INTEGRATING FIDO AUTHENTICATION & FEDERATION PROTOCOLS

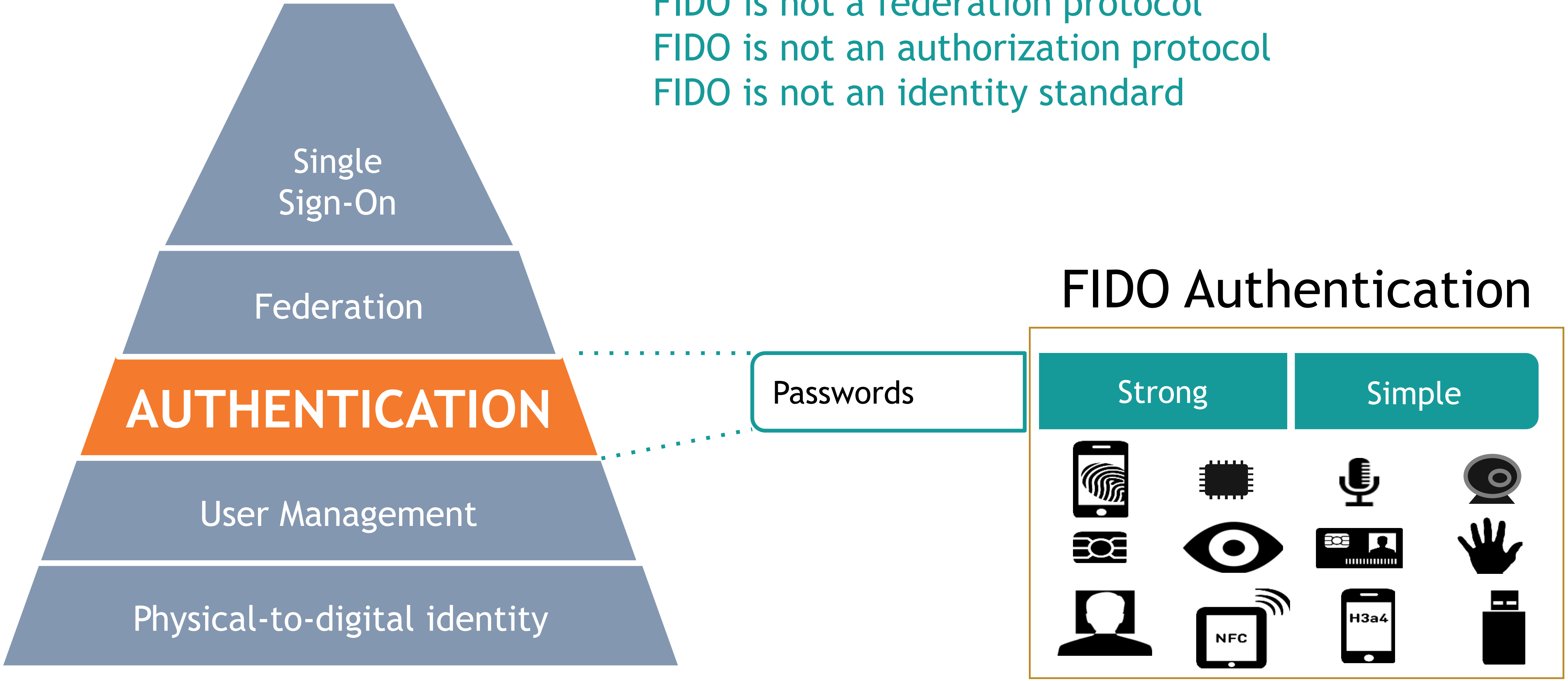
BEST PRACTICES FOR ENTERPRISE DEPLOYMENT

AGENDA

- Does FIDO complement Federation?
- What are the benefits in pairing FIDO and Federation?
- How to integrate FIDO with modern Federation protocols?

What is FIDO?

FIDO is an authentication protocol
FIDO is not a federation protocol
FIDO is not an authorization protocol
FIDO is not an identity standard



