OpenIDConnect

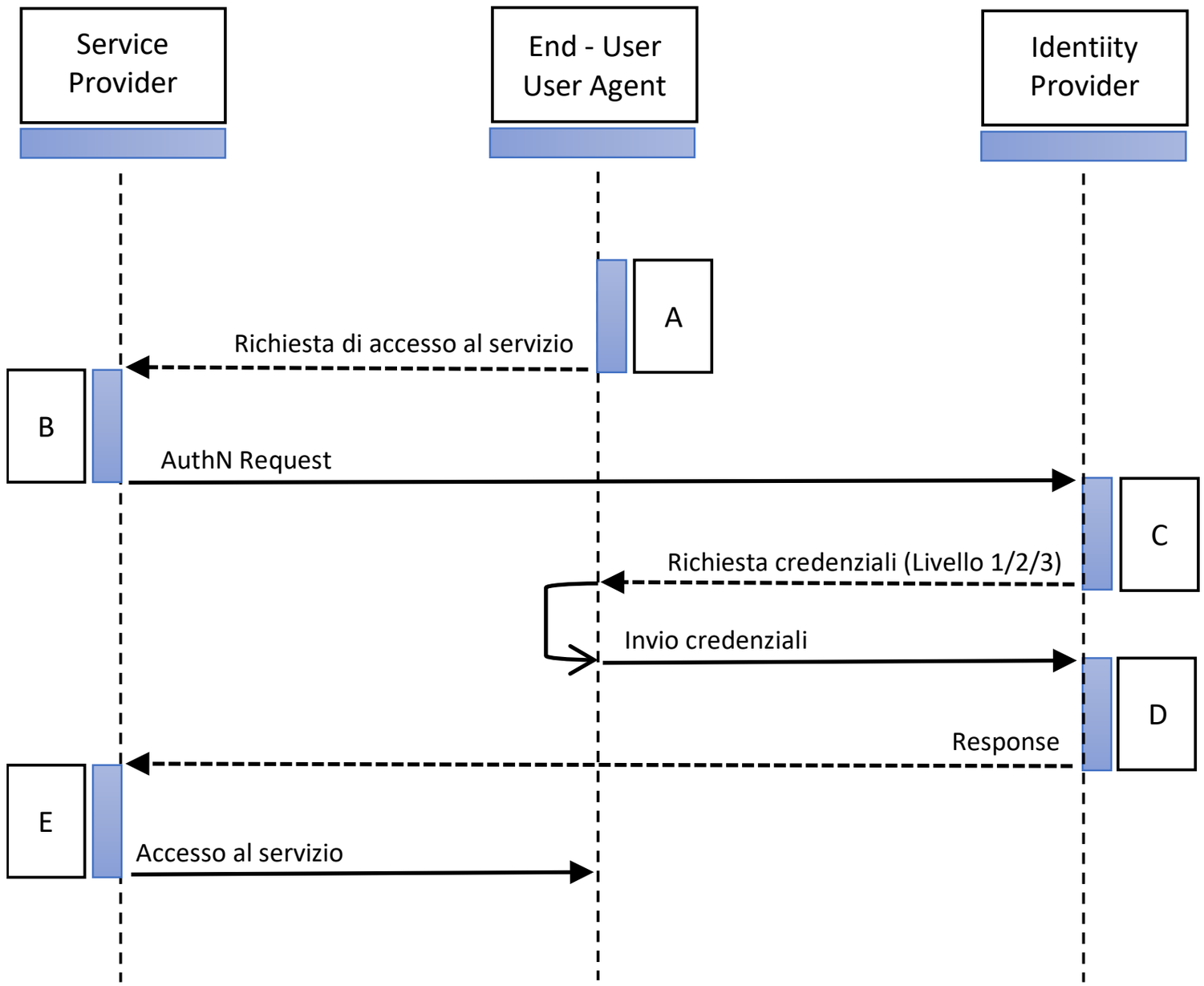
nel Sistema Pubblico d'Identità Digitale italiano

(SPID)

