|  |  |
| --- | --- |
|  | UNIVERZITA KARLOVA |
|  |

**Specifikace autentizace prostřednictvím CAS**

**Projekt:**

RUK - OV - Dodávka, podpora a rozvoj CAFM systému na Univerzitě Karlově

**Fáze:**

VZ

Obsah

[1 Úvod 3](#_Toc171604967)

[2 Definice pojmů 3](#_Toc171604968)

[3 Obecná pravidla pro komunikaci 3](#_Toc171604969)

[4 Množina poskytovaných údajů 3](#_Toc171604970)

[5 Autentizační protokoly 4](#_Toc171604971)

[5.1 OIDC (OpenID Connect) 4](#_Toc171604972)

[5.2 OAuth2 5](#_Toc171604973)

[5.3 CASv3 5](#_Toc171604974)

[5.4 Shibboleth/SAML2 6](#_Toc171604975)

[5.5 LDAP 6](#_Toc171604976)

# Úvod

Cílem tohoto dokumentu je specifikovat požadavky a možnosti integrace pořizovaného CAFM systému s CAS.

# Definice pojmů

**Autentizace** – proces ověření totožnosti uživatele. Výsledkem procesu je unikátní identifikátor uživatele, zpravidla osobní číslo.

**Autentizační server** – aplikace běžící na serveru, která umožňuje provádět autentizaci uživatelů. Zpravidla má k dispozici databázi uživatelů s jejich identifikačními údaji, případně může použít (delegovat) jiný autentizační server.

**Autentizační protokol** – komunikační protokol mezi klientem (aplikací) a autentizačním serverem, který umožňuje provést autentizaci a předat její výsledek klientovi.

**SSO (Single Sign On)** - vlastnost některých autentizačních protokolů, které umožňují provést autentizaci na základě již existující a ověřené session uživatele vůči autentizačnímu serveru.

**CAS** (Centrální Autentizační Služba) - soubor databází, aplikací a protokolů, které poskytují definovanou množinu služeb (databázi uživatelů, adresářové služby, identity management, autentizační služby).

**Administrátor CAS** – správce, který je zodpovědný za konfiguraci a provoz CAS.

**Klient (služba)** - aplikace nebo její část, která používá autentizační protokol vůči CAS.

**Administrátor služby** – správce, který je zodpovědný za konfiguraci a provoz aplikace – klienta CAS.

# Obecná pravidla pro komunikaci

Veškerá komunikace se servery CAS musí být chráněna použitím TLS protokolu se zapnutým šifrováním a ověřením identity serveru. Servery CAS používají serverové certifikáty vydané certifikační autoritou Terena TCS CA 4.

Všechny webové služby, s kterými CAS komunikuje, musí být jednoznačně identifikovány pomocí certifikátů vydaných podporovanou certifikační autoritou a při komunikaci s nimi musí být zapnuté šifrování dat a ověření identity serveru.

# Množina poskytovaných údajů

Sada dostupných údajů (atributů) je uvedena v následující tabulce:

|  |  |
| --- | --- |
| uid | Přihlašovací jméno. |
| mail | E-mailová adresa. |
| telephonenumber | Telefonní číslo (pracovní). |
| cn | Celé jméno. |
| givenname | Křestní jméno. |
| sn | Příjmení. |
| cunipersonalid | Osobní číslo. |
| cuniprincipalname | Přihlašovací jméno v IS. |
| edupersonentitlement | Přidělená oprávnění. |
| edupersonscopedaffiliation | Vztah k fakultám UK. |
| cuniscopedaffiliation | Vztah ke katedrám UK. |
| mobile | Telefonní číslo (mobil). |
| cuniauthorizedmail | Ověřená e-mailová adresa. |

Aktuálně poskytované atributy jsou součástí registrace každého klienta.

# Autentizační protokoly

Zde je přehled poskytovaných autentizačních protokolů v pořadí od preferovaných a doporučovaný postup pro jejich využití.

Všechny autentizační protokoly jsou schopné poskytovat výše definované atributy, aktuálně poskytnutá množina se může lišit dle registrace klienta.

## OIDC (OpenID Connect)

Standardizovaný SSO protokol pro autentizaci a získání informací o přihlášených uživatelích, viz https://openid.net/connect/. CAS podporuje tyto vlastnosti OIDC:

* Authorization Code Flow
* Implicit Flow
* Dynamic Discovery
* JWKS CAS OIDC endpointy mají společný URL prefix https://cas.cuni.cz/cas/oidc, popis jednotlivých endpointů je uveden v dokumentaci CAS OIDC serveru.

Postup registrace klienta:

1. administrátor aplikace pošle správci CAS žádost o registraci klienta, tato žádost musí obsahovat následující údaje:

* název služby,
* popis služby,
* odkaz na dokument popisující pravidla zacházení s osobními údaji v rámci služby (dle GDPR),
* kontakt na administrátora aplikace,
* callback URL pro OIDC

1. administrátor CAS provede registraci klienta a zašle zpět client\_id a client\_secret nutné pro konfiguraci OIDC klienta.

