de segurança e privacidade no processo de autenticação e identificação.

Através do Autenticação.Gov é possível a criação de credenciais comuns a todos os sites da Administração Pública, assegurando que o utilizador se necessita de autenticar apenas uma única vez para executar um ou vários serviços que podem ser iniciados em portais transversais (como o Portal do Cidadão ou o Portal da Empresa).

Permite também proceder à autenticação de um utilizador com recursos a outros certificados digitais que não o do Cartão de Cidadão, possibilitando e alargando o leque de autenticação disponível para as Entidades que pretendam delegar a autenticação nesta componente.

1.2 Estrutura do documento

O presente documento encontra-se organizado nos seguintes capítulos:

- Principais Funcionalidades – onde se descreve os principais objetivos e funcionalidades da solução;
- Visão Geral da Solução – onde é apresentada de forma sumária, a visão geral da solução, bem como os diversos atores no fluxo de autenticação de um Utilizador;
- Integração com o Autenticação.Gov do Cartão de Cidadão – onde se descrevem as adaptações necessárias à utilização do Autenticação.Gov;
- Utilização da funcionalidade de *Single Sign On* – onde é descrito o funcionamento em modo de sessão, com o Autenticação.Gov;
- Autenticação com certificados que não do Cartão de Cidadão – descreve a utilização do Autenticação.Gov com certificados digitais associados à Ordem dos Advogados, Notários ou Solicitadores;
- Grupos de confiança dos atributos do Autenticação.Gov – descreve-se os níveis de confiança atribuídos aos atributos utilizados;
- Utilização de assinaturas digitais – onde se exemplifica a utilização da assinatura eletrónica a usar nos pedidos de autenticação;
- Exemplo de autenticação – demonstrativos da utilização dos processos de autenticação com o Autenticação.Gov;
- Especificações Técnicas – onde se encontram as definições técnicas para integração com o Autenticação.Gov.

1.3 Definições

- GOV – Nas imagens onde está a designação "GOV" deve-se ler "Autenticação.Gov"
- Fornecedor de Atributos - Entidade que, com base na identificação unívoca do Cidadão pode fornecer dados qualificados do mesmo.
- PI – Plataforma de Interoperabilidade;
- Identificação sectorial – identificação de um Cidadão numa entidade participante da iniciativa do Cartão de Cidadão (e.g. Número de Identificação Fiscal, identificador do cidadão na entidade Autoridade Tributária e Aduaneira).
- STORK – *Secure identity across borders linked*. Iniciativa europeia de identificação eletrónica transfronteiriça;

2 Principais Funcionalidades

Assumindo-se como componente base para autenticação (particularmente com o Cartão de Cidadão) a nível nacional e internacional, a introdução das funcionalidades do Autenticação.Gov permitem a normalização do ato de autenticação eletrónica para as entidades que dela necessitem. Esta autenticação realiza-se com a possibilidade de transmissão de informação adicional do utilizador, informação esta que o utilizador explicitamente autoriza.

As principais funcionalidades e objetivos do Autenticação.Gov são:

- Identificação sectorial com base no Cartão de Cidadão – Baseado na credenciação do cidadão durante a emissão do Cartão de Cidadão, aliado à Federação de Identidades da Plataforma de Interoperabilidade da Administração Pública, o processo de autenticação no Autenticação.Gov permite a identificação sectorial e segura de um Cidadão;

- Disponibilização de atributos sectoriais – A utilização do Cartão de Cidadão permite a obtenção de identificadores (NIF, NISS, NSNS) ou outros atributos sectoriais, através da utilização da Plataforma de Interoperabilidade;

- Simplificação do processo de autenticação – O processo de autenticação do utilizador pode ser delegado ao Autenticação.Gov, que é responsável pela validação de certificados, obtenção de atributos qualificados, devolvendo o valor deste atributos à entidade que solicitou a autenticação;

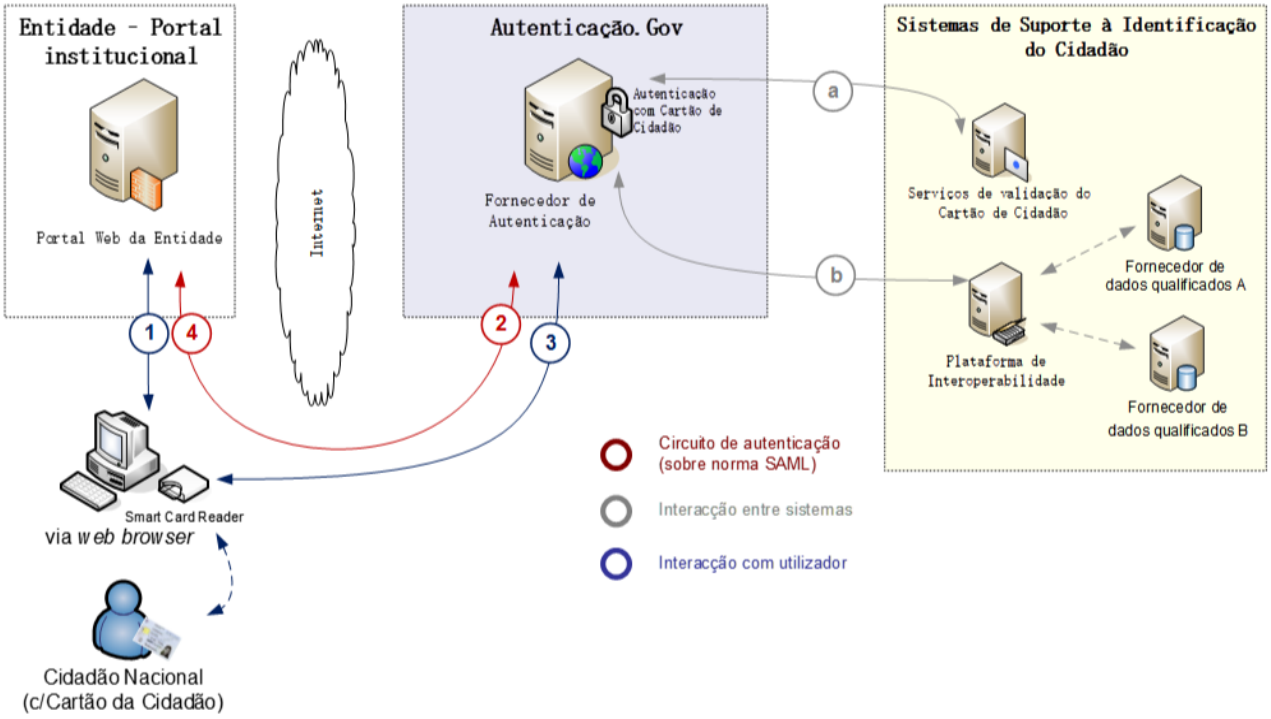
- Normalização do processo de autenticação – O processo de autenticação é realizado com vários níveis de segurança e qualidade de serviço, dependente do certificado usado na autenticação ou através da Chave Móvel Digital. É garantida a utilização da estrutura de chave pública do Cartão de Cidadão (PKI do Cartão de Cidadão), com recurso à validação OCSP (*Online Certificate Status Protocol*) dos certificados de autenticação, sempre que esta se encontre

disponível. É efetuada a validação contra CRL (*Certificate Revogation List*) para os certificados para os quais o serviço OCSP não se encontre disponível (não é o caso do Cartão de Cidadão);

- O utilizador possui pleno conhecimento e opção sobre os dados a serem fornecidos – O utilizador é parte ativa na transmissão de atributos às entidades que os solicitam. Para que a troca de informação seja realizada, o utilizador tem que dar a sua permissão explícita.
  Em qualquer altura, o utilizador pode cancelar o processo de autenticação para a entidade requisitante. Futuramente poderá consultar o histórico de autenticações realizadas com o Autenticação.Gov.

3 Visão Geral da Solução

A figura seguinte pretende exemplificar, de forma sumária e transversal, a utilização do Autenticação.Gov com base num caso de uso de autenticação de um utilizador junto de uma entidade utilizando o Cartão de Cidadão.



No diagrama acima identificam-se as seguintes interações:

1. O utilizador pretende aceder à área privada do portal de uma entidade, na qual é necessário que comprove a sua identidade;

2. O portal da entidade delega a autenticação e redireciona o utilizador para o Autenticação.Gov, juntamente com um pedido de autenticação assinado digitalmente;

3. O Autenticação.Gov valida o pedido de autenticação recebido e solicita a autenticação do utilizador com recurso ao seu Cartão de Cidadão pedindo a

inserção do seu PIN de autenticação. Durante este processo, o Autenticação.Gov efetua as seguintes operações internas:

a) Valida as credenciais do utilizador com recurso à PKI do Cartão de Cidadão via OCSP;
b) Obtém atributos que sejam solicitados pelo portal da entidade junto dos vários fornecedores de atributos qualificados. Esta operação é efetuada via Plataforma de Interoperabilidade. Este processo pode incluir a obtenção de dados da Federação de Identidades ou de outras Entidades.

4. A identificação e atributos do utilizador são autenticadas e assinados digitalmente pelo Autenticação.Gov, após o que redireciona o utilizador de volta ao portal da entidade original. Cabe à entidade a validação das credenciais do Autenticação.Gov e utilização dos atributos do cidadão.

Dado que no processo de autenticação poderão ser solicitados mais dados que os presentes no *chip* do Cartão de Cidadão ou do certificado digital de autenticação, mostra-se necessário a obtenção destes dados junto de fornecedores de atributos qualificados para o efeito.

Define-se como um **Fornecedor de Atributos** uma entidade que possua e disponibilize, de acordo com a identificação e autorização (explícita ou implícita) do utilizador, dados qualificados sobre ele.

A utilização do mecanismo de autenticação centralizada no Autenticação.Gov permite ao utilizador a simplificação do procedimento de autenticações posteriores quando interage com vários portais da Administração Pública. Ou seja, permite-se assim a autenticação dos cidadãos entre *sites* da Administração Pública (ou entidades privadas) solicitando-se apenas as credenciais do utilizador uma vez apenas, revalidando-se estas credenciais junto do Autenticação.Gov sem necessidade de nova inserção de PIN de autenticação.

Neste contexto, aplicam-se as seguintes etapas e funcionalidades:

- **Primeira Autenticação** – O Autenticação.Gov irá solicitar a credencial para autenticação e fornecimento de atributos, devolvendo o resultado ao portal que a requereu;

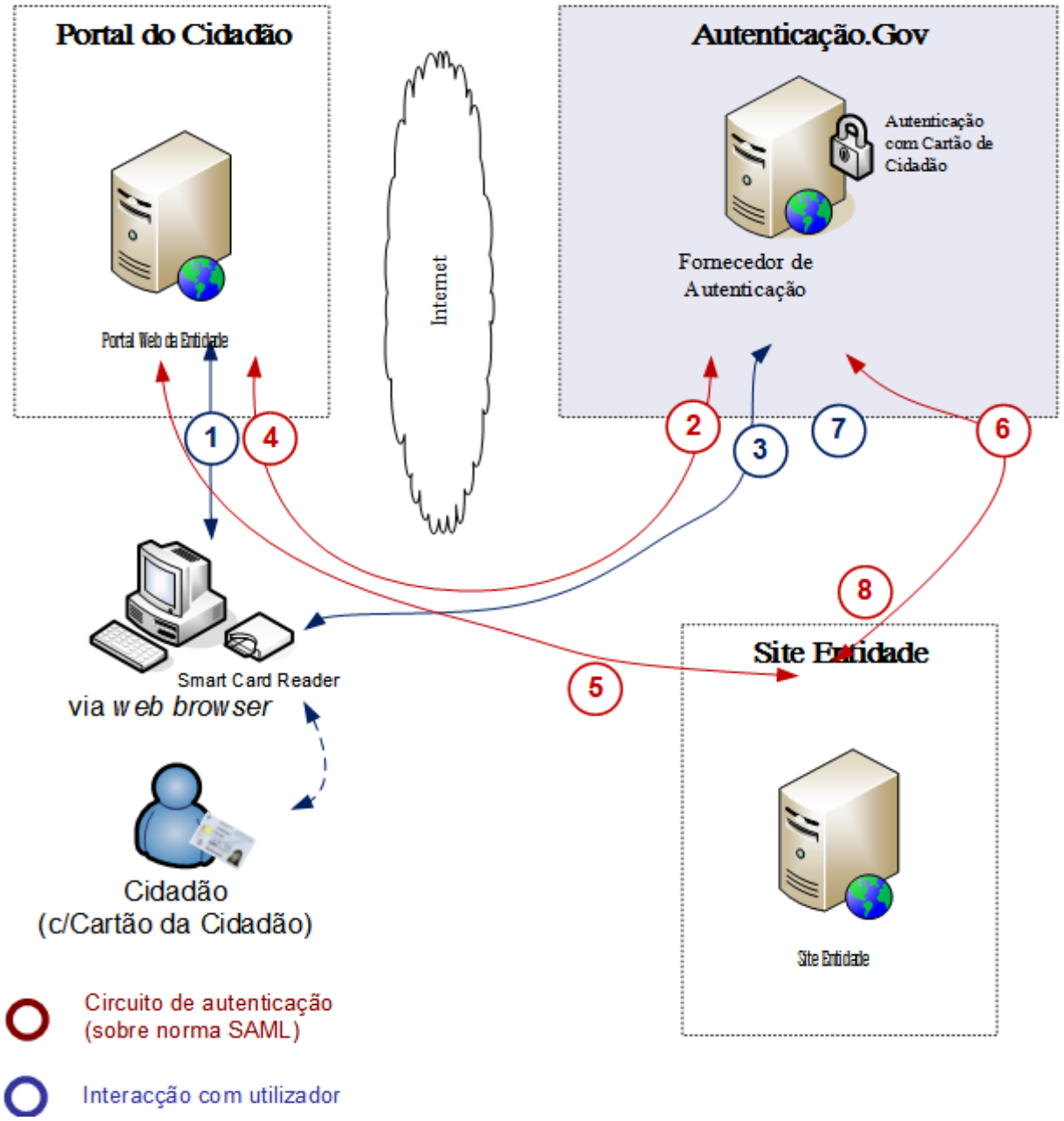
- **Revalidação da Autenticação** – Caso o utilizador já se tinha autenticado com sucesso no Autenticação.Gov, sempre que seja solicitada uma nova autenticação, este processo é simplificado:

    - Se forem solicitados os mesmos atributos da última autenticação e estes tenham sido obtidos com um nível de confiança igual ou superior, não será necessária nova introdução de PIN;
    - Caso sejam pedidos atributos diferentes, então o Autenticação.Gov irá requisitar ao utilizador nova inserção de PIN.

  O utilizador será sempre informado explicitamente deste processo, necessitando de dar a sua autorização para a recolha dos atributos;

- **Terminar Sessão (Logout)** – Caso o utilizador já se encontre autenticado e pretenda terminar a sua sessão, o Fornecedor de Serviço terá de propagar o término de sessão para o Autenticação.Gov.

De forma a assegurar a autenticação comum entre diferentes portais de entidades (onde poderão residir os serviços e formulários eletrónicos), as entidades deverão ainda implementar o mecanismo de SSO descrito na figura seguinte.



Na figura supra, as mensagens 1 a 4 são similares às indicadas na secção anterior. As mensagens 5 a 8 têm por objetivo:

5. O portal da entidade redireciona para site de uma segunda entidade com pedido de autenticação;

6. O *site* da entidade revalida a credencial eletrónica junto do Autenticação.Gov;

7. Cabe ao Autenticação.Gov reemitir uma credencial específica para o *site* da entidade e caso estejam a ser solicitados diferentes atributos ou atributos adicionais aos inicialmente disponibilizados, solicitar uma autenticação adicional do utilizador;

8. O s*ite* de entidade valida a nova credencial e autentica utilizador (e executa o serviço eletrónico).

4 Integração com o Autenticação.Gov do Cartão de Cidadão

Na utilização do Autenticação.Gov, as entidades podem assumir duas vertentes distintas decorrente da sua utilização:

- **Agir como utilizadores da autenticação Web** – utilização do Autenticação.Gov como componente de autenticação e de obtenção de atributos (de **implementação obrigatória** no âmbito do objetivo definido neste documento);

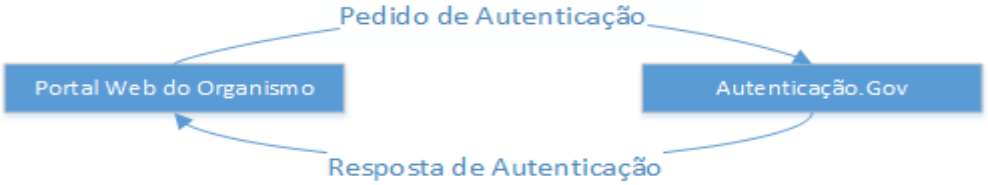
- **Participar como fornecedores de atributos** – utilização do Autenticação.Gov como entidade que fornece, de acordo com a autorização do utilizador, dados qualificados sobre ele (de **implementação opcional** no âmbito do objetivo definido neste documento – relevante para disponibilização de atributos do cidadão geridos pelas entidades).

Os próximos capítulos detalham cada uma destas vertentes.

4.1 Entidade no papel de utilizadora da autenticação web

O formato de dados trocados entre o Autenticação.Gov e as entidades é baseado em SAML v2.0 (*Security Assertion Markup Language*), de forma a assegurar a autenticidade e integridade de todas as transações. A utilização do *SAML HTTP Post Binding* associado ao *SAML Web Browser SSO Profile* permite que a autenticação seja efetuada tecnicamente pelo *browser* do utilizador, sem necessidade de ligação física entre as entidades e o Autenticação.Gov.

As comunicações entre o Autenticação.Gov e as entidades são efetuadas sobre HTTP em canal cifrado – *Secure Socket Layer* (SSL) ou *Transport Layer Security*(TLS). Esta comunicação é realizada sobre Internet.



