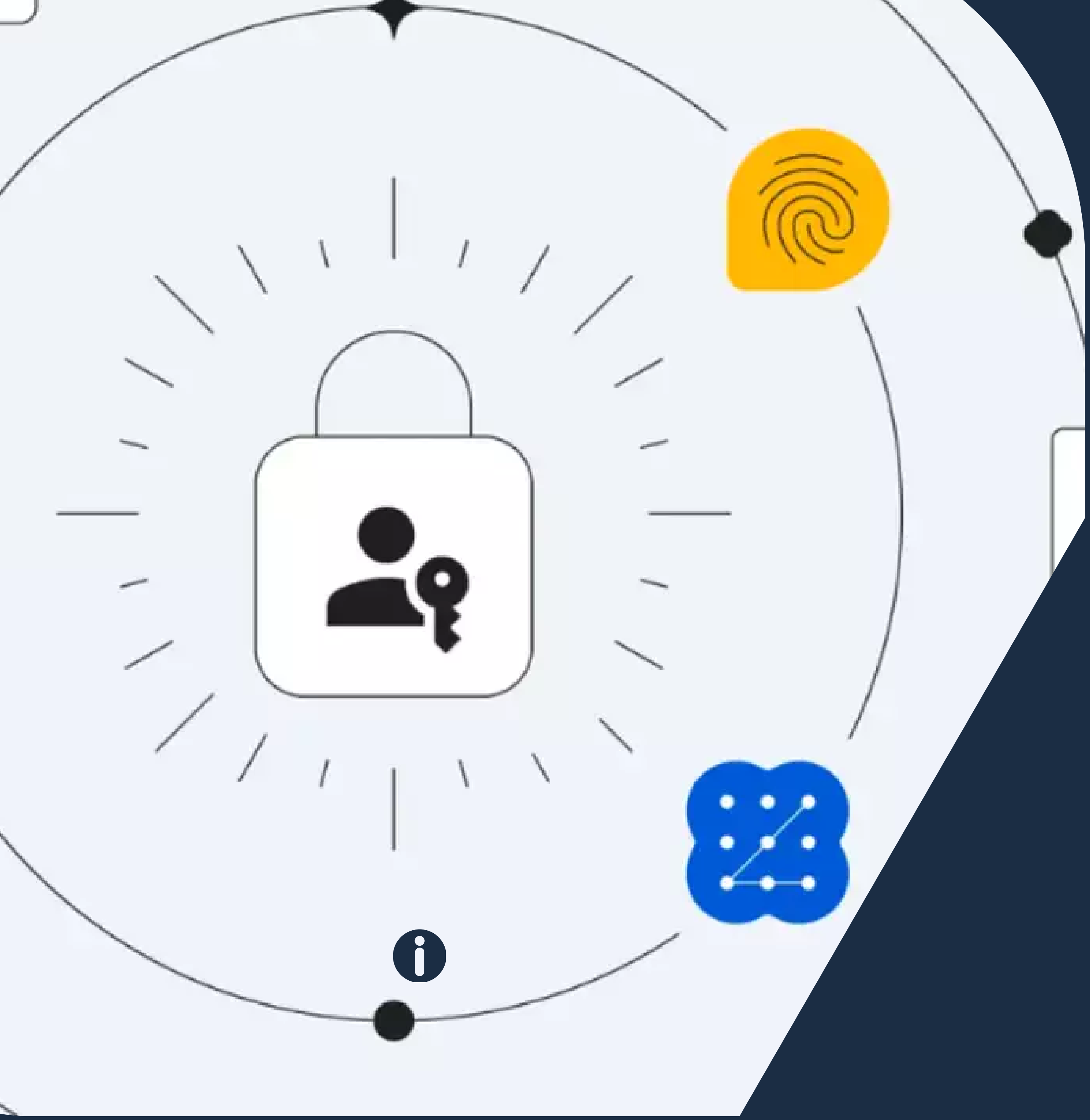
