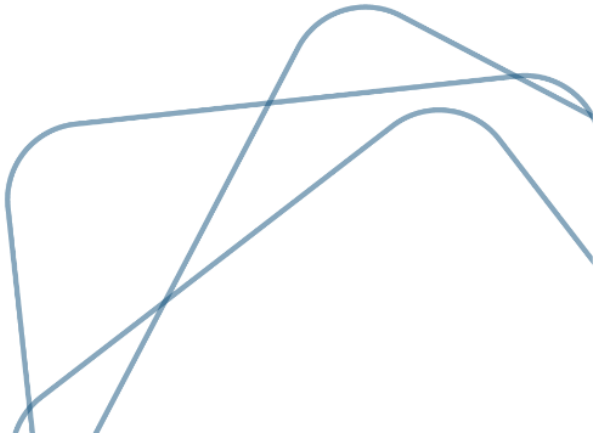
AUTENTIKA

Guia para desenvolvedores

nosi
we believe in...

Definições, siglas e abreviaturas

AD	Active Directory
RTPE	Rede Tecnológica e Privativa do Estado
OAuth	Open Standard For Authorization
OpenID Connect	Identity Layer on top of OAuth 2.0
SSO	Single Sign-on
WSO2	Integration Vendor Company
WSO2 IS	WSO2 Identity Server



Índice

Introdução

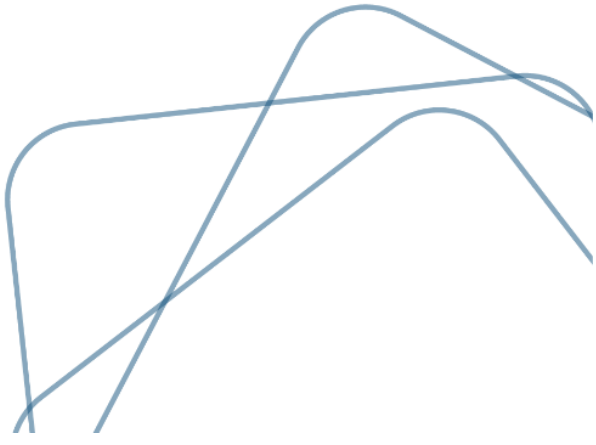
AUTENTIKA é a plataforma de gestão de identidade eletrónica e autenticação do estado de Cabo Verde.

Facilita a identificação segura e confiável entre os cidadãos e os provedores de serviços online. Os cidadãos utilizam várias aplicações no seu dia a dia para usufruir de serviços online disponibilizados pelas entidades do estado e entidades privadas. Para melhorar a experiencia na utilização desses serviços, o AUTENTIKA fornece o serviço de Single Sign-on (SSO).

Tem como objetivo principal disponibilizar ao Estado, mecanismos de gestão de dados de identidade e controlo de acesso de uma forma centralizada. Essa plataforma permite a aplicações terceiras (previamente registadas) autenticarem os seus utilizadores e fornece meios para garantir o SSO.

É responsável pela gestão os dados de identidade, a autenticação e a autorização. Os processos de autenticação e autorização serão garantidos por protocolos como o SAML, OAuth 2.0, OpenID Connect, garantindo sempre que nenhuma aplicação tenha acesso ás credenciais dos utilizadores.

Na sua implementação foi utilizada o produto de WSO2 nomeadamente o WSO2 Identity Server (WSO2 IS).



Guia para desenvolvedores

Como iniciar

Iniciando

Esta secção orientará você sobre como iniciar a integração da sua aplicação com o AUTENTIKA, incluindo o registo da sua aplicação no AUTENTIKA, a descrição dos dados do utilizador que será retornada pelo AUTENTIKA e a implementação do protocolo OpenID Connect.

Registo da aplicação

Para que a sua aplicação possa autenticar os seus utilizadores via AUTENTIKA, o mesmo tem de estar registado como um provedor de serviço no AUTENTIKA. Para iniciar o processo de registo, entre em contacto com a nossa equipa.