Livelli SPID

OpenID Connect in SPID

SPID SAML



1. Facilità di integrazione in sistemi eterogenei (single-page app, web, backend, mobile, IoT).

2. Integrazione di componenti di terze parti in modalità sicura, interoperabile e scalabile.

3. Sicurezza.

4. Diffusione e utilizzo da parte di un gran numero di servizi on line.

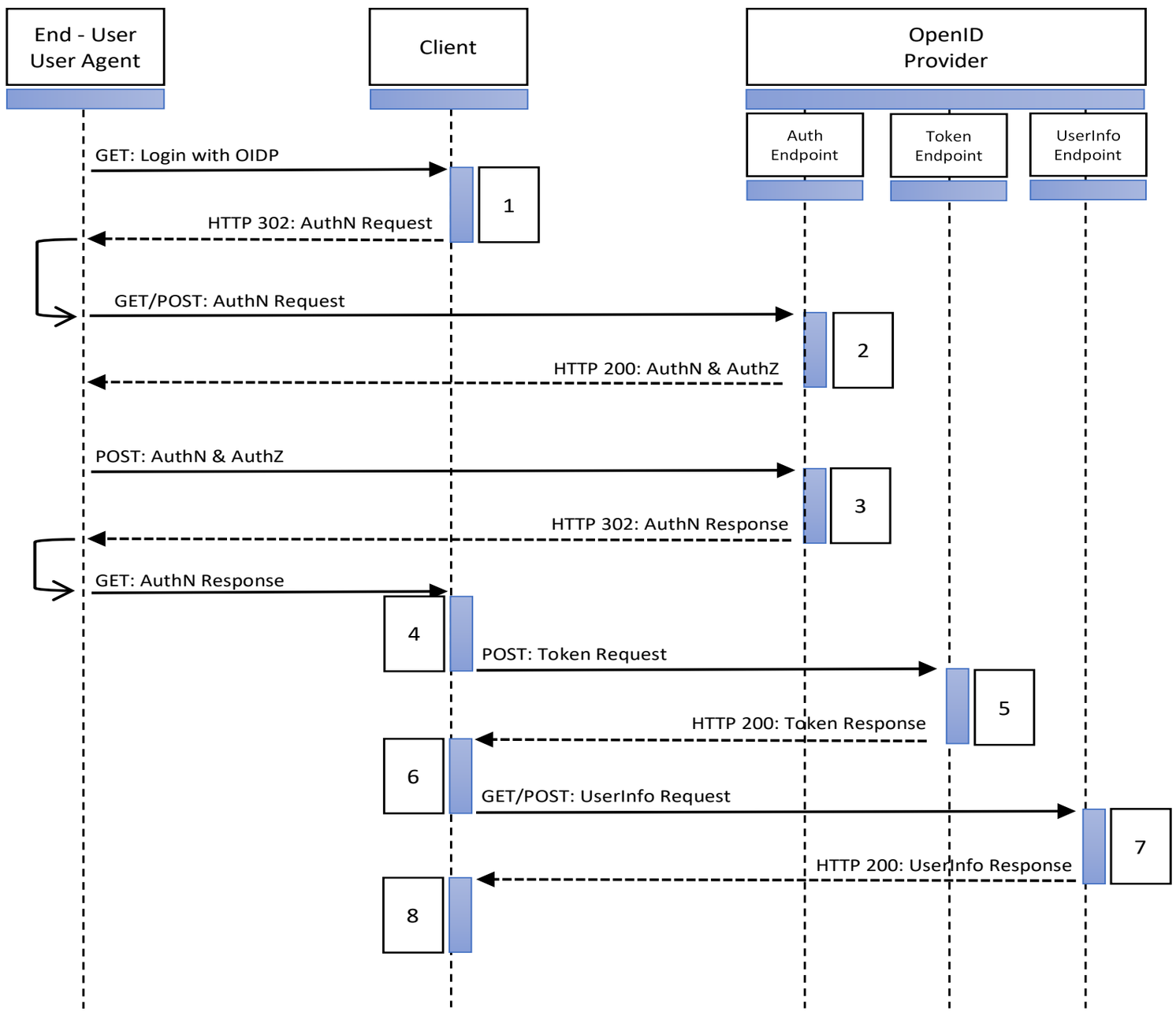

OpenID
Working Group
iGov
Public Sector Profile

SAML vs OIDC

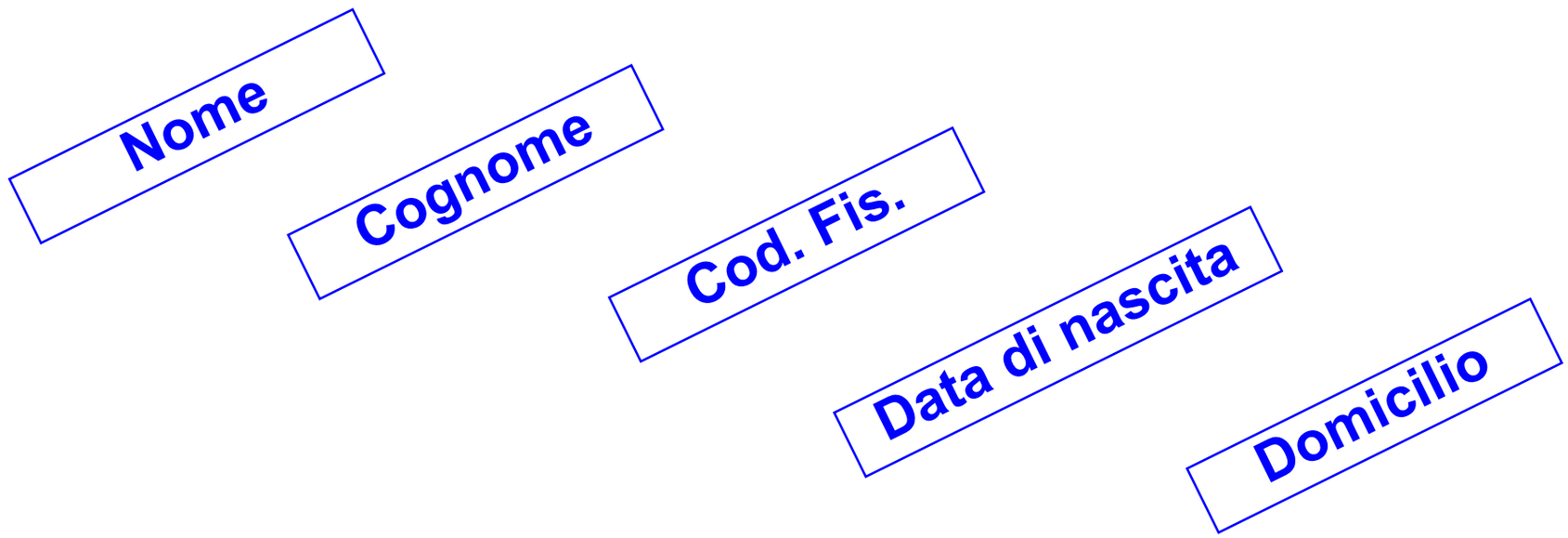
SAML 2.0	OpenID Connect
Assertion	*ID Token*
Attribute query	*UserInfo Endpoint*
Authentication request	*Authentication request*
ForceAuthn	*prompt=login*
Identity Provider (IdP)	*OpenID Provider (OP)*
IdP metadata	*OpenID Provider metadata*
Issuer	*Issuer*
Logout	*Revoke*
NameID policy	*Subject identifier type*
Passive Authentication	*prompt=none*
Service Provider (SP)	*Relying Party (RP)*
SP metadata	*Client metadata*
Subject	*Subject Identifier*
Attributes	*Claims*

OpenID Connect in SPID

Flusso Authorization Code

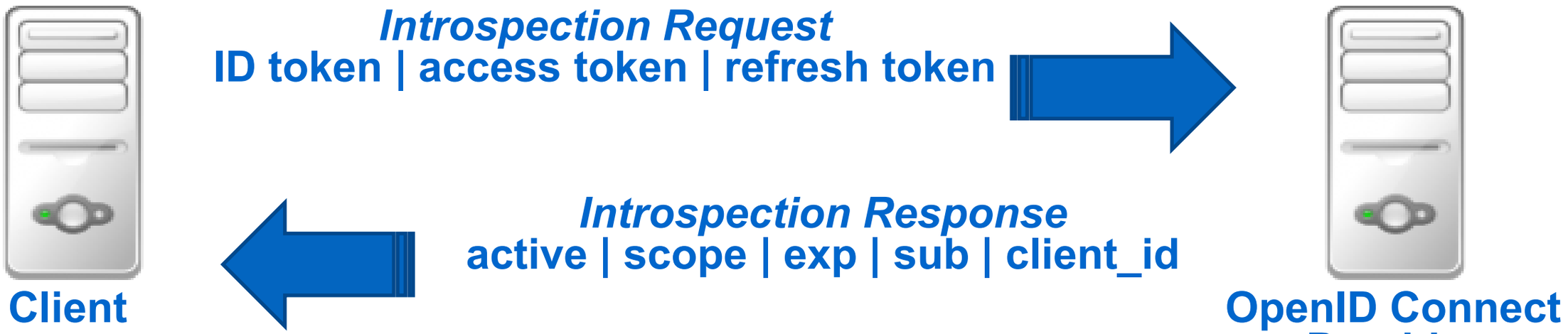


CLAIMS



Proof Key of Code Exchange

Introspection



Revocation


Revocation Request
ID token | access token | refresh token
Response
Codice HTTP 200
Client
OpenID Connect Provider

