

Fornecedor de Identidade na RCTSaai



Todos os pedidos de esclarecimento devem ser enviados para: noc@fccn.pt.

1º Passo - Pedido formal de ligação

Para pertencer à federação de Identidade RCTS como Fornecedor de Identidade, a organização candidata tem de ser elegível para participação na RCTS e tem de ser uma entidade utilizadora da RCTS (através da ligação da sua rede à RCTS).

Para realizar o pedido formal de ligação devem enviar um email para o endereço de correio noc@fccn.pt com os seguintes documentos devidamente preenchidos:

- [Pedido de Ligação à Federação de Identidade RCTS](#)
- [Declaração de Práticas de Gestão de Identidade](#)



Objectivo

A declaração tem como objetivo descrever o ciclo de vida da gestão de identidades, incluindo os processos de inscrição, manutenção e remoção de informação de identidade no sistema de gestão de identidades.

A declaração tem de descrever o conjunto de processos administrativos, procedimentos e tecnologias relevantes usadas no ciclo de vida da gestão de identidades. Os processos, procedimentos e tecnologias descritos na declaração têm de ser capazes de suportar, de forma consistente e segura, o ciclo de vida da gestão de identidades.

Devem preencher uma declaração por cada fornecedor de identidade que pretendem integrar na federação.

2º Passo - Assinatura do protocolo de adesão

Após a avaliação e aprovação da(s) Declarações de Práticas de Gestão de Identidade pela equipa de operação da federação, são enviados os documentos referentes ao protocolo de adesão da Federação de Identidade RCTS por email à organização.

Todos os documentos estão disponíveis para assinatura tradicional e digital. É recomendado a utilização da assinatura digital.

Como requisito os membros tem de publicar a sua Política de Utilização Aceitável (AUP).



Política de Utilização Aceitável (AUP)

Os membros têm de publicar a sua Política de Utilização Aceitável (AUP) para os serviços abrangidos pela política da federação de Identidade RCTS. A AUP TEM DE cobrir todas as atividades e/ou comportamentos considerados inaceitáveis aquando da utilização do serviço. É recomendada a formalização da aceitação da AUP por cada um dos Utilizadores antes do início da utilização do serviço.

3º Passo - Instalação do Fornecedor de Identidade em ambiente de testes

A instalação e configuração dos Fornecedores de Identidade fica a cargo de cada um dos membros da RCTSaai, prestando a FCCN o apoio necessário a essa instalação.

Software SAML 2.0 suportado pela equipa de operação da federação:

? Anexo Desconhecido

Pacote de software Open Source com mais expressão e utilização desenvolvido pela Internet2. Baseado em Standards o Shibboleth pode ser instalado em várias arquitecturas (baseado em SAML 2.0/ JAVA).

? Anexo Desconhecido

Aplicação desenvolvida em PHP nativo pela UNINETT no contexto do eduGAIN. O SimpleSAMLphp suporta vários protocolos de federação, mecanismos de autenticação e pode ser utilizado em simultâneo como Service Provider e Identity Provider (baseado em SAML 2.0/PHP) .

A configuração inicial do fornecedor de identidade tem de realizar-se obrigatoriamente no ambiente de testes. Para realizar esta configuração é necessário contactar a equipa de operação da federação, devem realizar este contacto através do endereço de correio noc@fccn.pt.

Para realizar a passagem para o ambiente de produção é necessário cumprir os seguintes requisitos:

- Utilização de um certificado de servidor com Extended Validation (maior credibilidade de que o utilizador está autenticar-se na sua instituição)
- Utilização de um layout responsive e que permita ao utilizador identificar-se com a instituição
- Existência dos seguintes links:
 - Link de Suporte aos utilizadores: página web onde os utilizadores podem consultar informação adicional sobre a forma de obter suporte da sua instituição
 - Link para Informação de Segurança: página web onde os utilizadores podem consultar informação sobre os mecanismos de segurança usados nos processos de autenticação
 - Link Recuperação de Password: página web onde os utilizadores podem obter informação sobre como recuperar ou alterar a sua palavra passe