Devem fornecer os seguintes detalhes:

- ***Nome da aplicação:*** um nome que identifica a aplicação. Esse nome é apresentado ao utilizador na página de consentimento;
- ***Url de redireccionamento:*** endereço da aplicação para onde o utilizador será redirecionado após autenticar-se;
- ***Lista de atributos:*** listagem dos atributos do utilizador que devem ser retornados para a aplicação. Existem algumas restrições de atributos que podem ser retornados, dependendo da natureza da aplicação. Ex: email, nome...
- ***Métodos de autenticação:*** O AUTENTIKA disponibiliza 3 métodos de autenticação nomeadamente:

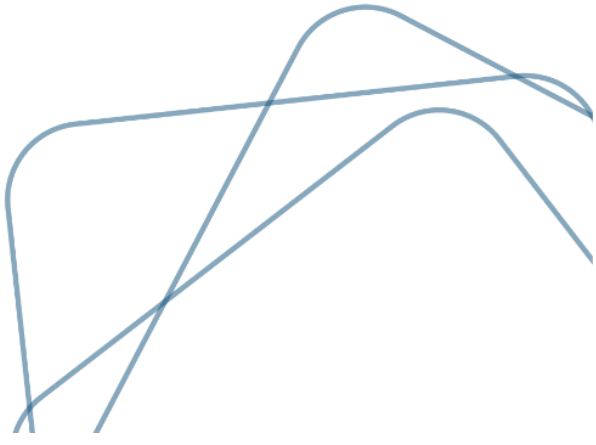
- ***Autenticação Básica:*** permite ao cidadão, com recurso a um email e palavra-passe (Canta de RPTE ou PortonDeNosIlha) fazer a sua autenticação.

- ***Autenticação com Documento de Identificação:*** método de autenticação que permite ao cidadão, nacional ou, com recurso ao seu documento de Identificação (CNI) e respetivo código PIN de autenticação.

- ***Autenticação com Chave Móvel Digital de Cabo Verde:*** Permite associar um número de telemóvel ao número de Identificação civil. É composta por um código numérico de autenticação (PIN) permanente, escolhido e alterável pelo cidadão, bem como, por um código numérico de segurança de utilização única e temporária, gerado pelo sistema em cada autenticação.

Após o registo, são fornecidos os seguintes detalhes ao desenvolvedor da aplicação:

- Um identificador único da aplicação (Client ID)
- Uma chave secreta (Client Secret)
- Endpoints do OpenID Connect



Dados do utilizador

Após a autenticação do utilizador, a sua aplicação poderá fazer uma requisição para os dados de seu perfil, incluindo o seu nome e o seu email.

O AUTENTIKA apenas partilha os dados do utilizador após o mesmo dar o seu consentimento (o consentimento é solicitado ao utilizador durante o processo de autenticação). O AUTENTIKA utiliza o email como o principal identificador do utilizador.

OpenID Connect

AUTENTIKA utiliza o protocolo OpenID Connect (OIDC) para permitir as aplicações verificar a identidade dos utilizadores e obter as informações do seu perfil.

O **OIDC** é um protocolo de autenticação implementada sobre o protocolo OAuth 2.0, fornecendo segurança no processo de autenticação e ao mesmo tempo, garantindo uma boa experiência de utilização por parte dos utilizadores.

Para mais informações sobre como o AUTENTIKA suporta o OIDC clique aqui

OpenID Connect 2.0

O **OIDC** é um protocolo de autenticação implementada sobre o protocolo OAuth 2.0. Enquanto que o protocolo OAuth 2.0 é destinado ao controlo de acesso e partilha de recursos o protocolo OIDC é destinado a autenticação de utilizadores.

Este protocolo garante a implementação do Single Sign-on (SSO) de forma segura. O SSO permite aos utilizadores autenticarem uma única vez e ter acesso a múltiplas aplicações.

