AZORID

Protocolo e Especificação Técnica

Versão 1.0, 2026-09-11

GOVERNO DOS AÇORES
SECRETARIA REGIONAL DAS FINANÇAS, PLANEAMENTO E ADMINISTRAÇÃO PÚBLICA

datapoint .software

PRR Plano de Recuperação e Resiliência
GOVERNO DOS AÇORES
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

MODERNIZAÇÃO E DIGITALIZAÇÃO DA ADMINISTRAÇÃO PÚBLICA-RAA C19

Índice

1. Revisões . . . 1
2. Introdução . . . 2
    2.1. Âmbito . . . 2
    2.2. Objetivo . . . 2
    2.3. Terminologia . . . 2
3. Protocolo . . . 4
    3.1. Conceitos básicos sobre dados de conta . . . 4
    3.2. Autenticação e autorização . . . 4
    3.3. Certificação de atributos . . . 6
    3.4. Notificação de alterações de identidade (Shared Signals Framework) . . . 7
    3.5. Representação . . . 8
4. Scopes e Atributos . . . 10
    4.1. Utilização . . . 10
    4.2. Scopes de sistema . . . 10
    4.3. Dados comuns . . . 11
    4.4. Dados de entidade . . . 12
    4.5. Dados de cidadão . . . 14
    4.6. Scopes *legacy* . . . 14
5. Adesão . . . 16
    5.1. Pedido de acesso . . . 16
    5.2. Atribuição de acesso . . . 16
6. Configurações e endereços . . . 18
    6.1. Dados de configuração OpenID Connect . . . 18
    6.2. Dados de configuração do Shared Signals Framework . . . 19
Anexo A: Scopes Legacy . . . 20
7. Referências . . . 22

1. Revisões

Data	Versão	Descrição
2026-02-25	DRAFT	Revisão inicial do manual.
2026-04-24	DRAFT	Atualização de endereços dos endpoints de configuração.
2026-09-11	DRAFT	Documentação do Backchannel Logout; documentação do atributo `identity_certified`; reforço da aplicação dos scopes `account_type.citizen`/`account_type.organization`; scopes *legacy* movidos para anexo próprio.
2026-09-22	1.0	Documentação do mecanismo de notificação de alterações de identidade (Shared Signals Framework).

2. Introdução

2.1. Âmbito

O projeto AzorID é um sistema de gestão de identidades e autenticação, desenvolvido para fornecer uma solução centralizada, segura e desmaterializada para a autenticação de cidadãos e organizações nos serviços públicos da região.

2.2. Objetivo

Este documento tem como objetivo descrever o processo de integração de sistemas cliente com os serviços de autenticação AzorID, detalhando os requisitos técnicos, os fluxos de autenticação suportados, as melhores práticas de segurança e as considerações a ter em conta durante a implementação.

É ainda delineado o processo de pedido de acesso, incluindo os passos necessários para a obtenção de credenciais, a definição de *scopes* de acesso e a configuração de ambientes de teste.

Este documento não descreve extensivamente o detalhe técnico do processo de integração uma vez que o mesmo é baseado na especificação [OpenID]. A documentação "Guia prático de integração OpenID" entregue em conjunto com este documento detalha o processo técnico com exemplos.

2.3. Terminologia

Termo	Definição
Access Token	Chave utilizada para autenticação nos endpoints da API, podendo ser transmitida por diversas vias
API	Application Programming Interface: conjunto de definições e protocolos para a construção e integração de software
Endpoint	Um ponto de acesso específico na API para realizar uma operação de consulta ou escrita
GUID	Identificador Global Único utilizado para identificar recursos
HTTP	HyperText Transfer Protocol: protocolo de comunicação utilizado para a transferência de dados na web
IDP	Identity Provider: sistema provedor de identidades, responsável pelo processo de autenticação e autorização
OAuth2	Um padrão de autorização que permite a um sistema (cliente) aceder a dados de um utilizador noutro serviço (servidor de recursos), sem que o utilizador tenha de partilhar as suas credenciais
OpenID	Uma extensão ao padrão OAuth 2.0, adicionando funcionalidades padronizadas para autenticação de utilizadores e fornecimento de informações associadas

Termo	Definição
Scope	Grupo de permissões associado ao pedido de autenticação ou a uma chave de acesso

3. Protocolo

3.1. Conceitos básicos sobre dados de conta

O sistema gere contas de utilizador, que podem pertencer a cidadãos ou organizações.