Single Sign-On

Federation

AUTHENTICATION

User Management

Physical-to-digital identity

Passwords

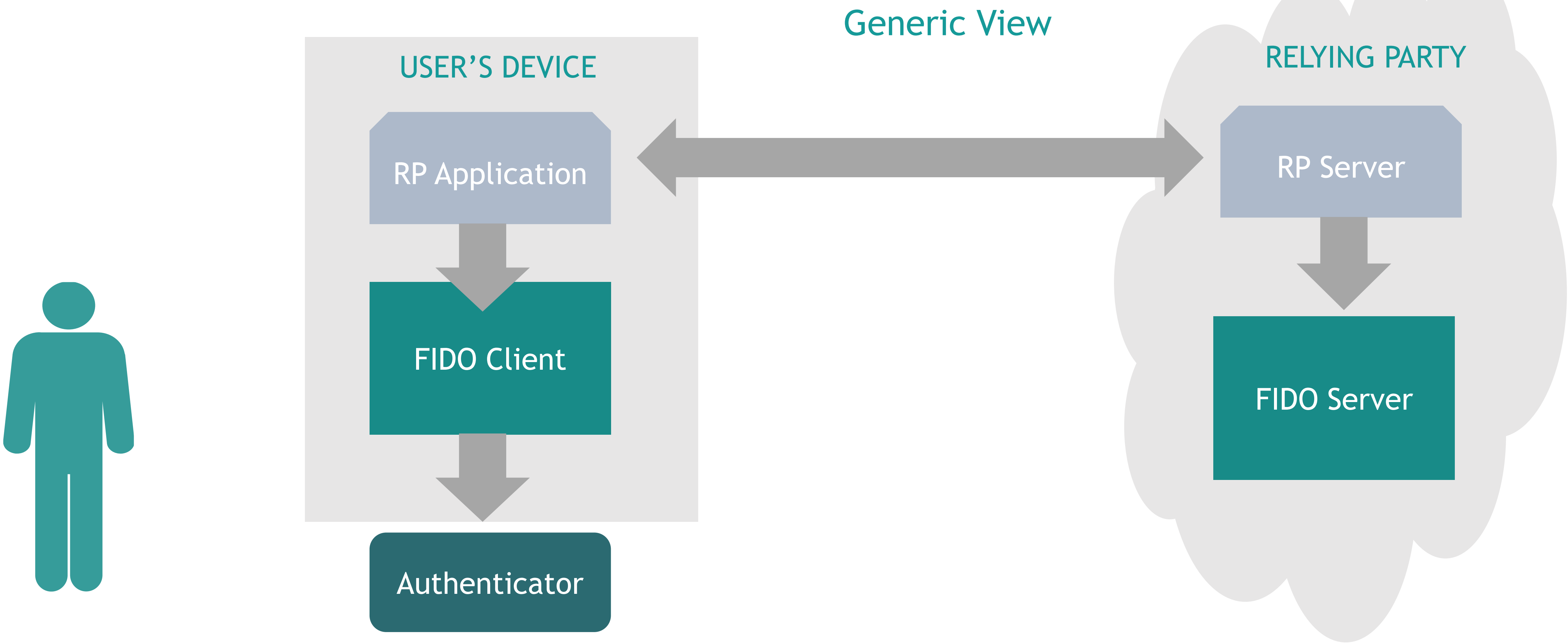
FIDO Authentication

Strong

Simple

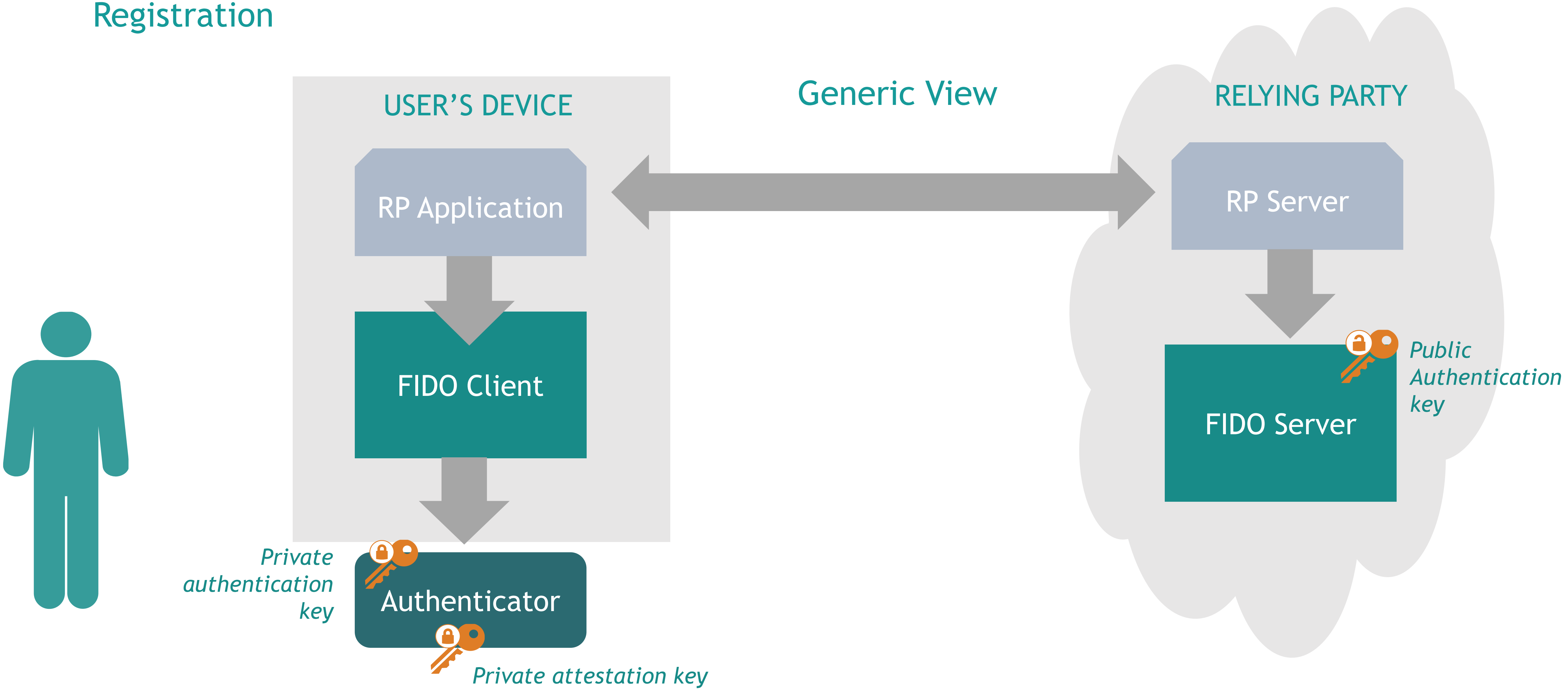
How does FIDO Work?

Architecture



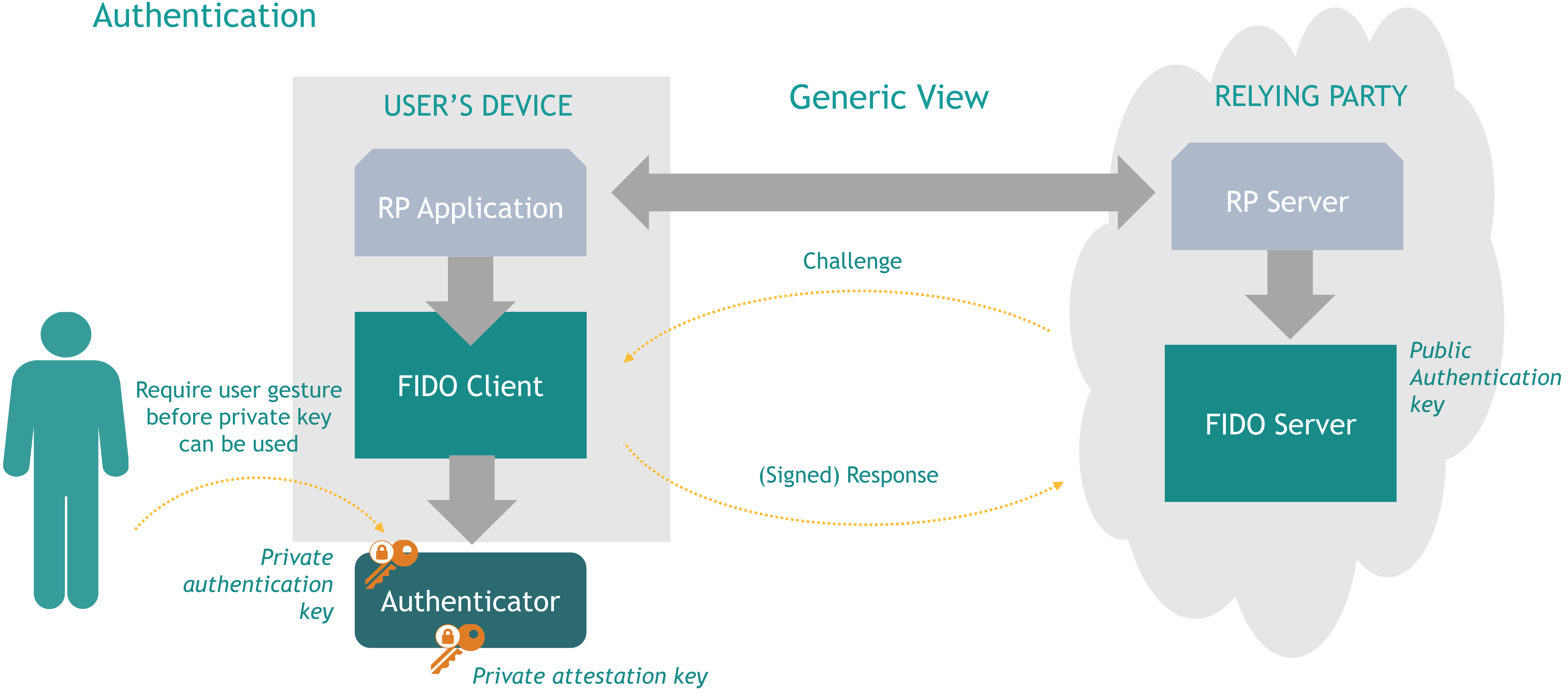
How does FIDO Work?