Como funciona

Os passos a seguir ilustram como funciona a autenticação dum utilizador numa aplicação via AUTENTIKA:

- Quando o utilizador iniciar o processo de autenticação na aplicação, a aplicação envia uma requisição de autorização ao AUTENTIKA (redireciona o utilizador para o AUTENTIKA);
- O AUTENTIKA autentica o utilizador ou solicita as credenciais de acesso caso o utilizador ainda não estiver autenticado e solicita o consentimento (autorização) do utilizador para a partilha dos dados de perfil com a aplicação;
- Após o utilizador autenticar e autorizar a partilha dos dados, o AUTENTIKA redireciona o utilizador para a aplicação e envia á aplicação um código de acesso;
- A aplicação faz uma requisição ao AUTENTIKA, passando o código de acesso e solicitando o token de acesso;
- O AUTENTIKA valida o código e retorna á aplicação o token de acesso;
- A aplicação requisita os dados do utilizador ao AUTENTIKA, identificando-se com o token de acesso.

Token de acesso

Os tokens de acesso são credenciais utilizadas pelas aplicações para consumir uma determinada API. O AUTENTIKA gera e faz a gestão do ciclo de vida dos tokens.

Token de identidade (ID Token)

O ID token é uma JSON Web Token (JWT) que contem os dados de perfil de um utilizador (e outros metadados), sendo composto pelo cabeçalho, corpo e assinatura. É consumida pela aplicação para obter os dados de perfil do utilizador (como por exemplo o nome e o email).

Exemplo duma ID token:


```
{
 "sub"      : "pedro.ramos@nosi.cv",
 "iss"      : "https://autentika.gov.cv/oauth2/oidcdiscovery",
 "aud"      : "74zdFEfgdZ6L1Ze82ZID8",
 "auth_time" : 1563964449,
 "iat"      : 1563968049,
 "exp"      : 1563964449
}
```

Claims

Uma claim é uma informação que caracteriza uma entidade (como por exemplo o nome ou o email). Uma JWT contém um conjunto de claims.

Endpoints do OpenID Connect

Authorization Endpoint

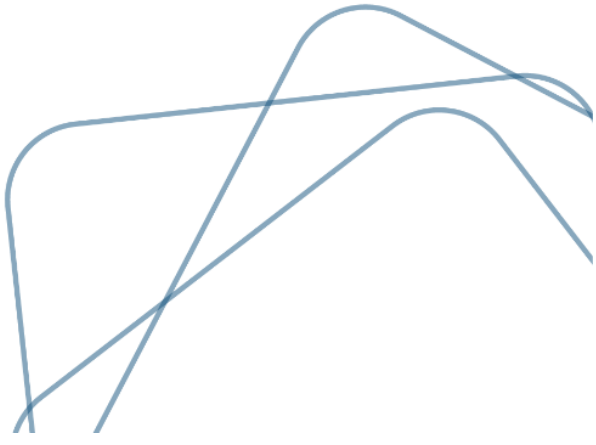
Este é o endpoint do AUTENTIKA onde o utilizador é solicitado para autenticar e autorizar a partilha dos dados de seu perfil (como por exemplo nome e email) com uma determinada aplicação.

Quando um utilizador aceder uma aplicação que requer autenticação, ele é redirecionado para este endpoint. Esse é o único endpoint em que o utilizador interage com o AUTENTIKA (normalmente via um browser web).

Token Endpoint

O Token Endpoint é utilizado pelas aplicações para obter tokens, incluindo o ID Token e o Access Token. Para autenticar-se nesse endpoint, a aplicação deve apresentar o seu ID e a sua chave secreta na requisição.

A chamada a este endpoint deve ser realizada com o método POST e a comunicação deve utilizar o protocolo TLS.



UserInfo Endpoint

As aplicações utilizam o UserInfo Endpoint do AUTENTIKA para obter claims (atributos) do utilizador autenticado. Apenas são retornados os atributos autorizados pelo utilizador.