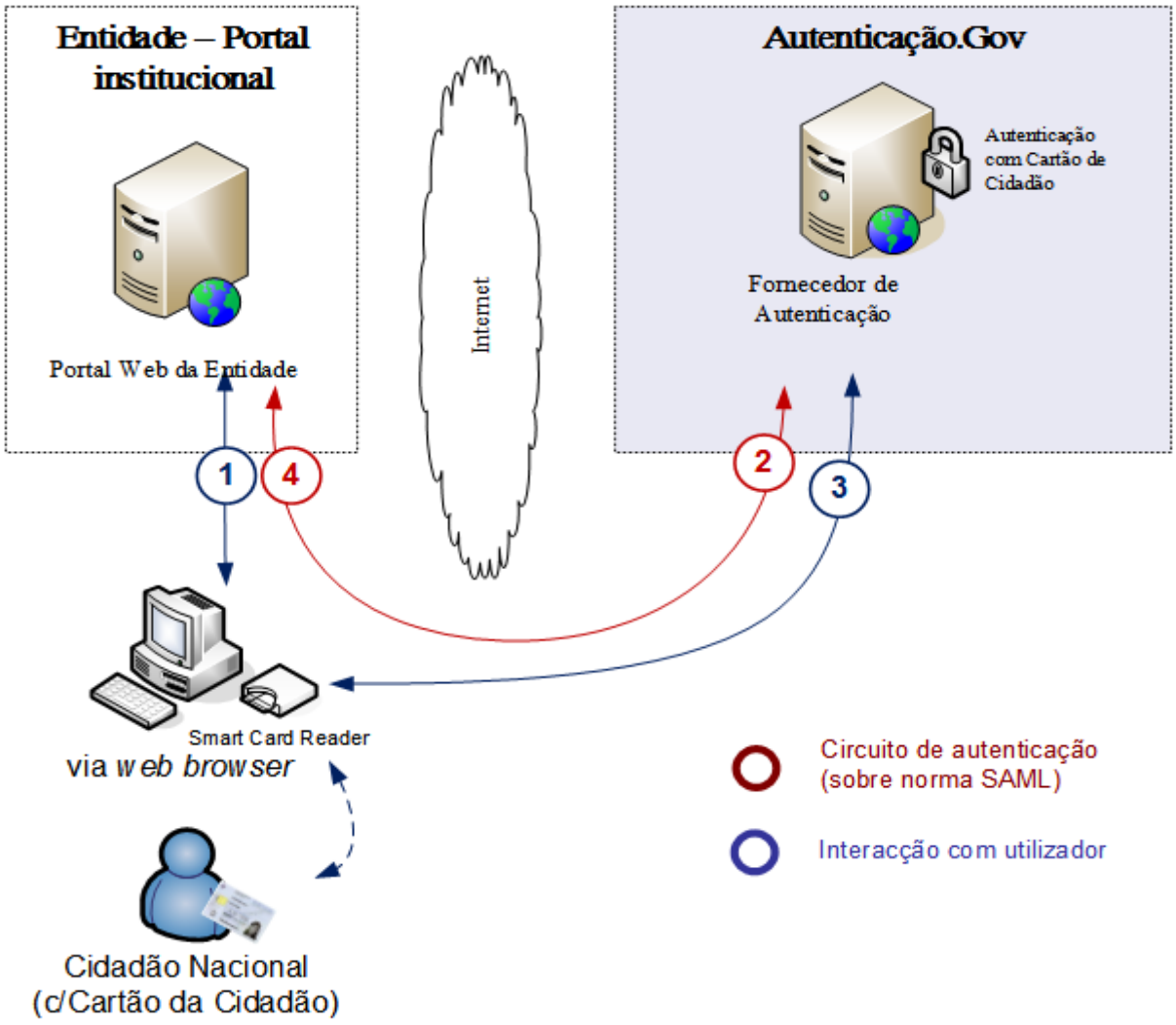
O Autenticação.Gov responde à entidade com informação autorizada pelo utilizador. A resposta inclui os atributos solicitados no pedido de autenticação. Esta ligação é também efetuada sobre HTTP em canal cifrado – SSL ou TLS.

A utilização de canais cifrados, associado ao formato específico SAML garante que a troca de dados seguir as seguintes considerações:

- **Privacidade de dados** – a utilização de canais cifrados garante que os dados do utilizador se mantêm privados, impedindo a sua visualização por terceiros (ex. visualização de dados por *sniffer* de rede);

- **Integridade de dados** – o protocolo SAML, através de assinatura digital nos pedidos e respostas de autenticação SAML, garante a integridade de dados de modificações não autorizadas (ex. ataque por *Man-in-the Middle)*.

De acordo com o anteriormente descrito, a utilização da autenticação pelo Autenticação.Gov é efetuado somente através de ambiente Web e sobre Internet.



A imagem acima descreve as interações entre o portal da entidade e o Autenticação.Gov, usando o *browser* do utilizador como intermediário.

As adaptações a realizar pela entidade recaem nos pontos 2 e 4, que correspondem respetivamente à criação do pedido de autenticação SAML e no consumo da resposta proveniente do Autenticação.Gov:

- **Pedido de autenticação** - Corresponde ao pedido de identificação por parte da entidade. Permite reconhecer a origem do pedido, através da assinatura

digital por um certificado digital x.509v3 associado à entidade. O pedido contém quais os atributos que devem ser obtidos (ex. NIF);

- **Resposta de autenticação** – contém o resultado da autenticação efetuada pelo Autenticação.Gov. Encontra-se na resposta os atributos solicitados previamente pela entidade. Esta mensagem é assinada digitalmente pelo Autenticação.Gov de forma a garantir a integridade da informação.

Nos próximos sub-capítulos apresentam-se exemplos de pedidos de autenticação SAML, sendo que as especificações técnicas detalhadas encontram-se no capítulo 10.

Exemplo de mensagem de pedido de autenticação SAML

A mensagem seguinte exemplifica um pedido de autenticação proveniente do portal da Entidade, junto do Autenticação.Gov, onde é solicitado um atributo, neste caso *AttributeName*:

```
<samlp:AuthnRequest
                ID="_1e736a31-a41c-4c35-b17f-0f9ab4c741b3"
                Version="2.0"
                IssueInstant="2011-02-17T11:15:24Z"
                Destination="https://autenticacao.gov..ptDefault.aspx"
                ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                AssertionConsumerServiceURL="https://www.ServiceProvider.pt/HandleRequest"
                ProviderName="Service Provider Name"
                xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://www.ServiceProvider.pt</saml:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <Reference URI="#_1e736a31-a41c-4c35-b17f-0f9ab4c741b3">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                                <InclusiveNamespaces PrefixList="#default samlp saml ds xs xsi"
xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                        </Transform>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <DigestValue>oypLiC5MkXdKFbs0pA25Z/mt4jk=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>...signatureValue...</SignatureValue>
                <KeyInfo>
                        <X509Data>
                                <X509Certificate>...x509Data...</X509Certificate>
                        </X509Data>
```

```
                </KeyInfo>
        </Signature>
        <samlp:Extensions>
                <fa:RequestedAttributes xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos">
                        <fa:RequestedAttribute Name="AttributeName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri" isRequired="true"/>
                </fa:RequestedAttributes>
        </samlp:Extensions>
</samlp:AuthnRequest>
```

Nota: O elemento de assinatura digital foi retirado para efeitos de simplificação.

Exemplo de mensagem de resposta a pedido de autenticação SAML

A mensagem seguinte exemplifica a resposta a um pedido de autenticação, fornecendo a resposta ao atributo *AttributeName*, com o valor *AttributeValue*:

```
<saml2p:Response xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" ID="_0314efee-a385-4ca9-afab-4bffbb6a788b" InResponseTo="_1e736a31-a41c-4c35-
b17f-0f9ab4c741b3" Version="2.0" IssueInstant="2011-02-17T11:17:14.6349444Z"
Destination="https://www.ServiceProvider.pt/HandleResponse" Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified">
        <saml2:Issuer>https://autenticacao.cartaodecidadao.pt</saml2:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <Reference URI="#_0314efee-a385-4ca9-afab-4bffbb6a788b">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <DigestValue>qqC76JmDP+2i1s0oxY8EsSD4tic=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>...signatureValue...</SignatureValue>
                <KeyInfo>
                        <X509Data>
                                <X509Certificate>...x509Data...</X509Certificate>
                        </X509Data>
                </KeyInfo>
        </Signature>
        <saml2p:Status>
                <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </saml2p:Status>
        <saml2:Assertion Version="2.0" ID="_b1c88f11-50fd-4a22-988e-9ce4573049e0" IssueInstant="2011-02-17T11:17:14.6349444Z">
                <saml2:Issuer>https://autenticacao.cartaodecidadao.pt</saml2:Issuer>
                <saml2:Subject>
                        <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</saml2:NameID>
                        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
                                <saml2:SubjectConfirmationData NotOnOrAfter="2011-02-17T11:22:14Z"
Recipient="https://www.ServiceProvider.pt" InResponseTo="_1e736a31-a41c-4c35-b17f-0f9ab4c741b3" Address="127.0.0.1"/>
                        </saml2:SubjectConfirmation>
                </saml2:Subject>
                <saml2:Conditions NotBefore="2011-02-17T11:17:14Z" NotOnOrAfter="2011-02-17T11:22:14Z">
                        <saml2:AudienceRestriction>
                                <saml2:Audience>https://www.ServiceProvider.pt</saml2:Audience>
```

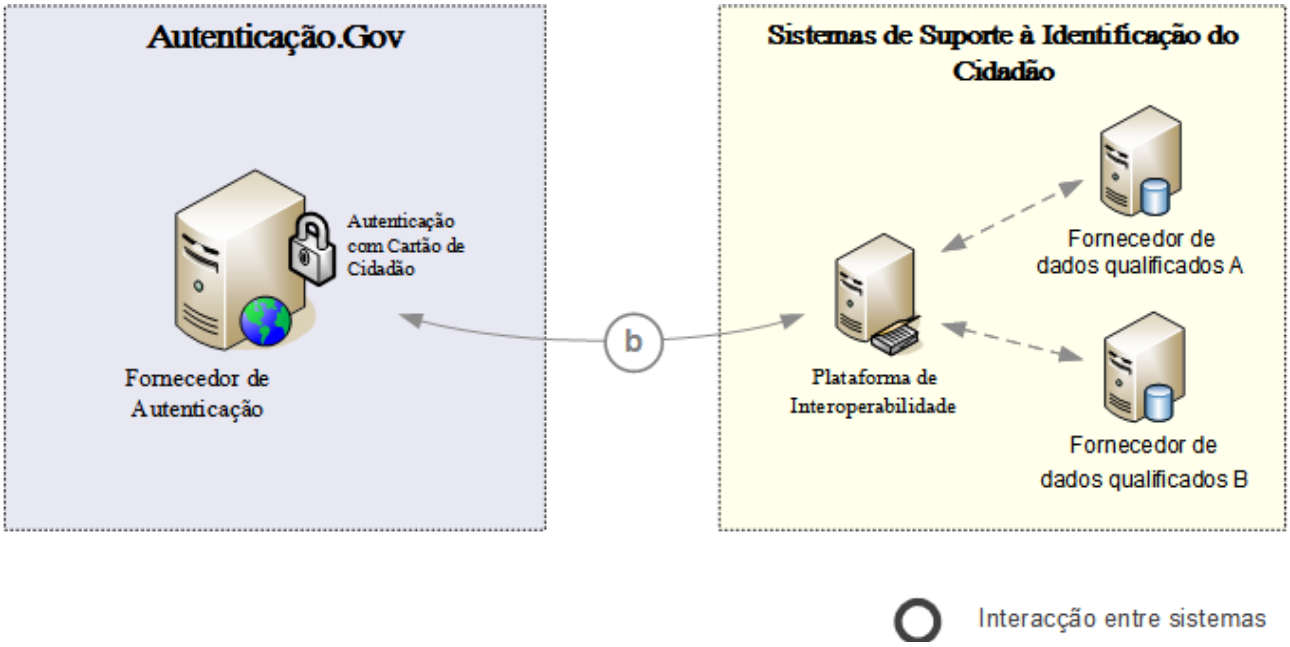
```
                    </saml2:AudienceRestriction>
                    <saml2:OneTimeUse/>
                </saml2:Conditions>
                <saml2:AuthnStatement AuthnInstant="2011-02-17T11:17:14.6349444Z">
                    <saml2:AuthnContext/>
                </saml2:AuthnStatement>
                <saml2:AttributeStatement>
                    <saml2:Attribute Name="AttributeName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
fa:AttributeStatus="Available">
                        <saml2:AttributeValue xmlns:q1="http://www.w3.org/2001/XMLSchema"
xmlns:d5p1="http://www.w3.org/2001/XMLSchema-instance" d5p1:type="q1:string">AttributeValue</saml2:AttributeValue>
                    </saml2:Attribute>
                </saml2:AttributeStatement>
            </saml2:Assertion>
</saml2p:Response>
```

Nota: O elemento de assinatura digital foi retirado para efeitos de simplificação.

4.2 Entidade no papel de fornecedor de atributos

Numa fase do fluxo de autenticação, já posterior à verificação da autenticidade do Cartão de Cidadão, o Autenticação.Gov irá obter os atributos necessários para responder ao pedido de autenticação da entidade requisitante.

Caso os dados solicitados não se encontrem no certificado público do Cartão de Cidadão ou no próprio *chip* deste, o Autenticação.Gov irá promover a sua obtenção junto de Fornecedores de Atributos externos, conforme ilustrado na figura seguinte.



O pedido de obtenção de um atributo será gerado pelo Autenticação.Gov, com o consentimento do utilizador e posteriormente enviado ao correspondente fornecedor de atributos. Este pedido materializa-se na invocação de um serviço eletrónico no respetivo fornecedor de atributos que contem a seguinte informação:

- **Número de Pedido** – Identificador unívoco do pedido de atributos. Este dado é interno ao Autenticação.Gov e é usado como forma de identificação e localização dos vários pedidos de atributos realizados;

- **Identificador do Cidadão –** O pedido de atributos é acompanhado pelo respetivo identificador sectorial cifrado, proveniente da Federação de Identidades da Plataforma de Interoperabilidade. Este assegura a identificação unívoca junto do fornecedor de atributos;

- **Prestador de Serviços Requerente** – Representa o URL como descrição do prestador de serviços que solicitou originalmente os dados;

- **Data e hora** – Identificação temporal da criação do pedido de atributos;

- **Nome do Cidadão** – Nome do cidadão sobre a qual os atributos se referem;

- **Atributos solicitados** – Lista de atributos que são solicitados pelo prestador de serviços e consentidos pelo cidadão.

Os atributos são autorizados pelo utilizador no decorrer do processo de autenticação junto do Autenticação.Gov, cujo pedido aos respetivos fornecedores será assinado digitalmente por este. Com base na assinatura digital do pedido, os fornecedores de atributos podem comprovar a sua autenticidade e validade.

Após receção e validação digital de um pedido de atributos, o fornecedor do atributo deverá responder a este serviço eletrónico, com a seguinte informação:

- **Número de Pedido** – Identificador unívoco do pedido de atributos. Este valor será igual ao número de pedido da mensagem original. Serve como elemento de relação e de apoio à localização dos vários pedidos de atributos realizados;

- **Data e hora** – Identificação temporal da criação da resposta ao pedido de atributos;

- **Atributos** – Lista de atributos original, com preenchimento dos respetivos valores. A cada atributo encontra-se associado um estado que identifica o resultado da operação de obtenção do valor:

    - *Disponível* – O valor do atributo foi encontrado e devolvido. Este valor é obrigatório sempre que um atributo é devolvido com valor.
    - *Não Disponível* – Não foi possível encontrar o valor de atributo para o utilizador em causa.
    - *Não Permitido* – O fornecedor de atributos não permitiu ativamente a obtenção de atributos.

Devido à utilização de assinatura digital como forma de validação do pedido de atributos, o conjunto de dados validados desta forma não poderá ser alterado ou adulterado. Por esta razão, os elementos que foram alvo de validação por assinatura

digital não podem ser alterados, nem mesmo pela Plataforma de Interoperabilidade, o que impossibilita a normalização de dados, vulgo "mapeamentos".

Exemplo de mensagem de pedido de Atributos - "FAObterAtributos"

A mensagem seguinte exemplifica um pedido de atributos, neste caso NIC e Nome, realizada pelo Autenticação.Gov a um Fornecedor de Atributos, via Plataforma de Interoperabilidade.

```
<fa:FAObterAtributos xmlns:fa="http://autenticacao.cartaodecidadao.pt/servicos"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <fa:IdentificadorCidadao>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</
fa:IdentificadorCidadao>
        <fa:PedidoAtributos>
                <fa:NumeroPedido>ED6F7BBC-1A42-11DF-A5E3-C17D56D89593</fa:NumeroPedido>
                <fa:NomeCidadao>José Manuel Silva</fa:NomeCidadao>
                <fa:PrestadorServicosRequerente>http://www.portaldocidadao.pt</fa:PrestadorServicosRequerente>
                <fa:DataHora>2001-12-17T09:30:47.0Z</fa:DataHora>
                <fa:Atributos>
                        <fa:Atributo Nome="http://autenticacao.cartaodecidadao.pt/atributos/2010/01/cidadao/
NomeCompleto"/>
                        <fa:Atributo Nome="http://autenticacao.cartaodecidadao.pt/atributos/2010/01/cidadao/NIC"/>
                </fa:Atributos>
                <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                        (...)
                </ds:Signature>
        </fa:PedidoAtributos>
</fa:FAObterAtributos>
```

Nota: O elemento de assinatura digital foi retirado para efeitos de simplificação.

Exemplo de mensagem de resposta a pedido de atributos - "FARespostaObterAtributos"

A mensagem seguinte exemplifica a resposta a um pedido de atributos, neste caso NIC e Nome. Este serviço será realizado pelo fornecedor de atributos com destino ao Autenticação.Gov, via Plataforma de Interoperabilidade.

```
<fa:FARespostaObterAtributos mlns:fa="http://autenticacao.cartaodecidadao.pt/servicos">
        <fa:NumeroPedido>ED6F7BBC-1A42-11DF-A5E3-C17D56D89593</fa:NumeroPedido>
        <fa:DataHora>2001-12-17T09:30:47.0Z</fa:DataHora>
        <fa:Atributos>
                <fa:Atributo Nome="http://autenticacao.cartaodecidadao.pt/atributos/2010/01/cidadao/NomeCompleto"
Resultado="Disponivel">José Manuel Silva</fa:Atributo>
```

```
                <fa:Atributo Nome="http://autenticacao.cartaodecidadao.pt/atributos/2010/01/cidadao/NIC"
Resultado="Disponivel">123456789</fa:Atributo>
        </fa:Atributos>

</fa:FARespostaObterAtributos>
```

Atributos disponíveis – Cartão de Cidadão

Dado que existem atributos que não se encontram presentes no Cartão de Cidadão, seja no certificado público de autenticação ou no *chip*, o Autenticação.Gov irá promover a sua obtenção junto dos fornecedores de atributos qualificados correspondentes.

