CAAIS: Autentizace uživatelů pomocí SAML

Verze 1.1

6.5.2022



Zpracoval: Milan Babic

Obsah

[1. Úvod 5](#_Toc103021736)

[2. Proces autentizace pomocí SAML 6](#_Toc103021737)

[2.1. Diagram autentizace uživatele 6](#_Toc103021738)

[2.2. Předpoklady pro SAML autentizaci 7](#_Toc103021739)

[2.2.1 Registrace a konfigurace AIS v CAAIS 7](#_Toc103021740)

[2.2.2 Certifikáty 8](#_Toc103021741)

[2.2.3 Přístupové role pro AIS 8](#_Toc103021742)

[2.3. Zpracování osobních údajů 9](#_Toc103021743)

[3. Technická specifikace autentizace 10](#_Toc103021744)

[3.1. URL pro přihlášení v CAAIS 10](#_Toc103021745)

[3.2. URL pro příjem SAML response na straně AIS 10](#_Toc103021746)

[3.3. Seznam atributů uživatele (identity) v SAML response 11](#_Toc103021747)

[3.4. Definice SAML request 12](#_Toc103021748)

[3.5. Definice SAML response 13](#_Toc103021749)

[3.6. LoA (Úroveň záruk) 14](#_Toc103021750)

[3.7. URL s metadaty SAML autentizační služby 15](#_Toc103021751)

[4. Zkratky, pojmy, definice 17](#_Toc103021752)

[5. Přílohy 17](#_Toc103021753)

Seznam tabulek

[Tabulka 1: Seznam atributů - SAML Response 11](#_Toc103021754)

[Tabulka 2: Popis jednotlivých elementů - SAML2 AuthnRequest 12](#_Toc103021755)

[Tabulka 3: Popis jednotlivých elementů - SAML2 Response 13](#_Toc103021756)

[Tabulka 4: Popis jednotlivých atributů - element Assertion před zašifrováním 13](#_Toc103021757)

[Tabulka 5: Hodnoty LoA 15](#_Toc103021758)

[Tabulka 6: Popis jednotlivých atributů v XML souboru s metadaty 15](#_Toc103021759)

Verze dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| **Verze** | **Stručný popis změn** | **Zpracoval** | **Datum** |
| 1.0 | Nový dokument | Milan Babic | 6.5.2022 |
| 1.1 | Přidání atributů do odpovědi (viz kapitola 3.3) + rozšíření o další funkcionality SAML kompatibilní se standardem (viz nová kapitola 4) | Milan Babic | 15.11.2023 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Úvod

Účelem tohoto dokumentu je popsat technické detaily uživatelské autentizace do agendových informačních systémů (AIS), které jsou registrovány v systému CAAIS. Uživatel používá přihlašovací údaje do systému CAAIS-IdP (modul interního IdP CAAIS), který zde plní funkci autentizačního informačního systému dle § 56a zákona č. 111/2009 Sb., o základních registrech.

Komunikace a předávání údajů o uživateli je prováděna pomocí protokolu SAML 2.0, který se využívá pro výměnu autentizačních a autorizačních dat. Prostřednictvím SAML 2.0 protokolu se v rámci přesměrovávání uživatele mezi AIS a CAAIS předává definovaná sada atributů (viz kapitola 3.3), která je podmnožinou všech atributů, které jsou o uživateli (identitě) v systému CAAIS-IdP vedeny. Při autentizaci SAML protokolem se ani nevolají žádné další webové služby CAAIS (např. editační) pro získání ostatních atributů.

# Proces autentizace pomocí SAML

Proces autentizace uživatele, otevírajícího si stránku AIS pomocí protokolu SAML 2.0 skrze CAAIS, je popsán v následující části.

V SAML jsou definovány 3 základní role účastnící se komunikace:

* principal = uživatel
* service provider = v našem případě AIS
* identity provider = v našem případě CAAIS-IdP