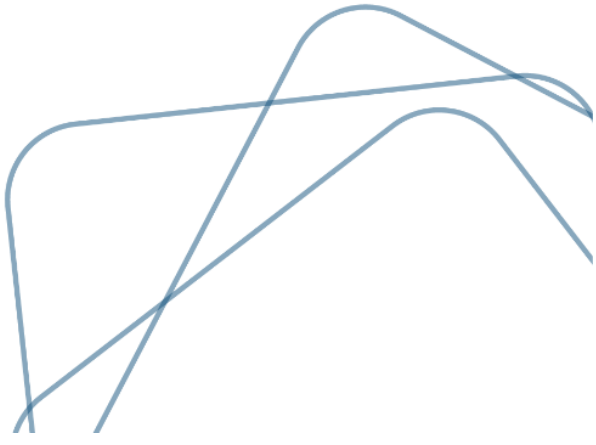
Para identificar-se, a aplicação deve apresentar um token de acesso válido. A chamada a este endpoint pode ser feita utilizando tanto o método GET como o método POST, mas a comunicação deve utilizar o protocolo TLS.

Na resposta do AUTENTIKA os claims são apresentados num objeto JSON em forma de pares chave (nome do atributo) e valor (valor do atributo).

Endpoints adicionais

A listagem a seguir descreve endpoints adicionais:

- **Token Revocation Endpoint**: Permite às aplicações revogar um token de acesso ou uma refresh token
- **Token Introspection Endpoint:** Endpoint para validar um token. A resposta ao chamar esse endpoint inclui a validade do token e quantos segundos restam para o token tornar inválido (para o fim do seu tempo de vida)
- **Session IFrame Endpoint**: Permite ás aplicações monitorar o estado da autenticação do utilizador no AUTENTIKA (verificar se o utilizador continua autenticado ou fez o logout).



- **Logout Endpoint**: É utilizado pela aplicação para redirecionar o utilizador para a página de logout do AUTENTIKA. Na página de logout o AUTENTIKA disponibiliza a opção de logout ao utilizador.

Atributos do utilizador (Claims)

Definição de Claim

Cada dado que caracteriza ou está associado a um utilizador é designado de claim. Como exemplo de claims temos o nome, o email e a data de nascimento do utilizador. O perfil do utilizador consiste num conjunto de claims. AUTENTIKA permite a partilha dos claims com o consentimento do utilizador, durante o processo de autenticação. A partilha dos claims com outras aplicações é realizada via Token de Identidade (ID Token), ou seja, um conjunto de claims são empacotados numa Token de Identidade antes do seu envio para a aplicação.

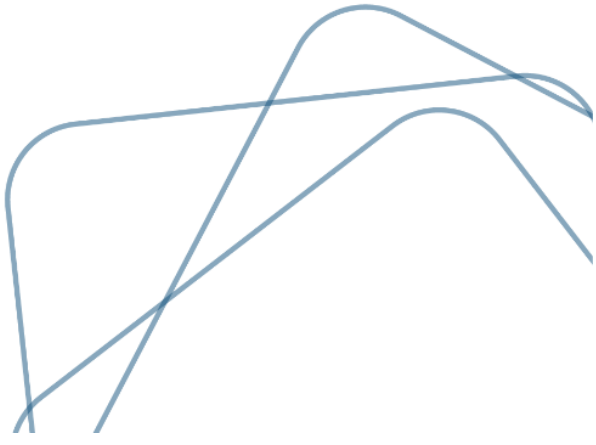
Especificação de atributos

Por padrão o AUTENTIKA partilha apenas o email do utilizador com outras aplicações. No momento de registo da aplicação o desenvolvedor deve especificar todos os atributos de deseja que seja retornada pelo AUTENTIKA.

Na especificação um atributo pode ser caracterizado como opcional ou obrigatório:

- Um atributo opcional será retornado apenas se estiver preenchido no perfil do utilizador. Caso não estiver preenchido será retornada um valor nulo;
- Um atributo obrigatório será sempre retornado á aplicação. Caso não estiver preenchido no perfil do utilizador, o AUTENTIKA solicita ao utilizador durante o processo de autenticação.

Por exemplo, considere o cenário em que o AUTENTIKA está configurado para retornar os atributos email, nome, telefone e data de nascimento a uma aplicação. Considere que os atributos email, nome e data de nascimento são obrigatórios e no perfil do utilizador os atributos telefone e data de nascimento não estão preenchidos. Nesse caso, apenas o valor do atributo telefone será retornada como nulo. O atributo data de nascimento será solicitada durante o processo de autenticação.