Cada conta possuí um estado de certificação, que determina se o titular da conta está validado. Este estado de certificação global implica que o identificador primário (NIF/NIPC) e o nome foram validados como pertencendo ao titular da conta, **mas não necessariamente que outros atributos associados à conta estejam certificados**.

Este estado de certificação global é disponibilizado ao sistema cliente através do atributo `identity_certified` (`true`/`false`), incluído em todos os tokens emitidos — independentemente dos scopes `account.*` solicitados — permitindo ao cliente determinar diretamente se a conta autenticada corresponde a uma identidade certificada.

Existe ainda o conceito de certificação individual de atributos. A certificação de cada atributo é independente e pode ser validada ou não, dependendo do processo de verificação realizado para cada um.

O pedido de autenticação e autorização pode ainda ser condicionado por dois scopes complementares — `account.filter_uncertified_data` e `account.enforce_certified_identity` — que controlam, respetivamente, que atributos são devolvidos e se a autenticação de contas não certificadas é permitida. Estes scopes são independentes entre si e podem ser combinados livremente; o comportamento resultante de cada combinação está detalhado na secção Scopes de sistema.

3.2. Autenticação e autorização

É implementado o fluxo de autenticação e autorização baseado no protocolo OpenID Connect, que é uma extensão do protocolo OAuth2. Este protocolo é amplamente adotado para autenticação de utilizadores e autorização de acesso a recursos protegidos, proporcionando uma experiência de autenticação segura e padronizada.

Qualquer integração deverá seguir as especificações dos respetivos protocolos, nomeadamente os documentos referenciados [OpenID] e [RFC6749], para garantir a compatibilidade e segurança da integração.

3.2.1. Autenticação via fluxo "Authorization Code Flow"

O fluxo de autenticação recomendado para a maioria dos casos de uso é o fluxo "Authorization Code Flow", que é adequado para aplicações web e móveis. Este fluxo envolve a obtenção de um código de autorização, que é posteriormente trocado por um token de acesso e um token de ID. O processo de autenticação inclui os seguintes passos:

1. O cliente redireciona o utilizador para a página de autenticação do IDP (`authorization_endpoint`), incluindo os parâmetros necessários, como `client_id`, `redirect_uri`, `response_type=code` e `scope`.
2. O utilizador autentica-se no IDP e concede as permissões solicitadas pelo cliente.
3. O IDP redireciona o utilizador de volta para o `redirect_uri` do cliente, incluindo o código de autorização

como um parâmetro na URL em caso de sucesso.

4. O cliente troca o código de autorização por um token de acesso e um token de ID, enviando um pedido ao IDP (`token_endpoint`), incluindo os parâmetros `grant_type=authorization_code`, `code`, `redirect_uri`, `client_id` e `client_secret`.

NOTA	O passo descrito no ponto 4 é realizado pelo servidor do cliente e não pelo navegador do utilizador, garantindo que o `client_secret` é mantido seguro e não exposto ao utilizador final.

NOTA	O cliente pode adicionar o parâmetro `prompt=login` durante o redirecionamento para o `authorization_endpoint` caso pretenda forçar o utilizador a autenticar-se novamente, mesmo que já tenha uma sessão ativa.

3.2.2. Logout

O sistema disponibiliza um endpoint de logout (`end_session_endpoint`), que permite ao sistema cliente terminar a sessão do utilizador na sua própria aplicação e, opcionalmente, terminar em simultâneo a sessão ativa do utilizador no AzorID.

Para tal, o cliente deve redirecionar o utilizador para o `end_session_endpoint`, incluindo os seguintes parâmetros:

1. `id_token_hint`: o token de ID obtido anteriormente durante o processo de autenticação, utilizado para identificar a sessão e o cliente associados;
2. `post_logout_redirect_uri`: o URL para o qual o utilizador deve ser reencaminhado após o processo de logout;
3. `state` (opcional): um valor arbitrário que será devolvido inalterado ao cliente no reencaminhamento final, útil para preservar o estado da aplicação cliente.

Caso o utilizador tenha uma sessão ativa no AzorID, é apresentada uma página onde este pode optar por terminar apenas a sessão na aplicação cliente, ou terminar em simultâneo a sua sessão no AzorID. Após esta escolha, o utilizador é reencaminhado para o `post_logout_redirect_uri` indicado, incluindo o parâmetro `state`, caso tenha sido fornecido.