Registro SPID

Metadata OP

issuer	https://op.fornitore_identita.it	✓
jwks_uri	https://registry.spid.gov.it/...	✓
op_name	Fornitore d'Identità	✓
op_url	https://fornitore_identita.it	✓
token_endpoint_auth_metod_support	**private_key_jwt**	✓
acr_values_supported	**https://www.spid.gov.it/SpidL1** **https://www.spid.gov.it/SpidL2** **https://www.spid.gov.it/SpidL3**	✓
request_parameter_supported	**true**	✓

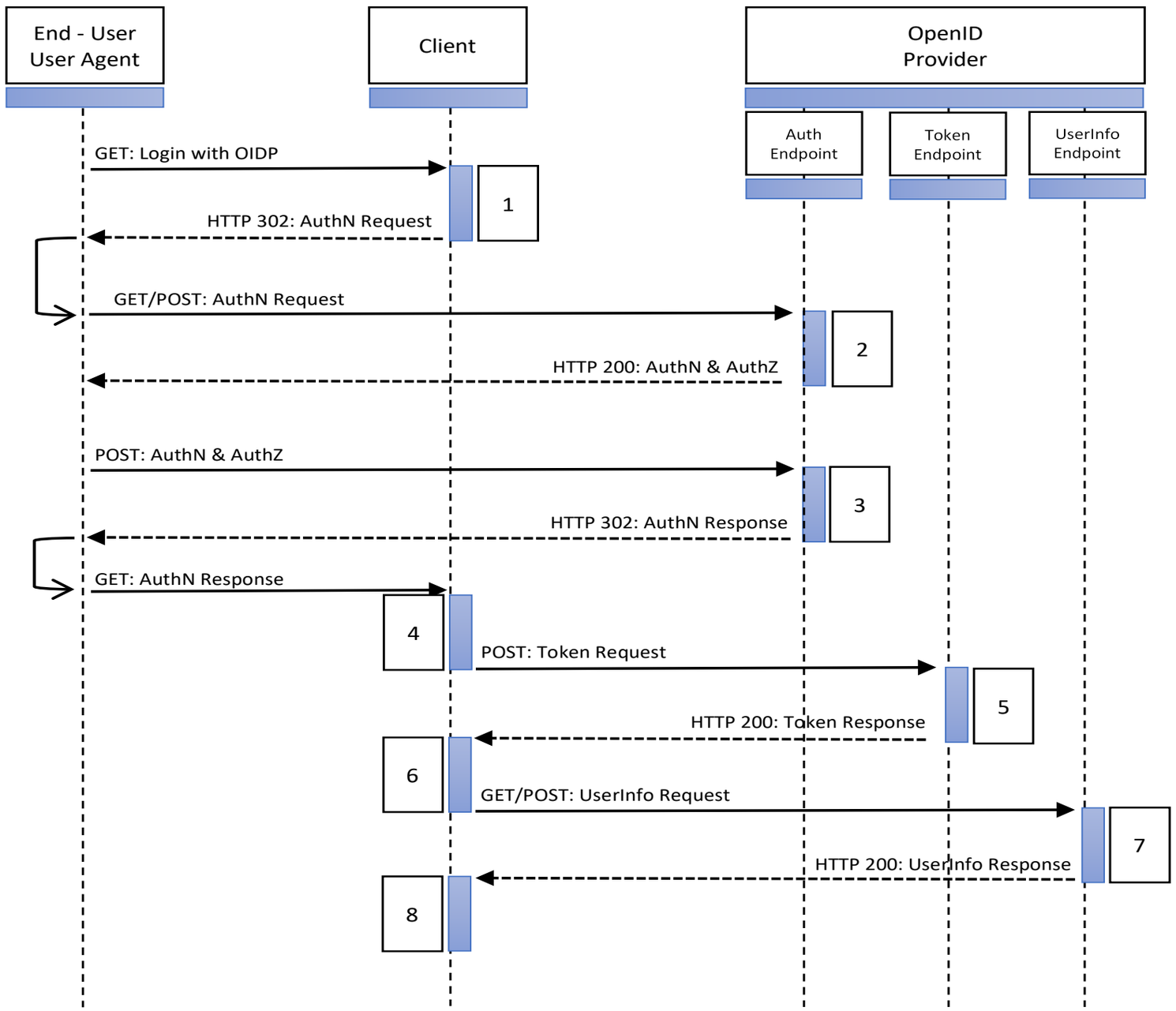
OpenID Connect in SPID

Metadata RP

client_id	https://rp.fornitore_servizi.it	✓
jwks_uri	https://registry.spid.gov.it/...	✓
client_name	Fornitore di servizi	✓
response_types	**code**	✓
grant_types	**authorization_code** **refresh_token**	✓