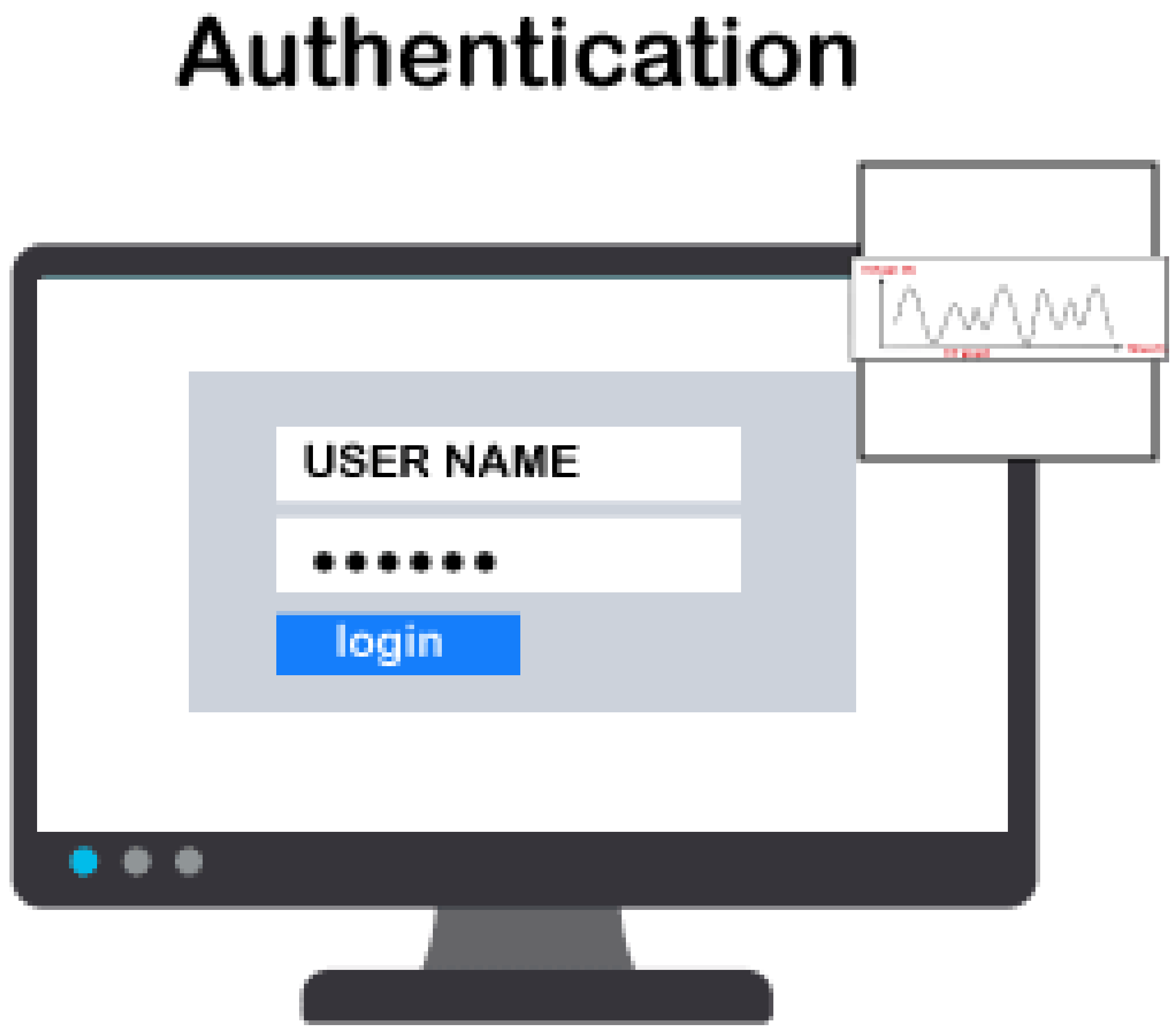


