Dokumentace

k projektu Czech POINT

JIP/KAAS: Autentizace uživatelů založená na SAML

Vytvořeno dne: 18. 4. 2019
Aktualizováno: 11. 10. 2021
Verze: 1.7

Obsah

1. Úvod

1.1. Účel dokumentu

Tento dokument obsahuje technický popis autentizace uživatelů do registrovaných agendových informačních systémů (AIS) za využití přihlašovacích údajů do Czech POINT, kdy se údaje o autentizovaném uživateli předávají prostřednictvím protokolu SAML 2.0.

KAAS předává prostřednictvím protokolu SAML pouze vybrané identitní atributy o úspěšně autentizovaném uživateli. Např. nejsou předávány role přidělené uživateli. Autentizaci založenou na protokolu SAML tedy nelze využít k získání přístupových práv uživatele (tj. k jeho autorizaci).

1.2. Manažerské shrnutí

Komponenty JIP/KAAS Czech POINT zastávají funkci tzv. autentizačního informačního systému podle § 56a zákona č. 111/2009 Sb., o základních registrech.

V tomto dokumentu naleznete technický popis autentizace uživatelů do registrovaných AIS, založené na protokolu SAML 2.0. Tento protokol definuje pravidla pro výměnu autentizačních a autorizačních informací.

Autentizace uživatelů založená na protokolu SAML, implementovaná v JIP/KAAS Czech POINT, poskytuje pouze omezenou množinu identitních atributů o autentizovaném uživateli. Pokud potřebujete o uživateli vědět více informací, musíte použít klasické autentizační webové služby KAAS.

Během autentizace založené na SAML rovněž nedochází k volání žádné webové služby KAAS, veškerá data jsou předávána jako parametry v rámci redirectů uživatele mezi AIS a KAAS.

Tento dokument je určen pro vývojáře AIS, kteří potřebují do svých systémů implementovat autentizaci uživatelů za využití přihlašovacích údajů do Czech POINT a hodlají použít protokol SAML pro získání informací o autentizovaném uživateli.

1.3. Definice pojmů

Zkratka nebo pojem	Vysvětlení
AIFO	Agendový identifikátor fyzické osoby
AIS	Agendový informační systém
Autentizace	Ověření identity uživatele
Autorizace	Zjištění přístupových práv uživatele po jeho úspěšné autentizaci
CMS	Centrální místo služeb
GUID	Globally unique identifier
Identity Provider	SAML: Provádí ověření identity „principala" a výsledek ověření předává Service Providerovi.
JIP	Jednotný identitní prostor, adresářová služba obsahující údaje pro autentizaci a autorizaci uživatelů.
KAAS	Katalog autentizačních a autorizačních služeb
KIVS	Komunikační infrastruktura veřejné správy
Principal	SAML: Požaduje po Service Providerovi poskytnutí určité služby. Obvykle se jedná o lidského uživatele.

