

Die Dressings: Protokolle SAML, OAuth, OpenID Connect

Martin Kaufmann, Stefan Kunz

Cnlab Herbsttagung
KOSMOS, Zürich, 7. September 2022

Federated Identity



To continue, log in to Spotify.

 CONTINUE WITH FACEBOOK

 CONTINUE WITH APPLE

 CONTINUE WITH GOOGLE

OR

Email address or username

Email address or username

Password

Password

[Forgot your password?](#)

☒ Remember me

LOG IN

Don't have an account?

SIGN UP FOR SPOTIFY

Source: <https://www.bingegauge.com/fix-cant-login-reset-spotify-password/>

Delegated Authorization



Discord

You agree that Discord will be able to:

View your Spotify account data

[Learn more](#)

View your activity on Spotify

[Learn more](#)

Take actions in Spotify on your behalf

[Learn more](#)

You can remove this access at any time at spotify.com/account.

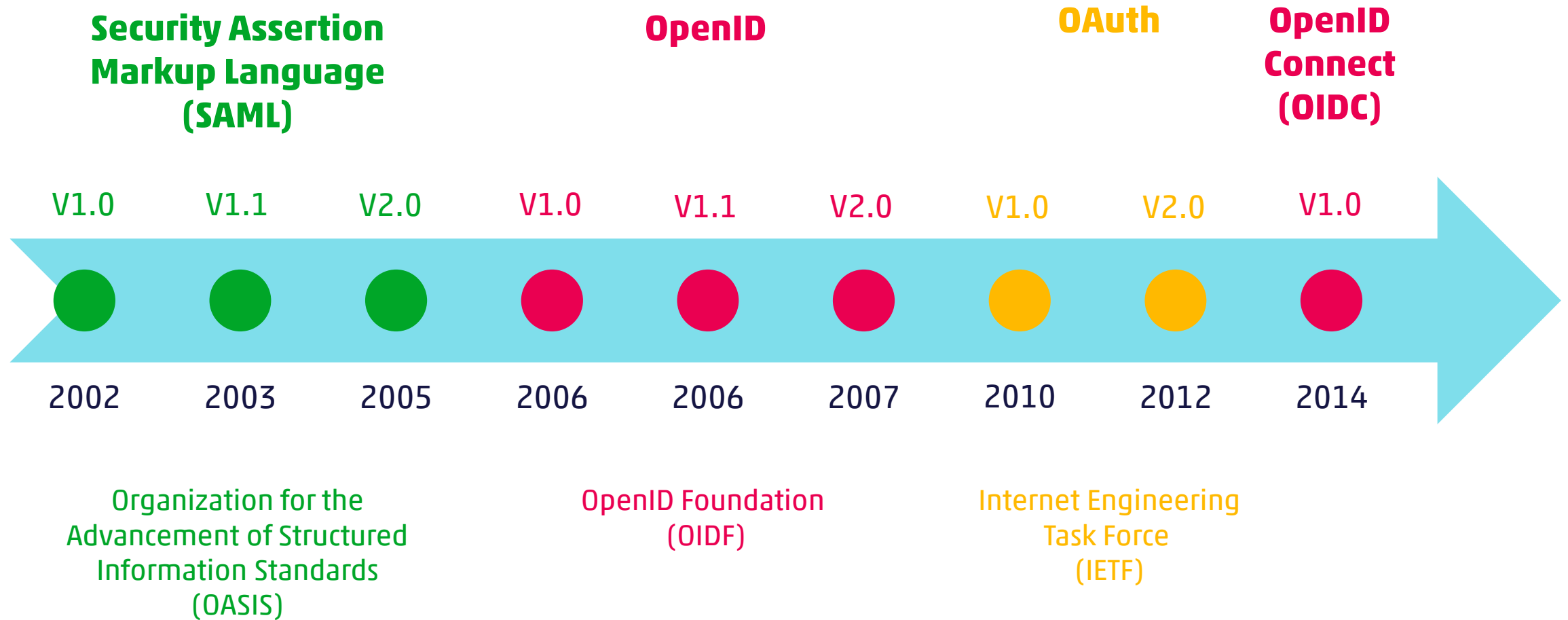
For more information about how Discord can use your personal data, please see Discord's privacy policy.