Registration

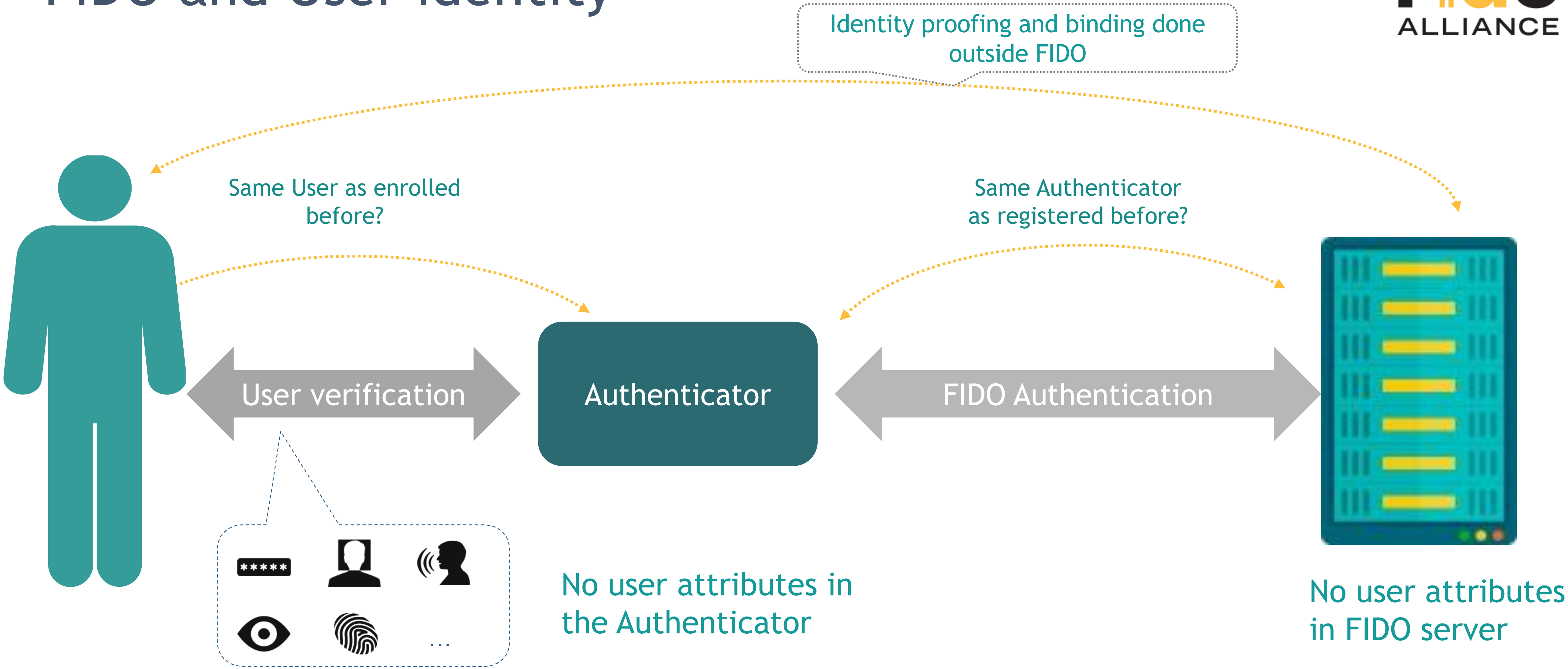


How does FIDO Work?

Authentication



FIDO and User Identity



Identity proofing and binding done outside FIDO

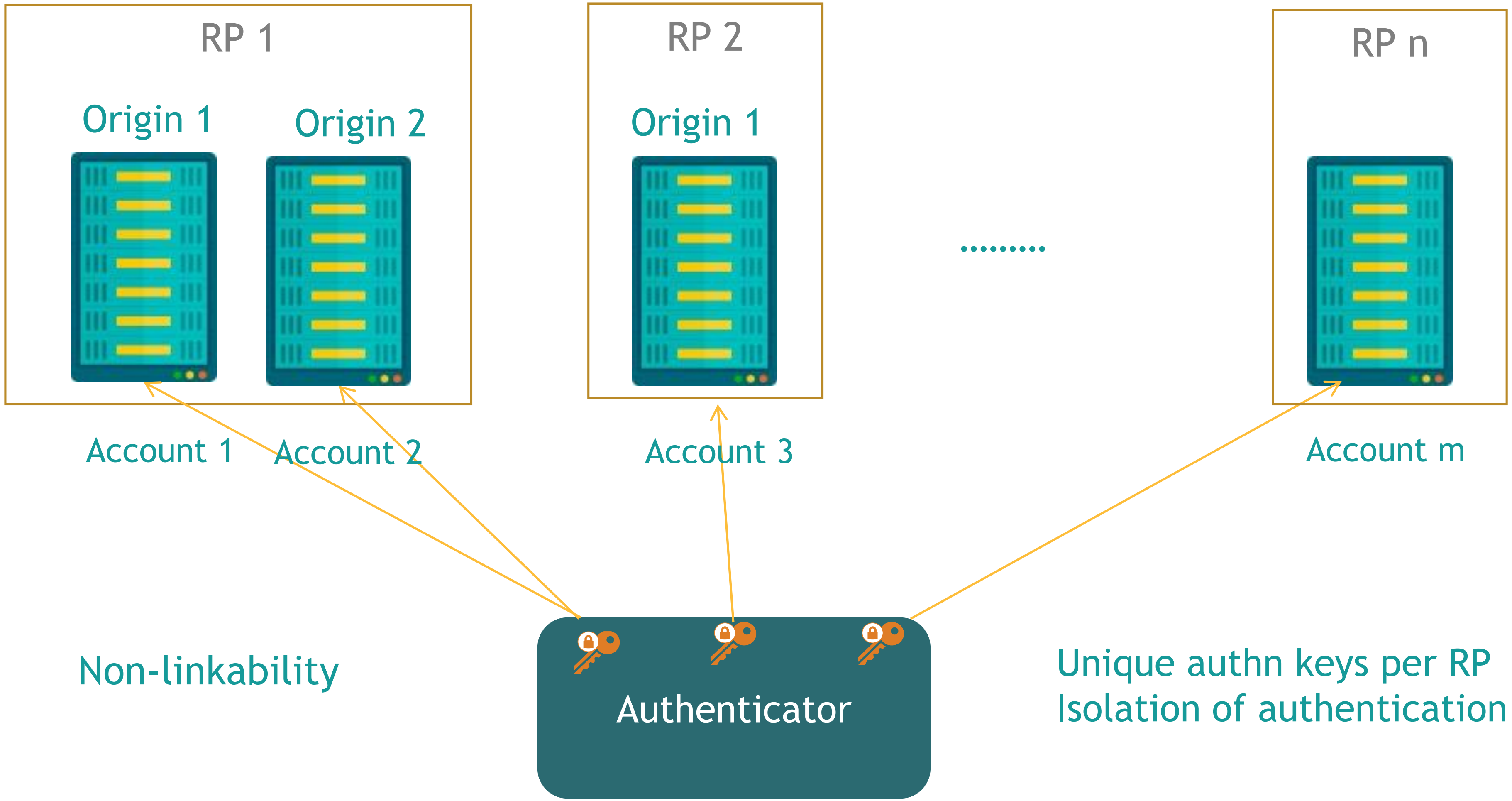
Same User as enrolled before?