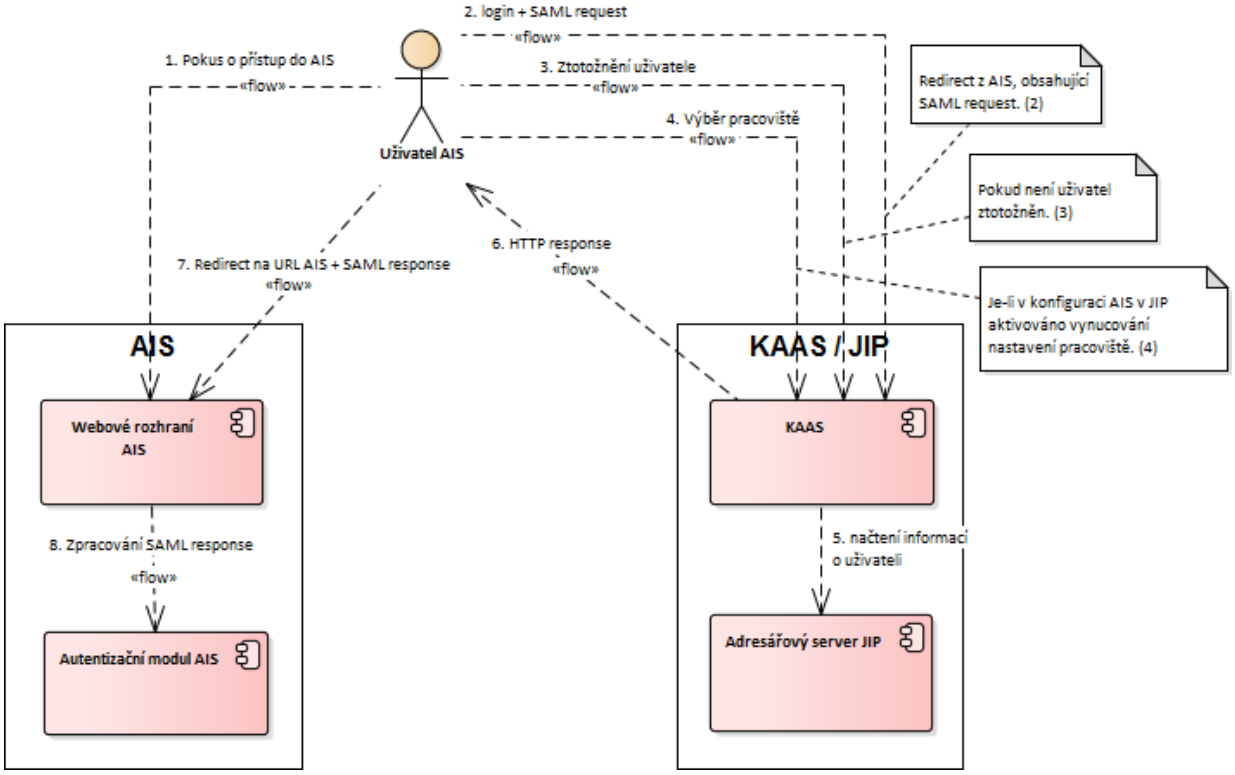
Zkratka nebo pojem	Vysvětlení
Pseudonym	Jedinečný, bezvýznamový identifikátor uživatele pro daný AIS. Platí, že daný AIS obdrží vždy stejný pseudonym pro stejného uživatele. Dva různé AISy však obdrží různé pseudonymy pro stejného uživatele. Nejedná se o AIFO ze základních registrů ani o GUID či username z JIP Czech POINT.
SAML	Security Assertion Markup Language Protokol pro výměnu autentizačních a autorizačních dat
Service Provider	SAML: Poskytuje určité služby a potřebuje autentizovat „principaly“.
SOVM	Seznam orgánů veřejné moci
URL	Uniform Resource Locator
XML	Extensible Markup Language

2. Procesní popis autentizace založené na SAML

V následujících kapitolách je popsán postup, jak AIS provádí autentizaci přistupujícího uživatele založenou na protokolu SAML 2.0 a s využitím komponent JIP/KAAS.

Z pohledu SAML vystupuje uživatel v roli „principal", AIS v roli „Service Provider" a komponenty JIP/KAAS v roli „Identity Providera".

2.1. Postup autentizace uživatele založené na SAML



Uživatel přistoupí na webovou stránku AIS (1).

Systém rozpozná, že uživatel není autentizován. Vygeneruje SAML request a přesměruje uživatele se zakódovaným SAML requestem podle specifikace v kapitole 3.1 na webovou stránku KAAS. Uživatel si na přihlašovací webové stránce KAAS vybere, jakým způsobem se přihlásí, a zadá příslušné přihlašovací údaje (2).

Pokud nebyl uživatel dosud ztotožněn, KAAS zobrazí webovou stránku pro ztotožnění osoby a uživatel musí zadat údaje pro provedení ztotožnění. KAAS, jakožto autentizační informační systém, získá z registru obyvatel AIFO a osobní údaje uživatele podle § 56a zákona č. 101/2009 Sb., o základních registrech (3).

Pokud je v konfiguraci AIS v JIP aktivováno vynucování nastavení pracoviště, KAAS dále zobrazí uživateli webovou stránku pro nastavení pracoviště a uživatel musí buď potvrdit jemu aktuálně přiřazené pracoviště, nebo ze seznamu vybrat správné pracoviště, v němž vykonává činnost (4).

KAAS ověří, že autentizační metoda, kterou uživatel použil, splňuje požadavky na způsob autentizace, nastavené v konfiguraci AIS v JIP. KAAS dále ověří správnost zadaných přihlašovacích údajů uživatele. Po úspěšné autentizaci načte KAAS z JIP informace o uživateli (5).