AGREE

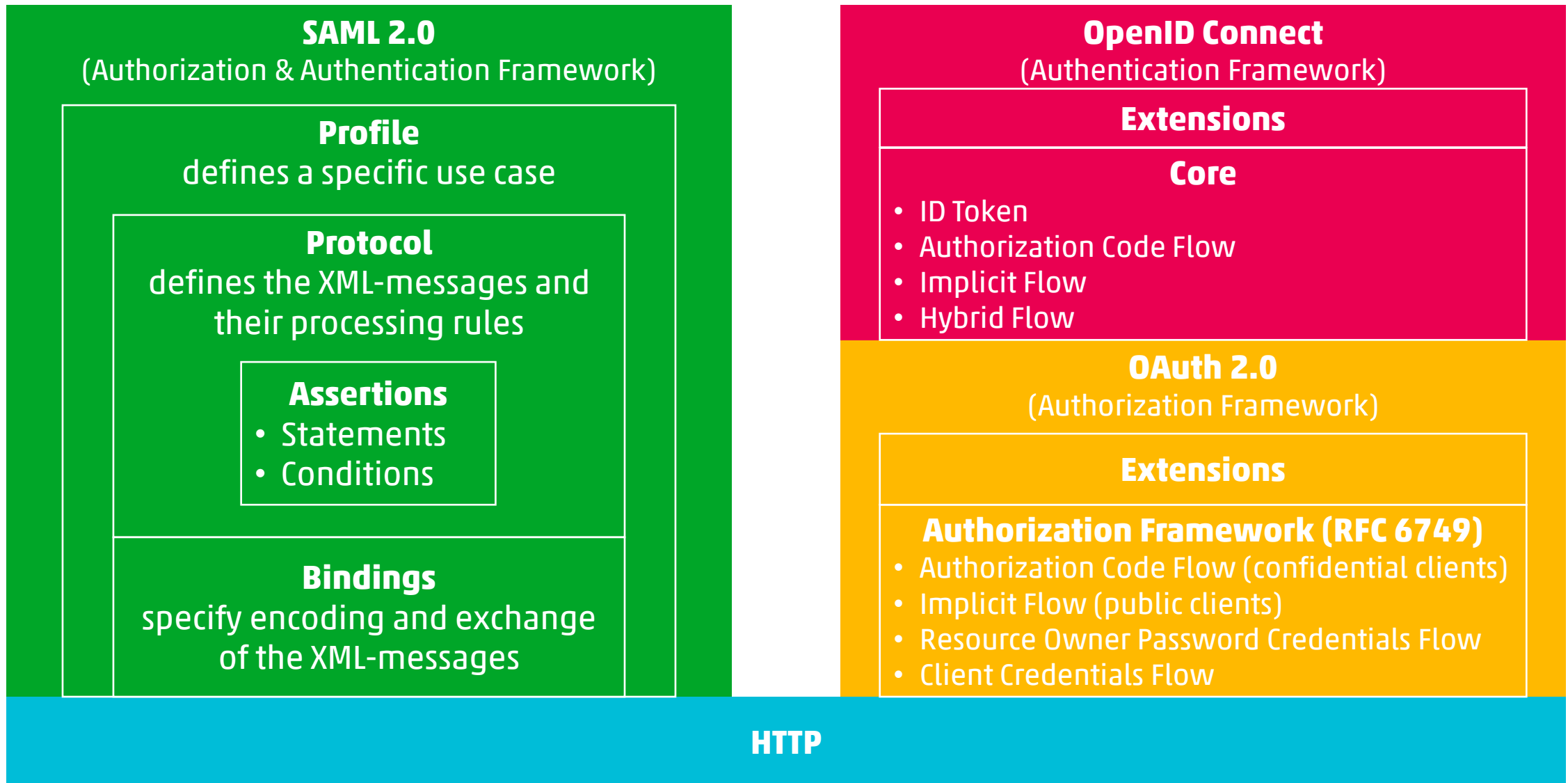
CANCEL



Timeline



Spezifikationen



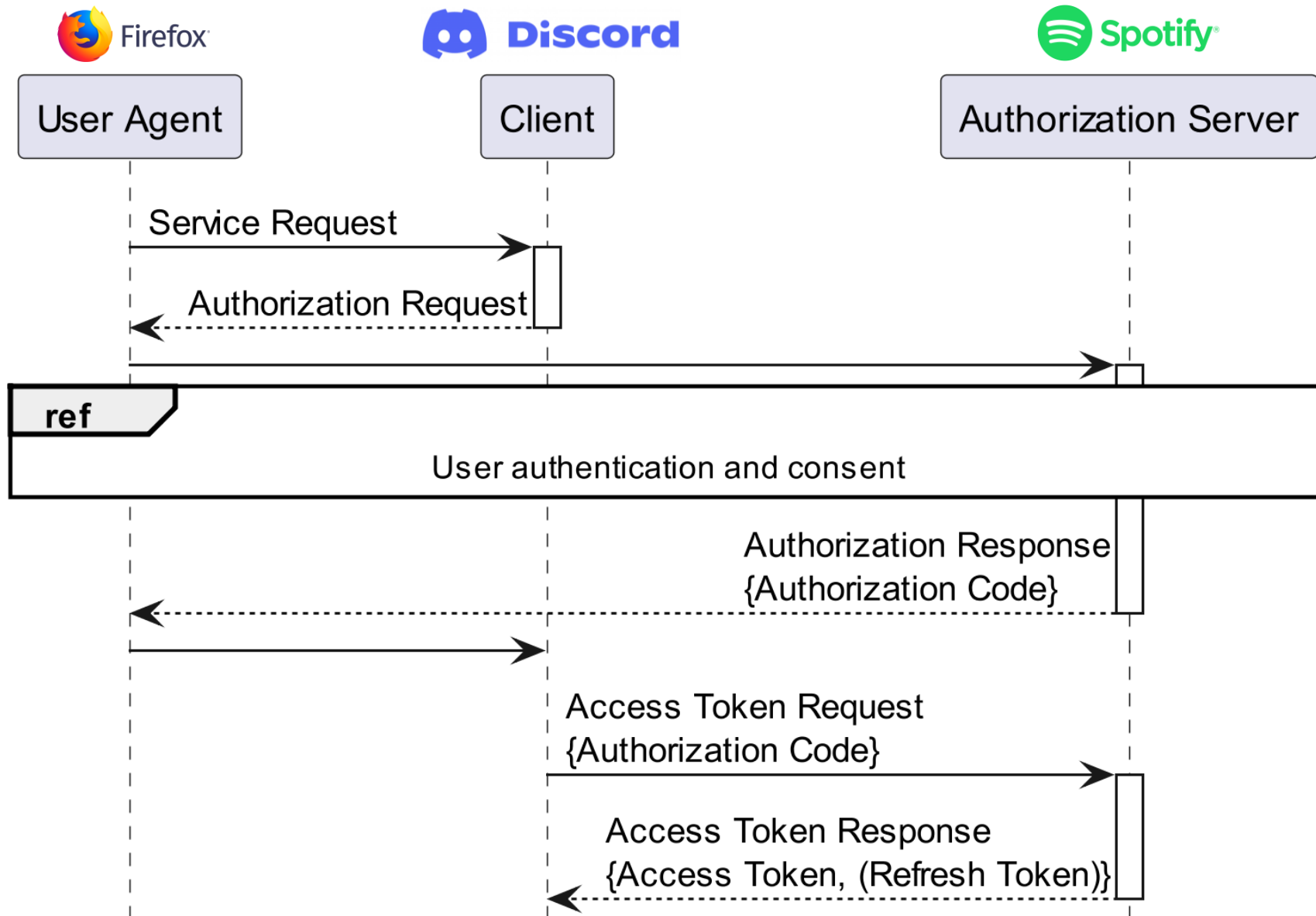
Liste der Spezifikationen

OAuth 2.0	
RFC 6749	The OAuth 2.0 Authorization Framework
RFC 6750	The OAuth 2.0 Authorization Framework: Bearer Token Usage
RFC 6819	OAuth 2.0 Threat Model and Security Considerations
RFC 7009	OAuth 2.0 Token Revocation
RFC 7521	Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants
RFC 7522	Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants
RFC 7523	JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
RFC 7591	OAuth 2.0 Dynamic Client Registration Protocol
RFC 7592	OAuth 2.0 Dynamic Client Registration Management Protocol
RFC 7635	Session Traversal Utilities for NAT (STUN) Extension for Third-Party Authorization
RFC 7636	Proof Key for Code Exchange by OAuth Public Clients
RFC 7662	OAuth 2.0 Token Introspection