A listagem seguinte resume os atributos (e respetivos fornecedores) que se encontram disponíveis no Autenticação.Gov:

Atributo	Identificador	Fornecedor de Atributo
Identificação Civil	http://interop.gov.pt/MDC/Cidadao/NIC	Cartão de Cidadão
Nome Próprio	http://interop.gov.pt/MDC/Cidadao/NomeProprio	Cartão de Cidadão
Apelido	http://interop.gov.pt/MDC/Cidadao/NomeApelido	Cartão de Cidadão
Data de Nascimento	http://interop.gov.pt/MDC/Cidadao/DataNascimento	Cartão de Cidadão
Nome Completo	http://interop.gov.pt/MDC/Cidadao/NomeCompleto	Cartão de Cidadão
Identificação Fiscal	http://interop.gov.pt/MDC/Cidadao/NIF	Cartão de Cidadão e Autoridade Tributária
Identificação na Seg. Social	http://interop.gov.pt/MDC/Cidadao/NISS	Cartão de Cidadão e Segurança Social
Identificação no Serviço Nacional Saúde	http://interop.gov.pt/MDC/Cidadao/NSNS	Cartão de Cidadão
Identificação Fiscal (Cifrada)	http://interop.gov.pt/MDC/Cidadao/NIFCifrado	Plataforma de Interoperabilidade

Atributo	Identificador	Fornecedor de Atributo
Identificação na Seg. Social (Cifrada)	http://interop.gov.pt/MDC/Cidadao/NISSCifrado	Plataforma de Interoperabilidade
Identificação Civil (Cifrada)	http://interop.gov.pt/MDC/Cidadao/NICCifrado	Plataforma de Interoperabilidade
Identificação no Serviço Nacional Saúde (Cifrada)	http://interop.gov.pt/MDC/Cidadao/NSNSCifrado	Plataforma de Interoperabilidade
Nacionalidade	http://interop.gov.pt/MDC/Cidadao/Nacionalidade	Cartão de Cidadão
Idade	http://interop.gov.pt/MDC/Cidadao/Idade	Cartão de Cidadão
Número de série do certificado	http://interop.gov.pt/MDC/Cidadao/NumeroSerie	Cartão de Cidadão
Foto	http://interop.gov.pt/MDC/Cidadao/Foto	Cartão de Cidadão
Data de Validade	http://interop.gov.pt/MDC/Cidadao/DataValidade	Cartão de Cidadão
Altura	http://interop.gov.pt/MDC/Cidadao/Altura	Cartão de Cidadão
Nome Próprio do Pai	http://interop.gov.pt/MDC/Cidadao/NomeProprioPai	Cartão de Cidadão
Apelido do Pai	http://interop.gov.pt/MDC/Cidadao/NomeApelidoPai	Cartão de Cidadão
Nome Próprio da Mãe	http://interop.gov.pt/MDC/Cidadao/NomeProprioMae	Cartão de Cidadão
Apelido da Mãe	http://interop.gov.pt/MDC/Cidadao/NomeApelidoMae	Cartão de Cidadão
Indicações Eventuais	http://interop.gov.pt/MDC/Cidadao/IndicacoesEventuais	Cartão de Cidadão
Número do Documento	http://interop.gov.pt/MDC/Cidadao/NoDocumento	Cartão de Cidadão
Zona Leitura Ótica 1	http://interop.gov.pt/MDC/Cidadao/mrz1	Cartão de Cidadão

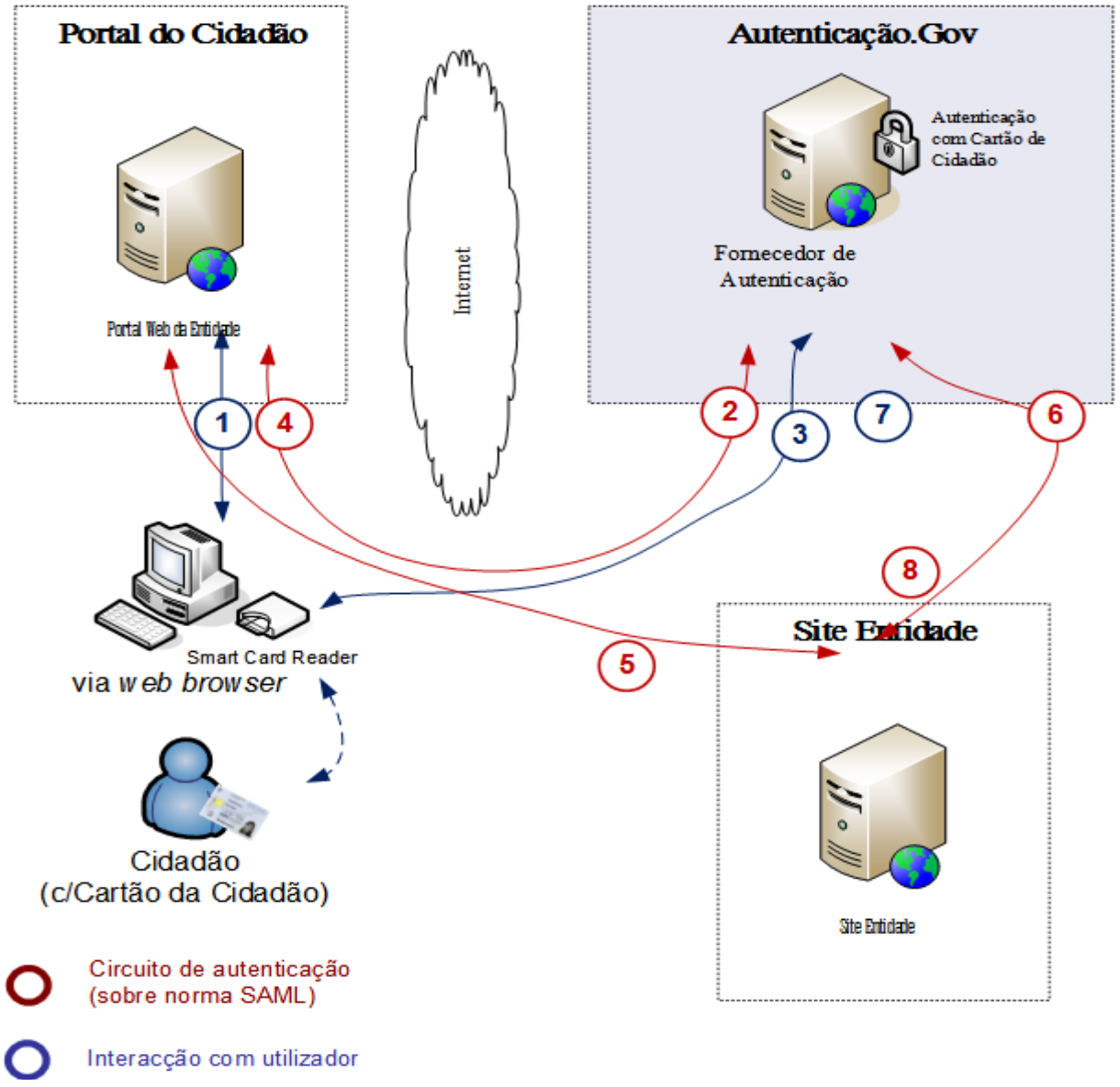
Atributo	Identificador	Fornecedor de Atributo
Zona Leitura Ótica 2	http://interop.gov.pt/MDC/Cidadao/mrz2	Cartão de Cidadão
Zona Leitura Ótica 3	http://interop.gov.pt/MDC/Cidadao/mrz3	Cartão de Cidadão
Versão do Cartão	http://interop.gov.pt/MDC/Cidadao/VersaoCartao	Cartão de Cidadão
Número Cartão PAN	http://interop.gov.pt/MDC/Cidadao/CartaoPAN	Cartão de Cidadão
Data de Emissão	http://interop.gov.pt/MDC/Cidadao/DataEmissao	Cartão de Cidadão
Entidade Emissora	http://interop.gov.pt/MDC/Cidadao/EntidadeEmissora	Cartão de Cidadão
Tipo de Documento	http://interop.gov.pt/MDC/Cidadao/TipoDocumento	Cartão de Cidadão
Local de Pedido	http://interop.gov.pt/MDC/Cidadao/LocalDePedido	Cartão de Cidadão
Versão	http://interop.gov.pt/MDC/Cidadao/Versao	Cartão de Cidadão
Distrito	http://interop.gov.pt/MDC/Cidadao/Distrito	Cartão de Cidadão
Concelho	http://interop.gov.pt/MDC/Cidadao/Concelho	Cartão de Cidadão
Freguesia	http://interop.gov.pt/MDC/Cidadao/Freguesia	Cartão de Cidadão
Abreviatura de Tipo de Via	http://interop.gov.pt/MDC/Cidadao/AbrTipoDeVia	Cartão de Cidadão
Tipo de Via	http://interop.gov.pt/MDC/Cidadao/TipoDeVia	Cartão de Cidadão
Designação da Via	http://interop.gov.pt/MDC/Cidadao/DesignacaoDaVia	Cartão de Cidadão
Abreviatura do Tipo de Edifício	http://interop.gov.pt/MDC/Cidadao/AbrTipoEdificio	Cartão de Cidadão

Atributo	Identificador	Fornecedor de Atributo
Tipo de Edifício	http://interop.gov.pt/MDC/Cidadao/TipoEdificio	Cartão de Cidadão
Número de Porta	http://interop.gov.pt/MDC/Cidadao/NumeroPorta	Cartão de Cidadão
Andar	http://interop.gov.pt/MDC/Cidadao/Andar	Cartão de Cidadão
Lado	http://interop.gov.pt/MDC/Cidadao/Lado	Cartão de Cidadão
Lugar	http://interop.gov.pt/MDC/Cidadao/Lugar	Cartão de Cidadão
Localidade	http://interop.gov.pt/MDC/Cidadao/Localidade	Cartão de Cidadão
Código Postal 4 digitos	http://interop.gov.pt/MDC/Cidadao/CodigoPostal4	Cartão de Cidadão
Código Postal 3 digitos	http://interop.gov.pt/MDC/Cidadao/CodigoPostal3	Cartão de Cidadão
Localidade Postal	http://interop.gov.pt/MDC/Cidadao/LocalidadePostal	Cartão de Cidadão
Número de Controlo	http://interop.gov.pt/MDC/Cidadao/NumeroDeControlo	Cartão de Cidadão
Passaporte	http://interop.gov.pt/MDC/Cidadao/Passaport	Chave Móvel Digital

5 UTILIZAÇÃO DA FUNCIONALIDADE DE *SINGLE SIGN-ON*

De forma a assegurar a autenticação comum entre vários portais onde poderão residir os serviços e formulários eletrónicos, as entidades deverão ainda implementar funcionalidades que permitam a utilização do Cartão de Cidadão como forma de autenticação simplificada entre sites, numa lógica de *single sign-on*.

Após correta autenticação Web por parte do Cidadão, conforme descrito no capítulo 4.1, o Autenticação.Gov manterá internamente, informação de que o mesmo foi autenticado com sucesso. Torna-se assim possível a aplicação de uma lógica de s*ingle sign-on* (SSO), demonstrada na figura seguinte:



As mensagens 1 a 4 são similares às indicadas nas secções anteriores, sendo que as restantes têm por objetivo a validação do mecanismo de SSO. Utiliza-se o Portal do Cidadão como exemplo do Portal que inicia o fluxo de autenticação:

5. Portal do Cidadão redireciona para zona de acesso restrito no site da entidade;

6. Durante a verificação de permissões de acesso à zona de acesso restrito, o portal da entidade deve verificar junto do Autenticação.Gov, se o cidadão já se encontra autenticado com o seu Cartão de Cidadão:
   - Caso se encontre já autenticado, o portal da entidade deve redirecionar o utilizador para o Autenticação.Gov de **forma automática**;
   - Caso não tenha sido previamente autenticado, o portal da entidade pode dar a possibilidade de efetuar o login local ou via Autenticação.Gov, de acordo com a escolha do Cidadão.

7. O Autenticação.Gov irá validar e reemitir uma credencial específica para o *site* da entidade e, opcionalmente, solicitar autenticação adicional do cidadão (e.g., caso estejam a ser solicitados dados adicionais aos que foram inicialmente disponibilizados);

8. *Site* de entidade valida credencial e autentica cidadão (e executa serviço eletrónico).

Em situações específicas, poderá ser necessário evitar, para efeitos de usabilidade, a exibição da página do Autenticação.Gov que pede o consentimento da recolha de atributos ao utilizador. Incluem-se nestes casos, situações onde haja uma página de um *site* embebida noutro portal *(iframe*).

De forma a contemplar o caso acima, o portal que pretende autenticação sem exibir a página de consentimento, deve solicitar um atributo específico (http://interop.gov.pt/MDC/FA/PassarConsentimento) de forma a garantir que a página não é exibida.

5.1 Verificação de autenticação prévia

A verificação de existência de autenticação prévia a ser realizado pelo portal da entidade tem como objetivo facilitar e melhorar a interface de autenticação entre o utilizador, o Portal onde o utilizador se encontra e o Autenticação.Gov.

Esta verificação deverá ser efetuada **pelo portal da entidade** e consistirá na consulta do retorno http de uma página alojada no Autenticação.Gov. Esta verificação junto do Autenticação.Gov deve ser executada sempre que se encontrem reunidas as seguintes condições:

- Tentativa de acesso a uma zona restrita do portal da entidade;
- Utilizador não se encontra autenticado no portal da entidade.

Para melhorar a experiência de utilização, aconselha-se que a verificação seja realizada por AJAX. Esta chamada baseia-se no protocolo Cross-Origin Resource Sharing[1] (CORS) sempre que o mesmo seja suportado pelo *browser* do cliente. Nas restantes situações deverá ser usado um *proxy flash* para garantir a máxima compatibilidade, baseado na biblioteca flXHR[2].

O exemplo abaixo demonstra a lógica que deve ser adicionada na zona de acesso restrito no portal do fornecedor de serviço:

```
var req;
var flproxy;
var isCors = false;

// Verifica o estado de autenticação junto do Autenticação.Gov do Cartão de Cidadão
// Se não possuír sessão no portal da entidade e já se encontrar autenticado no
Aut.Gov, redirecciona automaticamente para o Aut.Gov para revalidação da
autenticação
function VerifyFASSO() {
    //Verifica se utilizador já se encontra autenticado no portal da entidade
    if (querySt('IsAuthenticated') == undefined) {
        try {
            //Verifica utilização da norma CORS
            req = new XMLHttpRequest();
            if (req && "withCredentials" in req) {
                isCors = true;
            }
        }
        catch (e) {
        }
        if (!isCors) {
            //Caso CORS não seja suportado, faz 'fallback' para flXHR
            flproxy = new flensed.flXHR({ autoUpdatePlayer: true, instanceId:
"myproxy1", xmlResponseText: false, onreadystatechange: process, noCacheHeader:
false });
        }
        if (isCors && req != null) {
            //Usa CORS para efectuar o pedido AJAX
```

[1] http://www.w3.org/TR/cors/

[2] http://flxhr.flensed.com/ - Licenciamento MIT: http://flxhr.flensed.com/license.php

```
            req.open("GET",
"https://autenticacao.gov.pt/FA/IsUserAuthenticated.aspx", true);
            req.onreadystatechange = process;
            req.withCredentials = "true";
            req.send(null);
        }
        else {
            //Caso CORS não seja suportado, faz 'fallback' para flXHR
            flproxy.open("GET",
"https://autenticacao.gov.pt/FA/IsUserAuthenticated.aspx");
            flproxy.send();
        }
    }
}

//Processa resposta proveniente do Autenticação.Gov, via CORS
function process() {
    if (req.readyState == 4) {
        if (req.status == 200) {
            var response = req.responseText;
            if (response == "1") {
                //procedimento de redireccionamento automático para o
Autenticação.Gov;
            }
        }
    }
}

//Processa resposta proveniente do Autenticação.Gov, via flXHR
function processFlash(XHRobj) {
    if (XHRobj.readyState == 4) {
        if (XHRobj.status == 200) {
            var response = XHRobj.responseText;
            if (response == "1") {
                //procedimento de redireccionamento automático para o
Autenticação.Gov;
            }
        }
    }
}

VerifyFASSO();
```

Caso o retorno seja o valor 1, significará que o utilizador já se encontra autenticado perante o Autenticação.Gov, devendo o Portal da entidade redirecionar o utilizador para o mesmo, solicitando uma autenticação. O Autenticação.Gov efetuará a gestão e lógica de pedido de PIN, de acordo com as regras definidas:

- Será pedido um novo PIN, caso os atributos solicitados incluam atributos não fornecidos na última autenticação;

- Não será pedido PIN caso os atributos sejam iguais ou estejam contidos nos obtidos na última autenticação.

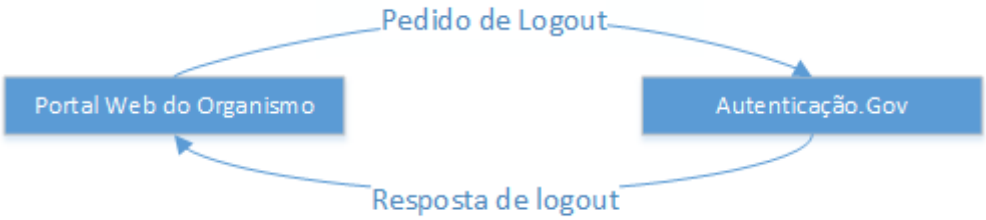
Caso o retorno seja 0, significará que o cidadão não se encontra autenticado perante o Autenticação.Gov. O portal da entidade poderá seguir a sua lógica de autenticação própria, optando mesmo assim por autenticação via Autenticação.Gov.

Nas situações em que se detete que o *browser* do utilizador não suporte Javascript, deverá o portal da entidade agir de acordo com as suas normas internas, sendo que se aconselha a que seja efetuado um pedido de autenticação ao Autenticação.Gov, para emissão (ou revalidação) do pedido de autenticação.

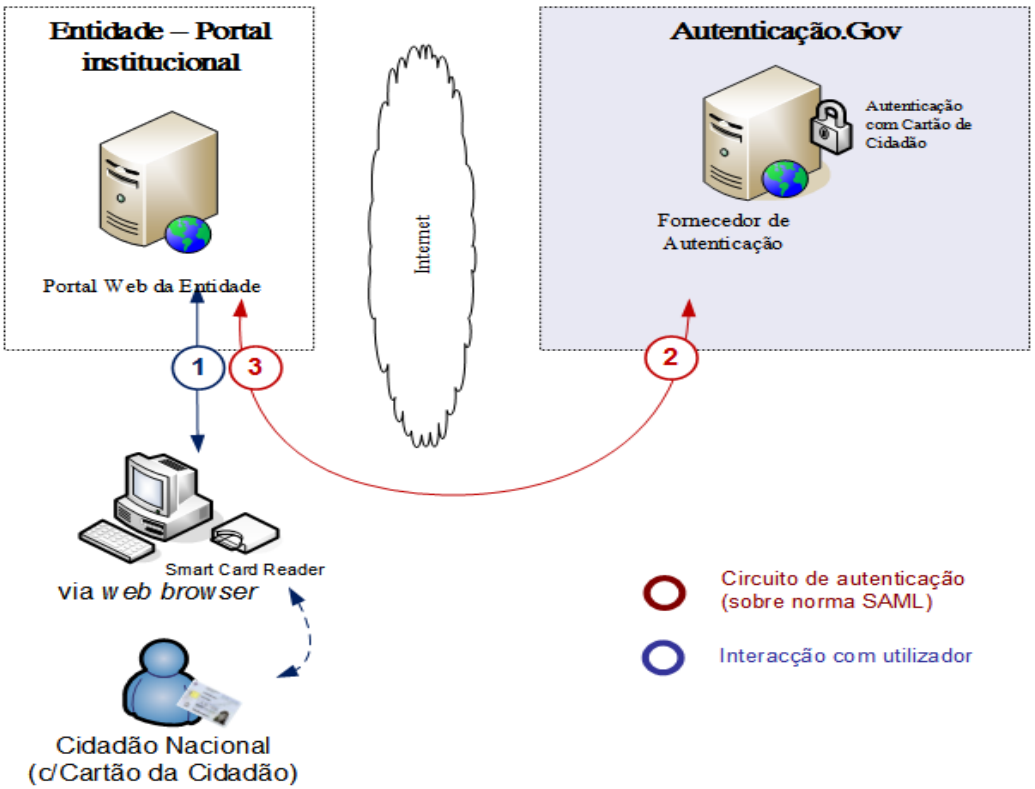
5.2 Logout pelo Portal da Entidade

Decorrente da utilização de mecanismo de SSO com o Cartão de Cidadão, o Autenticação.Gov disponibiliza um método que permite que o portal da entidade desencadeie o *logout* no Autenticação.Gov. O portal da entidade necessitará, à semelhança do pedido de autenticação, redirecionar o utilizador para o Autenticação.Gov com indicação de pedido de *logout*.