KAAS dále provede kontrolu rolí přidělených uživateli, zda je uživatel oprávněn přistoupit do AIS. Je-li kontrola úspěšná, pokračuje se dalším krokem, jinak je uživateli zobrazeno hlášení o zamítnutí přístupu.

KAAS vygeneruje SAML odpověď a přesměruje uživatele se zakódovanou SAML odpovědí na definovanou adresu AIS podle specifikace v kapitole 3.2 (6+7). KAAS ignoruje případné návratové URL uvedené v obdrženém SAML requestu.

AIS zpracuje přijatou SAML odpověď (8) a na základě získaných informací o uživateli posoudí, zda umožní uživateli přístup do AIS.

2.2. Předpoklady pro využívání autentizace založené na SAML

Pro využívání autentizace uživatelů založené na protokolu SAML platí v zásadě stejné předpoklady jako pro využívání klasických autentizačních webových služeb KAAS.

Další informace a důležité webové adresy jsou uvedeny v dokumentu „JIP/KAAS: Autentizační webová služba, Procesní popis".

2.2.1. Registrace AIS do JIP Czech POINT

Musí být provedena registrace informačního systému veřejné správy jako AIS do JIP Czech POINT. Pro registraci AIS se používá elektronický formulář, který se zasílá do další datové schránky Ministerstva vnitra.

2.2.2. Nastavení zaregistrovaného AIS v JIP Czech POINT

Po úspěšné registraci je dále potřeba, aby lokální administrátor subjektu, pod kterým byl daný AIS zaregistrován, provedl nastavení AIS v administrační aplikaci Správa dat SOVM. Především je zapotřebí nastavit tyto údaje:

- **URL webové služby** – návratová adresa, obsluhovaná AISem
- **Podepisovací certifikát** – AIS podepisuje pomocí tohoto certifikátu SAML request a KAAS následně používá tento certifikát k zašifrování SAML response. Další informace o podepisovacím certifikátu se nacházejí v kapitole 2.2.4.

Mezi další užitečné konfigurační parametry patří „Vyžadovaný způsob autentizace", „Vyžadovat nastavení pracoviště" a „Provozní informace".

2.2.3. Řízení přístupu uživatelů do AIS

Pro řízení přístupu uživatelů do AIS nabízí JIP Czech POINT mechanismus přístupových rolí. Po nadefinování přístupových rolí v nastavení AIS se tyto role přiřadí konkrétním subjektům, čímž se těmto subjektům povolí přístup do AIS. Lokální administrátoři těchto subjektů poté vybírají z množiny rolí přidělených subjektu a přidělují přístupové role konkrétním uživatelům.

Pokud nejsou v nastavení AIS definovány žádné přístupové role, KAAS povolí přístup do takového AIS všem uživatelům z jakéhokoliv subjektu. Řízení přístupu uživatelů je v tomto případě na zodpovědnosti daného AISu.

Pozor! V rámci autentizace založené na SAML není AISu poskytován seznam rolí přiřazených uživateli.

2.2.4. Podepisovací certifikát

AIS používá podepisovací certifikát při podepisování SAML requestu. Pro podepisovací certifikát AIS je zároveň zašifrován obsah SAML response. KAAS přitom z bezpečnostních důvodů používá k zašifrování podepisovací certifikát uložený v nastavení AIS v JIP a ne podepisovací certifikát nacházející se v SAML requestu.

AIS musí jako podepisovací certifikát používat komerční serverový certifikát vydaný komerční certifikační autoritou provozovanou českým kvalifikovaným poskytovatelem služeb vytvářejících důvěru (I.CA, PostSignum, eIdentity nebo Národní certifikační autorita).

Tento podepisovací certifikát musí být zaregistrován v nastavení AIS (viz kapitola 2.2.2). V jednom okamžiku lze mít v nastavení AIS v JIP zaregistrovaný pouze jeden podepisovací certifikát.

Teoreticky lze používat stejný komerční serverový certifikát v nastavení AIS v JIP jako autentizační i podepisovací certifikát. Z bezpečnostních důvodů ale doporučujeme používat různé certifikáty.

2.3. Seznam poskytovaných identitních atributů

Komponenta KAAS může vracet v SAML odpovědi následující údaje o autentizovaném uživateli.

AIS definuje v SAML requestu, které údaje po webové službě SAML požaduje. Mohou být definovány povinné i nepovinné údaje. Pokud AIS požaduje povinný identitní atribut, který není k dispozici, KAAS vrátí SAML odpověď se zprávou o neúspěšném přihlášení.