Same Authenticator as registered before?

No user attributes in the Authenticator

No user attributes in FIDO server

One Authenticator, Many Applications



Non-linkability

Unique authn keys per RP
Isolation of authentication transactions

FIDO Benefits to the User

Reduce the burden of remembering multiple passwords

Use a simple gesture for authentication

Reduce the burden of using a variety of two-factor authentication form factors

Use one authenticator with multiple applications

Preserve user privacy

Biometric data is local
No secrets on the server
No linkability between RPs

What Problems Does Federation Solve?

Without Federation,

Users have to:

- Remember multiple passwords
- Sign-in multiple times a day

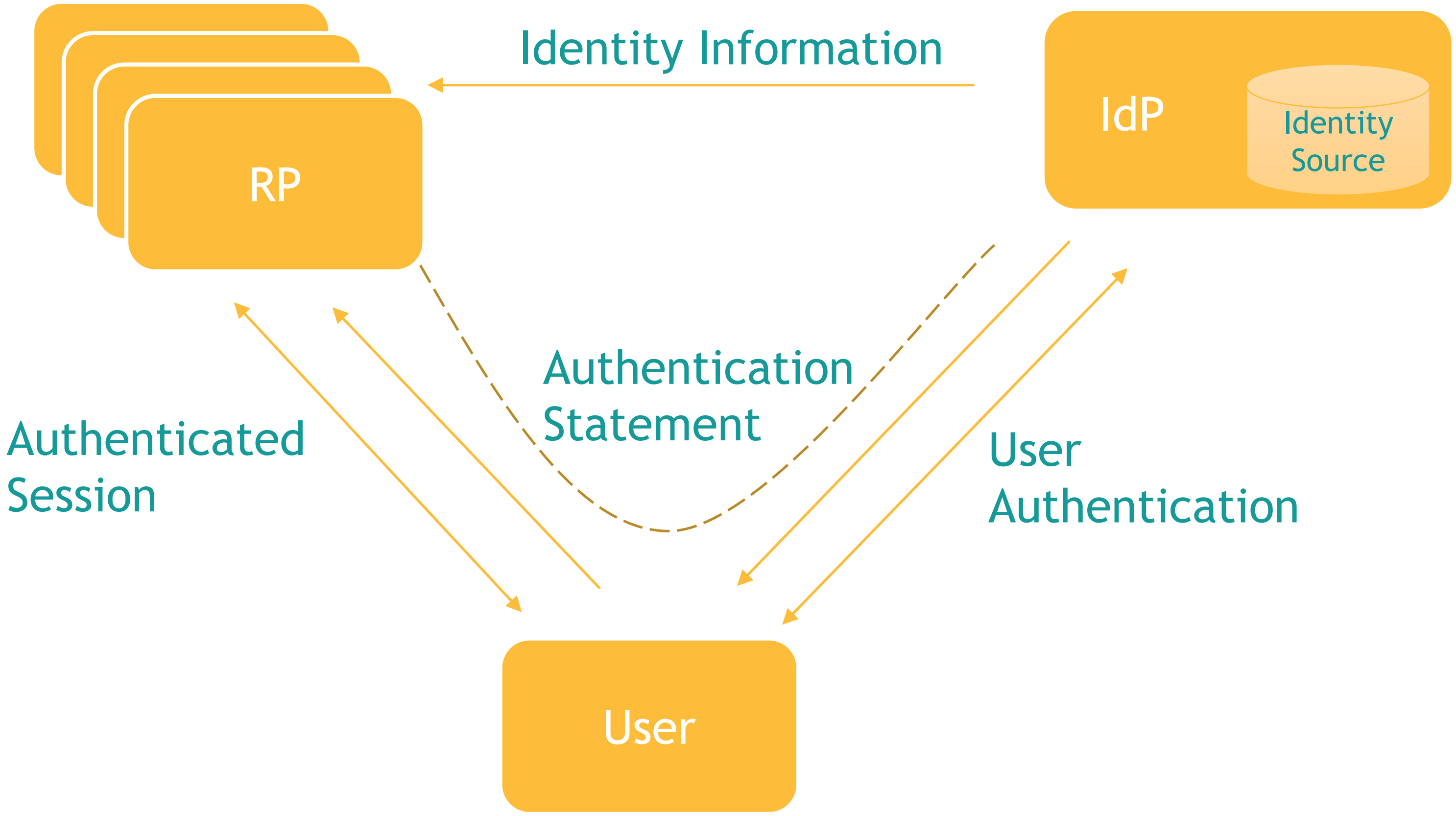
Administrators have to manage:

- Authentication policies,
- Group permissions and
- User accounts
- Across multiple domains

Reduced productivity
Increased number help desk calls
Increased administration overhead
Increased security risks