O formato de dados trocados entre o Autenticação.Gov e a entidade é idêntico à usada pela autenticação (ver capítulo 4.1). Neste caso é usado uma mensagem SAML específica do tipo *LogoutRequest*.



Tal como no processo de autenticação mantém-se toda a vertente de segurança nas transações entre o portal da entidade e o Autenticação.Gov.



A imagem acima descreve as interações entre o portal da entidade e o Autenticação.Gov num pedido de Logout.

As adaptações a realizar pela entidade recaem nos pontos 2 e 3, que correspondem respetivamente à criação do pedido de Logout SAML e no consumo da resposta proveniente do Autenticação.Gov:

- **Pedido de Logout** - Corresponde ao pedido de identificação por parte da entidade. Permitirá reconhecer a origem do pedido através da assinatura digital por um certificado digital x.509v3 associado à entidade;

- **Resposta de Logout** – contém o resultado do Logout efetuado no Autenticação.Gov. Esta mensagem é assinada digitalmente pelo Autenticação.Gov de forma a garantir a integridade da informação.

6 Autenticação com Certificados que não do Cartão de Cidadão

Quando o fornecedor de serviços requisitar a autenticação ou a obtenção de atributos junto do Autenticação.Gov, o utilizador terá de apresentar um certificado válido para proceder à sua autenticação ou recolha de atributos. Todo o mecanismo de autenticação, bem como a lógica de *Single Sing On,* mantém-se para estes certificados.

O Autenticação.Gov será também capaz de autenticar um utilizador num fornecedor de serviços com base em certificados válidos como é exemplo do certificado da Ordem dos Advogados. Nesta vertente o Autenticação.Gov irá proceder à autenticação e obtenção de atributos do utilizador, de forma idêntica ao que é efetuado com o Cartão de Cidadão.

Quando um fornecedor de serviços solicitar atributos terá de especificar quais os atributos e qual o certificado que o utilizador deverá fornecer na autenticação. Por predefinição será usada a cadeia de certificação do Cartão de Cidadão.

À data da edição deste documento são aceites os certificados emitidos ou credenciados pelas seguintes entidades:

1. Cartão de Cidadão
2. Ordem dos Advogados
3. Ordem dos Notários
4. Câmara dos Solicitadores
5. Cartão do CEGER (Centro de Gestão da Rede Informática do Governo)

Apenas o Cartão de Cidadão está apto a fazer uso dos fornecedores de atributos e da Plataforma de Interoperabilidade para a obtenção de atributos que não se encontrem no *chip* do Cartão de Cidadão ou do certificado digital de autenticação.

Outro recurso fornecido pelo Autenticação.Gov consiste em pedido de atributos genéricos. Estes atributos podem ser solicitados pelos fornecedores de serviços sem

especificar o certificado a usar, ficando o utilizador responsável pela escolha do certificado com que pretenda autenticar-se.

6.1 Atributos disponíveis

A seleção do certificado a ser usada é da responsabilidade do portal da entidade, que deverá indicar explicitamente qual a forma de autenticação que pretende que seja usada no Autenticação.Gov. Por sua vez, o Autenticação.Gov irá solicitar ao utilizador a identificação digital correspondente.

Na utilização de certificados que não sejam os do Cartão de Cidadão, encontram-se disponíveis os atributos específicos descritos nos capítulos seguintes.

De realçar que a utilização de outros certificados que não os do Cartão de Cidadão apenas se poderão obter atributos que se encontrem nesse mesmo certificado, não sendo possível a obtenção de atributos via Plataforma de Interoperabilidade.

Ordem dos Advogados

Atributos associados ao certificado digital credenciado pela **Ordem dos Advogados**:

Atributo	Identificador	Descrição
Nome Profissional	http://interop.gov.pt/MDC/Advogado/NomeProfessional	Nome Profissional
Nome Completo	http://interop.gov.pt/MDC/Advogado/NomeCompleto	Nome completo
Número de identificação profissional	http://interop.gov.pt/MDC/Advogado/NOA	Número de identificação na Ordem
Sociedade	http://interop.gov.pt/MDC/Advogado/NomeSociedade	Sociedade que representa

Atributo	Identificador	Descrição
Número de identificação da Sociedade	http://interop.gov.pt/MDC/Advogado/IdentificacaoSociedade	Número de identificação da Sociedade na Ordem
Correio eletrónico profissional	http://interop.gov.pt/MDC/Advogado/CorreioElectronico	Correio eletrónico registado na Ordem
Número de série do certificado digital	http://interop.gov.pt/MDC/Advogado/NumeroSerie	Número de série do certificado digital

Ordem dos Notários

Atributos associados ao certificado digital credenciado pela **Ordem dos Notários**:

Atributo	Identificador	Descrição
Nome próprio	http://autenticacao.cartaodecidadao.gov.pt/atributos/notarios/NomeProprio	Nome próprio
Apelido	http://interop.gov.pt/MDC/Notario/NomeApelido	Apelido
Nome completo	http://interop.gov.pt/MDC/Notario/NomeCompleto	Nome completo
Número de identificação profissional	http://interop.gov.pt/MDC/Notario/NON	Número de identificação profissional na Ordem dos Notários (desprovido do prefixo ONT)
Número mecanográfico da Ordem dos Notários	http://interop.gov.pt/MDC/Notario/NMECON	Número Mecanográfico da Ordem dos Notários (difere do atributo acima pela presença do prefixo ONT)
Nome do cartório	http://interop.gov.pt/MDC/Notario/NomeCartorio	Nome do Cartório onde atua

Atributo	Identificador	Descrição
Distrito do cartório	http://interop.gov.pt/MDC/Notario/DistritoCartorio	Localidade do cartório onde atua
Localidade do cartório	http://interop.gov.pt/MDC/Notario/LocalidadeCartorio	Distrito do cartório onde atua
Correio eletrónico profissional	http://interop.gov.pt/MDC/Notario/CorreioElectronico	Correio eletrónico profissional
Número de série do certificado digital	http://interop.gov.pt/MDC/Notario/NumeroSerie	Número de série do certificado digital

Ordem dos Solicitadores

Atributos associados ao certificado digital credenciado pela **Ordem dos Solicitadores**:

Atributo	Identificador	Descrição
Nome completo	http://interop.gov.pt/MDC/Solicitador/NomeCompleto	Nome completo
Número de identificação profissional	http://interop.gov.pt/MDC/Solicitador/NCS	Número de identificação na Ordem
Correio eletrónico profissional	http://interop.gov.pt/MDC/Solicitador/CorreioElectronico	Correio eletrónico registado na Ordem
Número de série do certificado digital	http://interop.gov.pt/MDC/Solicitador/NumeroSerie	Número de série do certificado digital

Cartão do CEGER

Atributos associados ao certificado digital credenciado pelo **CEGER**:

Atributo	Identificador	Descrição
Nome	http://interop.gov.pt/MDC/ECCE/Nome	Nome do Utilizador
Organismo	http://interop.gov.pt/MDC/ECCE/Organismo	Ministério
Ministério	http://interop.gov.pt/MDC/ECCE/Ministerio	Ministério
País	http://interop.gov.pt/MDC/ECCE/Pais	País
Cargo do titular	http://interop.gov.pt/MDC/ECCE/ CargoDoTitular	Cargo do titular
Nome do Utilizador de Windows 200X	http://interop.gov.pt/MDC/ECCE/MicrosoftUpn	Nome do Utilizador de Windows 200X

6.2 Atributos genéricos

O Autenticação.Gov será capaz de fornecer ou autenticar um utilizador com atributos genéricos perante um fornecedor de serviços. Se existir um pedido por parte do fornecedor de serviços de atributos genéricos, o Autenticação.Gov irá permitir ao utilizador a escolha do certificado para proceder à recolha desses atributos.

Aquando da utilização de atributos genéricos, o atributo "Certificado" (http://interop.gov.pt/MDC/Generico/Certificado) deve ser indicado no pedido de autenticação pelo fornecedor de serviços. Caso não se encontre presente, o Autenticação.Gov irá responder com erro. Este atributo será devolvido na resposta, com indicação do certificado selecionado pelo utilizador para efetuar a autenticação.

A tabela seguinte apresenta os valores disponíveis para utilização no atributo “Certificado”, que deve ser verificado para identificar qual certificado foi usado pelo utilizador na sua autenticação:

Certificado	Resposta Autenticação.Gov
Cartão de Cidadão	Citizen
Advogados	Lawyer
Notários	Notary
Solicitadores	Bailiff

A tabela seguinte mostra os atributos que podem ser fornecidos a partir de qualquer Certificado selecionado pelo utilizador:

Atributo	Identificador	Descrição
Nome do utilizador	http://interop.gov.pt/MDC/Generico/NomeCompleto	Nome profissional do utilizador, presente no certificado digital selecionado.
Número de identificação	http://interop.gov.pt/MDC/Generico/NumeroIdentificacao	Número de identificação do utilizador, presente no certificado digital selecionado.
Número de série do certificado	http://interop.gov.pt/MDC/Generico/NumeroSerie	Número de série identificativo do certificado, presente no certificado digital selecionado.

Os atributos genéricos serão obtidos de acordo com o certificado digital selecionado. Este determina o contexto dos valores destes atributos. Por exemplo, caso seja apresentado um certificado da Ordem dos Advogados, o atributo genérico "Número de Identificação" levará à recolha do atributo que corresponde à identificação do utilizador na Ordem dos Advogados.

O quadro seguinte apresenta a correspondência entre atributos genéricos e as entidades credenciadoras aceites pelo Autenticação.Gov:

Atributo Genérico	Entidade Credenciadora			
	Cartão Cidadão	Advogados	Notários	Solicitadores
Nome do utilizador	Nome Completo	Nome Completo	Nome Completo	Nome Completo

Atributo Genérico	Entidade Credenciadora			
	Cartão Cidadão	Advogados	Notários	Solicitadores
Número de identificação	Número de identificação civil	Número da Ordem dos Advogados	Número da Ordem dos Notários	Número da Ordem dos Solicitadores
Número de série do certificado	Número de série do certificado	Número de série do certificado	Número de série do certificado	Número de série do certificado

7 Grupos de Confiança dos Atributos de Autenticação.Gov

7.1 Significado dos níveis de confiança

Atribui-se a cada atributo de um utilizador num processo de autenticação um nível de confiança para o valor valor obtido. Definem-se quatro níveis de confiança, de 1 a 4, sendo 1 o valor de confiança mínimo e 4 o máximo, para os valores dos atributos obtidos numa autenticação. Quando numa autenticação há mais que um atributo requerido, o nível global de confiança é o nível mínimo entre os níveis do conjunto de atributos obtidos.

Tal diferença de níveis baseia-se na confiança oferecida pela natureza das credenciais usadas numa autenticação bem como no próprio processo da sua obtenção no Autenticação.Gov. Por exemplo, o Cartão de Cidadão é emitido e entregue a um cidadão num processo que envolve a identificação pessoal assim como recolha de dados biométricos; o token criptográfico é suportado em hardware (chip constante no Cartão de Cidadão) com elevada segurança contra tentativas de violação física; o uso de um tal token num processo de autenticação na web oferece uma confiança superior à do clássico desafio utilizador/palavra-passe ou mesmo pela utilização de um certificado de autenticação suportado em ficheiro em software facilmente replicado e sujeito a apropriação indevida, consentida ou não pelo seu dono.

A introdução destes níveis permite oferecer às entidades fornecedoras de serviços a possibilidade de discriminarem o acesso a recursos restritos por nível de confiança. Por exemplo, um portal que tenha na sua área privada de utilizadores uma opção de subscrição de uma *newsletter* poderá aceitar um nível de confiança baixa na autenticidade das credenciais fornecidas pelo utilizador; já numa área em que o utilizador pode subscrever um serviço pago, o mesmo portal pode exigir o uso de credenciais de autenticação forte.

O significado e a metodologia de atribuição de cada um destes valores (1 a 4) será futuramente disponibilizada. Serve para o presente que se definem nas autenticações:

- O valor 4:
  - Autenticação com recurso a uma ou mais operações criptográficas efetuadas no Cartão de Cidadão em autenticação que resulta num conjunto de

informação fornecida ao Autenticação Gov que permite com o maior grau de certeza de que, no momento da autenticação, se utilizou um Cartão de Cidadão real com conhecimento do PIN de autenticação

  - Autenticação com renegociação SSL com certificado cliente da Ordem dos Notários, da Ordem dos Advogados ou da Câmara dos Solicitadores.

- O valor 3:
  - Autenticação com Chave Móvel Digital;
- O valor 2
  - Autenticação com Chavel Móvel Digital através do Twitter;
- O valor 1
  - Autenticação com Utilizador/Palavra-passe (também designado por Autenticação Simples) e Redes Sociais;

7.2 Definição técnica dos níveis de confiança

O Fornecedor de Serviço deve indicar numa extensão SAML o nível mínimo de confiança pretendido para os atributos pedidos.

Essa extensão define-se pela seguinte *schema*:

```
<xs:schema targetNamespace="http://autenticacao.cartaodecidadao.pt/atributos"
       xmlns="http://autenticacao.cartaodecidadao.pt/atributos"
       xmlns:xs="http://www.w3.org/2001/XMLSchema" >
```

```
  <xs:element name="FAAALevel">
    <xs:simpleType>
      <xs:restriction base="xs:integer">
        <xs:minInclusive value="1"/>
        <xs:maxInclusive value="4"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
</xs:schema>
```

Exemplo da extensão para o nível 3:

```
<fa:FAAALevel xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos">3</fa:FAAALevel>
```

Exemplo de um nó das extensões com a lista de atributos e o nível mínimo exigido:

```
<Extensions>
  <fa:RequestedAttributes xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos">
    <fa:RequestedAttribute Name="http://interop.gov.pt/MDC/Cidadao/NIC"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="True" />
    <fa:RequestedAttribute Name="http://interop.gov.pt/MDC/Cidadao/NIF"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="False" />
    <fa:RequestedAttribute Name="http://interop.gov.pt/MDC/Cidadao/Foto"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="False" />
    <fa:RequestedAttribute Name="http://interop.gov.pt/MDC/Cidadao/Morada"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="False" />
  </fa:RequestedAttributes>
  <fa:FAAALevel xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos">3</fa:FAAALevel>
</Extensions>
```

No caso de não ser definido o nível mínimo por não se incluir o nó <FAAALevel/>, assume-se o valor de confiança máximo. Para o exemplo seguinte serão obtidos os atributos disponíveis apenas para o nível 4:

```
<Extensions>
  <fa:RequestedAttributes xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos">
    <fa:RequestedAttribute Name="http://interop.gov.pt/MDC/Cidadao/NIC"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="True" />
  </fa:RequestedAttributes>
</Extensions>
```

Quando ausente a indicação do nível de confiança do Autenticação.Gov mas esteja presente o QAA do Stork, é assumido o nível do Autenticação.Gov correspondente.

```
<Extensions>
  <stork:QualityAuthenticationAssuranceLevel
    xmlns:stork="urn:oasis:names:tc:SAML:2.0:metadata">3</stork:QualityAuthenticationAssuranceLevel>
  <stork:... />
  <fa:RequestedAttributes xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos">
    <fa:RequestedAttribute Name="http://interop.gov.pt/MDC/Cidadao/NIC"
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="True" />
  </fa:RequestedAttributes>
</Extensions>
```

8 Política de Apresentação

8.1 Significado da política de apresentação

Os diferentes mecanismos de autenticação:

- Cartão de Cidadão;
- Chave Móvel Digital;
- Utilizador/Palavra-passe também designado por Autenticação Simples;
- Redes Sociais;

São disponibilizados no Autenticação.Gov através de abas selecionáveis pelo cidadão, em correspondência com o nível de confiança definido pelas entidades fornecedoras de serviço.

A Política de Apresentação permite selecionar gráficamente por indicação da entidade fornecedora do serviço um mecanismo de autenticação de entre os mecanismos de autenticação disponíveis após aplicação do nível de confiança. Assim, sempre que o nível de confiança permite a utilização de múltiplos mecanismos de autenticação, esta extensão permite que o fornecedor de serviço selecione a aba relativa ao mecanismo que prefere utilizar, que iniba a utilização de um ou vários mecanismos através da não exibição da aba respetiva.

A seguinte tabela ilustra as situações possíveis:

Mecanismo de Autenticação	Nível de confiança				Política de apresentação
	1	2	3	4	
Cartão de Cidadão				X	Não é possível estabelecer política de apresentação, só o cartão de cidadão está disponível.
Chave Móvel Digital			X		São exibidas duas abas, relativas ao cartão de cidadão e chave móvel digital, é possível selecionar uma aba e/ou esconder outra.
Chave Móvel Digital - Twitter		X			Situação análoga ao nível de confiança 3.
Autenticação Simples	X[1]				São exibidas três ou quatro abas ([1]conforme disponibilidade da autenticação através de redes sociais), é possível selecionar uma aba e/ou esconder uma, duas ou três abas (se disponíveis quatro).
Redes Sociais	X				São exibidas quatro abas, é possível selecionar uma aba e/ou esconder uma a três abas.

Na situação em que a política de apresentação definida pela entidade fornecedora de serviço é aplicada, se não existir definição para selecionar uma aba, será selecionada a aba que tiver associado o nível de confiança mais elevado do conjunto das abas a exibir.

Em caso de situação de conflito entre o nível de confiança e a política de apresentação ou mesmo conflito na própria política de apresentação, a política de apresentação será ignorada e será utilizada a política de apresentação que priveligia a utilização do mecanismo de autenticação mais seguro (cartão de cidadão).

O mapeamento das abas relativas aos mecanismos de autenticação é o seguinte:

- 'CC' - Aba relativa à autenticação através de Cartão de Cidadão;
- 'CMD' - Aba relativa à autenticação através de Chave Móvel Digital;
- 'UPP' - Aba relativa à autenticação através de Utilizador / Palavra-passe;
- 'RSS' - Aba relativa à autenticação através das Redes Sociais;

8.2 Definição técnica da política de apresentação

O Fornecedor de Serviço pode indicar numa extensão SAML a política de apresentação pretendida para as abas.