## Diagram autentizace uživatele



1. Uživatel otevře webovou stránku AIS
2. Pokud systém AIS zjistí, že není uživatel přihlášen, vygeneruje SAML request a uživatel je přesměrován na webovou stránku CAAIS se zakódovaným SAML requestem (viz kapitola 3.1). Na této přihlašovací stránce CAAIS si uživatel zvolí způsob přihlášení a zadá přihlašovací údaje.
3. Systém CAAIS ověří, že autentizační metoda vybraná uživatelem splňuje úroveň LoA, která je pro daný AIS nakonfigurována v CAAIS. Provádí-li se autentizace pomocí interního CAAIS-IdP, komponenta CAAIS-IdP ještě navíc ověří správnost zadaných přihlašovacích údajů uživatele vůči uloženým údajům.
4. Pokud je autentizace úspěšná, provede CAAIS načtení informací o uživateli ze své DB. Následně se v CAAIS na základě přístupových rolí přidělených uživateli ověří, zda je oprávněn přistoupit do AIS. Pokud ano, pokračuje se dalším krokem. Jinak se uživateli zobrazí hláška o zamítnutí přístupu.
5. CAAIS vygeneruje zakódovanou SAML response.
6. A uživatel je s touto odpovědí přesměrován na definovanou adresu AIS (viz kapitola 3.2). Případné návratové URL v obdrženém SAML requestu jsou ignorovány.
7. V systému AIS se zpracuje SAML response, ze kterého se vyčtou informace o uživateli a na základě nich se umožní/neumožní přístup uživateli do AIS.

## Předpoklady pro SAML autentizaci

Pro používání SAML autentizace platí podobné předpoklady, jako pro klasickou/přímou autentizační webovou službu CAAIS (viz dokument „CAAIS: Autentizační webová služba - Procesní popis“).

### Registrace a konfigurace AIS v CAAIS

AIS musí být v systému CAAIS nejdříve zaregistrován pod definovaný subjekt, což se provádí na základě elektronického formuláře, který zástupce AIS odesílá na definovanou datovou schránku.

U takto registrovaného AIS následně provede lokální administrátor subjektu konfiguraci těchto primárních údajů:

* **Povolená návratová URL pro SAML a OIDC** – seznam návratových adres AIS, kam je uživatel přesměrován po autentizaci
* **Podepisovací certifikát** – tímto certifikátem AIS podepisuje SAML request (více viz kapitola 2.2.2).
* **Šifrovací certifikát** – CAAIS používá tento certifikát k zašifrování SAML response.

### Certifikáty

Podepisovací certifikát používá AIS pro podepisování SAML requestu.

Pomocí šifrovacího certifikátu pak AIS šifruje SAML response. Z bezpečnostních důvodů CAAIS nepoužívá pro zašifrování podepisovací certifikát obsažený v SAML requestu, ale právě šifrovací certifikát přiložený v konfiguraci AIS v CAAIS.

Oba certifikáty musí být typu komerční serverový, musí být zaregistrovány v nastavení AIS (viz kapitola 2.2.1) a musí být vydané podporovanou certifikační autoritou:

* I.CA
* PostSignum
* eIdentity
* NCA

V konfiguraci AIS v CAAIS může být zaregistrován vždy jen jeden podepisovací a jeden šifrovací certifikát. Je však možné použít stejný certifikát pro oba tyto typy certifikátů.

### Přístupové role pro AIS

V systému CAAIS je možné jednotlivým AIS definovat přístupové role, které pak daný AIS využívá pro řízení přístupu uživatelů. Nejdříve se číselník těchto přístupových rolí vytvoří u AIS a pak se tyto role přidělí konkrétním subjektům, které mají mít přístup do tohoto AIS. Lokální administrátoři těchto subjektů pak tyto přístupové role přidělují jednotlivým uživatelům daného subjektu.

Pokud nemá AIS žádné takové přístupové role vytvořeny, povolí systém CAAIS přístup do takového AIS všem uživatelům z libovolného subjektu. Za nastavení těchto rolí je tedy zodpovědný AIS.

## Zpracování osobních údajů

Modul CAAIS-IdP (interní IdP v systému CAAIS) splňuje požadavky § 56a zákona č. 111/2009 Sb., o základních registrech pro autentizační informační systém. Na základě toho mohou být v CAAIS uloženy osobní údaje uživatelů, které jsou následně předávány systémům AIS.

# Technická specifikace autentizace

V následujících kapitolách jsou uvedeny podrobné specifikace pro komunikaci systémů AIS se systémem CAAIS pomocí protokolu SAML 2.0.