EVOLUTION OF AUTHENTICATION

What is Authentication?



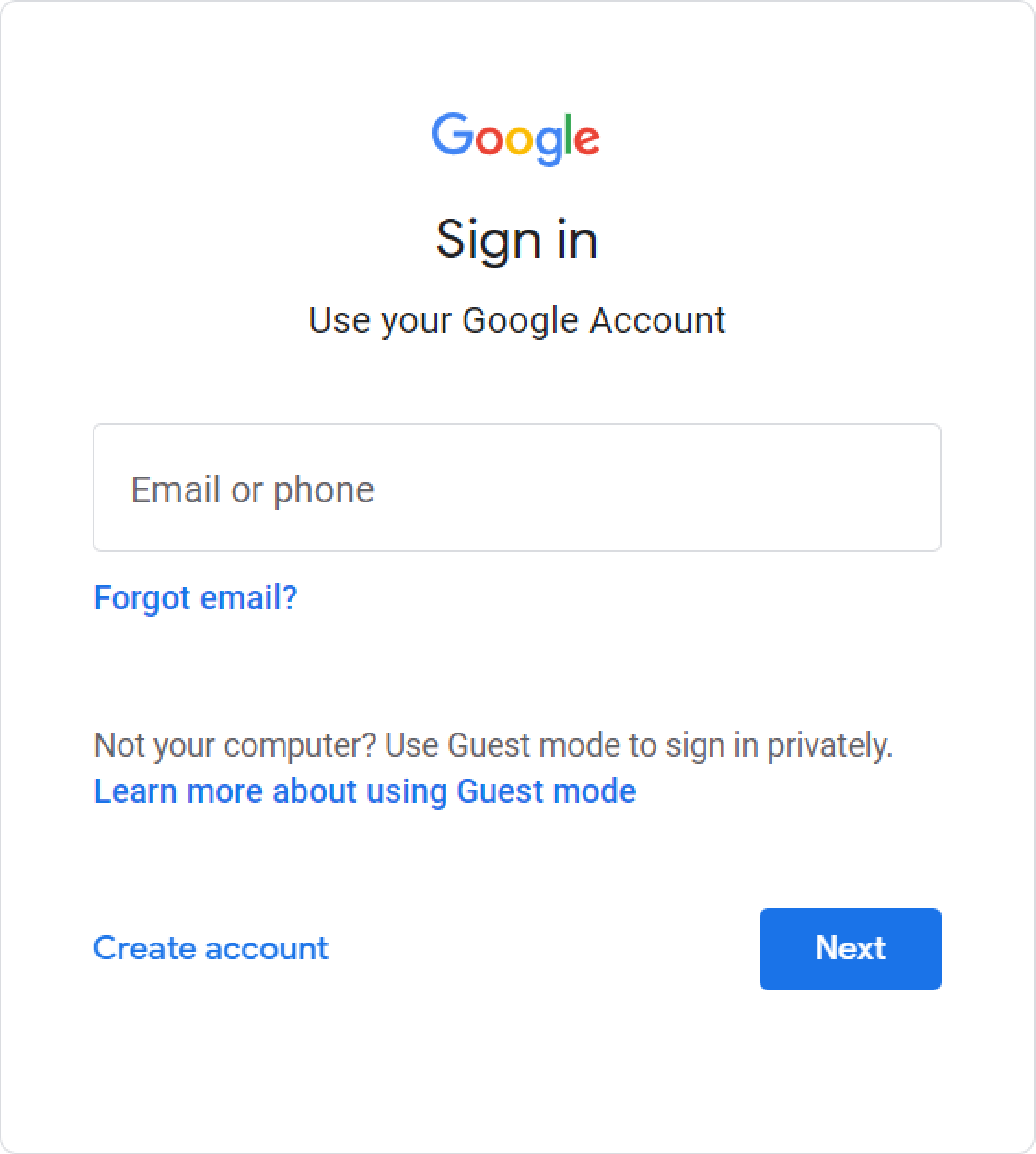
Confirms if users are who they say they are.