Como configurar SSO

O **Single Sign-on (SSO**) é um serviço que permite o utilizador identifica-se apenas uma vez e ter acesso a múltiplas aplicações, melhorando assim a sua experiência na utilização de serviços online. O AUTENTIKA permite a aplicações autenticar os seus utilizadores utilizando o protocolo OpenID Connect.

Este documento descreve como o AUTENTIKA implementa o protocolo OpenID Connect, incluindo os detalhes da iteração entre uma Aplicação e o AUTENTIKA durante o processo de autenticação

Implementar Autenticação OpenID

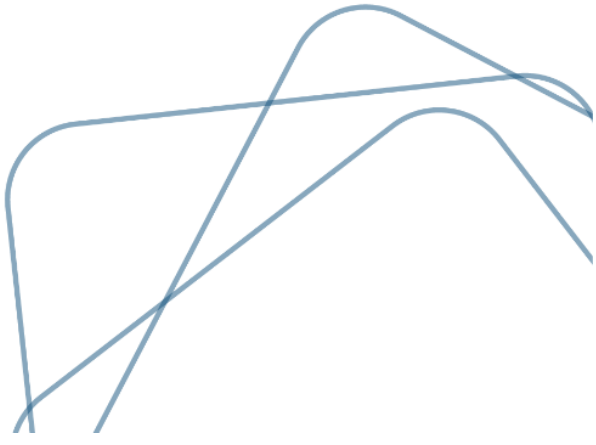
A sua aplicação deve implementar as especificações da Autenticação OpenID.

Os principais frameworks de desenvolvimento modernos possuem bibliotecas/plugins que implementam as especificações da Autenticação OpenID.

É recomendado utilizar uma implementação já testada em vez de codificar a sua implementação de base, devido as implicações de segurança

Autenticar o utilizador

A autenticação do utilizador consiste em enviar uma requisição de autenticação, redirecionando o utilizador para o AUTENTIKA com o objetivo de obter uma Token de identidade (ID Token). O ID Token consiste numa JSON Web Token que codifica os dados de identidade do utilizador.



Existem diferentes tipos de concessão de autorização segundo a especificação. Neste documento está descrito a concessão de autorização utilizando um código (Authorization Code).

A aplicação executa os seguintes passos para autenticar o utilizador:

- Prepara e envia uma requisição de autenticação
- Requisita o token utilizando o código de autorização
- Utiliza o token para obter as informações do utilizador
- Autentica o utilizador

➢ Requisitar autenticação

A aplicação inicia o processo de autenticação, preparando uma requisição de autenticação e redirecionando o utilizador para o AUTENTIKA. Essa requisição é uma requisição de autorização OAuth 2.0 para autenticação do utilizador (o pedido de autenticação é especificado passando o valor OpenID no parâmetro scope).

Segue um exemplo de um redireccionamento de autenticação:

```
HTTP/1.1 302 Found

Location: https://autentika.gov.cv/oauth2/authorize?

        response_type=code

         &scope=openid

         &client_id=s6BhdRkqt3

         &state=af0ifjsldkj

         &redirect_uri=https%3A%2F%2Fexemplo.app.cv%2Fcb
```

A listagem a seguir caracteriza cada um dos parâmetros da requisição acima:

Parâmetro	Obrigatório	Descrição
scope	Sim	Especifica o escopo da requisição. A requisição OpenID deve conter o valor ***onpenid*** nesse parâmetro. Valores adicionais podem ser incluidos no parâmetro scope
response_type	Sim	Indica o tipo de concessão de autorização. Utilize o valor *code* para a concessão do tipo código
client_id	Sim	O id que identifica a aplicação no AUTENTIKA. Esse valor é atribuído no momento do registo da aplicação no AUTENTIKA
state	Não*	Valor opaco utilizado para manter o estado entre a requisição e a chamada de volta (entre a aplicação e o AUTENTIKA)
redirect_uri	Sim	URI de redireccionamento por onde o utilizador será redirecionado após autenticar-se. Essa URI deve ser exatamente igual ao fornecido no registo da aplicação

* Não é obrigatório, mas é recomendado passar esse parâmetro.