How Federation Solves These Problems

Three-Party Trust Relationship



Identity Information

IdP

Identity Source

RP

Authentication Statement

Authenticated Session

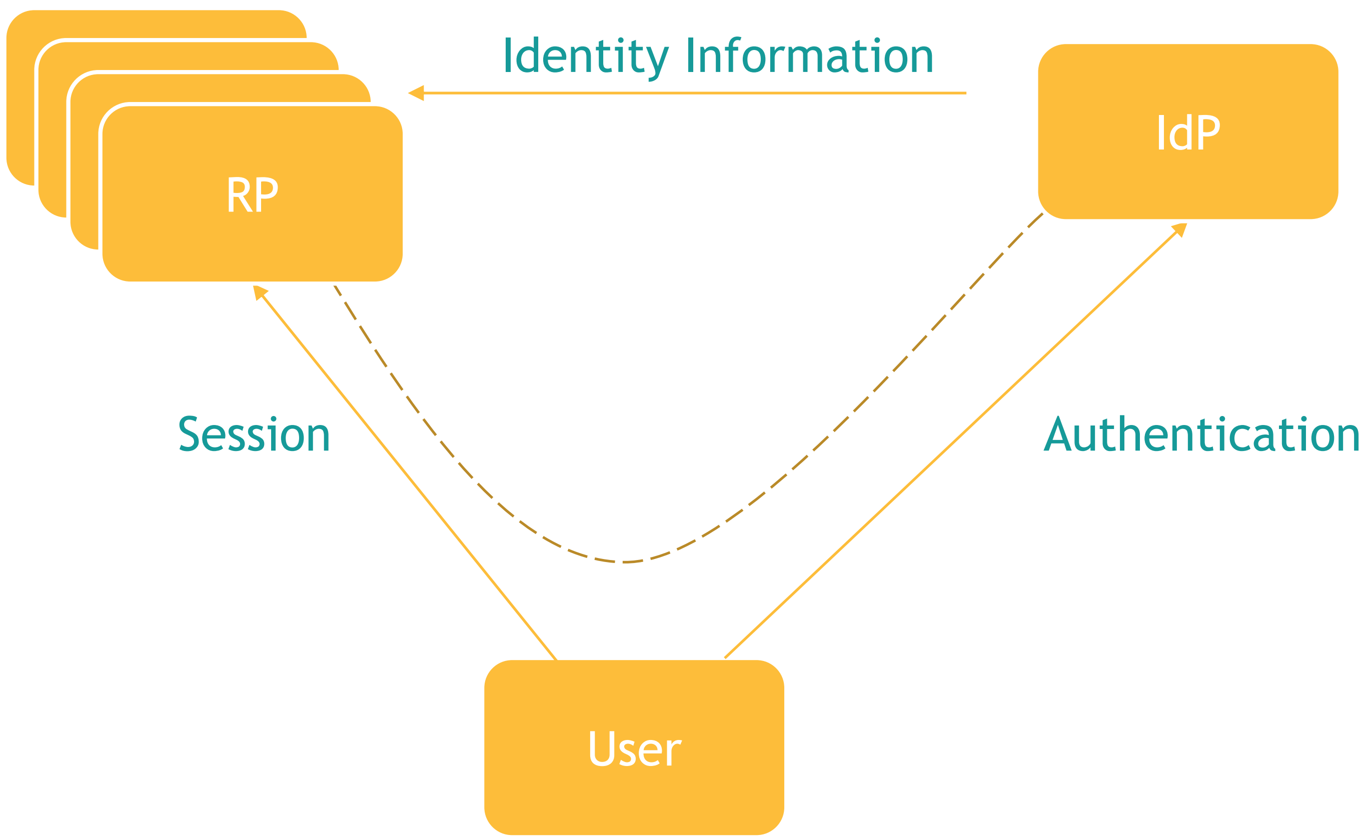
User Authentication

User

Federation Benefits to End Users

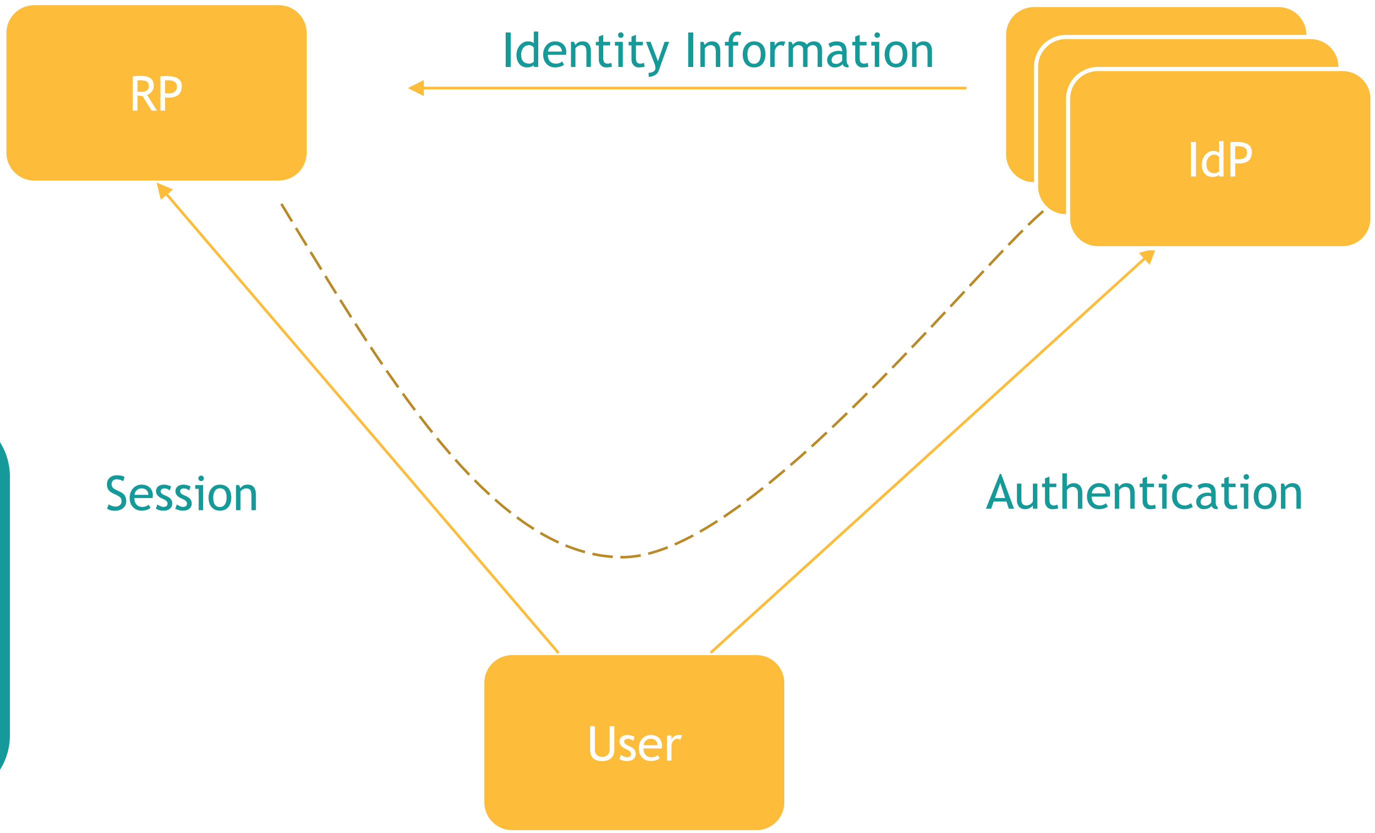
Users remember one password, sign in once and access multiple applications