Atribut	Identifikátor atributu	Popis
Příjmení	http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName	Příjmení
Jméno	http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName	Jméno, případně jména
Datum narození	http://eidas.europa.eu/attributes/naturalperson/DateOfBirth	Datum narození
Místo narození	http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth	Místo narození
Země narození	http://www.stork.gov.eu/1.0/countryCodeOfBirth	Země narození
Pseudonym	http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier	Jedinečný, bezvýznamový identifikátor uživatele pro daný AIS (jiný AIS obdrží jinou hodnotu identifikátoru)

2.4. Nakládání s osobními údaji

Komponenty JIP/KAAS Czech POINT jsou autentizačním informačním systémem podle § 56a zákona č. 111/2009 Sb., o základních registrech.

Na základě tohoto legislativního zmocnění jsou v JIP Czech POINT uloženy osobní údaje uživatelů, které jsou předávány agendovým informačním systémům.

Další informace o zpracování osobních údajů v autentizačním informačním systému jsou uvedeny v prohlášení o zpracování osobních údajů.

3. Technický popis autentizace založené na SAML

Pomocí autentizace založené na SAML může externí systém (AIS) získat informace o uživateli, který se svými přihlašovacími údaji autentizoval v perimetru KAAS za účelem získání přístupu do daného externího systému (AIS).

Informace o uživateli jsou předávány za použití protokolu SAML 2.0.

3.1. Rozhraní přihlašovací stránky KAAS

Po detekci nepřihlášeného uživatele provede AIS vygenerování SAML requestu a přesměrování uživatele se zakódovaným SAML requestem na webovou stránku KAAS.

Struktura SAML requestu a způsob jeho zakódování jsou popsány v kapitole 3.3.1.

V adrese je možné nepovinně uvést v parametru „RelayState" vlastní identifikátor požadavku. Tento identifikátor se následně vrací spolu s odpovědí. Pomocí tohoto parametru tak lze od sebe odlišit více odeslaných požadavků.

Adresy přihlašovací stránky KAAS:

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/samlAuthnRequest?SAMLRequest=*zakódovaný_SAML_request*&RelayState=*vlastní_identifikátor*
provozní	https://www.czechpoint.cz/as/samlAuthnRequest?SAMLRequest=*zakódovaný_SAML_request*&RelayState=*vlastní_identifikátor*

Poznámka: Uvedené adresy jsou dostupné jak v Internetu, tak i v síti KIVS.

3.2. Rozhraní webové stránky AIS pro příjem SAML response

Po úspěšném ověření uživatele KAAS vygeneruje SAML response a přesměruje uživatele se SAML response na URL adresu, která je definována v konfiguraci AIS v JIP.

Toto URL, které je v plné režii AIS, musí přijímat parametr „SAMLResponse", ve kterém je do AIS předávána zakódovaná SAML response.

Součástí URL může být také parametr „RelayState" obsahující hodnotu, která byla uvedena v požadavku.

Struktura SAML response a způsob jejího zakódování jsou popsány v kapitole 3.3.2.

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

https://*adresa_AIS_uložená_v_konfiguraci_AIS_v_JIP*?SAMLResponse=*zakódovaná_SAML_response*&RelayState=*identifikátor_z_požadavku*

3.3. Definice vyměňovaných SAML zpráv

3.3.1. Struktura SAML requestu

Při detekci nepřihlášeného uživatele provádí AIS redirect uživatele na webovou stránku KAAS (viz kapitola 3.1) a do redirectu vkládá zakódovaný SAML request.

Nezakódovaný SAML request je zprávou typu SAML2 AuthnRequest s následující XML strukturou:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest
```

```
      xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
      xmlns:eidas="http://eidas.europa.eu/saml-extensions"
      AssertionConsumerServiceURL="https://rpp-ais.egon.gov.cz/AISP/"
      Destination="https://www.test.czechpoint.cz/as/samlAuthnRequest"
      ForceAuthn="true"
      ID="_9cc475faf8730a3040b4324dd2d33ca7"
      IssueInstant="2021-05-19T14:26:51.858Z"
      Version="2.0">
   <saml2:Issuer
         xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
         Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">AIS26...0095</saml2:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
         <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <ds:Reference URI="#_9cc475faf8730a3040b4324dd2d33ca7">
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>cEv70CkJRnpiDsccpvVsHZCVhN/iTZoWo53P9wqpcjg=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>TGdofKsaNl5niobzECwZCEFI...F8pm+ObLDHggJppaZTsvNg==</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>