NOTA	O `post_logout_redirect_uri` deve ser previamente registado como um URL de pós-logout válido para o cliente, à semelhança do que é exigido para o `redirect_uri` no processo de autenticação.

3.2.3. Backchannel Logout

A partir do sistema AzorID o utilizador poderá pedir para terminar sessão de forma centralizada em *todos* os sistemas clientes onde tenha sessão ativa.

O AzorID concretiza esse pedido através do mecanismo de *Backchannel Logout* previsto no standard [OpenID]: ao terminar a sessão do utilizador, envia diretamente, servidor-a-servidor, uma notificação a cada um dos restantes sistemas clientes com sessão ativa para esse utilizador, para que cada um possa encerrar a respetiva sessão local de forma independente.

Para beneficiar deste mecanismo, o sistema cliente deve disponibilizar um endpoint HTTP próprio, registado junto da equipa técnica do AzorID durante o processo de adesão (de forma semelhante ao `redirect_uri`), capaz de receber e processar as notificações de logout enviadas pelo AzorID.

A notificação consiste num pedido `HTTP POST` a esse endpoint, contendo o parâmetro `logout_token` — um token assinado (JWT), à semelhança do `id_token` emitido durante a autenticação — que inclui os atributos `sub` (a conta) e `sid` (a autorização/sessão específica, o mesmo valor de `sid` presente no `id_token` /`access_token` originais). O sistema cliente deve validar este token e, com base no `sid` recebido, terminar a sessão local específica correspondente — não todas as sessões associadas a essa conta, uma vez que pode existir mais do que uma sessão local ativa para o mesmo `sub` (por exemplo, através de representação por diferentes representantes).

NOTA Os detalhes técnicos do pedido enviado pelo AzorID e do comportamento esperado do sistema cliente estão descritos no "Guia Prático de Integração OpenID".

3.3. Certificação de atributos

Salvo quando for solicitado o scope `account.filter_uncertified_data` (que restringe a resposta apenas a atributos certificados), não é garantido que toda a informação devolvida é certificada, pelo que o sistema cliente terá acesso a informação granular sobre o estado de certificação de atributos de forma individual.

Deste modo, é incluído o atributo `certification_state` com uma estrutura que indica o estado de certificação de cada atributo individualmente. Neste atributo, cada chave corresponde a um atributo específico (por exemplo, `fiscal_number`, `birth_date`, etc.) e o valor associado indica o estado de certificação desse atributo, podendo assumir os seguintes valores: `CERTIFIED`, `PENDING`, `UNCERTIFIED`.

3.3.1. Exemplo

Dados no token de acesso:

```
{
  "sub": "00000000-0000-0000-0000-000000000001",
  "name": "João Silva",
  "fiscal_number": "100000001",
  "birth_date": "1990-01-01",
  "certification_state": {
    "name": {
      "status": "CERTIFIED"
    },
    "fiscal_number": {
      "status": "CERTIFIED"
    },
    "birth_date": {
      "status": "UNCERTIFIED"
    }
  }
}
```

Se for efetuado o pedido ao endpoint `userinfo`, alem das informações presentes no exemplo relativas à

certificação, a resposta incluirá dados adicionais como a data de certificação e a entidade responsável, por exemplo:

```
{
  (...)
  "certification_state": {
    "name": {
      "status": "CERTIFIED",
      "certified_on": "2024-01-01T12:00:00Z",
      "certified_by": "Entidade Exemplo"
    },
    (...)
  }
}
```

3.4. Notificação de alterações de identidade (Shared Signals Framework)

O sistema permite ainda notificar, de forma proativa, os sistemas clientes sempre que ocorra uma alteração aos dados de identidade de uma conta — nomeadamente ao nome (`name`), ao identificador fiscal (`fiscal_number`) ou ao estado de certificação global (`identity_certified`).

O AzorID concretiza esta notificação através do mecanismo de *Shared Signals Framework* (SSF) previsto no standard [OpenIDSSF], através do respetivo perfil de entrega por *push*: ao ocorrer uma das alterações mencionadas, é enviada diretamente, servidor-a-servidor, uma notificação a cada sistema cliente subscrito, para que este possa atualizar os dados que mantém localmente.