OpenID Connect in SPID

Flusso Authorization Code

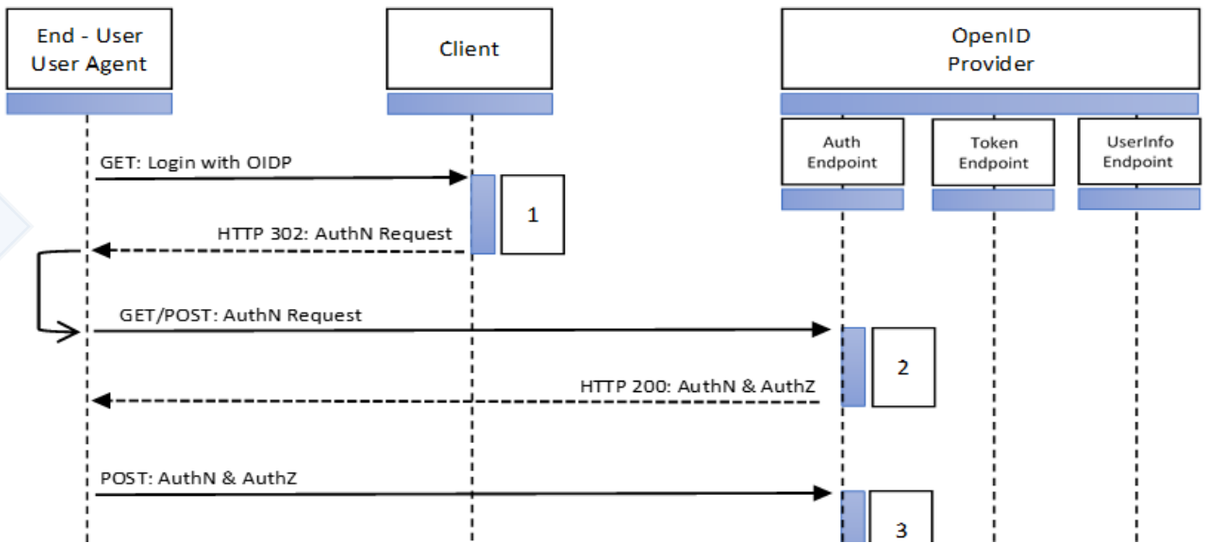


OpenID Connect in SPID

Authentication Request

GET | POST

```
https://op.fornitore_identita.it/
auth?request=eyJhbGciOi...
```



Request

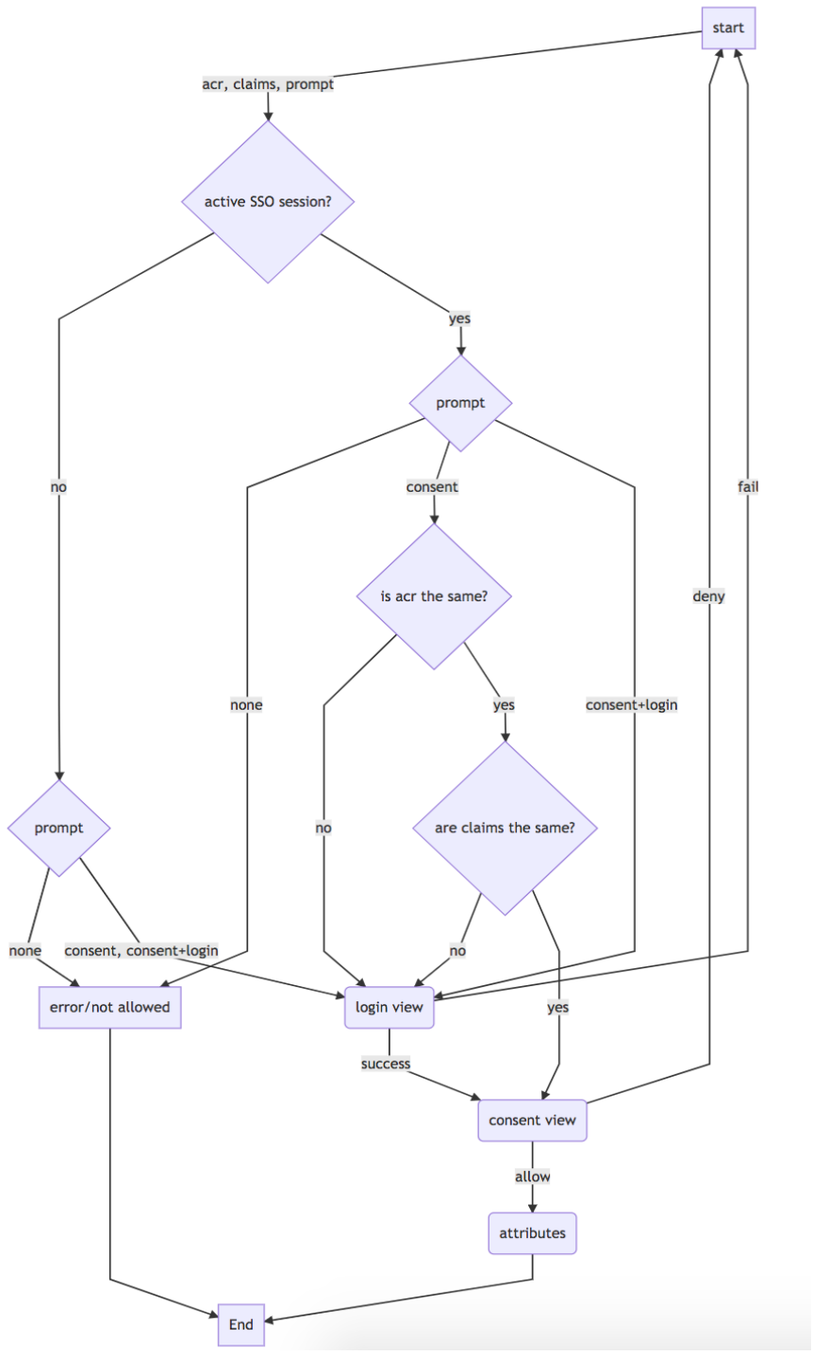
client_id	https://rp.fornitore_servizi.it	✓
response_type	**code**	✓
scope	**openid**	✓
code_challenge	qWJlMe0xdbXrKxTm72EpH659bUxAxw80	✓
nonce	MBzGqyf9QytD28eupyWhSqMj78WNqpc2	✓
prompt	login	✓
redirect_uri	https%3A%2F%2Frp.fornitore_servizi.it%2Fcallback	✓
acr_values	https://www.spid.gov.it/SpidL2 https://www.spid.gov.it/SpidL1	✓
claims	{ userinfo: { https://attributes.spid.gov.it/fiscalCodenull } }	✓

Authentication Request – Richiesta consenso

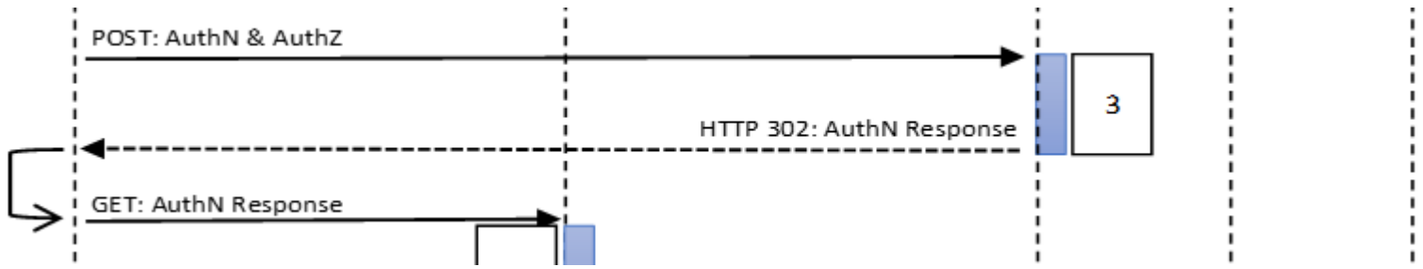
- **acr_values**: SpidL3,SpidL2, SpidL1
- **prompt** : login| consent| none
- **claims**: fiscalCode,name, familyName, …

Active SSO session?