Essa extensão define-se pela seguinte *schema*:

```
<xs:schema targetNamespace="http://autenticacao.cartaodecidadao.pt/presentationpolicy"
xmlns="http://autenticacao.cartaodecidadao.pt/presentation" xmlns:xs="http://www.w3.org/2001/
XMLSchema">
  <xs:element name="AuthTabPresentationPolicies">
   <xs:complexType>
    <xs:choice maxOccurs="unbounded">
     <xs:element name="hideAuthTab" type="TabId" maxOccurs="unbounded"/>
     <xs:element name="defaultSelectedAuthTab" type="TabId" maxOccurs="1"/>
    </xs:choice>
   </xs:complexType>
  </xs:element>
  <xs:complexType name="TabId">
   <xs:attribute name="TabId">
    <xs:simpleType>
     <xs:restriction base="xs:string">
```

```
        <xs:enumeration value="CC"/>
        <xs:enumeration value="CMD"/>
        <xs:enumeration value="UPP"/>
        <xs:enumeration value="RSS"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
 </xs:complexType>
</xs:schema>
```

Exemplo:

```
<fa:AuthTabPresentationPolicies
xmlns:fa="http://autenticacao.cartaodecidadao.pt/presentationpolicy">
  <fa:hideAuthTab TabId="CC"/>
  <fa:hideAuthTab TabId="CMD"/>
  <fa:defaultSelectedAuthTab TabId ="UPP"/>
</fa:AuthTabPresentationPolicies>
```

No exemplo acima assume-se que o nível de segurança foi configurado para permitir a exibição da aba relativa à autenticação através de Utilizador / Palavra-passe.

9 UTILIZAÇÃO DE ASSINATURAS DIGITAIS

A utilização da assinatura digital em XML encontra-se totalmente definida nas normas *W3C XML Signature*[3]. Este capítulo evidencia as principais características que o Autenticação.Gov irá usar e que podem ser comprovadas em cada pedido de atributos recebido pelas Entidades.

A forma de assinatura será do tipo *Enveloped* (http://www.w3.org/2000/09/xmldsig#enveloped-signature), que usará o algoritmo SHA-1 (http://www.w3.org/2000/09/xmldsig#rsa-sha1) como forma de *digest*.

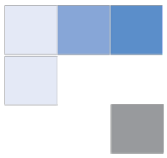
É usado XMLDSIG com *RSA with SHA* como suporte à criação e verificação da assinatura, sendo obrigatório o uso do algoritmo *Exclusive Canonicalization [Excl-C14N]* (http://www.w3.org/TR/2001/REC-xml-c14n-20010315) para normalização do xml a assinar. Não serão usadas outras transformações à exceção da indicação de *Enveloped* e *Exclusive Canonicalization.*

O elemento *X509Data* pertencente a *KeyInfo* conterá informação específica do certificado usado na assinatura (i.e. uma cópia do certificado) e deverá ser usado para a sua validação.

A mensagem seguinte apresenta um exemplo de uma assinatura digital efetuada sobre a mensagem *FAObterAtributos:*

```
<fa:FAObterAtributos xmlns:fa="http://autenticacao.cartaodecidadao.pt/servicos"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://autenticacao.cartaodecidadao.pt/servicos C:\DOCUME~1\Administrator\Desktop\CitizenConsent\
APINTE~2.XSD">
        <fa:IdentificadorCidadao>UjBsR09EbGhjZ0dTQUxNQUFBUUNBRU1tQ1p0dU1GUXhEUzhi</
fa:IdentificadorCidadao>
        <fa:PedidoAtributos>
                <fa:NumeroPedido>ED6F7BBC-1A42-11DF-A5E3-C17D56D89593</fa:NumeroPedido>
                <fa:NomeCidadao>José Manuel Silva</fa:NomeCidadao>
                <fa:PrestadorServicosRequerente>http://www.portaldocidadao.pt</fa:PrestadorServicosRequerente>
                <fa:DataHora>2001-12-17T09:30:47.0Z</fa:DataHora>
                <fa:Atributos>
                        <fa:Atributo Nome="http://autenticacao.cartaodecidadao.pt/atributos/2010/01/cidadao/
NomeCompleto"/>
```

[3] http://www.w3.org/TR/xmldsig-core/



```
                        <fa:Atributo Nome="http://autenticacao.cartaodecidadao.pt/atributos/2010/01/cidadao/NIC"/>
                </fa:Atributos>
                <ds:Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                        <ds:SignedInfo>
                                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315"/>
                                <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                                <ds:Reference URI="">
                                        <ds:Transforms>
                                                <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                        </ds:Transforms>
                                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                        <ds:DigestValue>MWCfrbhhIkxTFAFjWDLz1UsJWUE=</ds:DigestValue>
                                </ds:Reference>
                        </ds:SignedInfo>


<ds:SignatureValue>uVaWld4GEO6W9KFuc2O7HRbukJvsxqvIvjWJXi9XQ2n2kHV9DsKa4MPSVGT5rsAlDPe0oHQdhX7aE
U+oyBX8O1vPHh7LwnDp61D53GrtNcQbPbkRBFpobljuX9UCQlhDJnPNkjFe8EJoeO2Geus02JOkZw+Z0zTgWrk9fRhOevI=</
ds:SignatureValue>
                        <ds:KeyInfo>
                                <ds:X509Data>


<ds:X509Certificate>MIIB8zCCAVwgAwIBAgIQgfzbrIjhLL9FobStI2ub3zANCgYJKoZIhvcNCgEBBAUwEzERMA8GA1UEA
xMIVGVzdGUwHhcNCjAwMDEwMTAwMDAwMFoXDQozNjAxMDEwMDAwMDBaMBMxETAPBgNVBAMTCFRlc3Rl
MIGfMA0KBgkqhkiG9w0KAQEBBQOBjTCBiQKBgc77IBnz+oluFJUf/7bAybOLHeMz8ITFvqxOBqI/
B7rKVweAXjnN5AOrTo5IlkJKezfh6b9Qsg0KZddDf8z0b9uk/2sOGr1pYqsunLLBvw0KhZL1iUA5Icdksw0Kby/
jEZfaTJc1uOJj8rnqg84yOlrIqhZ575O6dohQMTWSv+paWe8CAwEBo0gwRjBEBgNVHQEEPTA7gBCOOHcajwnATYZ0t6w7
LVU0oRUwEzERMA8GA1UEAxMIVGVzdGWCEIH826yI4Sy/
RaG0rSNrm98wDQoGCSqGSIb3DQoBAQQFA4GBBL9Qhi6f1Z+/t8oNClwUBcd1FLDRfTdqOJOqtXNwimWKsdhP4p/
pwESGEXYeZG3i36JouhiMlRXlxMafHK6G9zAMzkDL13/
fgcrns4pjDyBw779Lt5JpniE136Gaxwg8S6FlpREjdaNfKPqe7JKAuu9ORDC0pUiUfCHWxCoqNos=</ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                </ds:Signature>
        </fa:PedidoAtributos>
</fa:FAObterAtributos>
```

10 Especificações Técnicas

A troca de dados com o Autenticação.Gov baseia-se em *Security Assertion Markup Language* (SAML), protocolo que visa garantir a autenticidade e privacidade de todas as transações.
SAML é um padrão baseado em XML que permite aos domínios web uma troca de dados de autenticação e autorização do utilizador de forma segura. Usando SAML, um fornecedor de serviços pode contactar um fornecedor de identidade on-line, para autenticar um utilizador que pretende aceder a um conteúdo protegido.

Além da autenticação do Cartão Cidadão, o Autenticação.Gov suporta a autenticação com certificados da Ordem dos Advogados, Notários e da Câmara dos Solicitadores. O processo de autenticação é o mesmo usado no Cartão de Cidadão português.

O público-alvo deste capítulo são as equipas técnicas que implementam a integração da autenticação com o Autenticação.Gov. As interações entre o Autenticação.Gov e fornecedor de serviço são baseadas em SAML 2.0 e na experiência portuguesa no projeto de identidade eletrónica transfronteiriça STORK (1).

10.1 Configurações

Para que se possa proceder à correta configuração de um portal junto do Autenticação.Gov, é necessário que sejam fornecidos à Agência para a Modernização Administrativa os seguintes dados:

- **CSR (Certificate Signing Request)** para gerar um certificado de utilização exclusiva nos pedidos SAML enviados ao Autenticação.Gov;

- **Identificador do portal** (ou *Issuer*) para efeitos de identificação unívoca no pedido SAML, cujo valor deve refletir o domínio do portal (ex. http://www.portaldocidadao.pt) e que é enviado no nó *<Issuer/>* nas mensagens AuthnRequest;

- **Descritivo institucional ou Designação do organismo** (ou *ProviderName*) para identificação textual *(valor human readable)* a apresentar ao cidadão no Autenticação.Gov (ex. “Portal do Cidadão”);

- **Designado qual o método utilizado para fornecer o endereço de logout que pretende utilizar**:
  - vertente estática - por configuração, sendo necessário providenciar um URL;
  - vertente dinâmica – por indicação no pedido SAML de logout, consultar seção 10.1.1.34 ;

- **Indicado um e-mail para notificações técnicas** - **não utilizar email pessoal**, utilizar email de equipa responsável;

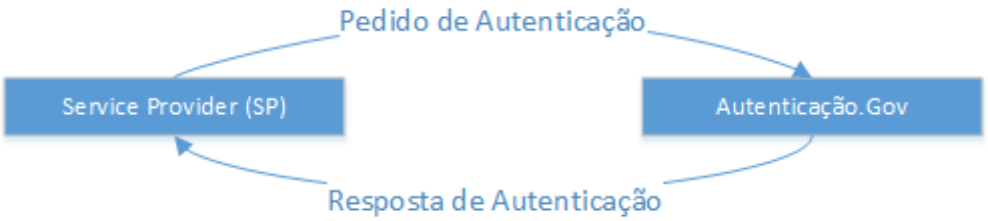
A equipa responsável pelo Autenticação.Gov fornecerá os dados necessários à integração do portal, nomeadamente:

- **Certificado X.509 com a cadeia de certificação**, este certificado permite validar as respostas devolvidas pelo Autenticação.Gov;
- **Certificado X.509 com a cadeia de certificação gerado a partir da CSR (Certificate Signing Request) enviada**, este certificado permitirá ao Autenticação.Gov validar os pedidos SAML enviados pelo fornecedor de serviços;
- **Endereço para receção de pedidos SAML**, para onde devem ser direcionados os pedidos de autenticação:
  - Ambiente de teste: https://preprod.autenticacao.gov.pt/fa/Default.aspx
  - Ambiente de produção: https://autenticacao.gov.pt/fa/Default.aspx

Autenticação

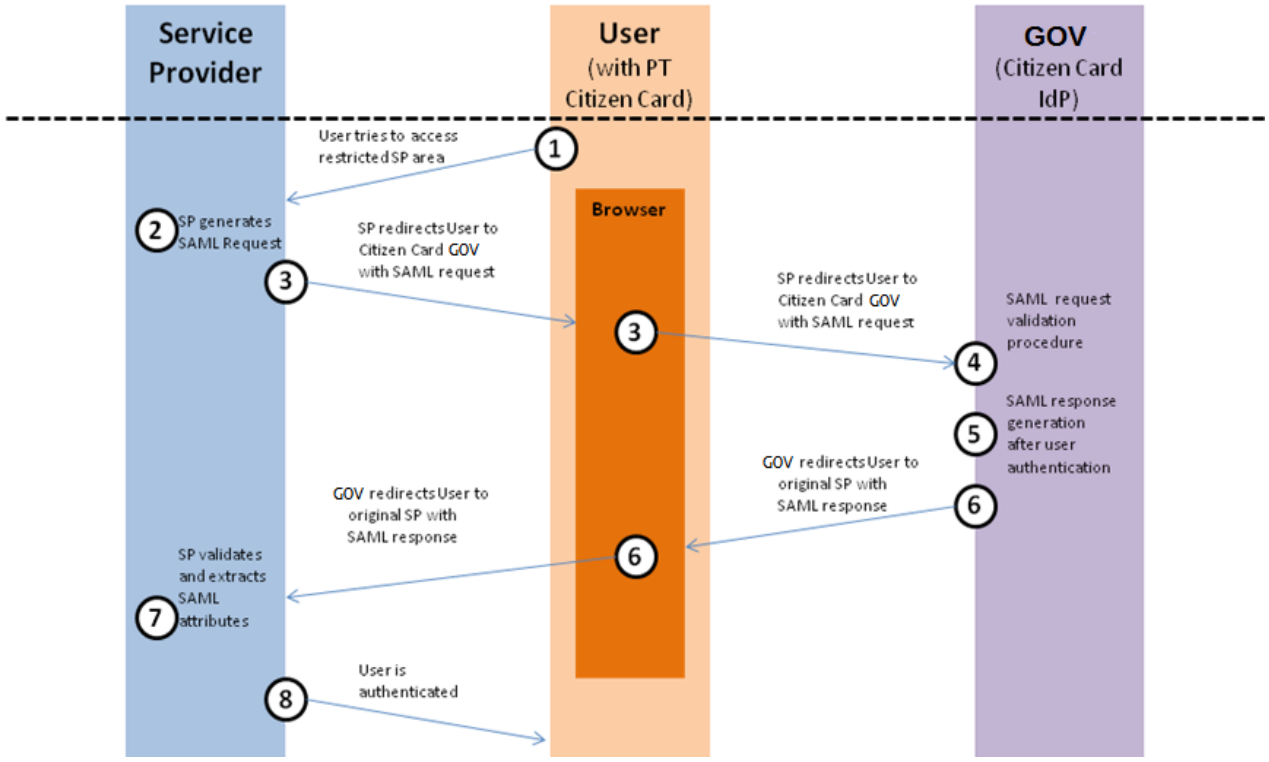
Fluxo de processo

O pedido de autenticação usa SAML 2.0 *Authentication Request Protocol* de acordo com as especificações SAML 2.0. As comunicações entre o *browser* do utilizador e o Autenticação.Gov terão que ser efetuadas sobre SSL V3+ ou TLS 1.0+.



O Autenticação.Gov irá responder ao fornecedor de serviços com a informação de autenticação verificada e confirmada pelo utilizador. Adicionalmente, o Autenticação.Gov irá incluir na resposta os atributos que foram solicitados no pedido de autenticação inicial. A resposta é igualmente sobre SSL V3+ ou TLS 1.0+.

O processo seguinte demonstra a perspetiva do utilizador (User) no acesso a uma área restrita do fornecedor de serviço (Service Provider)s com utilização do Autenticação.Gov (GOV).



O processo de autenticação segue os seguintes passos:

1) Utilizador tenta aceder a área privada, que requer autenticação. O fornecedor de serviços delega a autenticação no Autenticação.Gov;

2) O fornecedor de serviços gera o pedido SAML *AuthnRequest*. Este pedido identifica univocamente o fornecedor de serviços perante o Autenticação.Gov, constante também a lista dos atributos do cidadão necessários à sua identificação. Para além dos dados específicos do SAML, é enviado um parâmetro *RelayState* que o Autenticação.Gov devolve sem qualquer manipulação na resposta (se codificado em base 64, de outra forma não há garantia de que não seja modificado). Este parâmetro pode e deve ser usado para persistência de estado do lado do fornecedor de serviços;

3) O fornecedor de serviços redireciona o utilizador para a página de autenticação do Autenticação.Gov;

4) O Autenticação.Gov valida o pedido SAML, garantindo que o fornecedor de serviços se encontra autorizado a efetuar o processo de autenticação e que todos os dados pressentes no pedido SAML são corretos e válidos temporalmente;

5) O Autenticação.Gov solicita a autorização do utilizador para a obtenção dos dados dos atributos solicitados pelo fornecedor de serviços. Neste passo é também pedida a identificação do cidadão que se autentica com o seu Cartão de Cidadão por meio da execução de uma operação criptográfica que só é possível com o uso do PIN de autenticação. O utilizador tem a possibilidade de confirmar (ou negar) alguns ou todos os atributos solicitados pelo fornecedor de serviços;

6) O Autenticação.Gov gera a resposta SAML *Response* com os atributos solicitados no pedido de autenticação e redireciona o utilizador para o fornecedor de serviços;

7) O fornecedor de serviços é responsável pela validação e extração de atributos da resposta SAML *Response*. Deve garantir a correta interpretação e normalização das credenciais fornecidas pelo Autenticação.Gov para as credenciais internas que lhe permita decidir da autorização de acesso aos recursos pretendidos pelo utilizador.

8) Após conclusão de todo o processo com sucesso é permitido acesso à área restrita.

Todas as mesnsagens SAML são assinados digitalmente. A utilização de assinatura digital irá garantir a integridade da informação e a correta identificação de todos os participantes no processo de autenticação.

10.1.1.1Pedido de autenticação

O modelo de comunicação entre o Fornecedor de Serviços e o Autenticação.Gov baseia-se nos protocolos *SAML 2.0 profiles and bindings*:

- *HTTP Post Binding* (1);
- *Web Browser SSO Profile* (2) (o Autenticação.Gov apenas suporta um conjunto limitado de funcionalidades)

O pedido de autenticação SAML 2.0 é enviado do fornecedor de serviços para o Autenticação.Gov usando o *binding HTTP POST*:

```
<form action="https:// autenticacao.gov.pt/fa/Default..aspx "method="post">
        <input type="hidden" name="SAMLRequest" value="[Base64 encodedAuthentication Request]" />
        <input type="hidden" name="RelayState" value="State information to be persisted across operation" />
</form>
```

Nota: o parâmetro *RelayState* pode e deve ser usado pelo fornecedor de serviços para persistir uma referência opaca da sessão ou do estado no fornecedor de serviços. Não deve exceder os 80 caracteres e deve possuir mecanismos próprios de integridade. Se presente, o Autenticação.Gov irá processar o parâmetro de forma a filtrar eventuais vulnerabilidades. Como consequência desse processamento o Autenticação.Gov poderá devolver o parâmetro alterado ao fornecedor de serviços. Sugere-se a codificação do RelayState em base 64 para evitar alterações indesejadas no RelayState.

10.1.1.2Resposta de autenticação

O modelo de comunicação entre o fornecedor de serviços e o Autenticação.Gov baseiam-se nos protocolos *SAML 2.0 profiles and bindings*:

- *HTTP Post Binding* (1);
- *Web Browser SSO Profile* (2) (Autenticação.Gov apenas suporta um conjunto limitado de funcionalidades)

A resposta ao de autenticação SAML 2.0 é enviada do Autenticação.Gov para o fornecedor de serviços usando o *binding HTTP POST*:

```
<form action=" https://www.FornecedorDeServiços.xx /validar_resposta"method="post">
                    <input type="hidden" name="SAMLResponse" value="[Base64 encodedAuthentication Response]" />
        <input type="hidden" name="RelayState" value="State information persisted across operation" />
</form>
```

Nota: o parâmetro *RelayState* pode e deve ser usado pelo fornecedor de serviços para persistir uma referência opaca da sessão ou do estado no fornecedor de serviços. Não deve exceder os 1000 caracteres e deve possuir mecanismos próprios de integridade. Se presente, o Autenticação.Gov irá processar o parâmetro de forma a filtrar eventuais vulnerabilidades. Como consequência desse processamento o Autenticação.Gov poderá devolver o parâmetro alterado ao fornecedor de serviços. Sugere-se a codificação do RelayState em base 64 para evitar alterações indesejadas no RelayState.