Este mecanismo é independente e distinto do *Backchannel Logout* (Backchannel Logout) — apesar da arquitetura semelhante (pedido `HTTP POST` direto ao sistema cliente), servem propósitos diferentes e utilizam um endpoint e formato de mensagem próprios, não devendo ser confundidos.

Para beneficiar deste mecanismo, o sistema cliente deve disponibilizar um endpoint HTTP próprio, registado junto da equipa técnica do AzorID durante o processo de adesão (de forma semelhante ao `backchannel_logout_uri`), capaz de receber e processar as notificações enviadas pelo AzorID.

Estas notificações não incluem os novos valores dos dados alterados — apenas identificam que algo mudou (e, no caso de alterações de atributos, quais atributos) — cabendo ao sistema cliente obter os dados atualizados através dos mecanismos já existentes (por exemplo, um novo pedido ao endpoint `userinfo`, caso o utilizador tenha uma sessão ativa).

São suportados dois tipos de evento, cada um identificado pelo seu próprio identificador único:

Tipo de evento	Descrição
`https://azorid.azores.gov.pt/schemas/ssf/attribute-changed`	Notifica uma alteração ao nome (`name`) e/ou ao identificador fiscal (`fiscal_number`) de uma conta.

Tipo de evento	Descrição
`https://azorid.azores.gov.pt/schemas/ssf/identity-certification-status-changed`	Notifica uma alteração ao estado de certificação global da conta (`identity_certified`, ver Conceitos básicos sobre dados de conta).

NOTA Os detalhes técnicos do pedido enviado pelo AzorID e do comportamento esperado do sistema cliente estão descritos no "Guia Prático de Integração OpenID".

3.5. Representação

O sistema suporta o conceito de representação, permitindo que um cidadão (representante) atue em nome de outro cidadão ou organização (representado).

Partindo do pressuposto que o utilizador ao autenticar-se escolheu representar um terceiro, o sistema emitirá uma sessão e respetivo token de acesso onde os dados associados são os da parte **representada**, mas, adicionalmente, consta o atributo `impersonator` que indica informação do representante.

NOTA O atributo `impersonator` é incluído em todos os casos (`id_token`, `access_token` e em pedidos ao *endpoint* `userinfo`).

3.5.1. Exemplo

```
{
  "sub": "00000000-0000-0000-0000-000000000001",
  "name": "João Silva",
  "fiscal_number": "100000001",
  "birth_date": "1990-01-01",
  "impersonator": {
    "sub": "00000000-0000-0000-0000-000000000002",
    "name": "Maria Santos",
    "fiscal_number": "100000002",
    "services": [
      "SVC-CODE-1",
      "SVC-CODE-2"
    ]
  }
}
```

Deste exemplo, o cidadão representado é o João Silva, que tem o NIF 100000001, enquanto a representante é a Maria Santos, com o NIF 100000002, que está efetivamente a utilizar a aplicação.

É implicito que o representante, a existir, tem a sua identidade certificada.

NOTA Nos mesmos casos, é também incluído o atributo standard `act` (conforme [RFC8693]), com o mesmo identificador do representante presente em `impersonator.sub`, mas sem os restantes dados (`name`, `fiscal_number`, `services`). Tal como `impersonator`, `act` é incluído

em todos os casos (`id_token`, `access_token` e `userinfo`).

4. Scopes e Atributos

4.1. Utilização

No processo de autenticação, o cliente especifica obrigatóriamente scopes que podem:

- restringir o tipo de conta que pretende autenticar (cidadão ou organização);
- indicar o nível de certificação desejado;
- indicar os dados que pretende obter.

4.2. Scopes de sistema

Scope	Descrição
`openid`	Scope obrigatório para todos os pedidos de autenticação, que indica que o cliente deseja autenticar o utilizador e obter um token de ID.
`profile`	Scope que indica que o cliente pretende, alem de autenticação, obter informações sobre a conta.
`account.filter_uncertified_data`	**Filtragem de dados não certificados**: restringe os atributos devolvidos apenas aos que estejam certificados, omitindo os restantes. Sem este scope, são devolvidos todos os atributos disponíveis, indicando o respetivo estado de certificação em `certification_state`.
`account.enforce_certified_identity`	**Imposição de identidade certificada**: impede a conclusão da autenticação caso a conta não tenha a identidade certificada (`identity_certified: false`). Pode ser livremente combinado com `account.filter_uncertified_data`.
`account_type.citizen`	Restringe a autenticação a contas de cidadãos; uma tentativa de autenticação com uma conta de organização é rejeitada.
`account_type.organization`	Restringe a autenticação a contas de organizações; uma tentativa de autenticação com uma conta de cidadão é rejeitada.