- **prompt : none ✗ NON consentito**



Authentication Response



✓ Autenticazione avvenuta con successo

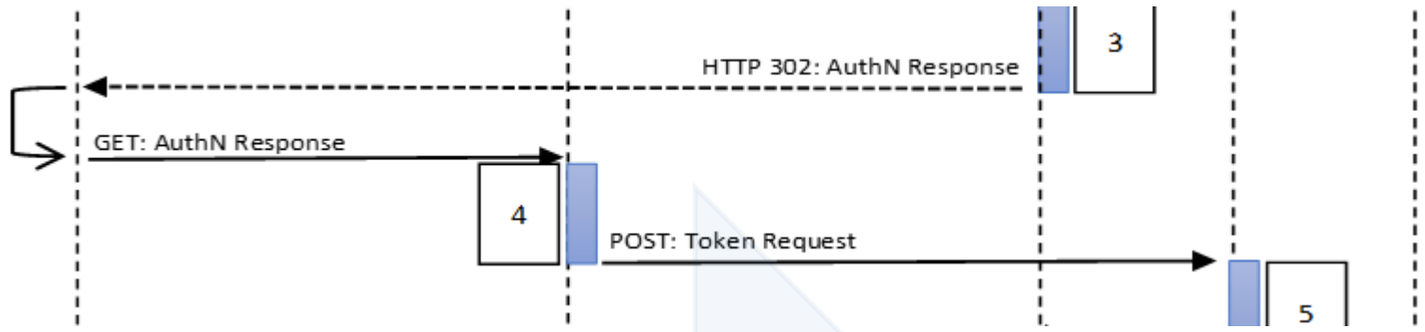
```
https://rp.fornitore_servizi.it/
callback?code=usDwMnEzJPpG5oaV8
x3j&state=fyZiOL9Lf2Ce...
```

✗ Errore durante il processo di autenticazione

```
https://rp.fornitore_servizi.it/
callback?error=access_denied
&error_description=xxx
&state=fyZiOL9Lf2Ce...
```

vedi Tabella anomalie SPID

Token Request



POST

```
https://op.fornitore_identita.it/token

client_id=https://rp.fornitore_servizi.it&
client_assertion=eyJhbGciOi...&
client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer&
code=usDwMnEzJPpG5oaV8x3j&
code_verifier=9g8S40MozM3NSqjHnhi7OnsE38jklFv2&
grant_type=authorization_code
```

client_assertion

iss	https://rp.fornitore_servizi.it	✓
iat	data/ora in cui è rilasciato il token	✓
exp	data/ora di scadenza della request	✓
jti	Identificatore univoco	✓

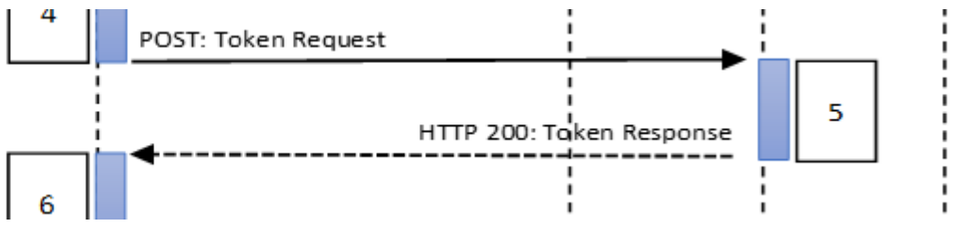
Autenticazione private_key_jwt

client_assertion è un JWT firmato con la chiave privata del RP. La chiave pubblica è presente sul registro SPID e indirizzata da **jwks_uri** del metadata RP

OpenID Connect in SPID

Token Response

```
{
  "access_token": "dC34Pf6kdG...",
  "token_type": "Bearer",
  "refresh_token": "wJ848BcyLP...",
  "expires_in": 1800,
  "id_token": "eyJhbGciOiJI..."
}
```



ID Token

iss	https://op.fornitore_identita.it	✓
sub	**PairwiseIdentifier**	✓
aud	https://rp.fornitore_servizi.it	✓
acr	https://www.spid.gov.it/SpidL2	✓
at_hash	*Hash dell'AccessToken*	✓
iat	*Data / ora di emissione del Token*	✓
nbf	*Data / ora di inizio validità del Token*	✓
exp	*Data / ora di scadenza del Token*	✓
jti	*Identificativo unico del Token*	✓
nonce	noncedel Client per evitare Replay Attack	✓

ID Token e AccessToken

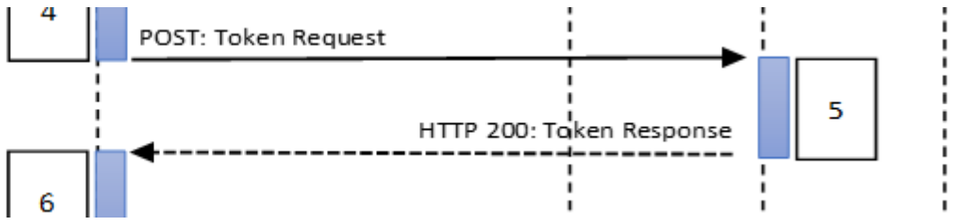
sono JWT firmati con la chiave privata del OP. La chiave pubblica è presente sul registro SPID e indirizzata da jwks_uri del metadata OP

ID Token non contiene gli attributi dell' utente ma solo la prova dell'avvenuta autenticazione.

Gli attributi dell'utente devono essere recuperati tramite chiamata ad **UserInfo**

Token Response - Errori

✗ Errore durante il processo di recupero del token




```
POST HTTP 400
{
  "error": "invalid_client",
  "error_description": "xxx"
}
```

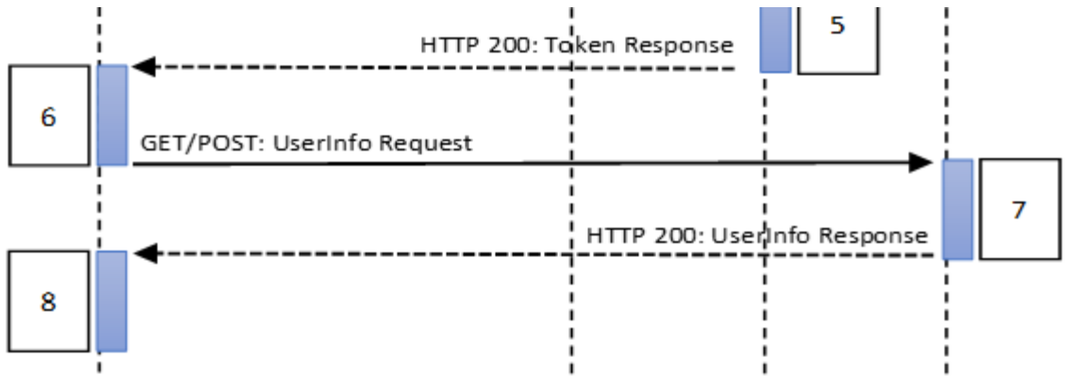
UserInfo

UserInfoRequest

GET | POST

```
https://op.fornitore_identita.it/userinfo

Authorization: Bearer dC34Pf6kdG
```