## URL pro přihlášení v CAAIS

Pokud systém AIS zjistí, že uživatel přistupující na stránku AIS není přihlášen, vygeneruje SAML request, zakóduje ho a přesměruje uživatele s tímto požadavkem na přihlašovací stránku CAAIS, která má následující adresu:

|  |  |
| --- | --- |
| Prostředí | Adresa |
| testovací NAKIT | https://rest-externalsaml2api.caais-test-ext.gov.cz/samlAuthnRequest?SAMLRequest=*zakódovaný\_SAML\_request*&RelayState=*vlastní\_identifikátor* |
| provozní | https://rest-externalsaml2api.*[doména]*/samlAuthnRequest?SAMLRequest=*zakódovaný\_SAML\_request*&RelayState=*vlastní\_identifikátor*  kde *[doména]* je **gov.cz** nebo **cms2.cz** |

Je-li potřeba na straně AIS odlišit více odeslaných požadavků, lze v adrese využít nepovinný "RelayState" pro uložení vlastního identifikátoru požadavku. V odpovídající odpovědi ze systému CAAIS se pak tento identifikátor také vrací.

Definice struktury SAML request a způsob kódování je uveden v kapitole 3.4.

## URL pro příjem SAML response na straně AIS

V systému CAAIS je v konfiguraci AIS definována URL, na kterou je po úspěšném ověření uživatel přesměrován. Na tuto URL se předává v CAAIS vygenerovaná a zakódovaná SAML response, ve které je předáván atribut "SAMLResponse" a případně také nepovinný atribut "RelayState" s identifikátorem uvedeným v požadavku. Na této URL operuje AIS a danou SAML response přijímá.

Základní struktura URL, na které CAAIS zasílá SAML response, je následující:

|  |
| --- |
| URL pro SAML response |
| https://*adresa\_AIS\_uložená\_v\_konfiguraci\_AIS\_v\_CAAIS*?SAMLResponse=*zakódovaná\_SAML\_response*&RelayState=*vlastní\_identifikátor\_z\_požadavku* |

Definice struktury této SAML response a způsob kódování je uveden v kapitole 3.5

## Seznam atributů uživatele (identity) v SAML response

CAAIS může vracet v SAML response následující údaje o autentizovaném uživateli.

Tabulka 1: Seznam atributů - SAML Response

|  |  |  |
| --- | --- | --- |
| Atribut | Identifikátor atributu | Atribut z datového modelu |
| Příjmení | http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName | "Profil"."Fyzická osoba"."příjmení" (Profile.PhysicalPerson.lastName) |
| Jméno | http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName | "Profil"."Fyzická osoba"."jméno" (Profile.PhysicalPerson.firstName) |
| Datum narození | http://eidas.europa.eu/attributes/naturalperson/DateOfBirth |  |
| Místo narození | http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth |  |
| Země narození | http://www.stork.gov.eu/1.0/countryCodeOfBirth |  |
| Pseudonym | http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier | "Mapování SeP"." SePBSI" (ServiceMapping.sepBsi) pro daný "Profil"."uživatelské jméno" (Profile.loginName), poznámka - BSI se generuje v CAAIS nové, nemigruje se z JIP/KAAS |
| Zkratka subjektu | LegalEntityShorcut | "Subjekt"."zkratka" (Subject.shortcut) |
| IČO subjektu | http://eidas.europa.eu/attributes/legalperson/LEI | "Subjekt"."ič" (Subject.identificationNumber) |
| Uživatelské jméno | Username | "Profil"."uživatelské jméno" (Profile.loginName) |
| Titul před jménem | DegreeBefore | "Profil"."Fyzická osoba"."titul před" (Profile.PhysicalPerson.degreeBefore) |
| Titul za jménem | DegreeAfter | "Profil"."Fyzická osoba"."titul za" (Profile.PhysicalPerson.degreeAfter) |
| Přístupové role | AccessRoles | "Profil"."Přístupová role" (Profile.AccessRole) pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající přístupové role. Dále se dotahují i delegované přístupové role přes "Vazební profil".  V seznamu přístupových rolí se vrací pouze role pro daný AIS, do kterého se uživatel autentizuje.  V atributu bude formát XML v base 64, např. takto:  <AccessRoles>  <AccessRoleCode>editor</AccessRoleCode>  <AccessRoleCode>spravce</AccessRoleCode>  </AccessRoles> |
| Kód přístupové role | AccessRoleCode | "Přístupová role"."zkratka" (AccessRole.shortcut) |
| Činnostní role | ActivityRoles | "Profil"."Činnostní role" (Profile.ActivityRole) – pouze ty, které jsou aktivní a mají aktivní přiřazení subjektu  Pokud má profil přiřazeny Skupiny rolí nebo Business role, dotahují se přes ně odpovídající činnostní role a agendy. Dále se dotahují i delegované činnostní role a agendy přes "Vazební profil".  V atributu bude formát XML v base 64, např. takto:  <ActivityRoles>  <Agenda>  <AgendaCode>K100</AgendaCode>  <ActivityRoleCode>CR1111</ActivityRoleCode>  <ActivityRoleCode>CR2222</ActivityRoleCode>  </Agenda>  </ActivityRoles> |
| Kód agendy | AgendaCode | "Činnostní role"."Agenda"."kód" (ActivityRole.Agenda.code) |
| Kód činnostní role | ActivityRoleCode | "Činnostní role"."kód" (ActivityRole.code) |
| Email | http://www.stork.gov.eu/1.0/eMail | "Profil"."email" (Profile.email) |
| Název subjektu | LegalEntityName | "Subjekt"."název" (Subject.name) |
| Email subjektu | LegalEntityEmail | "Subjekt"."Kontakt"."Email"."adresa" (Subject.Contact.Email.address) kde "Email"."Typ emailu"."název" (Email.EmailType.name) = "Oficiální" |
| Typ instituce | InstitutionType | "Subjekt"."Typ instituce"."kód" (Subject.InstitutionType.code) |
| Osoba ztotožněna | PersonIdentified | "Profil"."Fyzická osoba"."osoba evidována v rob" (Profile.PhysicalPerson.personInRob) |
| Datum úmrtí | DateOfDeath | "Profil"."Fyzická osoba"."datum úmrtí" (Profile.PhysicalPerson.deathDate) |
| Doklady | DocumentIds | V CAAIS je pouze 1 doklad |
| Doklad (+ atribut Typ) | DocumentId (+ atribut Type) | "Profil"."Fyzická osoba"."číslo dokladu" (Profile.PhysicalPerson.documentId) a "Profil"."Fyzická osoba"."druh dokladu" (Profile.PhysicalPerson.documentType)  V atributu bude formát XML v base 64, např. takto:  <DocumentIds>  <DocumentId Type=""ID"">111</DocumentId>  <DocumentId Type=""P"">222</DocumentId>  </DocumentIds> |
| Identifikátor OVM | PublicOrganizationIdentifier | "Subjekt"."kód ovm v rovm" (Subject.ovmInRovmCode) |
| Identifikátor SPUÚ | AuthorizedPrivateEntityPersonalDataUserIdentifier | "Subjekt"."kód spuú" (Subject.spuuCode) |
| Autorizační token | TimeLimitedId | Technický atribut pro ukládání tokenů (neuveden v DM) |