NOTA O scope `profile` é opcional, mas recomendado para a maioria dos casos de uso, pois permite que o cliente obtenha informações adicionais sobre a conta autenticada.

NOTA `account.filter_uncertified_data` e `account.enforce_certified_identity` são independentes entre si e podem ser combinados livremente — ver a matriz de comportamento abaixo. Não indicando nenhum dos dois, o sistema autentica contas independentemente do respetivo estado de certificação e devolve todos os atributos disponíveis.

NOTA Não indicando um dos scopes `account_type.citizen` ou `account_type.organization`, o sistema autentica tanto contas de cidadãos como de organizações. Os dois scopes são

mutuamente exclusivos — um pedido de autenticação que indique ambos é rejeitado com o erro `invalid_scope`.

NOTA

Quando `account.enforce_certified_identity` é utilizado e a condição de certificação não é cumprida, ou quando a conta autenticada não corresponde ao `account_type.*` pedido, a autenticação é interrompida e o utilizador é encaminhado para uma página informativa.

4.2.1. Matriz de certificação e controlo de acesso

A tabela seguinte resume as quatro combinações possíveis entre `account.filter_uncertified_data` e `account.enforce_certified_identity`, e o tratamento que o sistema cliente deve dar aos dados recebidos em cada caso.

Scopes `account.*`	**Permite login de contas não certificadas**	**Dados transmitidos**	**Tratamento esperado pelo cliente**
Sem scopes `account.*` (default)	Sim	Certificados e não certificados	A conta pode não estar certificada; o cliente deve validar sempre `certification_state` antes de confiar em qualquer atributo.
`account.enforce_certified_identity`	Não	Certificados e não certificados	A conta está garantidamente certificada (`identity_certified: true`), mas atributos individuais podem não estar — continuar a validar `certification_state`.
`account.filter_uncertified_data`	Sim	Apenas certificados	Os atributos devolvidos são fidedignos, mas a conta pode não estar certificada — não inferir o estado da conta apenas pela presença deste scope.
`account.filter_uncertified_data` + `account.enforce_certified_identity`	Não	Apenas certificados	Conta e atributos certificados; o cliente pode confiar integralmente na informação recebida, sem validações adicionais.

4.3. Dados comuns

Scope	**Atributo**	**Descrição**
`addresses`	`addresses`	Lista de endereços associados à conta, incluindo morada, código postal, localidade, etc.

Scope	Atributo	Descrição
contacts	phone	Número de telefone associado à conta.
	phone_country	Código do país associado ao número de telefone, representada pelo código ISO 3166-1 numérico do país.
	phone_country_code	Código do país associado ao número de telefone, representada pelo código ISO 3166-1 alpha-2 do país.
email	email	Endereço de email associado à conta.
picture	picture	Endereço (URL) da fotografia do cidadão ou do logótipo da entidade, validados pelos serviços do AzorID. A imagem só é devolvida a pedidos com o access_token do sistema cliente (ver o "Guia prático de integração OpenID").

NOTA

O atributo picture só é enviado quando a conta tem uma fotografia ou logótipo aprovado; não tem entrada em certification_state, porque uma imagem em análise nunca é enviada. A imagem é quadrada, com 512 × 512 píxeis, em JPEG (fotografias) ou PNG (logótipos). Uma nova imagem tem sempre um novo endereço.

NOTA

Para contas de entidade, phone e email correspondem aos contactos do responsável pela entidade, utilizados para notificações dos Serviços da Administração Pública Regional dos Açores. O número de telefone de uma entidade é sempre um número de telemóvel nacional, pelo que phone_country é sempre 620 e phone_country_code é sempre PT.

4.4. Dados de entidade

Scope	Atributo	Descrição
identification	fiscal_number	Número de identificação de pessoa coletiva (NIPC).
	social_designation	Designação social da empresa (e.g. "Datapoint - Sistemas de Informação, Lda.").
economical_activity	economical_activity_code	Código da atividade económica, de acordo com a classificação CAE (Classificação Portuguesa de Atividades Económicas).