UserInfoResponse `Content-Type: application/jwt`

sub	Identificatore del soggetto, come in IDToken	✓
iss	Identificatore del OP	✓
aud	Identificatore del RP (client_id)	✓
attributi	Claims richiesti con la richiesta di autenticazione	✓

IntrospectionRequest

POST

```
https://op.fornitore_identita.it/introspection

client_id=https://rp.fornitore_servizi.it&
client_assertion=eyJhbGciOi...&
client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer&
token=usDwMnEzJPpG5oaV8x3j...
```

IntrospectionResponse

client_id	Identificatore del RP	✓
sub	Identificatore del soggetto, come in ID Token	✓
exp	Scadenza del Token	✓
scope	Lista di scope richiesti all'autenticazione	✓
active	Valore booleano che indica la validità del Token	✓

RevocationRequest

POST

`https://op.fornitore_identita.it/revocation`

client_id=https://rp.fornitore_servizi.it&
client_assertion=eyJhbGciOi...&
client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer&
token=usDwMnEzJPpG5oaV8x3j...

RevocationResponse

`HTTP-Status 200 OK`

Refresh Token

- ✓ l'Utente deve essere informato della possibilità di utilizzare la sessione lunga revocabile
- ✓ Ad ogni avvio successivo al primo deve essere consentito l'accesso esclusivamente alle funzioni fruibili con il livello SPID L1
- ✓ Nel caso sia necessario accedere a funzionalità per le quali è richiesto un livello SPID superiore a L1 occorre effettuare una nuova autenticazione in base al livello richiesto
- ✓ Applicazioni mobile che fanno uso delle sessioni lunghe devono richiedere ad ogni avvio PIN o fattore biometrico
- ✓ **Il ripristino della sessione può essere utilizzato esclusivamente per ripristinare la sessione originaria**

Refresh Token

AuthenticationRequest

scope : **offline_access**

acr_values : ***deveesseresempreprepresenteancheSPID L1***

client_id	https://rp.fornitore_servizi.it
response_type	**code**
scope	**openid offline_access**
code_challenge	qWJlMe0xdbXrKxTm72EpH659bUxAxw80
nonce	MBzGqyf9QytD28eupyWhSqMj78WNqpc2
prompt	login
redirect_uri	https%3A%2F%2Frp.fornitore_servizi.it%2Fcallback
acr_values	**https://www.spid.gov.it/SpidL2** **https://www.spid.gov.it/SpidL1**
claims	{userinfo: {https://attributes.spid.gov.it/fiscalCode : null }}

TokenResponse

```
{
  "access_token": "dC34Pf6kdG...",
  "token_type": "Bearer",
  "refresh_token": "wJ848BcyLP...",
  "expires_in": 1800,
  "id_token": "eyJhbGciOiJI..."
}
```

RefreshRequest

POST

```
https://op.fornitore_identita.it/token

client_id=https://rp.fornitore_servizi.it&
grant_type=refresh_token
refresh_token=wJ848BcyLP...
```