<ds:X509Certificate>MIIC2DCCAcCgAwIBAgIEYJlS...NJCvEU0VeUho9YAu6I0ElmI8</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <saml2p:Extensions>
      <eidas:SPType>public</eidas:SPType>
      <eidas:RequestedAttributes>
         <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
         <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
         <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
         <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false"/>
         <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false"/>
         <eidas:RequestedAttribute Name="http://www.stork.gov.eu/1.0/countryCodeOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="false"/>
      </eidas:RequestedAttributes>
   </saml2p:Extensions>
   <saml2p:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent"/>
   <saml2p:RequestedAuthnContext Comparison="minimum">
      <saml2:AuthnContextClassRef
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://eidas.europa.eu/NotNotified/LoA/low</saml2:Au
thnContextClassRef>
   </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

Vysvětlivky:

Hodnota	Význam
AuthnRequest	Element obsahující atributy SAML requestu.
AssertionConsumerServiceURL	Tento element je z bezpečnostních důvodů ignorován! SAML response je zasílána na návratovou URL, která je definována v nastavení AIS v JIP Czech POINT.
Destination	URL adresa webové stránky KAAS (viz adresy v kapitole 3.1). Slouží jako důkaz, že request byl určen pro JIP/KAAS Czech POINT.

Hodnota	Význam
ID	Identifikátor SAML zprávy, definovaný AISem. KAAS poté vrací stejnou hodnotu identifikátoru v elementu „InResponseTo" v odpovídající SAML response.
IssueInstant	Datum a čas vygenerování SAML requestu. KAAS ignoruje z bezpečnostních důvodů SAML requesty starší než 60 minut od okamžiku jejich zpracování.
Issuer	Zkratka AIS, kterou lze zjistit v nastavení AIS v administrační aplikaci Správa dat.
Signature	Element obsahující podpis XML dat requestu včetně certifikátu pro ověření platnosti podpisu.
Extensions	Element obsahující rozšíření požadavku.
SPType	Typ Service Providera (veřejný, privátní). Momentálně se nerozlišuje typ Service Providera a tento element je ignorován.
RequestedAttributes	Seznam údajů o uživateli, které AIS požaduje po JIP/KAAS (více viz kapitola 2.3). Seznam údajů může obsahovat povinné i nepovinné atributy.
AuthnContextClassRef	Požadovaná úroveň záruk (tzv. Level of Assurance) – tj. jak „kvalitně" se uživatel musí přihlásit. V systému Czech POINT není fakticky používána (viz kap. 3.4).

Výše uvedený SAML request musí být před vložením do redirectu zkomprimován pomocí algoritmu Deflate, zakódován pomocí Base64 kódování a následně tzv. „URL enkódován" (nealfanumerické znaky jsou nahrazeny znakem „%" a hexadecimální číslicí; např. znak „+" je nahrazen posloupností znaků „%2B" nebo znak „/" je nahrazen posloupností „%2F").

Zakódovaný SAML request v URL má např. následující podobu (je uvedena pouze část zakódovaného SAML requestu a bez nepovinného parametru „RelayState"):

```
https://www.test.czechpoint.cz/as/samlAuthnRequest?SAMLRequest=1Vhbk6JIFn6fX1FhR
%2ByLUcXNG25XTSQgiAoqKiIvG1wSQSBB7vjrB7xUVc92z%2FZs7Mbu atd. atd.
```

3.3.2. Struktura SAML response

Po úspěšném ověření identity uživatele přesměruje komponenta KAAS uživatele na definovanou adresu, obsluhovanou AISem, a do redirectu vkládá zakódovanou SAML response a volitelně také parametr „RelayState", pokud se nacházel v obdrženém požadavku.