Ao receber esta requisição, o AUTENTIKA executa as seguintes ações:

- Autentica o utilizador
- Solicita o consentimento do utilizador
- Redireciona o utilizador para a aplicação (redirect_uri) com um código de autorização

Exemplo dum retorno para a aplicação:

```
HTTP/1.1 302 Found

Location: https://exemplo.app.cv/cb?

 code=SplxlOBeZQQYbYS6WxSbIA

 &state=af0ifjsldkj
```

A aplicação deve validar o parâmetro state e proceder para a troca do código pelo ID Token.

- **Requisitar o token**

A aplicação requisita o token de acesso e o ID Token ao AUTENTIKA, utilizando o código recebido e identificando-se com o seu ID e a sua chave secreta. Essa requisição deve ser realizada no backend e possui a vantagem de não expor os tokens ao agente do utilizador (web browser) e garantir a autenticação da aplicação no AUTENTIKA.

Segue-se um exemplo de uma requisição por um token:

```
POST /oauth2/token HTTP/1.1
Host: autentika.gov.cv
Content-Type: application/x-www-form-urlencoded
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
grant_type=authorization_code&code=SplxlOBeZQQYbYS6WxSbIA
&redirect_uri=https%3A%2F%2Fexemplo.app.cv%2Fcb
```

O ID da aplicação e a sua chave secreta são enviadas no cabeçalho de autorização (Authorization header).

Descrição dos parâmetros da requisição:

- **grant_type:** deve ser definido como "authorization_code"
- **code**: o código de autorização recebido do A
- **redirect_uri:** a mesma URI de redireccionamento utilizado nas etapas anteriores

Após validar a requisição o AUTENTIKA retorna um objeto JSON, incluindo o ID token e o token de acesso, como mostra o seguimento a seguir:

```
HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache
{
 "id_token": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjFlOWdkazcifQ.ewogImlzc
yI6ICJodHRwOi8vc2VydmVyLmV4YW1wbGUuY29tIiwKICJzdWIiOiAiMjQ4Mjg5
  NzYxMDAxIiwKICJhdWQiOiAiczZCaGRSa3F0MyIsCiAibm9uY2UiOiAibi0wUzZ
fV3pBMk1qIiwKICJleHAiOiAxMzExMjgxOTcwLAogImlhdCI6IDEzMTEyODA5Nz
AKfQ.ggW8hZ1EuVLuxNuuIJKX_V8a_OMXzR0EHR9R6jgdqrOOF4daGU96Sr_P6q
Jp6IcmD3HP99Obi1PRs-cwh3LO-p146waJ8IhehcwL7F09JdijmBqkvPeB2T9CJ
 NqeGpe-gccMg4vfKjkM8FcGvnzZUN4_KSP0aAp1tOJ1zZwgjxqGByKHiOtX7Tpd
QyHE5lcMiKPXfEIQILVq0pc_E2DzL7emopWoaoZTF_m0_N0YzFC6g6EJbOEoRoS
   K5hoDalrcvRYLSrQAZZKflyuVCyixEoV9GfNQC3_osjzw2PAithfubEEBLuVVk4
   XUVrWOLrLl0nx7RkKU8NXNHq-rvKMzqg"
 "access_token": "SlAV32hkKG",
 "token_type": "Bearer",
 "expires_in": 3600,
}
```

O seguimento a seguir exemplifica a resposta a uma requisição inválida:

```
HTTP/1.1 400 Bad Request
 Content-Type: application/json
 Cache-Control: no-store
 Pragma: no-cache
 {
  "error": "invalid_request"
 }
```

A aplicação deve validar o ID Token antes da sua utilização.

O token de acesso será utilizado na requisição de informações do perfil do utilizador.

Obter informações do utilizador

A aplicação utiliza o token de acesso na requisição às informações de perfil (claims) do utilizador autenticado. Na solicitação, pode especificar um escopo que inclui um conjunto de atributos ou pode especificar cada atributo individualmente.

A resposta do AUTENTIKA consiste num objeto JSON que contém os claims/atributos do utilizador em forma de pares nome e valor.