Pedido de autenticação

A especificação SAML 2.0 para pedido de autenticação será usada para solicitar a autenticação do utilizador de qualquer fornecedor de serviços.

Para se permitir o envio de dados adicionais (atributos do cidadão) solicitados no momento da autenticação, são usadas extensões SAML no elemento *<Extensions />* previsto no SAML.
O formato desta lista de atributos está definido nos meta-dados *<fap:RequestedAttributes>* *<fa:RequestedAttribute>* que são usados para esta finalidade. Exemplos são dados posteriormente neste documento.

10.1.1.3<samlp:AuthnRequest>

```
<sequence>
        <element ref="saml:Issuer" minOccurs="0"/>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="samlp:Extensions" minOccurs="0"/>
        <element ref="saml:Subject" minOccurs="0"/>
```

```
        <element ref="samlp:NameIDPolicy" minOccurs="0"/>
        <element ref="saml:Conditions" minOccurs="0"/>
        <element ref="samlp:RequestedAuthnContext" minOccurs="0"/>
        <element ref="samlp:Scoping" minOccurs="0"/>
</sequence>
<attribute name="ID" type="ID" use="required"/>
<attribute name="Version" type="string" use="required"/>
<attribute name="IssueInstant" type="dateTime" use="required"/>
<attribute name="Destination" type="anyURI" use="Opcional"/>
<attribute name="Consent" type="anyURI" use="Opcional"/>
<attribute name="ForceAuthn" type="boolean" use="Opcional"/>
<attribute name="IsPassive" type="boolean" use="Opcional"/>
<attribute name="ProtocolBinding" type="anyURI" use="Opcional"/>
<attribute name="AssertionConsumerServiceIndex" type="unsignedShort"use="Opcional"/>
<attribute name="AssertionConsumerServiceURL" type="anyURI"use="Opcional"/>
<attribute name="AttributeConsumingServiceIndex" type="unsignedShort"use="Opcional"/>

<attribute name="ProviderName" type="string" use="Opcional"/>
```

Atributo	Obrigatório	Valores	Notas
ID	Obrigatório	Tipo de dados xs:ID[4]	A definição de ID[5] (ver nota de rodapé 4) permite o uso de UUID[6] iniciado ou precedido por um dos caracteres permitidos em([7]) (e.g. "_0dec26dd-fc3b-47c6-af9d-1cd38db10c55")
Version	Obrigatório	2.0	Versão SAML
IssueInstant	Obrigatório		UTC como definido em http://www.w3.org/TR/xmlschema-2/#dateTime (ecemplo: 2011-08-09T18:43:09.6882193Z)
Destination	Obrigatório		URI indicando o endereço para onde o pedido SAMLRequest é enviado.[8]
Consent	Opcional	urn:oasis:names:tc:SAML:2.0:consent:unspecified	

[4] Definido em http://www.w3.org/TR/xmlschema-2/#ID, garantindo as proprieades referidas em http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf 1.3.4 ID and ID ReferenceValues

[5] Definição de ID no protocolo SAML em http://www.w3.org/TR/xmlschema-2/#ID e http://www.w3.org/TR/1999/REC-xml-names-19990114/#NT-NCName

[6] Internet Engeneering Task Force RFC4112 (http://www.ietf.org/rfc/rfc4122.txt)

[7] http://www.w3.org/TR/REC-xml/#NT-Lette

[8] http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf 3.2.1 Complex Type RequestAbstractType

Atributo	Obrigatório	Valores	Notas
ForceAuthn	Obrigatório	true	The user must be actively authenticated by the Autenticação.Gov
IsPassive	Obrigatório	False	Passive authentication is not permitted
ProtocolBinding	Obrigatório	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST	Currently only HTTP-Post binding is supported
AssertionConsumerServiceIndex	Não usado		This is unsupported and its use will result in an urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported
AssertionConsumerServiceURL	Obrigatório		URL to which Authentication Response must be sent. This must be via a secure SSL connection i.e. Https
AttributeConsumingServiceIndex	Não usado		This is unsupported and its use will result in an urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported
ProviderName	Obrigatório		Human readable name of the original service provider requesting the authentication. This value will be mutually agreed in the connection proposal phase between the SP and the Autenticação.Gov.[9]

10.1.1.4<samlp:issuer>

```
<element name="Issuer" type="saml:NameIDType"/>
<complexType name="NameIDType">
        <simpleContent>
                <extension base="string">
                        <attributeGroup re|="saml:IDNameQualifiers"/>
                        <attribute name="Format" type="anyURI" use="Opcional"/>
                        <attribute name="SPProvidedID" type="string" use="Opcional"/>
                </extension>
        </simpleContent>
</complexType>
```

9 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf 3.2.1 Complex Type RequestAbstractType

Obrigatoriedade: Obrigatório

O elemento <*Issuer*> contém um URI que identifica o Fornecedor de Serviços e deve ser mutuamente acordada com o Autenticação.Gov.

Atributo	Obrigatório	Valores	Notas
NameQualifier	Não usado		The security domain that qualifies that name.
SPNameQualifier	Não usado	2.0	Qualifying the name with a name of a service provider.
Format	Opcional		URI representing the classification of the identifier. Default is urn:oasis:names:tc:SAML:2.0:nameid-format:entity.
SPProvidedID	Não usado		Name identifier if different from the name in the contents of the element.

10.1.1.5<ds:signature>

Obrigatoriedade: Obrigatório

A assinatura digital XML autentica o fornecedor de serviços e garante a integridade da mensagem (sobre todo o pedido de autenticação). A assinatura deve ser uma *enveloped signature* e aplicada ao elemento <samlp:AuthnRequest> e todos os seus filhos.

A assinatura deve conter um único elemento <ds:Reference> contendo o valor do atributo ID do elemento <samlp:AuthnRequest>. <ds:Signature> encontra-se definida em http://www.w3.org/TR/xmldsig-core/#sec-Reference. O valor do atributo URI em <ds:Reference> terá que conter o mesmo valor do ID do documento em < samlp:AuthnRequest>, procedido do carácter '#'[10] (e.g. <Reference URI="#_2e19be9c-37bc-475c-93fd-b05e1970ba4d">...)

[10] http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf - 5.4.2 References

10.1.1.6<samlp:extensions>

Obrigatoriedade: Obrigatório

Este elemento contém uma extensão para o padrão SAML 2.0 pedido de autenticação. No Autenticação.Gov essas extensões incluem:

- Um elemento <*RequestedAttributes*> opcional para permitir o pedido de atributos adicionais;

Todos os atributos estendidos no Autenticação.Gov serão identificados no âmbito do *namespace* "http://autenticacao.cartaodecidadao.pt/atributos".

<fa:RequestedAttributes>

Obrigatoriedade: Obrigatório

Este elemento contém um ou mais <*fa:RequestedAttribute*>. O uso deste é o que permite solicitar ao Autenticação.Gov os atributos a serem adicionados à resposta de autenticação.

< fa:RequestedAttribute>

```
<complexType name="RequestedAttributeType">
        <sequence>
                <element ref="saml:AttributeValue" minOccurs="0" maxOccurs="unbounded"/>
        </sequence>
        <attribute name="Name" type="string" use="required"/>
        <attribute name="NameFormat" type="anyURI" use="Opcional"/>
        <attribute name="FriendlyName" type="string" use="Opcional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
        <attribute name="isRequired" type="boolean" use="Opcional"/>

</complexType>
```

Obrigatoriedade: Obrigatório

Um elemento <fa*:RequestedAttribute*> é necessário para cada atributo solicitado ao Autenticação.Gov no decurso de uma autenticação.

Atributo	Obrigatório	Valores	Notas
Name	Obrigatório		Agreed name of attribute required
NameFormat	Obrigatório		Agreed format of attribute required
FriendlyName	Opcional		A friendly name for the attribute that can be displayed to a user e.g. when requesting confirmation to send to SP. The friendly name should be in Portuguese.
isRequired	Opcional	boolean value	Indicates if the attribute is Obrigatório for the SP authentication purpose.

<saml:AttributeValue>

Obrigatoriedade: Opcional

O elemento *<saml:AttributeValue>* permite que o SP indique que o atributo pedido deve ter um dos valores especificados ou seja, retornar apenas este atributo se o valor deste atributo é um dos valores solicitados.

10.1.1.7<saml:Subject>

Obrigatoriedade: Não usado

10.1.1.8<saml:NameIdPolicy>

```
<element name="NameIDPolicy" type="samlp:NameIDPolicyType"/>
<complexType name="NameIDPolicyType">
        <attribute name="Format" type="anyURI" use="Opcional"/>
        <attribute name="SPNameQualifier" type="string" use="Opcional"/>
        <attribute name="AllowCreate" type="boolean" use="Opcional"/>
</complexType>
```

Obrigatoriedade: Opcional

Pedidos de formatos específicos e qualificação para o identificador que representa o sujeito - Nota: o elemento <*NameIdPolicy*> na resposta pode não ter os formatos específicos solicitados e qualificadores.

Atributo	Obrigatório	Valores	Notas
Format	Não usado		A URI defining the requested format of the NameId in the Response. Autenticação.Gov will not use NameId to contain the user's eId, it will be a separate attribute.
SPNameQualifier	Não usado		Requests that the assertion's subject identifier be returned in the namespace other than the requestor's.
AllowCreate	Não usado		Allows the SAML responder to create a new identifier for the subject.

10.1.1.9<saml:Conditions>

Obrigatoriedade: Não usado

10.1.1.10<samlp:RequestedAuthnContext>

Obrigatoriedade: Não usado

10.1.1.11<samlp:Scoping>

Obrigatoriedade: Não usado

<samlp:IDPList>

Obrigatoriedade: Não usado

<samlp:RequesterID>

Obrigatoriedade: Não usado

10.1.1.12 Exemplo de pedido de autenticação

```
<samlp:AuthnRequest
                ID="_1e736a31-a41c-4c35-b17f-0f9ab4c741b3"
                Version="2.0"
                IssueInstant="2011-02-17T11:15:24Z"
                Destination="https://autenticacao.gov.pt/fa/default.aspx"
                ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                AssertionConsumerServiceURL="https://www.ServiceProvider.pt/HandleRequest"
                ProviderName="Service Provider Name"
                xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
        <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://www.ServiceProvider.pt</
saml:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <Reference URI="#_1e736a31-a41c-4c35-b17f-0f9ab4c741b3">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                                <InclusiveNamespaces PrefixList="#default samlp saml ds xs
xsi" xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                        </Transform>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <DigestValue>oypLiC5MkXdKFbs0pA25Z/mt4jk=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>...signatureValue...</SignatureValue>
                <KeyInfo>
                        <X509Data>
                                <X509Certificate>...x509Data...</X509Certificate>
                        </X509Data>
                </KeyInfo>
        </Signature>
        <samlp:Extensions>
                <fa:RequestedAttributes xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos">
                        <fa:RequestedAttribute Name=" http://interop.gov.pt/MDC/Cidadao/NomeCompleto"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
                </fa:RequestedAttributes>
        </samlp:Extensions>
</samlp:AuthnRequest>
```

Resposta de autenticação

```
<sequence>
        <element ref="saml:Issuer" minOccurs="0"/>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="samlp:Extensions" minOccurs="0"/>
        <element ref="samlp:Status"/>
        <choice minOccurs="0" maxOccurs="unbounded">
                <element ref="saml:Assertion"/>
                <element ref="saml:EncryptedAssertion"/>
        </choice>
</sequence>
<attribute name="ID" type="ID" use="required"/>
<attribute name="InResponseTo" type="NCName" use="Opcional"/>
<attribute name="Version" type="string" use="required"/>
<attribute name="IssueInstant" type="dateTime" use="required"/>
<attribute name="Destination" type="anyURI" use="Opcional"/>

<attribute name="Consent" type="anyURI" use="Opcional"/>
```

Obrigatoriedade: Obrigatório

Atributo	Obrigatório	Valores	Notas
ID	Obrigatório	Tipo de dados xs:ID[11]	A definição de ID[12] (ver nota de rodapé 4) permite o uso de UUID[13] iniciado ou precedido por um dos caracteres permitidos em([14]) (e.g. "_0dec26dd-fc3b-47c6-af9d-1cd38db10c55")
InResponseTo	Obrigatório		The identifier (ID) of the request this response refers to.
Version	Obrigatório	2.0	
IssueInstant	Obrigatório		UTC Date & time when the response was issued.
Destination	Obrigatório		URI reference of the SP SAML Response processor this response is being sent to. Should be the same

[11] Definido em http://www.w3.org/TR/xmlschema-2/#ID, garantindo as proprieades referidas em http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf 1.3.4 ID and ID ReferenceValues

[12] Definição de ID no protocolo SAML em http://www.w3.org/TR/xmlschema-2/#ID e http://www.w3.org/TR/1999/REC-xml-names-19990114/#NT-NCName

[13] Internet Engeneering Task Force RFC4112 (http://www.ietf.org/rfc/rfc4122.txt)

[14] http://www.w3.org/TR/REC-xml/#NT-Lette

Atributo	Obrigatório	Valores	Notas
			as AssertionConsumerServiceURL in the associated Authentication Request.
Consent	Opcional	urn:oasis:names:tc:SAML:2.0:consent:obtained urn:oasis:names:tc:SAML:2.0:consent:prior urn:oasis:names:tc:SAML:2.0:consent:curent-implicit urn:oasis:names:tc:SAML:2.0:consent:curent-explicit urn:oasis:names:tc:SAML:2.0:consent:unspecified	Defines the type of user consent obtained from the user for this authentication and data transfer.

10.1.1.13<saml:Issuer>

```
<element name="Issuer" type="saml:NameIDType"/>
<complexType name="NameIDType">
        <simpleContent>
                <extension base="string">
                        <attributeGroup ref="saml:IDNameQualifiers"/>
                        <attribute name="Format" type="anyURI" use="Opcional"/>
                        <attribute name="SPProvidedID" type="string" use="Opcional"/>
                </extension>
        </simpleContent></complexType>
```

Obrigatoriedade: Obrigatório

O elemento *<Issuer>* contém um URI que identifica o SP e deve ser mutuamente acordada com o Autenticação.Gov.

Atributo	Obrigatório	Valores	Notas
NameQualifier	Não usado		The security domain that qualifies that name.
SPNameQualifier	Não usado		Qualifying the name with a name of a service provider.
Format	Opcional	urn:oasis:names:tc:SAML:2.0:nameidformat:entity	URI representing the classification of the identifier. Default is urn:oasis:names:tc:SAML:2.0:nameid-format:entity.
SPProvidedID	Não usado		Name identifier if different from the name in the contents of the element.

10.1.1.14<ds:Signature>

Obrigatoriedade: Não usado

10.1.1.15<samlp:Extensions>

Obrigatoriedade: Não usado

10.1.1.16<samlp:Status>

```
<element name="Status" type="samlp:StatusType"/>
<complexType name="StatusType">
        <sequence>
                <element ref="samlp:StatusCode"/>
                <element ref="samlp:StatusMessage" minOccurs="0"/>
                <element ref="samlp:StatusDetail" minOccurs="0"/>
        </sequence>
</complexType>

<element name="StatusCode" type="samlp:StatusCodeType"/>
<complexType name="StatusCodeType">
```

```
        <sequence>
                <element ref="samlp:StatusCode" minOccurs="0"/>
        </sequence>
        <attribute name="Value" type="anyURI" use="required"/>
</complexType>

<element name="StatusMessage" type="string"/>

<element name="StatusDetail" type="samlp:StatusDetailType"/>
<complexType name="StatusDetailType">
        <sequence>
                <any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </sequence>

</complexType>
```

Obrigatoriedade: Obrigatório

<samlp:StatusCode>

Obrigatoriedade: Obrigatório

Atributo	Obrigatório	Valores	Notas
value	Obrigatório	Values of section 3.2.2.2 in (OASIS Consortium, 2005)	A URI reference representing the status code value.

Especifica um conjunto de códigos de estado opcional e um valor de atributo que representa o estado do Pedido de Autenticação.

Uma lista de códigos de estados são definidos pela OASIS em SAML 2.0 e estes serão adotadas sempre que pertinente. Adicionalmente são usados códigos para situações específicas Autenticação.Gov.

O código de *status* será composto de dois elementos:

- Código de primeiro nível, indicando o estado da operação de autenticação. Este estado é incluído como um URI no atributo "Valor" do elemento <*samlp:StatusCode*>:

- Um código de status subordinado que fornece informações mais específicas sobre uma condição de erro. Este estado é incluído como um elemento filho <*samlp:StatusCode*>.

O estado de primeiro nível é obrigatório. O código de estado subordinado também é obrigatório se o erro produzido durante a operação de Autenticação.Gov for coberto por um dos códigos de estado subordinado a seguir definidos. Caso contrário é opcional.

Os valores para os dois níveis de códigos de estado estão listadas abaixo. Para mais informações, consulte a especificação SAML 2.0 (OASIS Consortium, 2005).

a) Estados de primeiro nível:

a. *urn:oasis:names:tc:SAML:2.0:status:Success* **–** Operação efetuada com sucesso..

b. *urn:oasis:names:tc:SAML:2.0:status:Requester* **–** Operação não efetuada devido a uma falha do fornecedor de serviços.

c. *urn:oasis:names:tc:SAML:2.0:status:Responder* **-** Operação não efetuada devido a uma falha por parte do Autenticação.Gov.

b) Estados subordinados:

a. *urn:oasis:names:tc:SAML:2.0:status:AuthnFailed* **–** Autenticação do utilizador falhou ou não foi realizada com sucesso.

b. *urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue* **–** Valor ou conteúdo inválido no pedido de atributos associados aos elementos <saml:Attribute> ou<saml:AttributeValue>.

c. *urn:oasis:names:tc:SAML:2.0:status:RequestDenied* **–** O Autenticação.Gov encontra-se funcional, mas optou por não

responder ao pedido de autenticação. Este código pode ser usado sempre que existe uma falha em validações de segurança associadas ao pedido SAML ou ao próprio fornecedor de serviços.

<samlp:Status-Message>

Obrigatoriedade: Opcional

Explica o valor de estado em termos percetíveis. A tabela abaixo define as mensagens de estado em português (e inglês para o contexto).
Se o código de estado subordinado é incluído na resposta, então a mensagem de estado deve ser o correspondente ao código de estado subordinado, e não o código de estado de primeiro nível.