Scope	Atributo	Descrição
`characterization`	`activity_start`	Data de início da atividade da empresa.
	`characterization`	Caracterização da empresa, indicando se é uma empresa individual, sociedade por quotas, etc.
	`commercial_designation`	Designação comercial da empresa (e.g. "Datapoint Software").
	`dimension`	Dimensão da empresa, indicando se é uma micro, pequena, média ou grande empresa.
	`legal_nature`	Natureza jurídica da empresa, indicando se é uma entidade pública, privada, sem fins lucrativos, etc.
`managers`	`managers`	Lista dos gestores afiliados à entidade, em que cada elemento contém os atributos seguintes.
	`managers[].sub`	Identificador da conta do gestor (o mesmo valor que é devolvido em `impersonator.sub` / `act.sub` quando o gestor se autentica em representação da entidade).
	`managers[].name`	Nome completo do gestor.
	`managers[].email`	Endereço de email do gestor, se disponível e certificado.
	`managers[].phone`	Número de telefone do gestor, se disponível e certificado.
	`managers[].phone_country`	Código do país associado ao número de telefone, representada pelo código ISO 3166-1 númerico do país.
	`managers[].phone_country_code`	Código do país associado ao número de telefone, representada pelo código ISO 3166-1 alpha-2 do país.

NOTA

Por questões de dimensão, o atributo `managers` é devolvido **exclusivamente** pelo *endpoint* `userinfo`, não sendo incluído no `id_token` nem no `access_token`, mesmo quando o scope `managers` é pedido.

NOTA

A lista `managers` inclui apenas gestores com afiliação ativa. Os contactos (`email`, `phone`, `phone_country` e `phone_country_code`) são incluídos apenas quando disponíveis e certificados, independentemente do scope `account.filter_uncertified_data`, e são omitidos caso contrário. Por esse motivo, o atributo `managers` não tem entrada em `certification_state`. Se a entidade não tiver gestores afiliados, é devolvida uma lista vazia.

Exemplo do atributo `managers` numa resposta do *endpoint* `userinfo`:

```
{
  "managers": [
    {
```

```
      "sub": "00000000-0000-0000-0000-000000000001",
      "name": "João Silva",
      "email": "joao.silva@example.com",
      "phone": "912345678",
      "phone_country": "620",
      "phone_country_code": "PT"
    },
    {
      "sub": "00000000-0000-0000-0000-000000000002",
      "name": "Maria Sousa"
    }
  ]
}
```

4.5. Dados de cidadão

Scope	Atributo	Descrição
name	name	Nome completo.
birth_date	birth_date	Data de nascimento.
gender	gender	Género.
marital_status	marital_status	Estado civil.
nationality	nationality	Nacionalidade, representada pelo código ISO 3166-1 numérico do país.
	nationality_code	Nacionalidade, representada pelo código ISO 3166-1 alpha-2 do país.
citizen_card	citizen_card_number	Número de identificação civil (NIC).
	citizen_card_expiration_date	Data de validade do cartão de cidadão.
passport	passport_number	Número de passaporte.
	passport_expiration_date	Data de validade do passaporte.
fiscal_number	fiscal_number	Número de identificação fiscal (NIF).
social_security_number	social_security_number	Número de identificação de segurança social (NISS).
patient_number	patient_number	Número de utente do sistema nacional de saúde (SNS).

4.6. Scopes *legacy*

O sistema suporta ainda um conjunto de scopes *legacy* definidos em especificações anteriores do AzorID, que se encontram obsoletos e não devem ser utilizados em novos desenvolvimentos, mas que continuam a ser suportados para garantir retro-compatibilidade com integrações já existentes.

A lista completa destes scopes e respetivos atributos está disponível no Anexo A.

5. Adesão

5.1. Pedido de acesso

Para um sistema externo interagir e usufruir dos serviços de autenticação AzorID, é necessário que o responsável pelo sistema efetue um pedido de acesso.

Em primeiro lugar, e tendo em conta que a integração com o sistema é assente sobre os conceitos de serviço e ponto de atendimento definidos no Catálogo de Entidades e Serviços (CES), o requerente deve garantir que as devidas parametrizações estão efetuadas no CES de modo a dar o seguimento ao pedido de acesso.