Three-Party Trust Relationship



Federation Benefits to Relying Parties

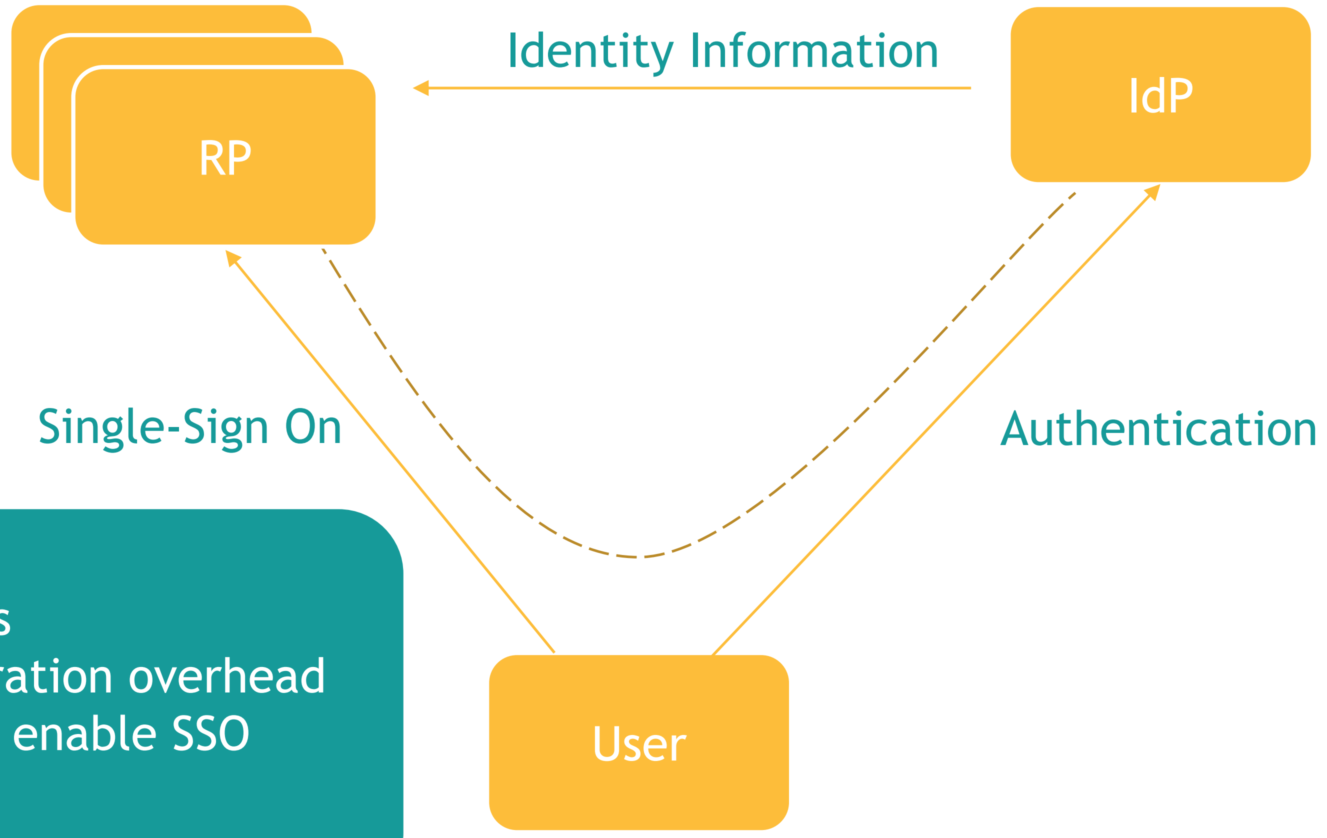
Three-Party Trust Relationship



RPs move user identity to trusted third-party authentication authorities

Federation Benefits to Identity Providers

Three-Party Trust Relationship



IdPs link user identity to multiple RPs

- Reduce security risk and administration overhead
- Enforce strong authentication and enable SSO
- Protect user identity attributes

The Downside of Federation

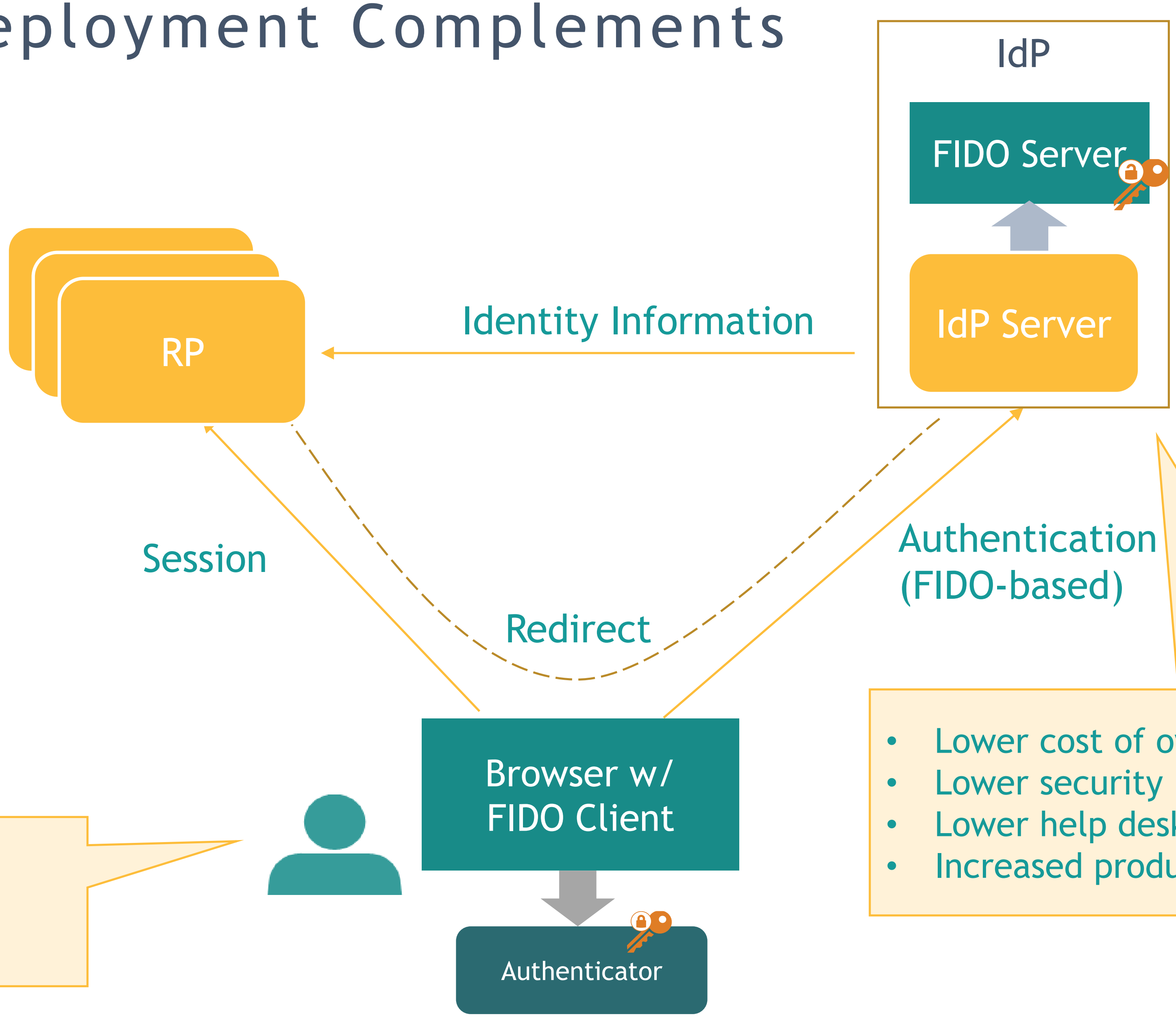
Users hate to use complex passwords for primary authentication