RFC 8252	OAuth 2.0 for Native Apps
RFC 8414	OAuth 2.0 Authorization Server Metadata
RFC 8628	OAuth 2.0 Device Authorization Grant
RFC 8693	OAuth 2.0 Token Exchange
RFC 8705	OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens
RFC 8707	Resource Indicators for OAuth 2.0
RFC 9068	JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens
RFC 9101	The OAuth 2.0 Authorization Framework: JWT-Secured Authorization Request (JAR)
RFC 9126	OAuth 2.0 Pushed Authorization Requests
RFC 9207	OAuth 2.0 Authorization Server Issuer Identification

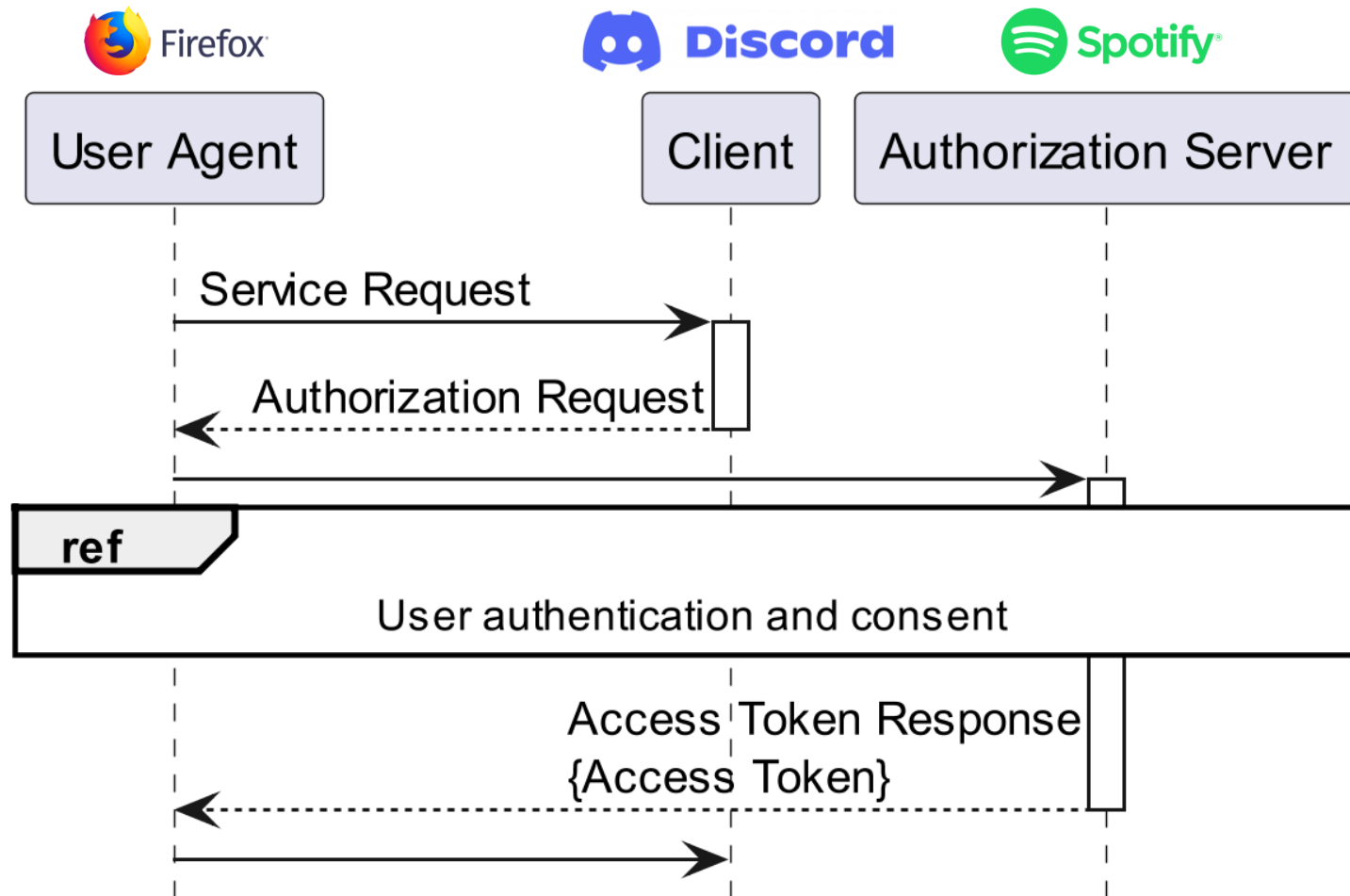
OpenID Connect
Core
Discovery
Dynamic Registration
OAuth 2.0 Multiple Response Types
OAuth 2.0 Form Post Response Mode
RP-Initiated Logout
Session Management
Front-Channel Logout
Back-Channel Logout
OpenID Connect Federation
Initiating User Registration via OpenID Connect