AIS do SAML requestu uvádí vybranou sadu z těchto atributů, které požaduje vrátit v SAML response. AIS může v SAML request definovat, zda požaduje vrátit atribut jako povinný nebo nepovinný. Pokud požaduje povinný atribut, na který ale nemá oprávnění, systém CAAIS v SAML response vrací chybovou zprávu o neúspěšném přihlášení.

## Definice SAML request

Jak bylo uvedeno v kapitole 3.1, AIS nepřihlášeného uživatele přesměruje na definovanou URL se zakódovaným SAML requestem. Níže je uvedena definice XML struktury pro nezakódovaný SAML request typu SAML2 AuthnRequest:

Tabulka 2: Popis jednotlivých elementů - SAML2 AuthnRequest

|  |  |
| --- | --- |
| Atribut | Popis atributu |
| AuthnRequest | Element obsahující vlastní atributy SAML requestu. |
| AssertionConsumerServiceURL | Standardně obsahuje URL pro odpověď. CAAIS však tuto hodnotu ignoruje a řídí se návratovou URL definovanou v konfiguraci AIS v CAAIS. |
| Destination | URL přihlašovací stránky CAAIS (viz kapitola 3.1). Z hodnoty atributu lze ověřit, že request přichází z AIS a je určen pro CAAIS. |
| ID | Jedinečné ID SAML requestu, který si definuje AIS. CAAIS v SAML response vrací stejnou hodnotu v atributu "InResponseTo". |
| IssueInstant | Datum a čas vygenerování SAML requestu.  CAAIS z důvodu bezpečnosti ve chvíli zpracování ignoruje SAML requesty starší než 60 minut. |
| Issuer | Zkratka AIS uvedená v CAAIS |
| Signature | Podpis XML dat requestu + certifikát pro ověření platnosti tohoto podpisu. |
| Extensions | Rozšíření požadavku. |
| SPType | Typ Service Providera (veřejný, privátní). V systému CAAIS se aktuálně hodnota tohoto atributu ignoruje. |
| RequestedAttributes | Seznam povinných/nepovinných údajů uživatele, které AIS požaduje vrátit z CAAIS (viz kapitola 3.3). |
| AuthnContextClassRef | Požadované LoA (detail viz kapitola 3.6). |