Organizations have major concerns about password security

Stronger and more convenient authentication methods are needed

FIDO is the Solution

How FIDO Deployment Complements Federation

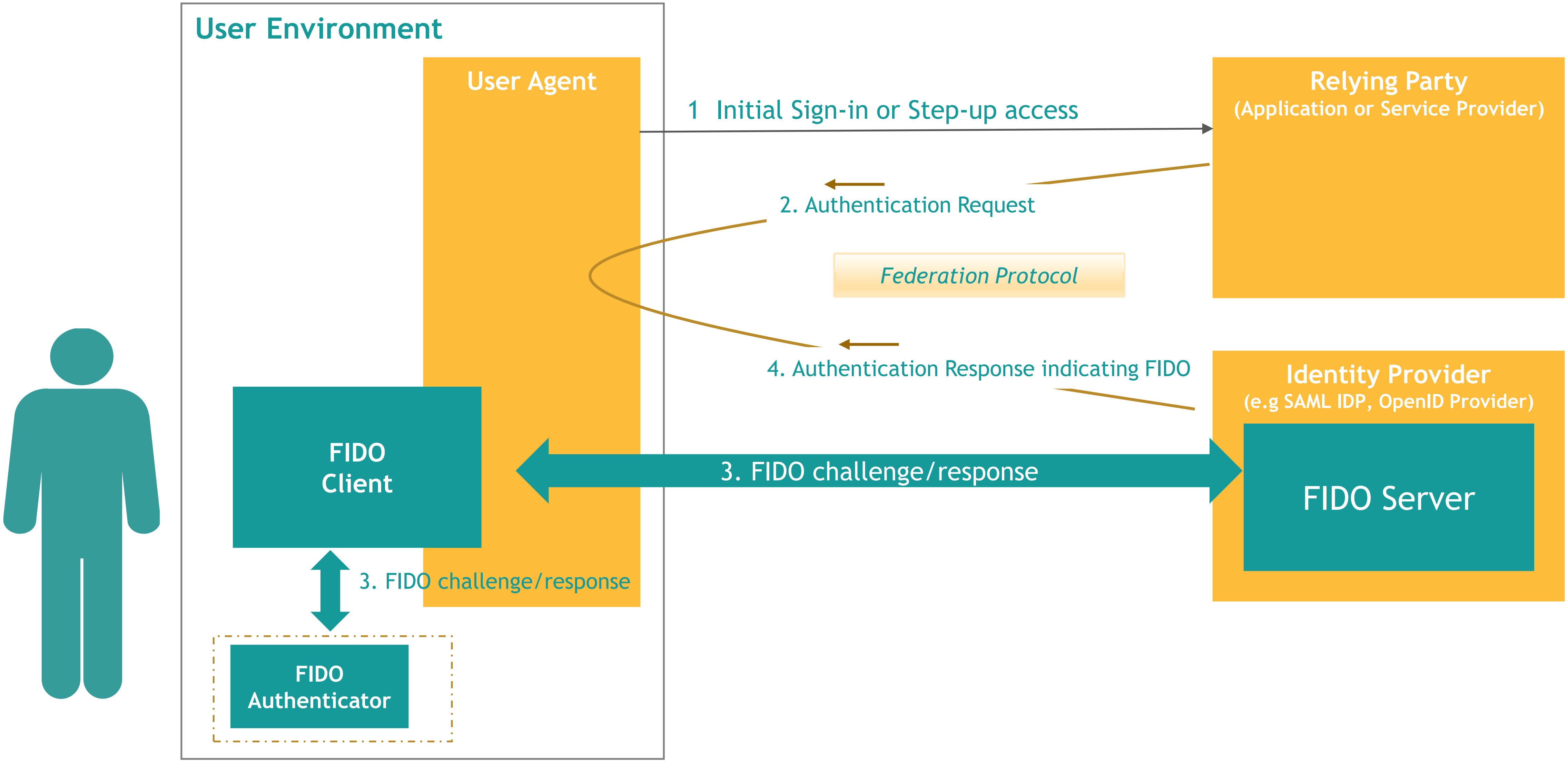


No changes to RP applications

One authenticator, one credential for multiple RPs

- Lower cost of ownership
- Lower security risks
- Lower help desk calls
- Increased productivity

Federated Authentication Flow with FIDO


User Environment
User Agent
1 Initial Sign-in or Step-up access
Relying Party
(Application or Service Provider)
2. Authentication Request
Federation Protocol
4. Authentication Response indicating FIDO
Identity Provider
(e.g SAML IDP, OpenID Provider)
FIDO Client
3. FIDO challenge/response
FIDO Server
3. FIDO challenge/response
FIDO Authenticator

How to Apply FIDO-based Authentication

Preconfigured IdP Authentication Policy

- Global or per-RP policy set in the IdP

Just-in-Time RP Authentication Policy

- Specified by RP in the authentication request using authn context class reference
  - AuthnContextClassRef parameter in SAML
  - Acr_values request parameter in OIDC
- IdP returns information indicating that FIDO-based auth was used
  - Using AuthnContextClassRef in SAML
  - Using acr and amr claims In ID Token in OIDC

Use AuthnContextClassRef in SAML for JIT enforcement

Sample SAML Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
…
<samlp:RequestedAuthnContext Comparison="exact">
...
<saml:AuthnContextClassRef>urn:rsa:names:tc:SAML:2.0:ac:classes:MediumAssurance</saml:AuthnContextClassRef>
…
</samlp:RequestedAuthnContext>
…
</samlp:AuthnRequest>
```

Sample SAML Response

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ….
<saml:AuthnStatement AuthnInstant="2014-07-17T01:01:48Z" …..
….
<saml:AuthnContextClassRef>urn:rsa:names:tc:SAML:2.0:ac:classes:FIDO</saml:AuthnContextClassRef>
……
</saml:AuthnStatement>
…
</samlp:Response>
```

Use acr_values in OIDC for JIT enforcement

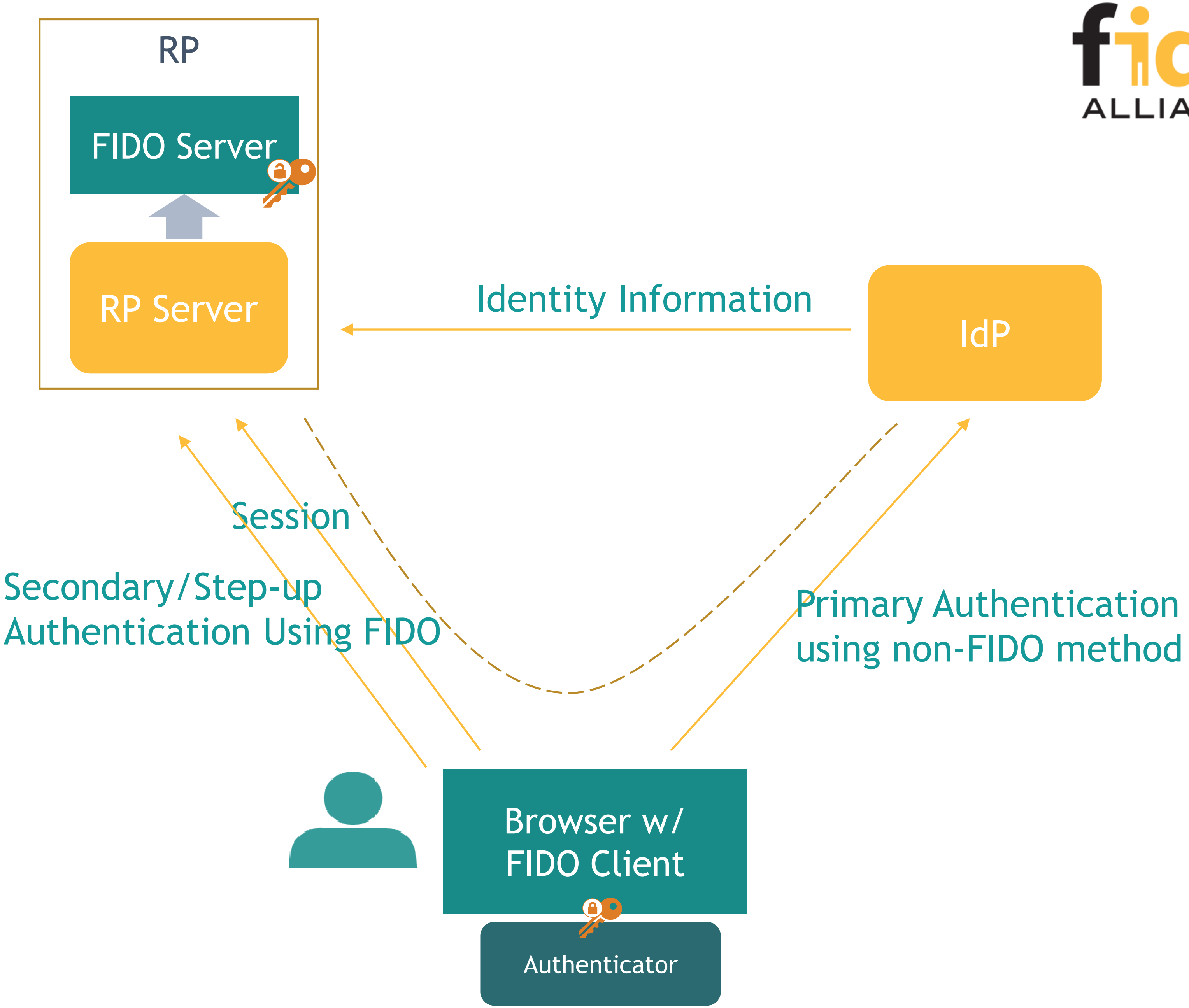
Sample OIDC Request/Response

```
EndpointURI: https://tenant.server.example.com/oidc/auth
Http Parameters: {
  response_type: id_token,
  client_id: rp_client,
  response_mode: query,
  redirect_uri: https://rp.example.com/oidc-rp/,
  scope: openid,
   ......
  acr_values: phr phrh mfa
```