Código Retorno	Mensagem (PT)	Mensagem (EN)
urn:oasis:names:tc:SAML:2.0:status:Success	-	-
urn:oasis:names:tc:SAML:2.0:status:Requester	O pedido não pode ser executado devido a um erro no pedido SAML proveniente do SP, identificado pelo seu URI	The request could not be performed due to an error on the SAML requester side (SP) identified by its URI.
urn:oasis:names:tc:SAML:2.0:status:Responder	O pedido não pode ser executado devido a um erro no pedido SAML no Autenticação.Gov, identificado pelo seu URI	The request could not be performed due to an error on the SAML responder side (Autenticação.Gov) identified by its URI.
urn:oasis:names:tc:SAML:2.0:status:AuthnFailed	Não foi possível autenticar o Cidadão (ou Utilizador)	It was unable to successfully authenticate the user
urn:oasis:names:tc:SAML:2.0:status:InvalidAttrNameOrValue	Conteúdo inválido ou não esperado nos elementos <saml:Attribute> ou <saml:AttributeValue>	Unexpected or invalid content was encountered within a <saml:Attribute> or <saml:AttributeValue> element
urn:oasis:names:tc:SAML:2.0:s	O pedido não foi	The request has not been

Código Retorno	Mensagem (PT)	Mensagem (EN)
tatus:RequestDenied	processado	processed.

<samlp:Status-Detail>

Obrigatoriedade: Não usado

10.1.1.17<saml:Assertion>

Obrigatoriedade: Obrigatório

A resposta de uma autenticação SAML deve conter o elemento <*Assertion*>.. O elemento <*Assertion*> conterá um único elemento <*Subject*> indicando ao utilizador qual a <*Assertion*> que o relaciona. Irá também conter um único elemento <*AuthnStatement* > contendo os resultados da autenticação de utilizador e um único elemento <*AttributeStatement*> contendo zero ou mais elementos <*attribute*>. Uma descrição detalhada do elemento <*Assertion*> é dada na secção abaixo.

10.1.1.18<saml:EncryptedAssertion>

Obrigatoriedade: Não usado

O Autenticação.Gov não implementa asserções cifradas dado que as comunicações já se baseiam num canal cifrado sobre SSL V3+ ou TLS v1.0+.

10.1.1.19Exemplo de resposta de autenticação

```
<saml2p:Response
                    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                    xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos"
                    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
                    ID="_0314efee-a385-4ca9-afab-4bffbb6a788b"
                    InResponseTo="_1e736a31-a41c-4c35-b17f-0f9ab4c741b3"
                    Version="2.0"
                    IssueInstant="2011-02-17T11:17:14.6349444Z"
                    Destination="https://www.ServiceProvider.pt/HandleResponse"
                    Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified">
    <saml2:Issuer>https://autenticacao.cartaodecidadao.pt</saml2:Issuer>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
```

```
                    <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <Reference URI="#_0314efee-a385-4ca9-afab-4bffbb6a788b">
                            <Transforms>
                                <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                                <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                            </Transforms>
                            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                            <DigestValue>qqC76JmDP+2i1s0oxY8EsSD4tic=</DigestValue>
                        </Reference>
                    </SignedInfo>
                    <SignatureValue>...signatureValue...</SignatureValue>
                    <KeyInfo>
                        <X509Data>
                            <X509Certificate>...x509Data...</X509Certificate>
                        </X509Data>
                    </KeyInfo>
                </Signature>
                <saml2p:Status>
                    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
                </saml2p:Status>
                <saml2:Assertion Version="2.0" ID="_b1c88f11-50fd-4a22-988e-9ce4573049e0" IssueInstant="2011-02-
17T11:17:14.6349444Z">
                    …
                </saml2:Assertion>

</saml2p:Response>
```

SAML Assertion

Uma asserção SAML é um pacote de informações de segurança. Especifica que essa afirmação foi emitida por uma entidade num determinado momento e atesta a identidade da entidade da mesma, desde que as condições especificadas de validação tenham sido satisfeitas.

10.1.1.20<saml:Assertion>

```
<element name="Assertion" type="saml:AssertionType"/>
<complexType name="AssertionType">
        <sequence>
            <element ref="saml:Issuer"/>
            <element ref="ds:Signature" minOccurs="0"/>
            <element ref="saml:Subject" minOccurs="0"/>
            <element ref="saml:Conditions" minOccurs="0"/>
            <element ref="saml:Advice" minOccurs="0"/>
            <choice minOccurs="0" maxOccurs="unbounded">
```

```
                    <element ref="saml:Statement"/>
                    <element ref="saml:AuthnStatement"/>
                    <element ref="saml:AuthzDecisionStatement"/>
                    <element ref="saml:AttributeStatement"/>
                </choice>
        </sequence>
        <attribute name="Version" type="string" use="required"/>
        <attribute name="ID" type="ID" use="required"/>
        <attribute name="IssueInstant" type="dateTime" use="required"/>

</complexType>
```

Obrigatoriedade: Obrigatório

Atributo	Obrigatório	Valores	Notas
ID	Obrigatório	Tipo de dados xs:ID[15]	A definição de ID[16] (ver nota de rodapé 4) permite o uso de UUID[17] iniciado ou precedido por um dos caracteres permitidos em([18]) (e.g. "_0dec26dd-fc3b-47c6-af9d-1cd38db10c55")
Version	Obrigatório	2.0	SAML Version
IssueInstant	Obrigatório		UTC date & time assertion was issued

10.1.1.21<saml:Issuer>

```
<element name="Issuer" type="saml:NameIDType"/>
<complexType name="NameIDType">
        <simpleContent>
                <extension base="string">
                    <attributeGroup ref="saml:IDNameQualifiers"/>
                    <attribute name="Format" type="anyURI" use="Opcional"/>
                    <attribute name="SPProvidedID" type="string" use="Opcional"/>
                </extension>
        </simpleContent>
</complexType>
```

Obrigatoriedade: Obrigatório

[15] Definido em http://www.w3.org/TR/xmlschema-2/#ID, garantindo as proprieades referidas em http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf 1.3.4 ID and ID ReferenceValues

[16] Definição de ID no protocolo SAML em http://www.w3.org/TR/xmlschema-2/#ID e http://www.w3.org/TR/1999/REC-xml-names-19990114/#NT-NCName

[17] Internet Engeneering Task Force RFC4112 (http://www.ietf.org/rfc/rfc4122.txt)

[18] http://www.w3.org/TR/REC-xml/#NT-Lette

Este elemento identifica a entidade que gerou o <*saml:Assertion*>. O elemento <*saml:Issuer*> é obrigatório dentro de um <*saml:Assertion*> e contém um valor de *string* (URI), referindo-se à entidade emissora.
O elemento <*Issuer*> deve conter um URI que identifica o Autenticação.Gov emissor. Este URI deve ser mutuamente acordado com o fornecedor de serviços consumidor de asserções. Este valor mantém-se para qualquer resposta fornecida pelo Autenticação.Gov.

Atributo	Obrigatório	Valores	Notas
NameQualifier	Não usado		The security domain that qualifies that name.
SPNameQualifier	Não usado		Qualifying the name with a name of a service provider.
Format	Opcional	urn:oasis:names:tc:SAML:2.0:nameidformat:entity	URI representing the classification of the identifier. Default is urn:oasis:names:tc:SAML:2.0:nameid-format:entity.
SPProvidedID	Não usado		Name identifier if different from the name in the contents of the element.

10.1.1.22<ds:Signature>

Obrigatoriedade: Opcional

Se o *HTTP POST Binding* é usado, a asserção SAML terá que estar assinada.

A assinatura digital XML autentica o fornecedor de serviços e garante a integridade da mensagem (sobre todo o pedido de autenticação). A assinatura deve ser uma *enveloped signature* e aplicada ao elemento <*samlp:AuthnRequest*> e todos os seus filhos.
A assinatura deve conter um único elemento <ds:Reference> contendo o valor do atributo ID do elemento <samlp:AuthnRequest>. O formato de <ds:Signature>

encontra-se definido em http://www.w3.org/TR/xmldsig-core/#sec-Reference. O valor do atributo URI em <ds:Reference> terá que conter o mesmo valor do ID do documento em < samlp:AuthnRequest>, procedido do carácter '#'[19] (e.g. <Reference URI="#_2e19be9c-37bc-475c-93fd-b05e1970ba4d">...).
Obrigatoriamente são aplicadas as transformações *enveloped-signature* (http://www.w3.org/2000/09/xmldsig#enveloped-signature) e *exclusive XML canonicalization* (http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/) e apenas estas.

10.1.1.23<saml:Subject>

```
<complexType name="SubjectType">
        <choice>
                <sequence>
                        <choice>
                                <element ref="saml:BaseID"/>
                                <element ref="saml:NameID"/>
                                <element ref="saml:EncryptedID"/>
                        </choice>
                        <element ref="saml:SubjectConfirmation" minOccurs="0" maxOccurs="unbounded"/>
                </sequence>
                <element ref="saml:SubjectConfirmation" maxOccurs="unbounded"/>
        </choice>
</complexType>
```

Obrigatoriedade: Obrigatório

Indica a quem as asserções são dirigidas. No contexto do Autenticação.Gov apenas o element *<saml:NameID>* será suportado.

<saml:NameId>

Obrigatoriedade: Obrigatório

Reprensenta o sujeito.

Atributo	Obrigatório	Valores	Notas
NameQualifier	Obrigatório		Security or Admin Domain that qualifies the name.

[19] http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf - 5.4.2 References

Atributo	Obrigatório	Valores	Notas
			This should be the namespace of the Autenticação.Gov.
SPNameQualifier	Opcional		Further qualifies the name with a [group of] Service Provider. This should be the namespace of the original Service Provider
Format	Obrigatório	urn:oasis:names:tc:SAML:2.0:nameidformat:unspecified	A URI defining the format of the NameId. The User's eID is provided in a separate attribute. NameId should not be used to assert the subject's identity but may be used to assert return visits from a user using the same authentication.
SPProvidedID	Não usado		Name identifier if different from the name in the contents of the element.

<saml:EncryptedID>

Obrigatoriedade: Não usado

<xenc:EncryptedData>

Obrigatoriedade: Não usado

<xenc:EncryptedKey>

Obrigatoriedade: Não usado

<saml:SubjectConfirmation>

```
<complexType name="SubjectConfirmationType">
        <sequence>
                <choice minOccurs="0">
                        <element ref="saml:BaseID"/>
                        <element ref="saml:NameID"/>
                        <element ref="saml:EncryptedID"/>
                </choice>
                <element ref="saml:SubjectConfirmationData" minOccurs="0"/>
        </sequence>
        <attribute name="Method" type="anyURI" use="required"/>
</complexType>
```

Obrigatoriedade: Obrigatório

Atributo	Obrigatório	Valores	Notas
Method	Obrigatório	urn:oasis:names:tc:SAML:2.0:cm:bearer	Bearer is mandatory to allow in one SubjejctConfirmation to support the Browser SSO profile.

<saml:BaseId>, <saml:NameId>, <saml:EncryptedID>

Obrigatoriedade: Não usado

<saml:SubjectConfirmationData>

```
<complexType name="SubjectConfirmationDataType" mixed="true">
        <complexContent>
                <restriction base="anyType">
                        <sequence>
                                <any namespace="##any" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
                                <element ref="ds:KeyInfo" minOccurs="0"/>
                        </sequence>
                        <attribute name="NotBefore" type="dateTime" use="Opcional"/>
                        <attribute name="NotOnOrAfter" type="dateTime" use="Opcional"/>
                        <attribute name="Recipient" type="anyURI" use="Opcional"/>
                        <attribute name="InResponseTo" type="NCName" use="Opcional"/>
                        <attribute name="Address" type="string" use="Opcional"/>
                        <anyAttribute namespace="##other" processContents="lax"/>
                </restriction>
        </complexContent>
</complexType>
```

Obrigatoriedade: Obrigatório

Atributo	Obrigatório	Valores	Notas
NotBefore	Opcional		Not allowed under Browser SSO Profile i.e. where SubjectConfirmation method is bearer.
NotOnOrAfter	Obrigatório		Subject cannot be confirmed on or after this time.

Atributo	Obrigatório	Valores	Notas
			If SubjectConfirmation method is holder-of-key then this value must be less than or equal to the NotBefore attribute in the X.509 certificate.
Recipient	Obrigatório		URI reference of the SP this assertion is being sent to. This should be the same value as the AssertionConsumerServiceURL attribute in the Authentication Request
InResponseTo	Obrigatório		Id of the Request that requested this assertion
Address	Opcional		IP address of user that this assertion was issued to. Obrigatório for bearer SubjectConfirmation method as it allows Relying Parties to mitigate against a Man-In-The-Middle.

<ds:KeyInfo>

```
<element name="KeyInfo" type="ds:KeyInfoType"/>
<complexType name="KeyInfoType" mixed="true">
        <choice maxOccurs="unbounded">
                <element ref="ds:KeyName"/>
                <element ref="ds:KeyValue"/>
                <element ref="ds:RetrievalMethod"/>
                <element ref="ds:X509Data"/>
                <element ref="ds:PGPData"/>
                <element ref="ds:SPKIData"/>
                <element ref="ds:MgmtData"/>
                <any processContents="lax" namespace="##other"/>
        </choice>
        <attribute name="Id" type="ID" use="Opcional"/>
</complexType>
```

<ds:KeyInfo> encontra-se definido em XML Signature (W3C Consortium, 2009).

Obrigatoriedade: Opcional

Atributo	Obrigatório	Valores	Notas
ID	Não		

Atributo	Obrigatório	Valores	Notas
	usado		

10.1.1.23.1.1

<ds:X509Data>

Obrigatoriedade: Não usado

10.1.1.24<saml:Conditions>

```
<complexType name="ConditionsType">
        <choice minOccurs="0" maxOccurs="unbounded">
                <element ref="saml:Condition"/>
                <element ref="saml:AudienceRestriction"/>
                <element ref="saml:OneTimeUse"/>
                <element ref="saml:ProxyRestriction"/>
        </choice>
        <attribute name="NotBefore" type="dateTime" use="Opcional"/>
        <attribute name="NotOnOrAfter" type="dateTime" use="Opcional"/>
</complexType>
```

Obrigatoriedade: Obrigatório

Este elemento especifica as condições que devem ser validadas quando se utiliza o elemento <*Assertion*>. Essas condições devem ser as mesmas que as condições especificadas no pedido <*AuthnRequest*>.

Atributo	Obrigatório	Valores	Notas
NotBefore	Obrigatório		Assertion not valid before this time
NotOnOrAfter	Obrigatório		Assertion not valid on or after this time

10.1.1.25<saml:Condition>

Obrigatoriedade: Não usado

10.1.1.26<saml:AudienceRestriction>

```
<complexType name="AudienceRestrictionType">
        <complexContent>
                <extension base="saml:ConditionAbstractType">
                        <sequence>
                                <element ref="saml:Audience" maxOccurs="unbounded"/>
                        </sequence>
                </extension>
        </complexContent>
</complexType>
```

Obrigatoriedade: Obrigatório

Restringe a audiência desta asserção para o fornecedor de serviços e contém a referência URI para o qual está a ser enviado.

<saml:Audience>

```
<element name="Audience" type="anyURI"/>
```

Obrigatoriedade: Obrigatório

<saml:OneTimeUse>

Obrigatoriedade: Obrigatório

Define que esta asserção tem que ser utilizada de imediato e não pode ser mantida para uso futuro.

<saml:ProxyRestrictions>

Obrigatoriedade: Não usado

10.1.1.27<saml:Advice>

Obrigatoriedade: Não usado

10.1.1.28<saml:AuthnStatement>

```
<complexType name="AuthnStatementType">
        <complexContent>
                <extension base="saml:StatementAbstractType">
                        <sequence>
                                <element ref="saml:SubjectLocality" minOccurs="0"/>
                                <element ref="saml:AuthnContext"/>
                        </sequence>
```

```
                    <attribute name="AuthnInstant" type="dateTime" use="required"/>
                    <attribute name="SessionIndex" type="string" use="Opcional"/>
                    <attribute name="SessionNotOnOrAfter" type="dateTime" use="Opcional"/>
                </extension>
            </complexContent>
</complexType>
```

Obrigatoriedade: Obrigatório

Atributo	Obrigatório	Valores	Notas
AuthnInstant	Obrigatório		Date & Time User was actually authenticated
SessionIndex	Opcional		Index of the User's Autenticação.Gov session. Allow for increased interoperability with other profiles.
SessionNotOnOrAfter	Não usado		When the User's IdP session is deemed to have expired.

<saml:SubjectLocality>

```
<complexType name="SubjectLocalityType">
        <attribute name="Address" type="string" use="Opcional"/>
        <attribute name="DNSName" type="string" use="Opcional"/>
</complexType>
```

Obrigatoriedade: Obrigatório

Este elemento deve conter o nome de domínio DNS e endereço IP do sistema a partir do qual o utilizador foi autenticado.

Atributo	Obrigatório	Valores	Notas
Address	Obrigatório		IP address of authenticating user's client system
DNSName	Opcional		DNS Name of authenticating user's client system

<saml:AuthnContext>

Obrigatoriedade: Não usado

10.1.1.29<saml:AttributeStatement>

Obrigatoriedade: Opcional

Este elemento contém vários elementos <*attribute*> contendo informações de atributo associado com o tema SAML. Para cada atributo solicitado no elemento <*AuthnRequest*> o elemento <*AttributeStatement*> contém um elemento único <attribute> disponível.

<saml:Attribute>

```
<complexType name="AttributeType">
        <sequence>
                <element ref="saml:AttributeValue" minOccurs="0" maxOccurs="unbounded"/>
        </sequence>
        <attribute name="Name" type="string" use="required"/>
        <attribute name="NameFormat" type="anyURI" use="Opcional"/>
        <attribute name="FriendlyName" type="string" use="Opcional"/>
        <anyAttribute namespace="##other" processContents="lax"/>
</complexType>
```

Um elemento <*attribute*> é necessário para cada atributo solicitado no pedido original.
A lista de atributos disponíveis no Autenticação.Gov, incluindo seus nomes e formatos, é descrita no capítulo seguinte.

Atributo	Obrigatório	Valores	Notas
Name	Obrigatório		Agreed Name of Attribute Required
NameFormat	Obrigatório		Agreed Format of the Attribute Name
FriendlyName	Não usado		A friendly name for the attribute that can be displayed to a user. Autenticação.Gov is responsible for user consent so probably not required by SP.
fa:AttributeStatus	Opcional	Available NotAvailable Withheld	Used to signify whether or not the <Attribute> requested was ”Available”, ” NotAvailable” or “Withheld”. The default value is “Available” i.e. attribute value has been returned.

<saml:AttributeValue>

Obrigatoriedade: Opcional

Valor do atributo, se disponível. Este valor será codificado na base64 para interoperabilidade máxima (a validar em sede de integração).