S vygenerovaným SAML requestem je nutné provést následující akce, než bude přesměrován:

* komprimace algoritmem Deflate,
* zakódování pomocí Base64
* URL enkódování - nealfanumerické znaky se nahradí "%" a hexadecimální číslicí

## Definice SAML response

Jak bylo uvedeno v kapitole 3.2, CAAIS přesměruje úspěšně ověřeného uživatele na definovanou URL se zakódovanou SAML response (+ volitelně atribut "RelayState"). Níže je uvedena definice XML struktury pro nezakódovanou a nezašifrovanou SAML response typu SAML2 Response:

Tabulka 3: Popis jednotlivých elementů - SAML2 Response

|  |  |  |
| --- | --- | --- |
| Atribut | | Popis atributu |
| Response | Element obsahující vlastní atributy SAML response. | |
| Destination | URL pro příjem SAML response na straně AIS. Jde o návratovou URL definovanou v konfiguraci AIS v CAAIS. | |
| ID | Jedinečné ID SAML response, který definuje CAAIS. | |
| InResponseTo | Hodnota atributu "ID" ze SAML requestu. Slouží pro párování SAML requestu na SAML response na straně AIS. | |
| IssueInstant | Datum a čas vygenerování SAML response. | |
| Issuer | Identifikátor CAAIS-IdP ve funkci Identity Provider. | |
| Signature | Informace od podpisu XML dat. | |
| Status | Element s výsledkem autentizace pomocí SAML. | |
| StatusCode | Kód výsledku zpracování SAML requestu, tzn. výsledek autentizace. | |
| EncryptedAssertion | Element obsahující zašifrovanou SAML response. | |

Tabulka 4: Popis jednotlivých atributů - element Assertion před zašifrováním

|  |  |  |
| --- | --- | --- |
| Atribut | | Popis atributu |
| Issuer | Identifikátor CAAIS-IdP ve funkci Identity Provider. | |
| Signature | Podpis XML dat requestu + certifikát pro ověření platnosti tohoto podpisu. | |
| Subject | Základní informace autentizovaného uživatele (např. pseudonym). | |
| AttributeStatement | Element se seznamem atributů autentizovaného uživatele (identity), viz tabulka kapitola 3.3. | |
| AuthnContextClassRef | Skutečně dosažené LoA (detail viz kapitola 3.6). | |

S vygenerovanou SAML response je nutné provést následující akce, než bude vložena na definovanou URL:

* komprimace algoritmem Deflate,
* zakódování pomocí Base64
* URL enkódování - nealfanumerické znaky se nahradí "%" a hexadecimální číslicí

Po zašifrování šifrovacím certifikátem je element "EncryptedAssertion" určen pro následné podepsání podepisovacím certifikátem (oba certifikáty uloženy v konfiguraci AIS v CAAIS). V elementu "EncryptedAssertion" se nachází zašifrovaná data (uložena v elementu "CipherData") + další atributy týkající se šifrování.

|  |
| --- |
| Příklad - pro jednoduchost uveden začátek URL bez parametru "RelayState" |
| https://*adresa\_AIS*?SAMLResponse=7bvZjuRGki58f55CqLkMqLlvhZYOuAS3CJLBncGbA%2B77vvO1ziP8L%2FYzq1RqSa2ekXoa  .......... |

## LoA (Úroveň záruk)

V systému CAAIS je přiřazení úrovní záruk definováno pouze pro certifikované autentizační systémy (IdP) – např. NIA. Pokud se uživatel autentizuje pomocí NIA, vrací se v odpovědi přihlašovací metody do AIS taková úroveň LoA, kterou NIA předal.

Autentizuje-li se uživatel pomocí vnitřního systému CAAIS-IdP, vrací se v odpovědi vždy nejnižší úroveň LoA, podle toho, která byla použita v SAML (viz tabulka níže):

* http://eidas.europa.eu/NotNotified/LoA/low
* http://eidas.europa.eu/LoA/NotNotified/low“ (podle toho která hodnota byla použita v requestu).