Dokumentace CAS OIDC serveru je zde: <https://apereo.github.io/cas/6.6.x/authentication/OIDC-Authentication.html>

## OAuth2

Standardizovaný SSO protokol pro autentizaci (a autorizaci) aplikací, viz https://oauth.net/2/. CAS podporuje tyto typy grantů OAuth2:

* Authorization Code
* PKCE
* Refresh Token

CAS OAuth2 endpointy mají společný URL prefix <https://cas.cuni.cz/cas/oauth2>, popis jednotlivých endpointů je uveden v dokumentaci CAS OAuth2 serveru.

Postup registrace klienta:

1. administrátor aplikace pošle správci CAS žádost o registraci klienta, tato žádost musí obsahovat následující údaje:

* název služby,
* popis služby,
* odkaz na dokument popisující pravidla zacházení s osobními údaji v rámci služby (dle GDPR),
* kontakt na administrátora aplikace,
* callback URL pro OAuth2

1. administrátor CAS provede registraci klienta a zašle zpět client\_id a client\_secret nutné pro konfiguraci OAuth2 klienta.

Dokumentace CAS OAuth2 serveru je zde: <https://apereo.github.io/cas/6.6.x/authentication/OAuth-Authentication.html> .

## CASv3

Autentizační SSO protokol založený na ticketech, viz <https://apereo.github.io/cas/6.6.x/protocol/CAS-Protocol-Specification.html> CAS CASv3 endpointy mají společný URL prefix https://cas.cuni.cz/cas, popis jednotlivých endpointů je uveden v dokumentaci CAS CASv3 serveru.

Postup registrace klienta:

* + klienti v doméně cuni.cz mohou použít default registraci:
  + o registraci není třeba žádat,
  + na přihlašovací stránce se zobrazuje jako název a popis služby "Aplikace UK" a "Obecná webová aplikace UK".
  + klienti mimo doménu cuni.cz mohou použít default registraci:
  + o registraci není třeba žádat,
  + na přihlašovací stránce se zobrazuje jako název a popis služby "Web aplikace" a "Obecná webová aplikace mimo UK",
  + poskytuje omezenou sadu atributů – anonymizovaný identifikátor uživatele, jméno, e-mail.
  + pokud je třeba klienta registrovat zvlášť,

1. administrátor aplikace pošle správci CAS žádost o registraci klienta, tato žádost musí obsahovat následující údaje:

* název služby,
* popis služby,
* odkaz na dokument popisující pravidla zacházení s osobními údaji v rámci služby (dle GDPR),
* kontakt na administrátora aplikace,
* URL, které bude předáváno jako parametr service

1. administrátor CAS provede registraci klienta

Dokumentace CAS CASv3 serveru je zde: <https://apereo.github.io/cas/6.6.x/protocol/CAS-Protocol.html> .

## Shibboleth/SAML2

Federativní SSO autentizační protokol založený na SAMLv2 umožňuje uživatelům přihlašování identitou své domácí organizace ke všem službám poskytovaným federací. UK je členem národní federace identit eduid.cz, součástí CAS je i Shibboleth IdP, které interně používá CASv3 protokol vůči CAS serverům pro ověření uživatelů.

Shibboleth/SAML2 endpointy IdP UK mají společný prefix https://idp.cuni.cz/idp, popis jednotlivých endpointů je součástí technické dokumentace federace i metadat IdP UK.

Postup registrace klienta:

* + registraci klienta je třeba provést ve federaci eduid.cz,
  + administrátoři CAS jsou zároveň technickým kontaktem za UK, mohou tedy provést registraci klienta z UK ve federaci,
  + o registraci požádá administrátor aplikace, součástí žádosti musí být validní metadata registrovaného SP včetně všech údajů požadovaných federací. Dokumentace federace eduid.cz je zde: <https://www.eduid.cz/>

## LDAP

Protokol LDAP lze využít pro autentizaci uživatelů, ale pouze jako náhradní řešení v případě, že není možné implementovat některý z výše uvedených autentizačních protokolů. Servery LDAP jsou dostupné na URL ldaps://ldap-ha.cuni.cz/dc=cuni,dc=cz .

Postup registrace klienta:

1. administrátor aplikace pošle správci CAS žádost o registraci klienta, tato žádost musí obsahovat následující údaje:

* název služby,
* popis služby,
* rozsah IP adres, na kterých bude služba poskytována,
* odkaz na dokument popisující pravidla zacházení s osobními údaji v rámci služby (dle GDPR),
* kontakt na administrátora aplikace,
* zdůvodnění, proč nelze implementovat jiný autentizační protokol.

1. administrátor CAS provede registraci klienta a zašle zpět údaje potřebné pro konfiguraci LDAP klienta.