SAML 2.0
Assertions and Protocols (Core)
Bindings
Profiles
Metadata
Authentication Context
Conformance Requirements
Security and Privacy Considerations
Glossary
Metadata Profile for the OASIS Security Assertion Markup Language (SAML) V1.x
Metadata Extension for SAML V2.0 and V1.x Query Requesters
SAML V2.0 Metadata Interoperability Profile
SAML V2.0 Metadata Extensions for Login and Discovery User Interface

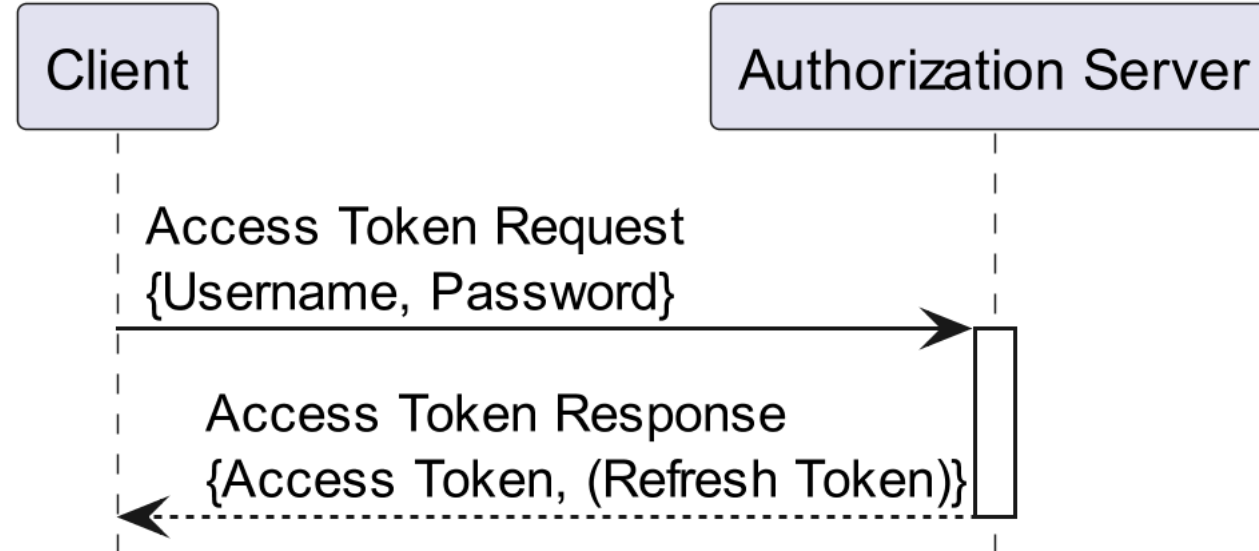
OAuth 2.0: Authorization Code Flow



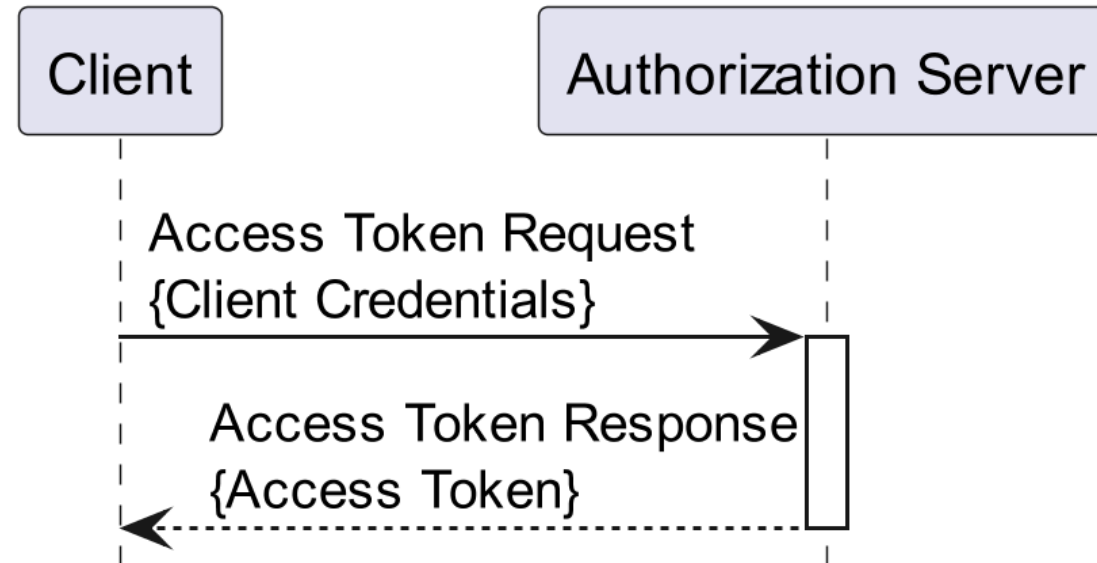
OAuth 2.0: Implicit Flow



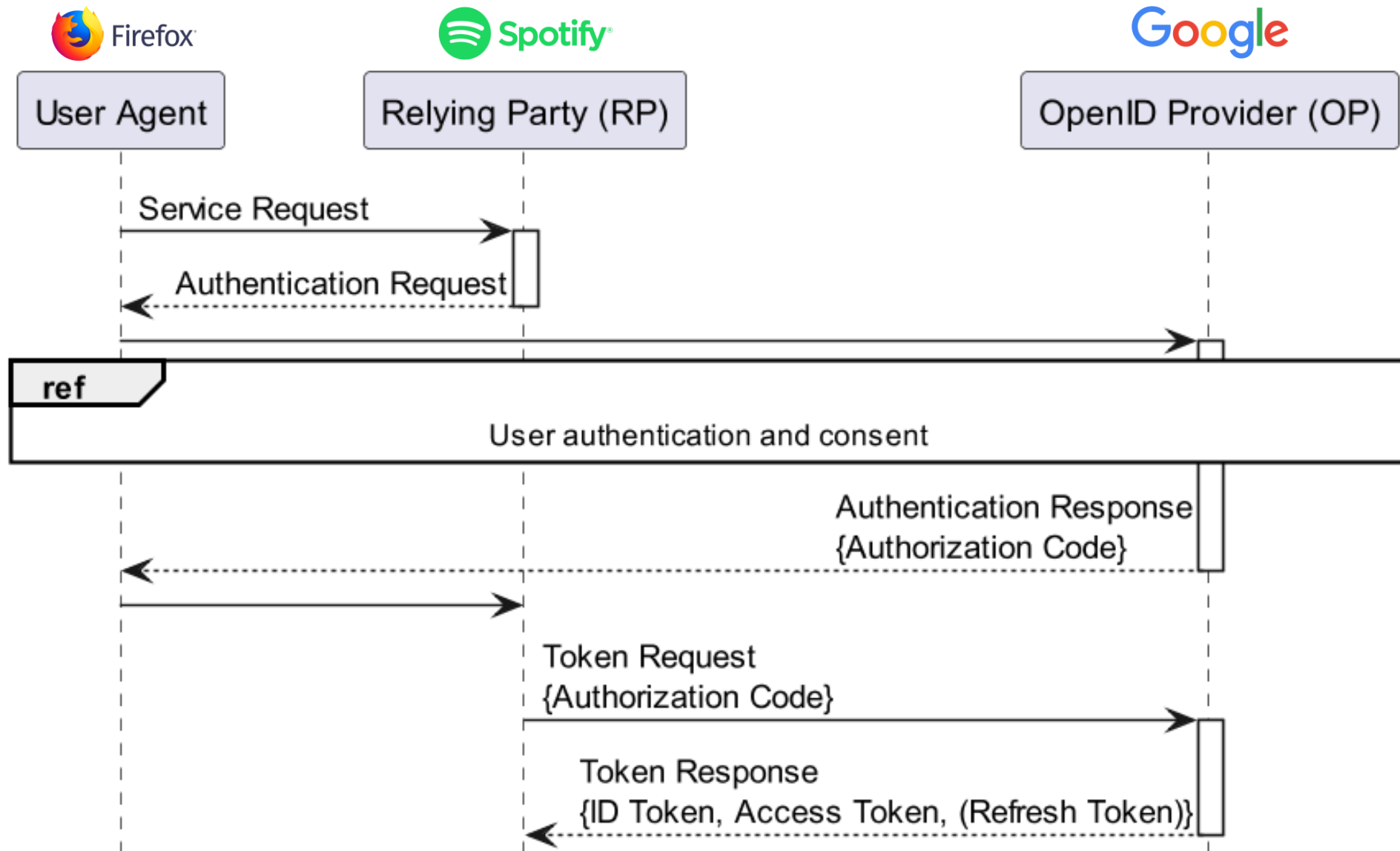
OAuth 2.0: Resource Owner Password Credentials Flow