Úroveň LoA znamená míru důvěryhodnosti, s jakou se uživatel autentizoval. Nejčastěji se používají úrovně nízká, značná a vysoká. V systému CAAIS se pracuje s těmito LoA:

Tabulka 5: Hodnoty LoA

|  |  |
| --- | --- |
| LoA | Standardizovaný identifikátor |
| nízká | http://eidas.europa.eu/NotNotified/LoA/low  http://eidas.europa.eu/LoA/low  http://eidas.europa.eu/LoA/NotNotified/low (hodnota někdy nesprávně používána zahraničními systémy, CAAIS ji také podporuje) |
| značná | http://eidas.europa.eu/NotNotified/LoA/substantial  http://eidas.europa.eu/LoA/substantial |
| vysoká | http://eidas.europa.eu/NotNotified/LoA/high  http://eidas.europa.eu/LoA/high |

Požadované LoA se uvádí v SAML requestu v atributu "AuthnContextClassRef". V atributu "Comparison" (hodnoty "exact", "minimum", "maximum" nebo "better") se pak definuje způsob porovnávání požadované LoA a dostupné LoA. Pro SAML requesty odesílané do systému CAAIS se doporučuje hodnota "minimum".

V SAML response se ve stejném atributu "AuthnContextClassRef" pak vyplní skutečné LoA podle způsobu autentizace uživatele.

## URL s metadaty SAML autentizační služby

Na následující URL adrese je k dispozici XML s metadaty služby:

|  |  |  |
| --- | --- | --- |
| Prostředí | | Adresa |
| testovací NAKIT | https://rest-externalsaml2api.caais-test-ext.gov.cz/samlIdpMetadata.xml | |
| provozní | https://rest-externalsaml2api.caais.*[doména]*/samlIdpMetadata.xml  kde *[doména]* je **gov.cz** nebo **cms2.cz** | |

Jsou v něm obsaženy informace o certifikátech (šifrovacím a podepisovacím), které webová služba používá a dále seznam atributů uživatele, které se vrací v odpovědi webové služby.

Tabulka 6: Popis jednotlivých atributů v XML souboru s metadaty

|  |  |  |
| --- | --- | --- |
| Atribut | | Popis atributu |
| Signature | Podpis XML souboru + certifikát pro ověření platnosti tohoto podpisu. | |
| KeyDescriptor use="encryption" | Šifrovací certifikát webové služby zakódován pomocí Base64. | |
| KeyDescriptor use="signing" | Podepisovací certifikát webové služby zakódován pomocí Base64. | |
| Attribute | Element obsahující informace o atributu uživatele, který se vrací v SAML response. Systém CAAIS vrací pouze takovou sadu atributů, o které je požádán v SAML requestu (automaticky se nevrací kompletní seznam atributů). | |

# Rozšíření funkcionalit SAML ve verzi 1.1

* Přidání dalších atributů do SAML response podle seznamu atributů v legacy autentizačních službách
* Rozšíření o podporu podepisování SAML requestů o variantu, kdy je podpis mimo XML (ve verzi 1.0 byla možná jenom varianta podpisu uvnitř XML). Tzn. doplnění HTTP Redirect o způsob podpisu, aby bylo kompletní HTTP Redirect binding (pro Web SSO, Single Logout)
* Do SAML doplněno SOAP rozhraní, jedná se o HTTP binding doplněný o SOAP hlavičky (pro Web SSO, Single Logout, Assertion Query/RequestRequest for Assertion by Identifier)
  + + HTTP artifact binding, pro použití v SOAP ve druhém kroku

# Zkratky, pojmy, definice

|  |  |
| --- | --- |
| **Zkratka nebo pojem** | **Vysvětlení** |
| AIFO | Agendový identifikátor fyzické osoby |
| AIS | Agendový informační systém |
| Autentizace | Ověření identity uživatele |
| Autorizace | Ověření přístupových oprávnění uživatele (často následuje po autentizaci). |
| CAAIS | Centrální autorizační a autentizační informační systém, náhrada JIP/KAAS |
| CAAIS-IdP | Interní Identity Provider v rámci systému CAAIS |
| GUID | Globally unique identifier |
| IdP | Identity Provider |
| JIP | Jednotný identitní prostor - zabezpečený adresář orgánů veřejné moci a uživatelských účtů úředníka, který je součástí systému |
| KAAS | Katalog autentizačních a autorizačních služeb |
| LoA | Level of Assurance = Úroveň záruk |
| SAML | Security Assertion Markup Language  Protokol pro výměnu autentizačních a autorizačních dat |
| SeP | Service Provider |
| URL | Uniform Resource Locator |
| XML | Extensible Markup Language |

# Přílohy

Dokument je bez příloh.