<saml:EncryptedAttribute>

Obrigatoriedade: Não usado

<xenc:EncryptedData>

Obrigatoriedade: Não usado

<xenc:EncryptedKey>

Obrigatoriedade: Não usado

10.1.1.30Exemplo de asserção SAML

```
<saml2:Assertion Version="2.0" ID="_b1c88f11-50fd-4a22-988e-9ce4573049e0" IssueInstant="2011-02-17T11:17:14.6349444Z">
	<saml2:Issuer>https://autenticacao.cartaodecidadao.pt</saml2:Issuer>
	<saml2:Subject>
		<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</saml2:NameID>
		<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
			<saml2:SubjectConfirmationData NotOnOrAfter="2011-02-17T11:22:14Z" Recipient="https://www.ServiceProvider.pt" InResponseTo="_1e736a31-a41c-4c35-b17f-0f9ab4c741b3" Address="127.0.0.1"/>
		</saml2:SubjectConfirmation>
	</saml2:Subject>
	<saml2:Conditions NotBefore="2011-02-17T11:17:14Z" NotOnOrAfter="2011-02-17T11:22:14Z">
		<saml2:AudienceRestriction>
			<saml2:Audience>https://www.ServiceProvider.pt</saml2:Audience>
		</saml2:AudienceRestriction>
		<saml2:OneTimeUse/>
	</saml2:Conditions>
	<saml2:AuthnStatement AuthnInstant="2011-02-17T11:17:14.6349444Z">
		<saml2:AuthnContext/>
	</saml2:AuthnStatement>
	<saml2:AttributeStatement>
		<saml2:Attribute Name="AttributeName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" fa:AttributeStatus="Available">
			<saml2:AttributeValue xmlns:q1="http://www.w3.org/2001/XMLSchema" xmlns:d5p1="http://www.w3.org/2001/XMLSchema-instance" d5p1:type="q1:string">AttributeValue</saml2:AttributeValue>
		</saml2:Attribute>
	</saml2:AttributeStatement>
```

```
</saml2:Assertion>
```

Fecho de sessão

Fluxo de processo

O pedido de fecho de sessão usa SAML 2.0 *logout protocol* de acordo com as especificações SAML 2.0. As comunicações entre o *browser* do utilizador e o Autenticação.Gov devem ser efetuadas sobre SSL V3+ ou TLS 1.0+.

O Autenticação.Gov pode redirecionar o utilizador para um url pré-definido no fornecedor de serviços (adicionado durante a configuração do fornecedor de serviços no Autenticação.Gov) ou pode em alternativa providenciar o url no pedido de logout.

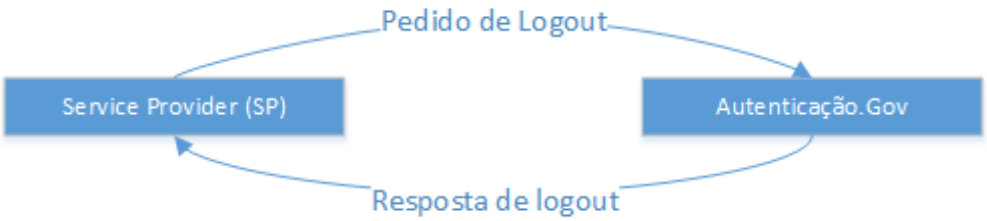
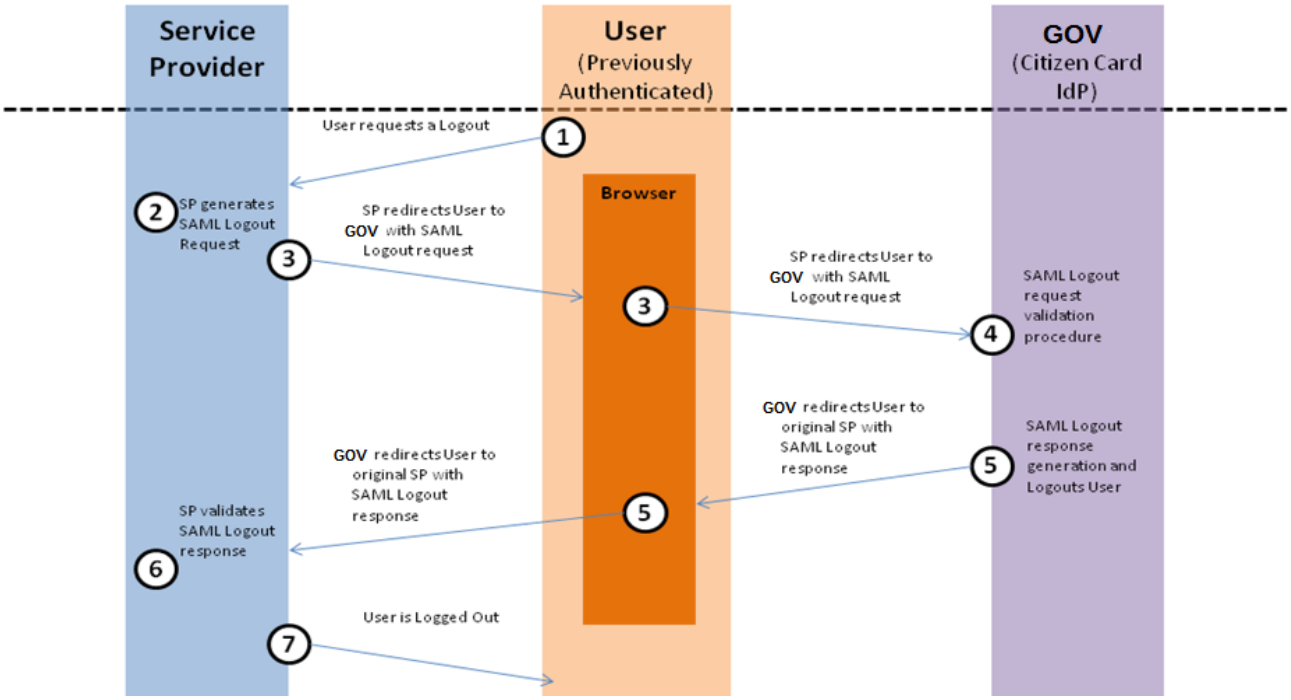


Figure 1 – Fluxo autenticação SAML

O Autenticação.Gov irá responder ao SP, com a informação de *logout*. Esta ligação é também suportada sobre SSL V3+ ou TLS 1.0+.

A figura seguinte representa o processo de *logout* com recurso ao Autenticação.Gov na perspetiva do utilizador.



O processo de *logout* seguirá os seguintes passos:

1) Utilizador pretende fechar a sessão no Autenticação.Gov;

2) O fornecedor de serviços gera pedido SAML para o Autenticação.Gov. À semelhança do pedido de autenticação, este irá identificar o fornecedor de serviços;

3) O fornecedor de serviços redireciona o utilizador para o logout do Autenticação.Gov, submetendo-lhe o pedido SAML;

4) O Autenticação.Gov valida o pedido e caso o utilizador possua sessão, termina-a;

5) O Autenticação.Gov gera resposta SAML e redireciona o utilizador para o fornecedor de serviços;

6) O fornecedor de serviços deve validar a resposta SAML para assegurar que o pedido foi realizado com sucesso. Deve também efetuar o fecho de sessão específico no seu portal;

7) Após conclusão do processo com sucesso, o utilizador deixará de ter sessão ativa no Autenticação.Gov.

Logout Request

10.1.1.31<samlp:LogoutRequest>

```
<sequence>
        <element ref="saml:Issuer" minOccurs="0"/>
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="samlp:Extensions" minOccurs="0"/>
        <element ref="samlp:SessionIndex" minOccurs="0"/>
        <element ref="saml:NameID"/>
</sequence>
<attribute name="ID" type="ID" use="required"/>
<attribute name="Version" type="string" use="required"/>
<attribute name="IssueInstant" type="dateTime" use="required"/>
<attribute name="Destination" type="anyURI" use="Opcional"/>
<attribute name="Consent" type="anyURI" use="Opcional"/>
<attribute name="NotOnOrAfter" type="dateTime" use="Opcional"/>
<attribute name="Reason" type="string" use="Opcional"/>
```

Obrigatoriedade: Obrigatório

Atributo	Obrigatório	Valores	Notas
ID	Obrigatório	Tipo de dados xs:ID[20]	A definição de ID[21] (ver nota de rodapé 4) permite o uso de UUID[22] iniciado ou precedido por um dos caracteres permitidos em([23]) (e.g. "_0dec26dd-

[20] Definido em http://www.w3.org/TR/xmlschema-2/#ID, garantindo as proprieades referidas em http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf 1.3.4 ID and ID ReferenceValues

[21] Definição de ID no protocolo SAML em http://www.w3.org/TR/xmlschema-2/#ID e http://www.w3.org/TR/1999/REC-xml-names-19990114/#NT-NCName

[22] Internet Engeneering Task Force RFC4112 (http://www.ietf.org/rfc/rfc4122.txt)

[23] http://www.w3.org/TR/REC-xml/#NT-Lette

Atributo	Obrigatório	Valores	Notas
			fc3b-47c6-af9d-1cd38db10c55”)
Version	Obrigatório	2.0	SAML Version
IssueInstant	Obrigatório		UTC date & time request was issued
Destination	Obrigatório		URI reference of SAML Request is being sent to
Consent	Opcional	urn:oasis:names:tc:SAML:2.0:consent:unspecified	
NotOnOrAfter	Não usado		
Reason	Não usado		

10.1.1.32<samlp:issuer>

Obrigatoriedade: Obrigatório

Igual à especificação *AuthnRequest*.

10.1.1.33<ds:signature>

Obrigatoriedade: Obrigatório

Igual à especificação *AuthnRequest*.

10.1.1.34<samlp:extensions>

Obrigatoriedade: Opcional

Este elemento contém uma extensão para o padrão SAML 2.0 pedido de logout. No Autenticação.Gov essa extensão inclui:

- Um elemento *<LogoutUrl>* opcional para providenciar uma URI para receção da resposta de logout;

Este atributo estendido no Autenticação.Gov será identificado no âmbito do *namespace* "http://autenticacao.cartaodecidadao.pt/logout".

<fa:LogoutUrl>

Obrigatoriedade: Opcional

Este elemento contêm uma URI, com o objetivo de indicar onde o fornecedor de serviços pretende receber a resposta de logout.

```
<xs:schema targetNamespace="http://autenticacao.cartaodecidadao.pt/logout"
xmlns="http://autenticacao.cartaodecidadao.pt/logout"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
        <xs:element name="LogoutUrl">
                <xs:simpleType>
                        <xs:restriction base="xs:anyURI">
                                <xs:pattern value="https://.+"/>
                        </xs:restriction>
                <xs:simpleType>
        </xs:element>
</xs:schema>
```

10.1.1.35<saml:NameID>

```
<element name="NameID" type="samlp:NameIDType"/>
<complexType name="NameIDType">
        <simpleContent>
                <attributeGroup ref=”saml:IDNameQualifiers”/>
                <attribute name="Format" type="anyURI" use="Opcional"/>
                <attribute name="SPProviderID" type="string" use="Opcional"/>
        </simpleContent>
</complexType>
```

Obrigatoriedade: Obrigatório

Atributo	Obrigatório	Valores	Notas
NameQualifier	Não usado		The security domain that qualifies that name.
SPNameQualifier	Não usado		Qualifying the name with a name of a service provider.
Format	Opcional	urn:oasis:name	URI representing the classification of the identifier.

Atributo	Obrigatório	Valores	Notas
		s:tc:SAML:2.0:consent:unspecified	Default is urn:oasis:names:tc:SAML:2.0:consent:unspecified
SPProvidedID	Não usado		Name identifier if different from the name in the contents of the element.

10.1.1.36<samlp:SessionIndex>

Obrigatoriedade: Não usado

10.1.1.37Exemplo de pedido de fecho de sessão

Com url pré-configurado

```
<saml2p:LogoutRequest
                xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos"
                ID="_5936a065-8ed5-4cb8-9fd4-3c808acbfb7b"
                Version="2.0"
                IssueInstant="2011-02-09T11:39:01.0343448Z"
                Destination="https://autenticacao.gov.pt/Default.aspx"
                Consent="urn:oasis:names:tc:SAML:2.0:logout:user"
                xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
        <saml2:Issuer>http://www.serviceprovider.pt/</saml2:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <Reference URI="#_5936a065-8ed5-4cb8-9fd4-3c808acbfb7b">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <DigestValue>KivtKyBDpS4v9OECsXY6l1aTBNg=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>...signatureValue...</SignatureValue>
                <KeyInfo>
                        <X509Data>
                                <X509Certificate>...x509Data...</X509Certificate>
                        </X509Data>
                </KeyInfo>
```

```
        </Signature>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</saml2:NameID>

</saml2p:LogoutRequest>
```

Sem url pré-configurado / Indicando Url específico

```
<saml2p:LogoutRequest
                xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos"
                ID="_5936a065-8ed5-4cb8-9fd4-3c808acbfb7b"
                Version="2.0"
                IssueInstant="2011-02-09T11:39:01.0343448Z"
                Destination="https://autenticacao.gov.pt/Default.aspx"
                Consent="urn:oasis:names:tc:SAML:2.0:logout:user"
                xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
        <saml2:Issuer>http://www.serviceprovider.pt/</saml2:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <Reference URI="#_5936a065-8ed5-4cb8-9fd4-3c808acbfb7b">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <DigestValue>KivtKyBDpS4v9OECsXY6l1aTBNg=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>...signatureValue...</SignatureValue>
                <KeyInfo>
                        <X509Data>
                                <X509Certificate>...x509Data...</X509Certificate>
                        </X509Data>
                </KeyInfo>
        </Signature>
        <Extensions>
                <fa:LogoutUrl xmlns:fa="http://autenticacao.cartaodecidadao.pt/logout">https://(...)</fa:LogoutUrl>
        </Extensions>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</saml2:NameID>

</saml2p:LogoutRequest>
```

Logout Response

```
<sequence>
        <element ref="saml:Issuer" minOccurs="0"/>
```

```
        <element ref="ds:Signature" minOccurs="0"/>
        <element ref="samlp:Extensions" minOccurs="0"/>
        <element ref="samlp:Status"/>
</sequence>
<attribute name="ID" type="ID" use="required"/>
<attribute name="InResponseTo" type="NCName" use="Opcional"/>
<attribute name="Version" type="string" use="required"/>
<attribute name="IssueInstant" type="dateTime" use="required"/>
<attribute name="Destination" type="anyURI" use="Opcional"/>
<attribute name="Consent" type="anyURI" use="Opcional"/>
```

Obrigatoriedade: Obrigatório

Atributo	Obrigatório	Valores	Notas
ID	Obrigatório	Tipo de dados xs:ID[24]	A definição de ID[25] permite o uso de UUID[26] iniciado ou precedido por um dos caracteres permitidos em([27]) (e.g. "_0dec26dd-fc3b-47c6-af9d-1cd38db10c55")
InResponseTo	Opcional		The identifier (ID) of the request this response refers to. If the request message expired, this field is not used.
Version	Obrigatório	2.0	
IssueInstant	Obrigatório		UTC Date & time response was issued.
Destination	Não usado		
Consent	Opcional	urn:oasis:names:tc:SAML:2.0:consent:unspecified	

[24] Definido em http://www.w3.org/TR/xmlschema-2/#ID, garantindo as proprieades referidas em http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf 1.3.4 ID and ID ReferenceValues

[25] Definição de ID no protocolo SAML em http://www.w3.org/TR/xmlschema-2/#ID e http://www.w3.org/TR/1999/REC-xml-names-19990114/#NT-NCName

[26] Internet Engeneering Task Force RFC4112 (http://www.ietf.org/rfc/rfc4122.txt)

[27] http://www.w3.org/TR/REC-xml/#NT-Lette

10.1.1.38<saml:Issuer>

Obrigatoriedade: Obrigatório

Igual à especificação *AuthnResponse*.

10.1.1.39<ds:Signature>

Obrigatoriedade: Não usado

10.1.1.40<samlp:Extensions>

Obrigatoriedade: Não usado

10.1.1.41<samlp:Status>

```
<element name="Status" type="samlp:StatusType"/>
<complexType name="StatusType">
        <sequence>
                <element ref="samlp:StatusCode"/>
                <element ref="samlp:StatusMessage" minOccurs="0"/>
                <element ref="samlp:StatusDetail" minOccurs="0"/>
        </sequence>
</complexType>

<element name="StatusCode" type="samlp:StatusCodeType"/>
<complexType name="StatusCodeType">
        <sequence>
                <element ref="samlp:StatusCode" minOccurs="0"/>
        </sequence>
        <attribute name="Value" type="anyURI" use="required"/>
</complexType>

<element name="StatusMessage" type="string"/>

<element name="StatusDetail" type="samlp:StatusDetailType"/>
<complexType name="StatusDetailType">
        <sequence>
                <any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </sequence>

</complexType>
```

Obrigatoriedade: Obrigatório

<samlp:StatusCode>

Obrigatoriedade: Obrigatório

Igual à especificação *AuthnResponse*.

10.1.1.42 Exemplo de resposta ao pedido de fecho de sessão

```
<saml2p:LogoutResponse
                xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:fa="http://autenticacao.cartaodecidadao.pt/atributos"
                ID="_f171c8a1-0616-421b-9fbf-34be422c414f"
                InResponseTo="_49800585-b491-46d3-b8c8-efc743eccd52"
                Version="2.0"
                IssueInstant="2011-02-08T17:51:17.7593424Z"
                Destination="http://www.serviceProvider"
                Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
                xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
        <saml2:Issuer>http://www.ServiceProvider.pt/</saml2:Issuer>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <Reference URI="#_f171c8a1-0616-421b-9fbf-34be422c414f">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
                                        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <DigestValue>cX/NPb/aoCOcUK+4GOPwsndZ5rE=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>...signatureValue...</SignatureValue>
                <KeyInfo>
                        <X509Data>
                                <X509Certificate>...x509Data...</X509Certificate>
                        </X509Data>
                </KeyInfo>
        </Signature>
        <saml2p:Status>
                <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
        </saml2p:Status>

</saml2p:LogoutResponse>
```

11 REFERÊNCIAS

1. **STORK Consortium.** STORK Framework - D5.8.1 Technical design. *Stork eId - Secure Identity Across Borders Linked.* [Online] September 8, 2009. https://www.eid-stork.eu/.

2. **OASIS Consortium.** Assertions and Protocols for the OASIS Security Assertion Markup Languange (SAML) v2.0. *OASIS - Organization for the Advancement of Structured Information Standards.* [Online] March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

3. —. Security Assertion Markup Language (SAML) v2.0. *OASIS - Organization for the Advancement of Structured Information Standards.* [Online] March de 2005. http://www.oasis-open.org/specs/index.php#saml.

4. **W3C Consortium.** XML Signature Syntax and Processing (Second Edition) - W3C Recommendation 10 June 2008. *W3C - World Wide Web Consortium.* [Online] June 10, 2009. http://www.w3.org/TR/xmldsig-core/.

5. —. XML Encryption Syntax and Processing. *W3C - World Wide Web Consortium.* [Online] 2 de December de 2002. http://www.w3.org/TR/xmlenc-core/.