??? ???????? SAML 2.0 — ?????? ??? ???????? ???????

??????????

SAML 2.0 (Security Assertion Markup Language) — стандарт обмена данными аутентификации и авторизации между IdP и SP на основе XML (OASIS, 2005).

???????? ????

Роль	Описание	Пример
IdP (Identity Provider)	Аутентифицирует пользователя и выдаёт assertions	ADFS, Keycloak, Okta, Azure AD
SP (Service Provider)	Принимает assertions и предоставляет доступ	Принтум, веб-приложение
Пользователь (User Agent)	Браузер, который перенаправляется между IdP и SP	Браузер пользователя

???? assertions

Тип	Содержимое
Authentication assertion	Кто пользователь, когда и как аутентифицирован
Attribute assertion	Атрибуты пользователя (email, группы, роль)
Authorization assertion	Права доступа (используется редко)

SP-initiated flow (???????? ?????????????)

```
1. Пользователь  →  SP:    обращается к защищённому ресурсу
2. SP            →  Браузер: HTTP 302, AuthnRequest (SAML Request)
3. Браузер       →  IdP:   перенаправление с AuthnRequest
4. IdP           →  Пользователь: форма входа (если нет сессии)
5. IdP           →  Браузер: HTTP 200 + форма с SAML Response (POST binding)
6. Браузер       →  SP:    POST с SAML Response (assertion)
7. SP            →  Пользователь: доступ разрешён
```

Bindings

Binding	Механизм передачи
HTTP Redirect	AuthnRequest передаётся в URL (GET), подписывается query string
HTTP POST	Response передаётся в теле формы (Base64-encoded XML)
HTTP Artifact	Ссылка на assertion; SP забирает напрямую у IdP

??????????

- Assertions подписываются IdP с помощью X.509-сертификата.
- SP проверяет подпись перед обработкой.
- Assertion содержит `NotBefore` и `NotOnOrAfter` — временное окно действия.
- Для защиты от replay-атак используется `InResponseTo` и однократное использование assertion ID.

????? ? SSO ? ???????

Принтум (в роли SP) может принять аутентификацию от корпоративного IdP по SAML 2.0. Пользователь, уже вошедший в корпоративный IdP, получает доступ к Личному кабинету без ввода пароля.

TODO: уточнить — какие атрибуты assertion Принтум использует для сопоставления пользователя (NameID, email, UPN).

Revision #4
Created 2026-05-10 11:16:04 UTC by DD
Updated 2026-06-01 13:26:13 UTC by Андрей Толкачев