Nezakódovaná SAML response je zprávou typu SAML2 Response s následující XML strukturou:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response
      xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
      Destination="https://rpp-ais.egon.gov.cz/AISP/"
      ID="_3a0d6a203ec2a2ac2864a2ee50d6c1bf"
      InResponseTo="_9cc475faf8730a3040b4324dd2d33ca7"
      IssueInstant="2021-05-19T14:26:51.971Z"
      Version="2.0">
   <saml2:Issuer
         xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
         Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://www.test.czechpoint.cz/as/samlAuthnRequest</saml2:Issuer>
   <saml2p:Status>
      <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
```

```
   </saml2p:Status>
   <saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
      <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="_75c32efcbccb4c615d38214a915582c0" Type="http://www.w3.org/2001/04/xmlenc#Element">
         <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <xenc:EncryptedKey Id="_d1b694a880223b2fa401f8600db887e6">
               <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
               </xenc:EncryptionMethod>
               <xenc:CipherData>

<xenc:CipherValue>fsE+oePf4QAC2wQYqnRj+PkB...0fFEoAvO5QJjgqkuUdapQw==</xenc:CipherValue>
               </xenc:CipherData>
            </xenc:EncryptedKey>
         </ds:KeyInfo>
         <xenc:CipherData>

<xenc:CipherValue>dXbgAKbjx0uslTlzB0x8k8W4...La+kR7DU5FwVwXJ0TIx4ooNF</xenc:CipherValue>
         </xenc:CipherData>
      </xenc:EncryptedData>
   </saml2:EncryptedAssertion>
</saml2p:Response>
```

Element „EncryptedAssertion" v SAML response obsahuje zašifrovaná data pro podepisovací certifikát AIS, který je uložen v nastavení AIS v JIP (k šifrování se nepoužívá podepisovací certifikát AIS v SAML requestu). Ve výše uvedeném příkladu se nachází zašifrovaná data v elementu „CipherData". Pro názornost uvádíme, jak tato zašifrovaná data vypadají v otevřeném tvaru před zašifrováním:

```
<saml2:Assertion
      xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
      ID="_61110e595df739800de9f667e0ca4df0"
      IssueInstant="2021-05-19T14:26:51.972Z"
      Version="2.0">
   <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://www.test.czechpoint.cz/as/samlAuthnRequest</saml2:Issuer>
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
         <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <ds:Reference URI="#_61110e595df739800de9f667e0ca4df0">
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>5aDfMtw3uU6j/Mlp6Dnb32xL5Bsmy6q8AgizoA93F3g=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>fo+dN2hb+4+brN1PUK7Ucy79...AlD5VnurnXUkc8OsM/vAIA==</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>

<ds:X509Certificate>MIIC2DCCAcCgAwIBAgIEYJlS...F0y//287wRAbLFkKGA5YPclZ</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <saml2:Subject>
      <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent">cz/cz/ctoth</saml2:NameID>
      <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
         <saml2:SubjectConfirmationData
            InResponseTo="_9cc475faf8730a3040b4324dd2d33ca7"
            NotBefore="2021-05-19T14:26:51.972Z"
            NotOnOrAfter="2021-05-19T16:26:51.972Z"
            Recipient="https://rpp-ais.egon.gov.cz/AISP/"/>
      </saml2:SubjectConfirmation>
   </saml2:Subject>
   <saml2:Conditions NotBefore="2021-05-19T14:26:51.972Z" NotOnOrAfter="2021-05-19T16:26:51.972Z">
```