Este pedido deve incluir as seguintes informações indispensáveis:

Dado	**Descrição**
Nome do sistema cliente	Nome do sistema cliente / portal, visível para os utilizadores finais quando é solicitada a autenticação.
Tipologia do sistema cliente	Indicação se o sistema cliente é um portal, uma aplicação móvel, uma API, etc.
Interlocutor técnico	Nome e contacto do interlocutor responsável pela integração
Ponto de Atendimento	Identificação do ponto de atendimento a ser associado à integração.
Endereço do sistema cliente	URL de acesso ao portal, plataforma ou aplicação do sistema cliente.
Scopes de acesso pretendidos	Lista dos *scopes* de acesso pretendidos, indicando as funcionalidades e os dados que o sistema cliente pretende aceder através da integração com a plataforma AzorID.
Redirect URL	Um ou vários URLs de redirecionamento para os quais os utilizadores podem ser encaminhados após autenticação.
Post-Logout URL	Um ou vários URLs de redirecionamento para os quais os utilizadores podem ser encaminhados após logout.
Backchannel Logout Endpoint URL	Um URL para o endpoint do sistema cliente a ser invocado aquando de um pedido de término de sessão externo.
SSF Receiver Endpoint URL	Um URL para o endpoint do sistema cliente a ser invocado aquando de alterações aos dados de identidade de uma conta (ver Notificação de alterações de identidade (Shared Signals Framework)).

5.2. Atribuição de acesso

Após a parametrização do sistema cliente será atribuído um identificador (`Client ID`) e, caso aplicável, uma chave (`Client Secret`) a serem comunicados ao responsável pelo pedido.

NOTA	O `Client Secret` é um dado sensível que deve ser guardado de forma segura e **não pode ser partilhado ou exposto publicamente**. O responsável pelo sistema cliente deve assegurar

a confidencialidade do `Client Secret` para evitar acessos não autorizados. Em caso de suspeita de comprometimento do `Client Secret`, o responsável deve notificar imediatamente a equipa técnica para revogação e reemissão de novas credenciais.

6. Configurações e endereços

6.1. Dados de configuração OpenID Connect

Em conformidade com a especificação [OpenID], o sistema expõe um endpoint global de configuração, localizado em `/.well-known/openid-configuration`, que fornece referências aos restantes endpoints disponíveis para autenticação, obtenção de *tokens* e consulta de dados (*userinfo*), bem como outras informações relevantes para a integração.

Esta informação pode ser obtida para cada ambiente, respetivamente, despoletando um pedido a um dos seguintes endereços conforme aplicável.

Ambiente	Endereço
Produção	`https://azorid.azores.gov.pt/.well-known/openid-configuration`
Qualidade	`https://azorid-qa.azores.gov.pt/.well-known/openid-configuration`

Recomenda-se como boa prática a obtenção desta informação de configuração diretamente do endpoint `openid-configuration`, de forma a garantir que os dados utilizados na integração estão sempre atualizados e em conformidade com as especificações do sistema.

Na impossibilidade de obter esta informação diretamente do endpoint de forma dinâmica, os dados de configuração essenciais para a integração podem ser consultados na tabela abaixo.

6.1.1. Ambiente de produção

Endpoint	Endereço
`Issuer`	`https://azorid.azores.gov.pt`
`Authorization Endpoint`	`https://azorid.azores.gov.pt/openid/authorize`
`Token Endpoint`	`https://azorid.azores.gov.pt/openid/token`
`Userinfo Endpoint`	`https://azorid.azores.gov.pt/openid/userinfo`
`Logout Endpoint`	`https://azorid.azores.gov.pt/openid/logout`

6.1.2. Ambiente de qualidade

Endpoint	Endereço
`Issuer`	`https://azorid-qa.azores.gov.pt`
`Authorization Endpoint`	`https://azorid-qa.azores.gov.pt/openid/authorize`
`Token Endpoint`	`https://azorid-qa.azores.gov.pt/openid/token`
`Userinfo Endpoint`	`https://azorid-qa.azores.gov.pt/openid/userinfo`
`Logout Endpoint`	`https://azorid-qa.azores.gov.pt/openid/logout`

6.1.3. Exemplo de resposta do endpoint de configuração

```
{
    "issuer": "https://azorid.azores.gov.pt",
    "authorization_endpoint": "https://azorid.azores.gov.pt:443/openid/authorize",
    "jwks_uri": "https://azorid.azores.gov.pt:443/openid/jwks",
    "token_endpoint": "https://azorid.azores.gov.pt:443/openid/token",
    "userinfo_endpoint": "https://azorid.azores.gov.pt:443/openid/userinfo",
    "end_session_endpoint": "https://azorid.azores.gov.pt:443/openid/logout",
    (...)
}
```

NOTA

Além dos endpoints mencionados, a resposta inclui outros campos que podem ser relevantes para a integração, como `jwks_uri` para obtenção das chaves públicas usadas na validação dos tokens JWT bem como o nome do `issuer` para comparação com o valor presente no token.