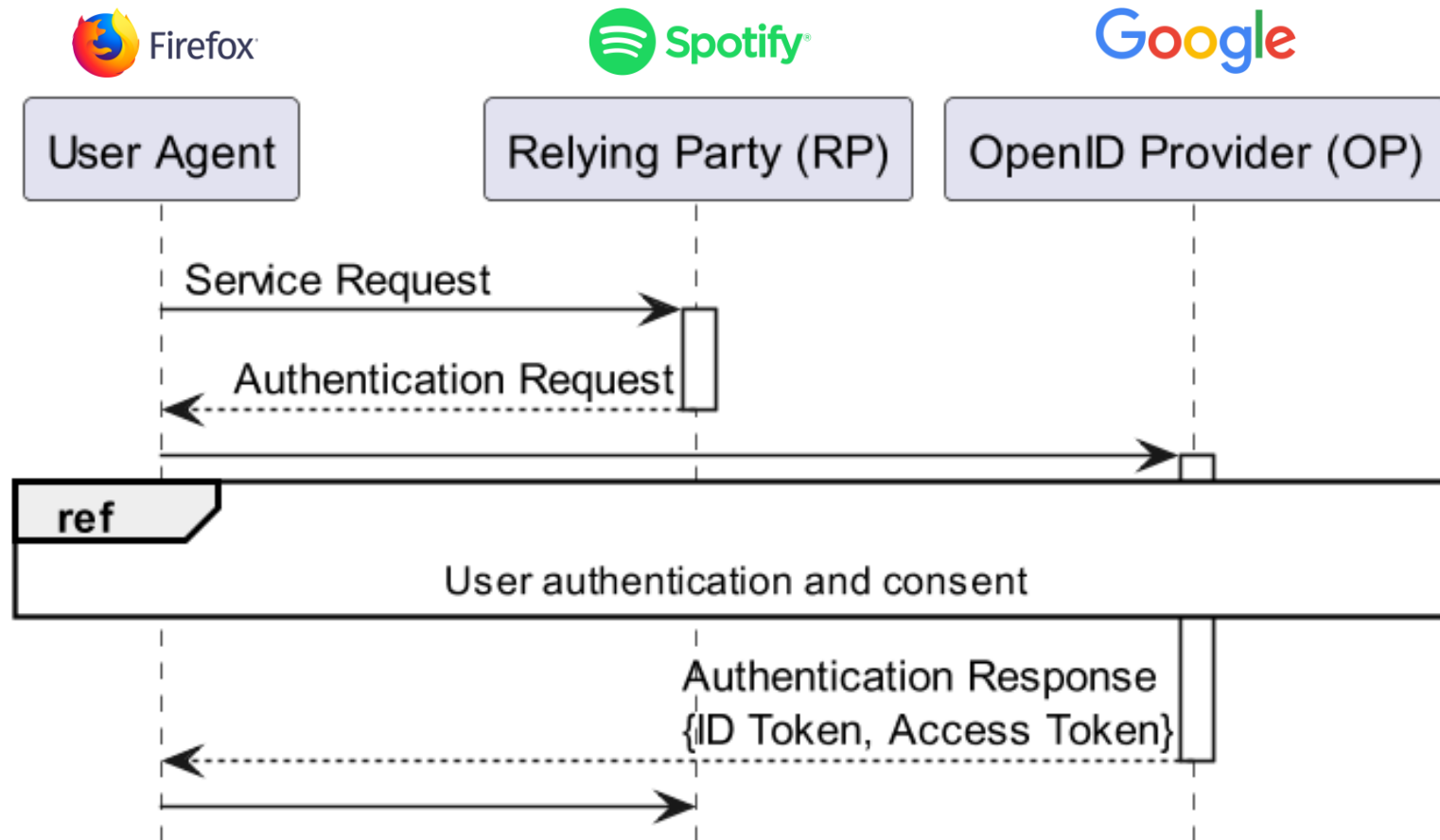
OAuth 2.0: Client Credentials Flow



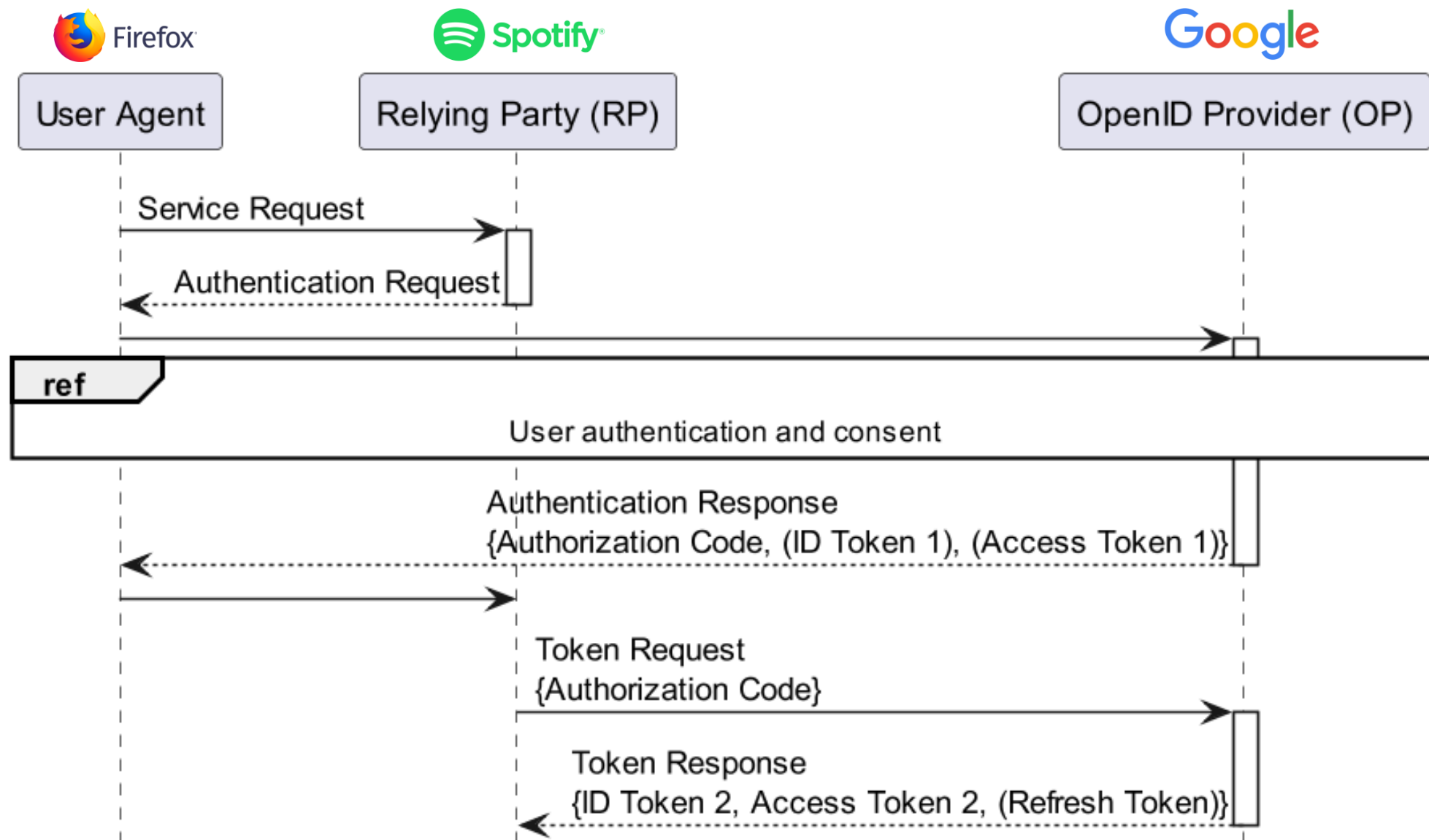
OpenID Connect: Authorization Code Flow



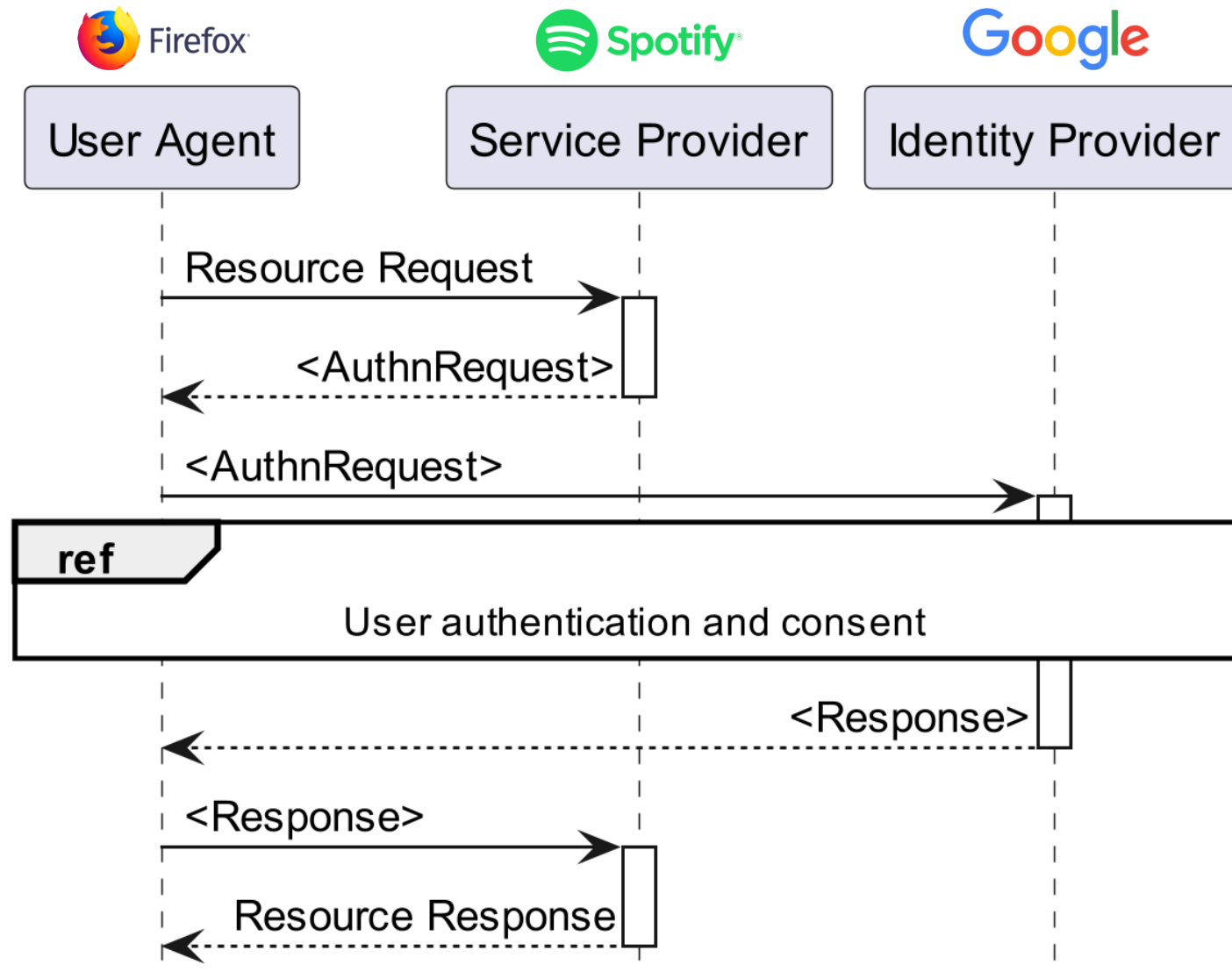
OpenID Connect: Implicit Flow



OpenID Connect: Hybrid Flow



SAML 2.0: Web Browser SSO Profile & Enhanced Client or Proxy (ECP) Profile



Framework-Vergleich (1/2)

 User Agent	 Client	 Authorization Server
 User Agent	 Relying Party	 OpenID Provider
 User Agent	 Service Provider	 Identity Provider

		OAuth 2.0				OpenID Connect			SAML 2.0	
		Authorization Code	Implicit	Password	Client Credentials	Authorization Code	Implicit	Hybrid	Web SSO	EHCP
Confidential Clients		✓	✓	✓	✓	✓	✓	✓	✓	✓
Public Clients		⊖	✓	✓	⊖	⊖	✓	⊖	n/a	n/a
Token	Signatur	□	□	□	□	✓	✓	✓	□	□
	Verschlüsselung	□	□	□	□	□	□	□	□	□
	Self-Contained Token	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Opaque Token	✓	✓	✓	✓	✓	✓	✓	□	□


 = Pflicht,
  = optional,
  = nicht unterstützt,