Exemplo da geração automática do ficheiro de metadados da FCCN após o preenchimento na interface do RCTSaai-RR:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui" xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi" xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol" xmlns:wayf="http://sdss.ac.uk/2006/06/WAYF" xmlns:elab="http://eduserg.org.uk/labels" xmlns:ukfedlabel="http://ukfederation.org.uk/2006/11/label" xmlns:init="urn:oasis:names:tc:SAML:profiles:SSO:request-init" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xi="http://www.w3.org/2001/XInclude" entityID="https://idp.fccn.pt/idp/shibboleth">
  <md:Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="https://www.fccn.pt" registrationInstant="2011-12-16T09:00:00Z"/>
  </md:Extensions>
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol urn:oasis:names:tc:SAML:1.1:protocol">
    <md:Extensions>
      <shibmd:Scope regexp="false">fccn.pt</shibmd:Scope>
    <mdui:UIInfo>
      <mdui:DisplayName xml:lang="en">FCT|FCCN</mdui:DisplayName>
      <mdui:DisplayName xml:lang="pt">FCT|FCCN</mdui:DisplayName>
      <mdui:InformationURL xml:lang="en">https://www.fccn.pt/en/</mdui:InformationURL>
      <mdui:InformationURL xml:lang="pt">https://www.fccn.pt</mdui:InformationURL>
      <mdui:Logo width="300" height="55">https://rctsaai-rr.fccn.pt/rr/logos/FCT-FCCN_cmyk.png</mdui:Logo>
    </mdui:UIInfo>
    <mdui:DiscoHints>
      <mdui:GeolocationHint>geo:38.7591742762959,-9.142287969589233</mdui:GeolocationHint>
      <mdui:DomainHint>fccn.pt</mdui:DomainHint>
    </mdui:DiscoHints>
  </md:Extensions>
  <md:KeyDescriptor>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>
MIIDFzCCAf+gAwIBAgIUgjtXRHoicZCdPTxK6N9BrR1vZ8wDQYJKoZIhvcNAQEF
BQAwFjEUMBIGALUEAxMLaWRwLmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWhcNMzEx
MjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTEx
WjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEg
YDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtp
ZHAuZmZjY24ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24.
ucHQwHhcNMTEwMjE1MTUzOTExWjAAMRQwEgYDVQQDEwtpZHAuZmZjY24ucHQwHhcNMTE
wMjE1MTUzOTExWjAAMRQwEgYDVQQDEw
```

```

aWJib2xldGgwHQYDVR0OBBYEFAPVb6XSbr8AYJEn/xiLnVzx8KSoMA0GCSqGSIb3
DQEBBQUAA4IBAQDF0YZ3v7xshyEUHIRxc8c2jM2cJOUBRj7aOqnJvOnK7FI/AaSG
qtEMx9RJ+NHxr5sALx1/DBulXPedtubfueL0C5ky4H8a78LRqH3x50oZto+Oq1DG
hZr/kURJyAM9dzi8BYZx5K2wB9vvJO2DICmmla20DTlKPY8NMZwtFbwfMloQduMi
bLamlwEq+9o8TKYrw4C0pBGa8nY9gDjBlyzbT04VAuqctQL0+Sw+cXFDEk2JLbCl
Bo4JbRU3T37aRSPJmLSx/LEQMBKP3cqlq+eig/e6thk3SA494XDUF1O6V+0XQF+u
G5N6Vkl0FX4oQt/9e14FaHZtwfb5uf02x6oO
</ds:X509Certificate>
  </ds:X509Data>
  </ds:KeyInfo>
</md:KeyDescriptor>
<md:NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
<md:SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest" Location="
https://idp.fccn.pt/idp/profile/Shibboleth/SSO"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
https://idp.fccn.pt/idp/profile/SAML2/POST/SSO"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
Location="https://idp.fccn.pt/idp/profile/SAML2/POST-SimpleSign/SSO"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
https://idp.fccn.pt/idp/profile/SAML2/Redirect/SSO"/>
</md:IDPSSODescriptor>
<md:Organization>
  <md:OrganizationName xml:lang="pt">FCCN - unidade da FCT I.P.</md:OrganizationName>
  <md:OrganizationName xml:lang="en">FCCN</md:OrganizationName>
  <md:OrganizationDisplayName xml:lang="pt">FCCN - unidade da FCT I.P.</md:OrganizationDisplayName>
  <md:OrganizationDisplayName xml:lang="en">FCCN</md:OrganizationDisplayName>
  <md:OrganizationURL xml:lang="pt">https://www.fccn.pt</md:OrganizationURL>
  <md:OrganizationURL xml:lang="en">https://www.fccn.pt</md:OrganizationURL>
</md:Organization>
<md:ContactPerson contactType="technical">
  <md:GivenName>Esmeralda</md:GivenName>
  <md:SurName>Pires</md:SurName>
  <md:EmailAddress>mailto:rctsaai@fccn.pt</md:EmailAddress>
</md:ContactPerson>
<md:ContactPerson contactType="support">
  <md:GivenName>Equipa</md:GivenName>
  <md:SurName>RCTSaai</md:SurName>
  <md:EmailAddress>mailto:rctsaai@fccn.pt</md:EmailAddress>
</md:ContactPerson>
</md:EntityDescriptor>

```

É necessário que os valores dos atributos a serem enviados para os serviços estejam de acordo com os esquemas utilizados na RCTSaai. Para mais informações sobre os atributos e respetivos valores consulte o link [Atributos RCTSaai e eduGAIN](#).

O novo serviço de monitorização RCTSaai requer que cada instituição membro forneça credenciais de testes. Em breve será disponibilizado o "Weathermap RCTSaai".