Por exemplo, a requisição às informações do utilizador incluindo o escopo email (scope=openid%20email) segue o seguinte formato:

```
HTTP/1.1 302 Found
Location: https://autentika.gov.cv/oauth2/authorize?
        response_type=code
        &scope=openid%20email
        &client_id=s6BhdRkqt3
        &state=af0ifjsldkj
        &redirect_uri=https%3A%2F%2Fexemplo.app.cv%2Fcb
```

Exemplo da resposta com as informações do utilizador (ao chamar o /oauth2/userinfo), seria por exemplo:

```
HTTP/1.1 200 OK
 Content-Type: application/json
 {
  "sub": "248289761001",
  "name": "Pedro Ramos",
  "given_name": "Pedro",
  "email": "pedro.ramos@nosi.cv",
}
```

São retornados apenas os atributos que o utilizador tiver preenchido no seu perfil.

Garanta que a sua aplicação solicite apenas os atributos essenciais, pois o aumento do número de atributos solicitados diminui a chance do utilizador conceder a autorização (aprovar a partilha dos dados).

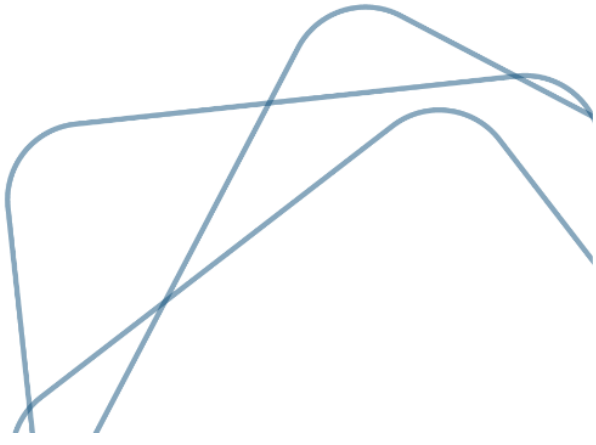
Autenticar o utilizador na aplicação

Após obter as informações do utilizador a aplicação determina se trata de um novo utilizador ou se trata de um utilizador já registado.

Caso for um utilizador já registado, por exemplo uma aplicação web poderá iniciar a sessão para esse utilizador. Ao navegar entre as páginas a aplicação verifica se o utilizador está autenticado a partir dos dados de sessão.

Caso for a primeira vez que o utilizador visita a aplicação (novo utilizador), é criada a sua conta com base nas informações recebidas do Autentika (como por exemplo o nome e o

email). Caso essas informações não forem suficientes para o registo a aplicação poderá solicitar dados adicionais ao utilizador.



Perguntas frequentes

O que é AUTENTIKA?

AUTENTIKA é o servidor de identidade e de gestão de acesso do Estado de Cabo Verde. Aplicações e serviços do estado podem utilizar o AUTENTIKA para autenticar os utilizadores e garantir o Single Sign-on de forma segura.

O que é o Single Sign-on (SSO)?

O Single Sign-on é um serviço que permite o utilizador autenticar-se apenas uma vez e tem acesso a múltiplas aplicações, melhorando assim a sua experiência na utilização de serviços online.

Como é feita a autenticação no AUTENTIKA?

O AUTENTIKA disponibiliza os seguintes métodos de autenticação:

- **Autenticação Básica** - com recurso a um email e palavra-passe;
- **Autenticação com Chave Móvel Digital de Cabo Verde** - com recurso a um número de telemóvel, PIN de autenticação e código temporário;
- **Autenticação com Documento de identificação civil** - com recurso a utilização do middleware, leitor de cartões, CNI e o respetivo PIN de autenticação.

Que aplicações podem utilizar o AUTENTIKA?

Qualquer aplicação que ofereça serviços uteis para os cidadãos cabo-verdianos.

Como uma aplicação integra com o AUTENTIKA?

Uma aplicação integra com o AUTENTIKA utilizando o protocolo OpenID Connect (OIDC).

O que é o protocolo OpenID Connect (OIDC)?

O OIDC é um protocolo de autenticação implementada sobre o protocolo OAuth 2.0.