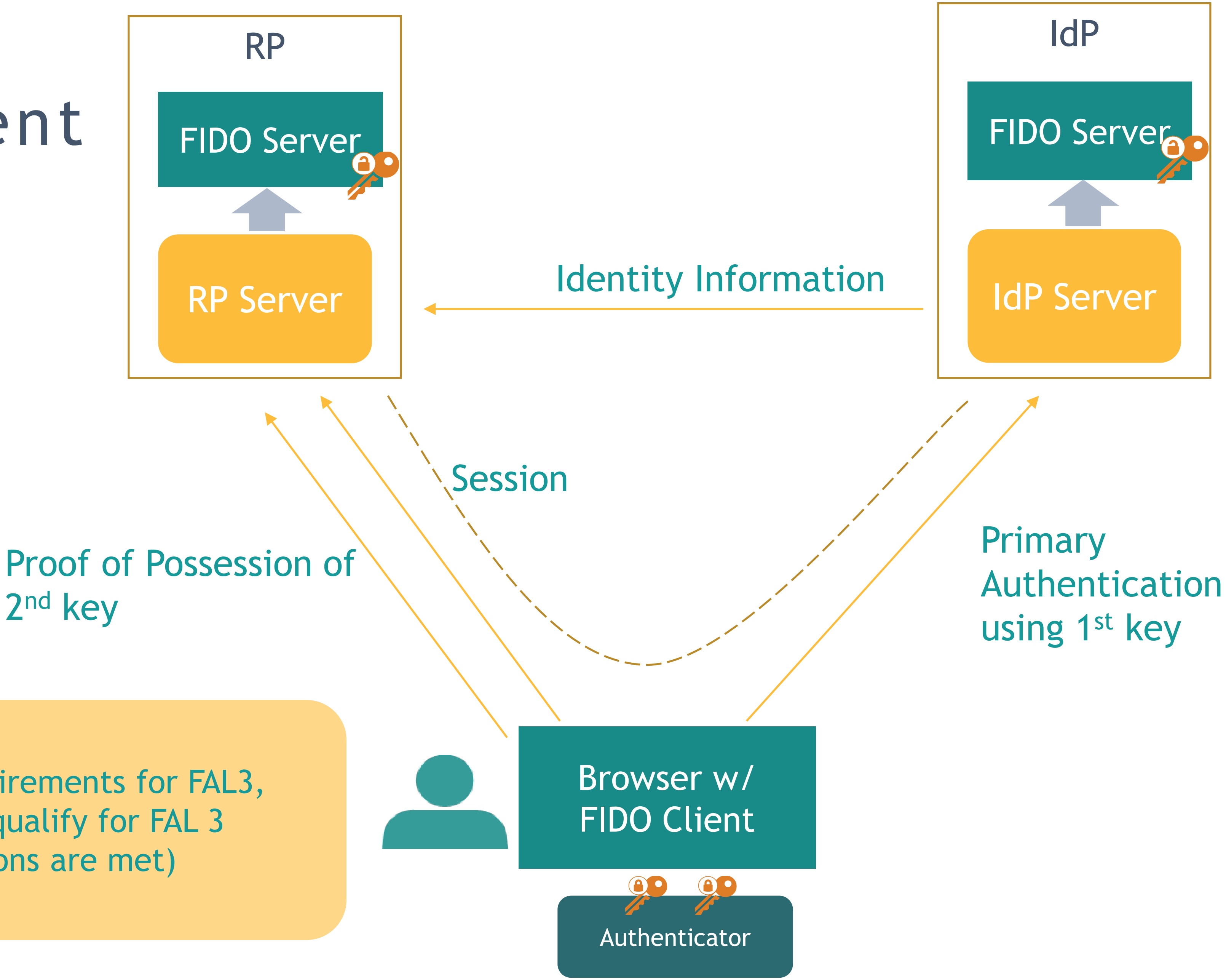
```
RedirectURI: https://rp.example.com/oidc-rp/
Http Parameters: {
.......
'id_token' content:
{
"auth_time":1490898779,
"exp":1490899139,
"sub":"someone@example.com",
.......
"iss":" https://tenant.server.example.com/oidc-fe",
"iat":1490898779,
"acr":“phrh",
"amr":[“hwk"]
}
}
```

ACR policy identifiers that can be satisfied by FIDO Authenticators are defined OpenID Connect (EAP) ACR Values specification

Other Deployment Options


RP
FIDO Server
RP Server
Identity Information
IdP
Session
Secondary/Step-up Authentication Using FIDO
Primary Authentication using non-FIDO method
Browser w/ FIDO Client
Authenticator

Other Deployment Options



Based on NIST 800-63-3 requirements for FAL3, this deployment model can qualify for FAL 3 (provided that other conditions are met)

Benefits of FIDO & Federation Integration

Users continue to enjoy the benefits of Federated SSO, while FIDO provides a more convenient, more secure and privacy preserving method of authentication

Organizations offer a streamlined authentication method without putting user identity attributes at risk

While using Federation Authentication, add FIDO support today and get its benefits

- 200+ Certified FIDO authenticators
- 85+ FIDO certified server implementations
  - Some are deployed as part of a Federated authentication solution

For more details on FIDO and Federation integration, read FIDO Alliance Enterprise Adoption Best Practices white paper