```
      <saml2:AudienceRestriction>
         <saml2:Audience>https://rpp-ais.egon.gov.cz/AISP/</saml2:Audience>
      </saml2:AudienceRestriction>
   </saml2:Conditions>
   <saml2:AttributeStatement>
      <saml2:Attribute FriendlyName="PersonIdentifier"
            Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
         <saml2:AttributeValue
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:type="eidasnp:PersonIdentifierType">2bd7efe068d6f1050195a5dc0eafb0cc09b699d17f1121192b46c6f274b8
3798</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="CurrentFamilyName"
            Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
         <saml2:AttributeValue
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="eidasnp:CurrentFamilyNameType">Tóth</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="CurrentGivenName"
            Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
         <saml2:AttributeValue
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="eidasnp:CurrentGivenNameType">Csaba</saml2:AttributeValue>
      </saml2:Attribute>
   </saml2:AttributeStatement>
   <saml2:AuthnStatement AuthnInstant="2021-05-19T14:26:51.972Z">
      <saml2:AuthnContext>
         <saml2:AuthnContextClassRef
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://eidas.europa.eu/NotNotified/LoA/low</saml2:Au
thnContextClassRef>
      </saml2:AuthnContext>
   </saml2:AuthnStatement>
</saml2:Assertion>
```

Vysvětlivky:

Hodnota	Význam
Response	Element obsahující atributy SAML response.
Destination	URL AIS, na které je SAML response odesílána. URL se načítá z nastavení AIS v JIP Czech POINT, ne z elementu „AssertionConsumerServiceURL" v SAML requestu!
ID	Identifikátor SAML zprávy, definovaný KAASem.
InResponseTo	Obsah elementu „ID" ze SAML requestu. AIS je tak schopen spárovat SAML response se správným SAML requestem.
IssueInstant	Datum a čas vygenerování SAML response.
Issuer	Identifikátor KAAS Czech POINT jakožto Identity Providera.
Signature	Element obsahující informace o podpisu XML dat.
Status	Element obsahující informace o výsledku autentizace založené na SAML.
StatusCode	Výsledek zpracování SAML požadavku a autentizace uživatele.
EncryptedAssertion	Element s obsahem SAML response zašifrovaným pro podepisovací certifikát AIS uložený v konfiguraci AIS v JIP (k šifrování se nepoužívá podepisovací certifikát AIS v SAML requestu).
Údaje v zašifrovaném obsahu SAML response:	
Issuer	Identifikátor KAAS Czech POINT jakožto Identity Providera.

Hodnota	Význam
Signature	Element obsahující podpis XML dat včetně certifikátu pro ověření podpisu.
Subject	Element obsahující základní informace o autentizovaném uživateli (např. pseudonym uživatele).
AttributeStatement	Element obsahující identitní atributy autentizovaného uživatele (viz tabulka v kapitole 2.3).
AuthnContextClassRef	Skutečně dosažená úroveň záruk (tzv. Level of Assurance) – tj. jak „kvalitně" se uživatel nakonec skutečně přihlásil. V systému Czech POINT není fakticky používána (viz kap. 3.4).

Výše uvedená SAML response je před vložením do URL zkomprimována pomocí algoritmu Deflate, zakódována pomocí Base64 kódování a následně tzv. „URL enkódována" (nealfanumerické znaky jsou nahrazeny znakem „%" a hexadecimální číslicí; např. znak „+" je nahrazen posloupností znaků „%2B" nebo znak „/" je nahrazen posloupností „%2F").

Zakódovaná SAML response v URL má např. následující podobu (je uvedena pouze část zakódované SAML response a bez nepovinného parametru „RelayState"):

```
https://adresa_AIS?SAMLResponse=7bvZjuRGki58f55CqLkMqLlvhZYOuAS3CJLBncGbA%2B77vvO1ziP8L%2FYzq1RqSa2ekXoa atd. atd.
```

3.4. Úroveň záruk (Level of Assurance)

Důležité: V systému Czech POINT není definováno přiřazení úrovní záruk pro jednotlivé metody přihlášení. Z tohoto důvodu autentizační služba JIP/KAAS vždy vrací v odpovědi „nejnižší možnou" hodnotu, tj. „http://eidas.europa.eu/NotNotified/LoA/low" nebo „http://eidas.europa.eu/LoA/NotNotified/low" (v závislosti na tom, která hodnota byla použita v requestu). To znamená, že úrovně záruk se v systému Czech POINT fakticky nepoužívají a tato kapitola je spíše informativní.

Parametr Úroveň záruk (Level of Assurance) poskytuje informaci, jak „kvalitně" prokázal uživatel svoji identitu. Rozlišuje se úroveň nízká, značná a vysoká (angl. low, substantial a high).

Úroveň záruk se specifikuje v požadavku na službu pro definici požadované úrovně záruk (element „AuthnContextClassRef"). Pomocí atributu „Comparison" se dále specifikuje způsob porovnávání požadované úrovně záruk vůči dostupným úrovním záruk. Atribut může nabývat hodnot „exact", „minimum", „maximum" nebo „better". V systému Czech POINT je doporučeno používat hodnotu „minimum" (viz příklad requestu výše).

Úroveň záruk je následně uvedena také ve vrácené odpovědi, kde se uvádí skutečná úroveň záruk vyplývající z uživatelem použité přihlašovací metody (opět v elementu „AuthnContextClassRef").

Systém Czech POINT rozlišuje následující identifikátory výše uvedených úrovní záruk:

Úroveň záruk	Identifikátor(y)
nízká	http://eidas.europa.eu/NotNotified/LoA/low http://eidas.europa.eu/LoA/NotNotified/low http://eidas.europa.eu/LoA/low
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

Poznámka: Hodnota „http://eidas.europa.eu/LoA/NotNotified/low" je ve skutečnosti chybná, ale některé systémy v zahraničí ji používají, proto je podporována i systémem Czech POINT. Správně však má být „http://eidas.europa.eu/NotNotified/LoA/low".

3.5. Metadata služby

Metadata služby obsahují:

- informace o šifrovacím a podepisovacím certifikátu, používaném webovou službou,
- seznam údajů o uživateli, které webová služba vrací v odpovědi

Metadata služby se nacházejí v XML souboru dostupném na následující adrese. Pro přístup k souboru není vyžadována autentizace.

Prostředí KAAS	Adresa
testovací	https://www.test.czechpoint.cz/as/samlIdpMetadata.xml
provozní	https://www.czechpoint.cz/as/samlIdpMetadata.xml

Ukázka souboru s metadaty:

```
<?xml version="1.0" encoding="windows-1252"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://www.test.czechpoint.cz/as/samlAuthnRequest" validUntil="2021-06-17T10:42:06.846Z">
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
         <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <ds:Reference URI="">
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
               <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
            <ds:DigestValue>5r1h5RMP2PhgJ42tOZI4R76FDDKs8cDSav46EbALf9U=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
<ds:SignatureValue>sOl4Q... mRg==</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
<ds:X509Certificate>MIIDH...60fk=</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <md:KeyDescriptor use="encryption">
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
               <ds:X509Certificate>MIIDH...60fk=</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:KeyDescriptor use="signing">
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
               <ds:X509Certificate>MIIDH...60fk=</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:KeyDescriptor>
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
               <ds:X509Certificate>MIIDH...60fk=</ds:X509Certificate>
            </ds:X509Data>
         </ds:KeyInfo>
      </md:KeyDescriptor>
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
```

```
        <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://www.test.czechpoint.cz/as/samlAuthnRequest"/>
        <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="PersonIdentifier"
Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
        <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
FriendlyName="CurrentFamilyName"
Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
        <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
FriendlyName="CurrentGivenName" Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
        <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="DateOfBirth"
Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
        <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="PlaceOfBirth"
Name="http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
        <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
FriendlyName="CountryCodeOfBirth" Name="http://www.stork.gov.eu/1.0/countryCodeOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
    </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Vysvětlivky:

Hodnota	Význam
Signature	Element obsahující podpis celého XML souboru a certifikát k ověření platnosti podpisu.
KeyDescriptor use="encryption"	Element obsahující šifrovací certifikát služby v kódování Base64.
KeyDescriptor use="signing"	Element obsahující podepisovací certifikát služby v kódování Base64.
Attribute	Element s informacemi o předávaném údaji o uživateli. Czech POINT nevrací automaticky všechny uvedené údaje o uživateli. Systém si musí o ně požádat v zasílaném requestu.

4. Seznam změn

Níže je uveden seznam změn v jednotlivých verzích dokumentu. Uvedeny jsou jen veřejně publikované verze. Seznam uváděných změn obsahuje vždy změny vůči poslední veřejně publikované verzi dokumentu.

Verze 1.7

- kap. 2.2.4 – na seznam podporovaných certifikačních autorit byla přidána Národní certifikační autorita

Verze 1.6

- kap. 3.3.1 – aktualizován element „AuthnContextClassRef" ve vzorovém SAML požadavku; do tabulky se seznamem elementů doplněna poznámka, že level of assurance se v Czech POINTu fakticky nepoužívá
- kap. 3.3.2 – aktualizován element „Audience" a „AuthnContextClassRef" ve vzorových datech před zašifrováním; do tabulky se seznamem elementů doplněna poznámka, že level of assurance se v Czech POINTu fakticky nepoužívá
- kap. 3.4, 3.5 – nové kapitoly

Verze 1.5

- kap. 3.1, 3.2 – do URL byl přidán parametr „RelayState"
- kap. 3.3.1 – aktualizován vzorový SAML požadavek
- kap. 3.3.2 – aktualizována vzorová SAML response a vzorová data před zašifrováním

Verze 1.4

- kap. 3.3.2 – opraven atribut „saml2:AuthnContextClassRef" v příkladu nezašifrovaných dat SAML odpovědi

Verze 1.3

- kap. 3.1 – odstraněny adresy s doménou czechpoint.cms2.cz

Verze 1.2

- kap. 3.1 – odstraněny již neplatné adresy z CMS 1

Verze 1.1

- označení „KAAS/JIP" v dokumentu změněno za užívanější „JIP/KAAS"

Verze 1.0

- první veřejně publikovaná verze dokumentu