AccessToken

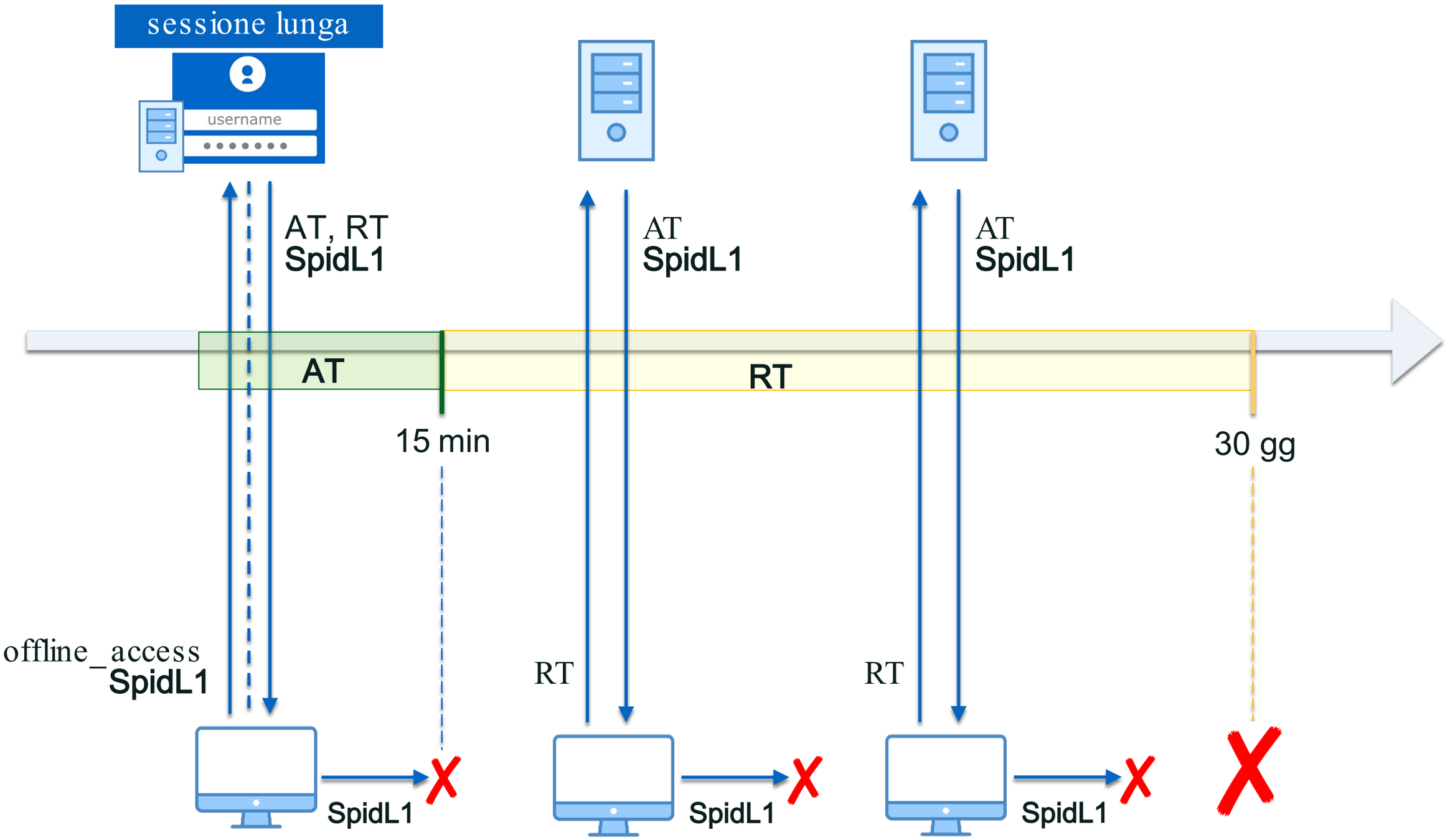
Validità massima **15 minuti**

RefreshToken

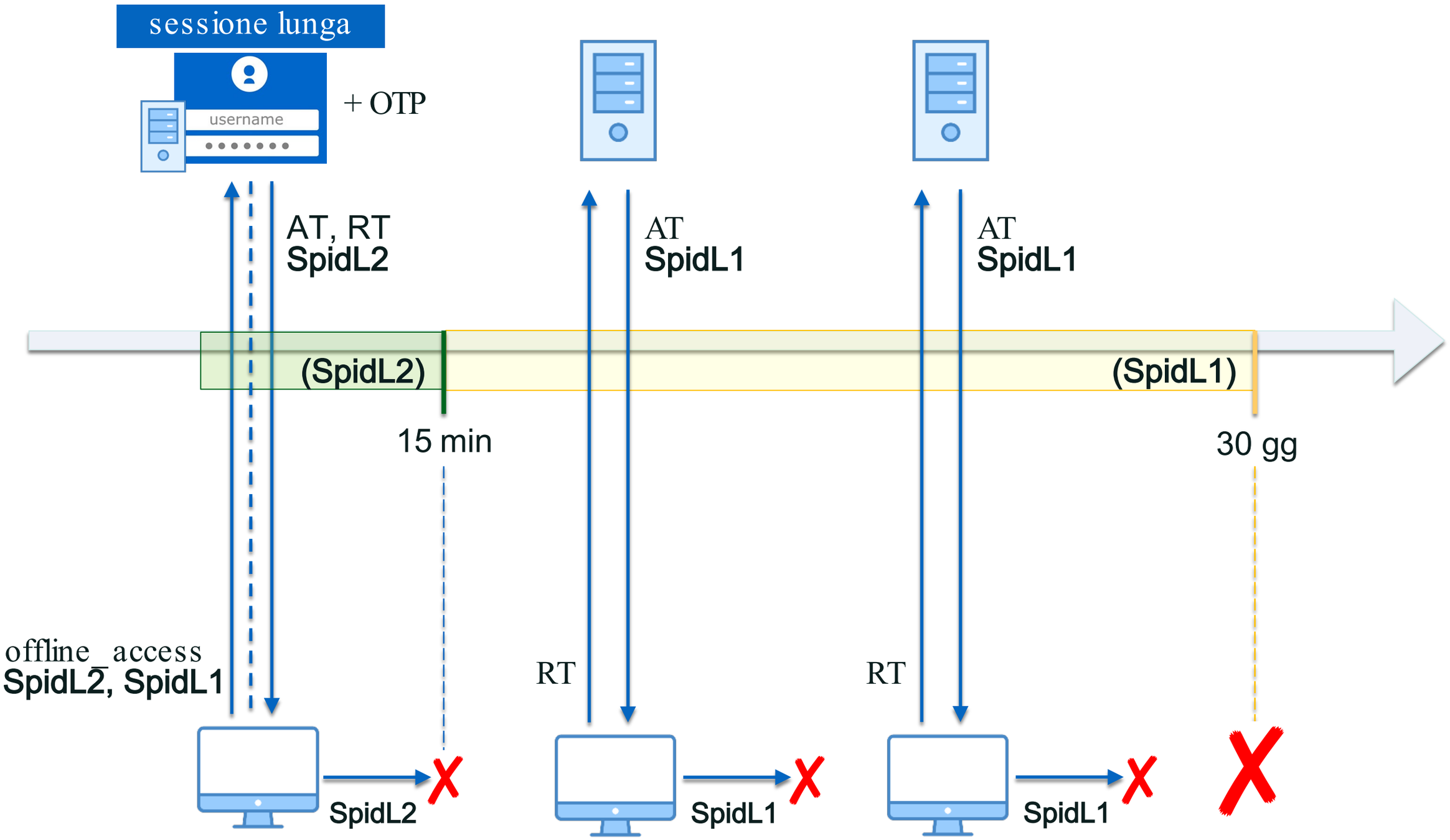
Validità massima **30 giorni**

Utilizzo :**illimitato** entro i 30 giorni

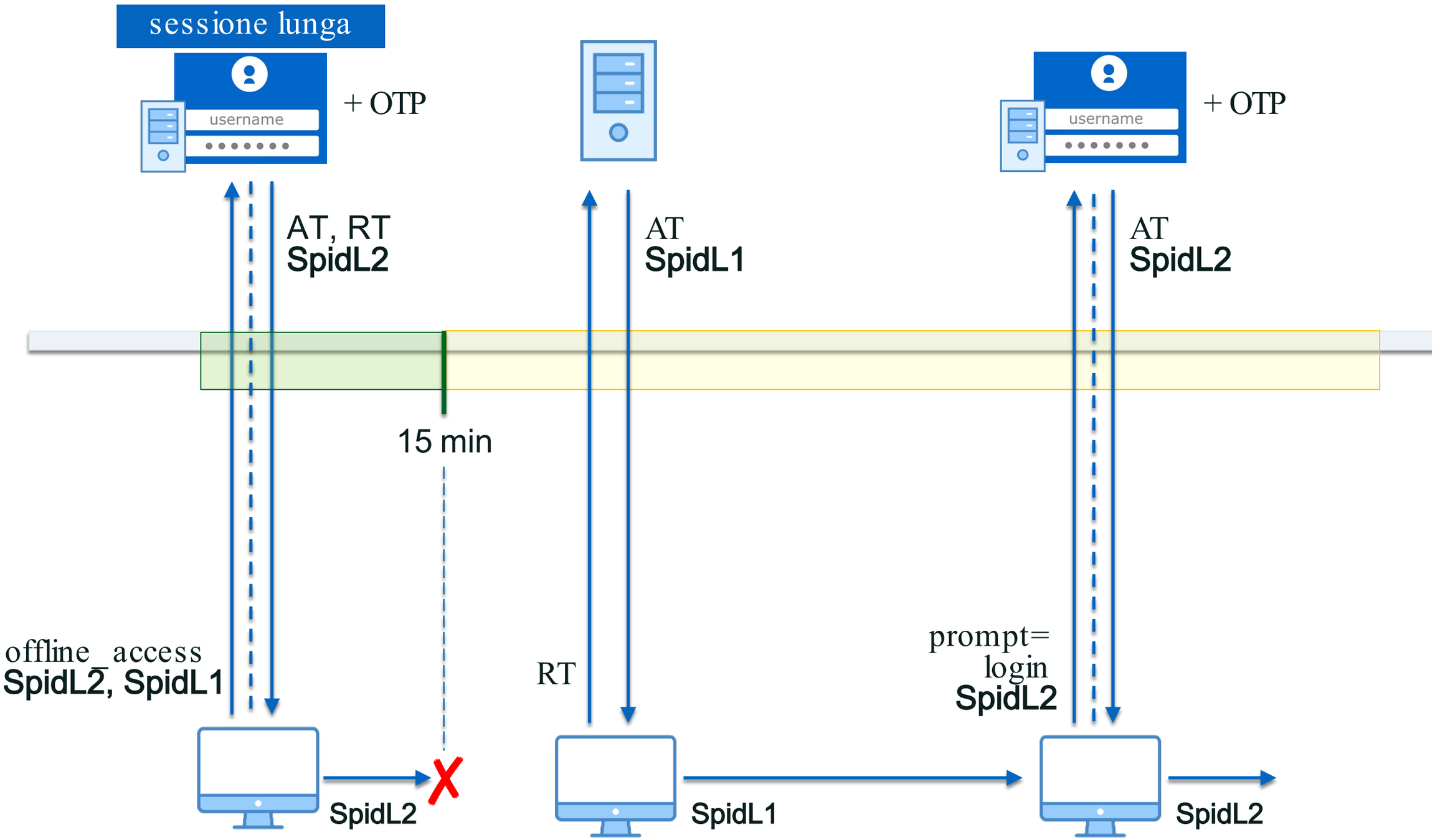
Refresh Token – Scadenza AT, RT



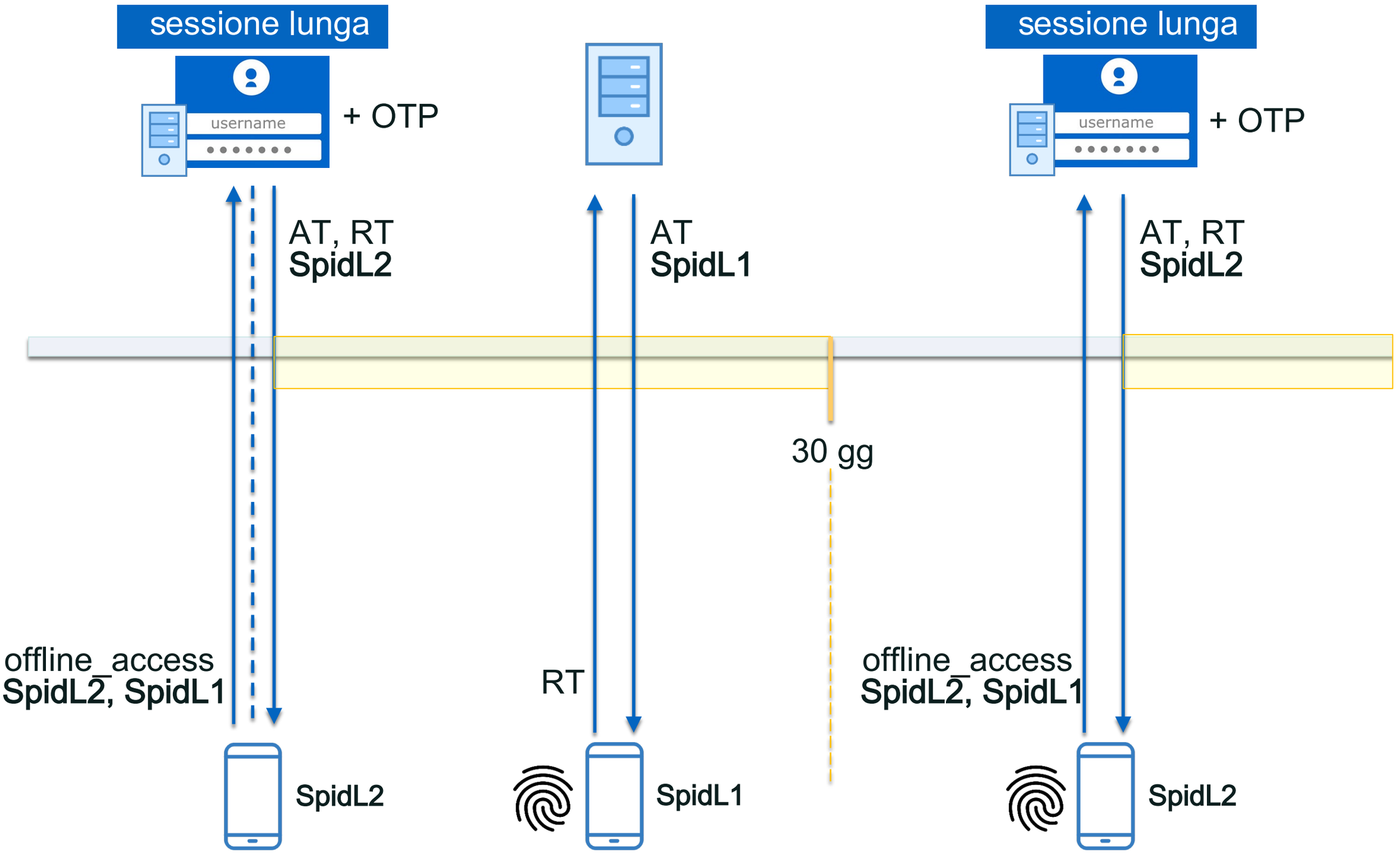
Refresh Token – Ripristino sessione



Refresh Token – Cambio Livello



Refresh Token – Applicazioni mobile



Gestione delle sessioni

OP devono offrire:

possibilità di visualizzare le sessioni lunghe attive

possibilità di revocare singolarmente una sessione attiva

possibilità di revocare in massa tutte le sessioni attive

possibilità di revocare tutte le sessioni attive al cambio password

Gestione dei Log

OP e RP sono tenuti a conservare per 24 mesi evidenze di:

- rilasciodi IDTokene AccessTokena fronte diautenticazione
- rilascio diRefreshTokena fronte di autenticazione
- rilascio di ID e AccessTokena fronte di utilizzo dRefreshToken

Rispetto della Privacy

Accesso ai Log riservato

Cifratura dei dati persistenti

Sviluppi futuri

- Registro SPID SAML e OpenID Connect
- Ambiente di Test OpenID Connect SPID
- SPID OpenID Connect Validator
- Indicazioni per l'utilizzo di JWS e JWE
- Public Key Infrastructure AgID

Grazie per l’attenzione

AGID | Agenzia per l’Italia Digitale

agid.gov.it