 n/a = nicht anwendbar

Framework-Vergleich (2/2)

 User Agent	 Client	 Authorization Server
 User Agent	 Relying Party	 OpenID Provider
 User Agent	 Service Provider	 Identity Provider

		OAuth 2.0				OpenID Connect			SAML 2.0	
		Authorization Code	Implicit	Password	Client Credentials	Authorization Code	Implicit	Hybrid	Web SSO	EHCP
Replay-Schutz		⊖	⊖	⊖	⊖	□	✓	□	✓	✓
Netzwerkverschlüsselung		✓	✓	✓	✓	✓	✓	✓	□	□
Client-Authentifizierung		✓	⊖	⊖	✓	✓	⊖	✓	□	✓
Schutz der Daten im User Agent	Autorisierungsanfrage (Integrität)	□	□	n/a	n/a	□	□	□	□	n/a
	Zugangsdaten (Vertraulichkeit)	✓	⊖	n/a	n/a	✓	⊖	✓	□	n/a


 = Pflicht,
  = optional,
  = nicht unterstützt,
 n/a = nicht anwendbar

Fazit

- Protokolle geben die Struktur und Mindestanforderungen vor für die Integration heterogener Systeme.
- Sicherheitseigenschaften (Tokenqualität, TLS,...) sind stark abhängig von der Umsetzung.
- **Alle 3 Frameworks erlauben es sichere Systeme zu implementieren.**



Quelle: [Wikipedia](#), Lizenz: [CC BY-SA](#)



Quelle: [coop.ch](#)

Quellen Framework-Vergleich

Thema	Titel
OAuth 2.0	RFC 6749: The OAuth 2.0 Authorization Framework (2012)
	RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage (2012)
	RFC 6819: OAuth 2.0 Threat Model and Security Considerations (2013)
	RFC 7636: Proof Key for Code Exchange by OAuth Public Clients (2015)
	RFC 9126: OAuth 2.0 Pushed Authorization Requests (2021)
OIDC	OpenID Connect Core 1.0 incorporating errata set 1 (2014)
	OpenID Connect Front-Channel Logout 1.0 – draft 06 (2022)
SAML 2.0	OASIS Standard: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 (2005)
	OASIS Standard: Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0 (2005)
	OASIS Standard: Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 (2005)

Vielen Dank für Ihre
Aufmerksamkeit_

Martin Kaufmann, Stefan Kunz

info@cnlab-security.ch
+41 55 214 33 40

cnlab security AG
Obere Bahnhofstrasse 32b
CH-8640 Rapperswil-Jona
Switzerland