6.2. Dados de configuração do Shared Signals Framework

Adicionalmente, e de forma independente do endpoint de configuração OpenID Connect, o sistema expõe um endpoint de descoberta próprio para o mecanismo de notificação de alterações de identidade (Notificação de alterações de identidade (Shared Signals Framework)), localizado em `/.well-known/ssf-configuration`. Os detalhes técnicos deste endpoint estão descritos no "Guia Prático de Integração OpenID".

Anexo A: Scopes Legacy

Scope	Atributo	Descrição
azi_address	azi_address	Linha da morada do cidadão (Rua, Porta, Andar, etc.).
azi_birthDate	azi_birthDate	Data de nascimento do cidadão.
azi_certification	azi_certification	Estado de certificação da conta.
azi_companyAddress	azi_companyAddress	Linha da morada da empresa (Rua, Porta, Andar, etc.).
azi_companyCae	azi_companyCae	Código da atividade económica da empresa.
azi_companyCaracterization	azi_companyCaracterization	Caracterização da empresa.
azi_companyComercialDesignation	azi_companyComercialDesignation	Designação comercial da empresa.
azi_companyDimension	azi_companyDimension	Dimensão da empresa.
azi_companyDistrict	azi_companyDistrict	Distrito da empresa.
azi_companyEmail	azi_companyEmail	Email da empresa.
azi_companyInitialActivityDate	azi_companyInitialActivityDate	Data de início da atividade da empresa.
azi_companyLegalNature	azi_companyLegalNature	Natureza jurídica da empresa.
azi_companyMunicipality	azi_companyMunicipality	Município da empresa.
azi_companyNipc	azi_nipc	NIPC da empresa.
azi_companyParish	azi_companyParish	Freguesia da empresa.
azi_companyPhone	azi_companyPhone	Telefone da empresa.
azi_companyPostalCode	azi_companyPostalCode	Código postal da empresa.
azi_companySocialDesignation	azi_companySocialDesignation	Denominação social da empresa.
azi_district	azi_district	Distrito do cidadão.
	azi_district_name	Nome do distrito do cidadão.
azi_email	email	Email do cidadão.
azi_fullName	azi_fullName	Nome completo do cidadão.
azi_gender	azi_gender	Género do cidadão.
azi_IdCardExpirationDate	azi_IdExpirationDate	Data de validade do cartão de cidadão.
azi_idCardNumber	azi_idCardNumber	Número do cartão de cidadão.

Scope	Atributo	Descrição
azi_maritalStatus	azi_maritalStatus	Estado civil do cidadão.
azi_mobilePhone	azi_mobilePhone	Telemóvel do cidadão.
azi_mobilePhoneNumber	azi_mobilePhoneNumber	Número de telemóvel do cidadão.
azi_municipality	azi_municipality	Município do cidadão.
	azi_municipality_name	Nome do município do cidadão.
azi_nationality	azi_nationality	Nacionalidade do cidadão.
azi_nif	azi_nif	NIF do cidadão.
azi_parish	azi_parish	Freguesia do cidadão.
	azi_parish_name	Nome da freguesia do cidadão.
azi_passportExpirationDate	azi_passportExpirationDate	Data de validade do passaporte.
azi_passportNumber	azi_passportNumber	Número do passaporte.
azi_placeOfBirth	azi_placeOfBirth	Naturalidade do cidadão.
azi_postalCode	azi_postalCode	ID do código postal do cidadão.
	azi_postalCode_name	Código postal do cidadão. (e.g.: "1234-567")
azi_socialSecurityNumber	azi_socialSecurityNumber	NISS do cidadão.

7. Referências

- OAuth 2.0 Authorization Framework
- OpenID Connect Core 1.0
- OAuth 2.0 Token Exchange
- OpenID Shared Signals Framework 1.0