NYPD
Authorization
Authentication

Authorization

Gives permission to users to access a resource.

miniOrange



Google

Sign in

Use your Google Account

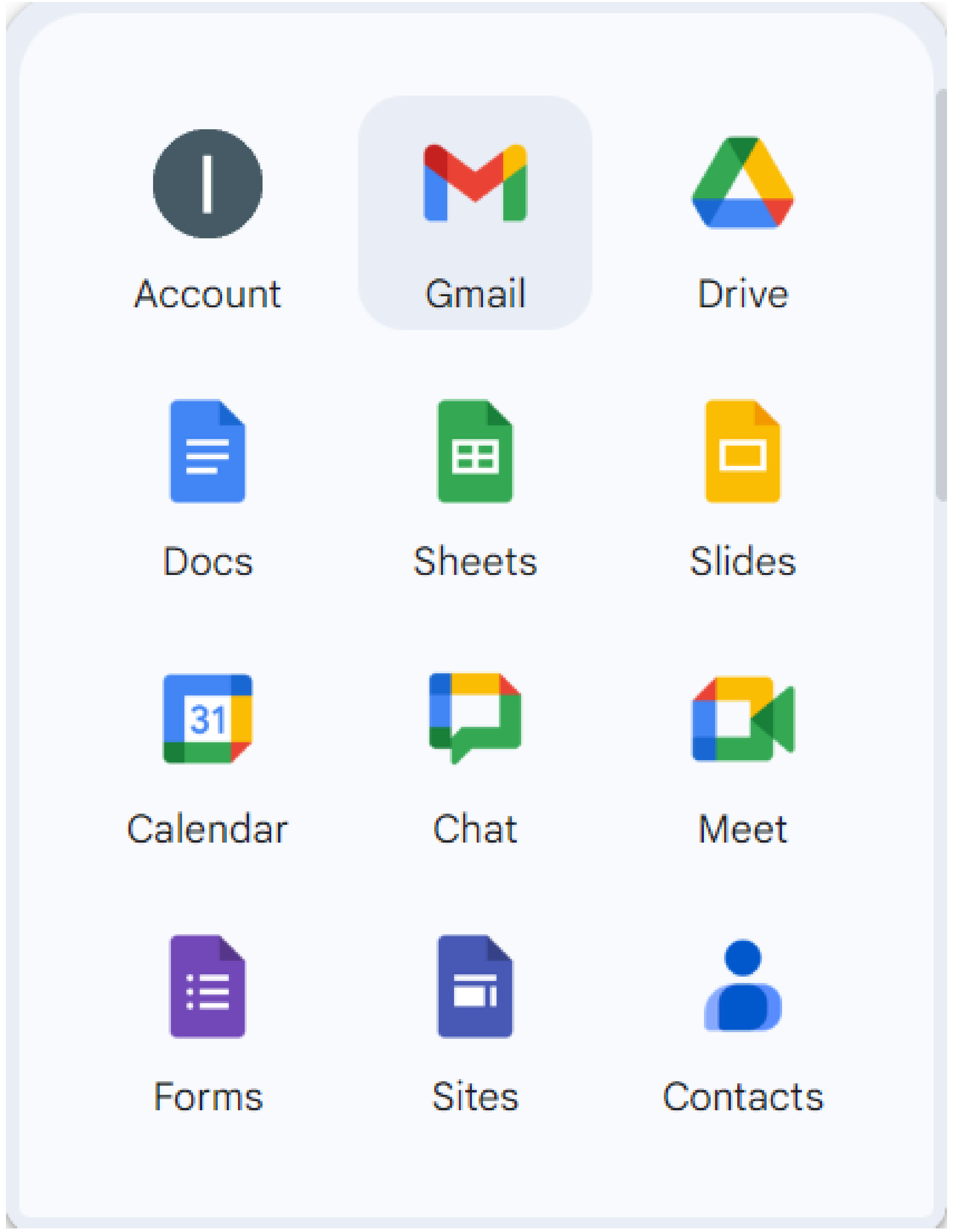
Email or phone

Forgot email?

Not your computer? Use Guest mode to sign in privately.
Learn more about using Guest mode

Create account

Next



About us

Gaurav Todwal

Identity Management Enthusiast

Ishita Pabbi

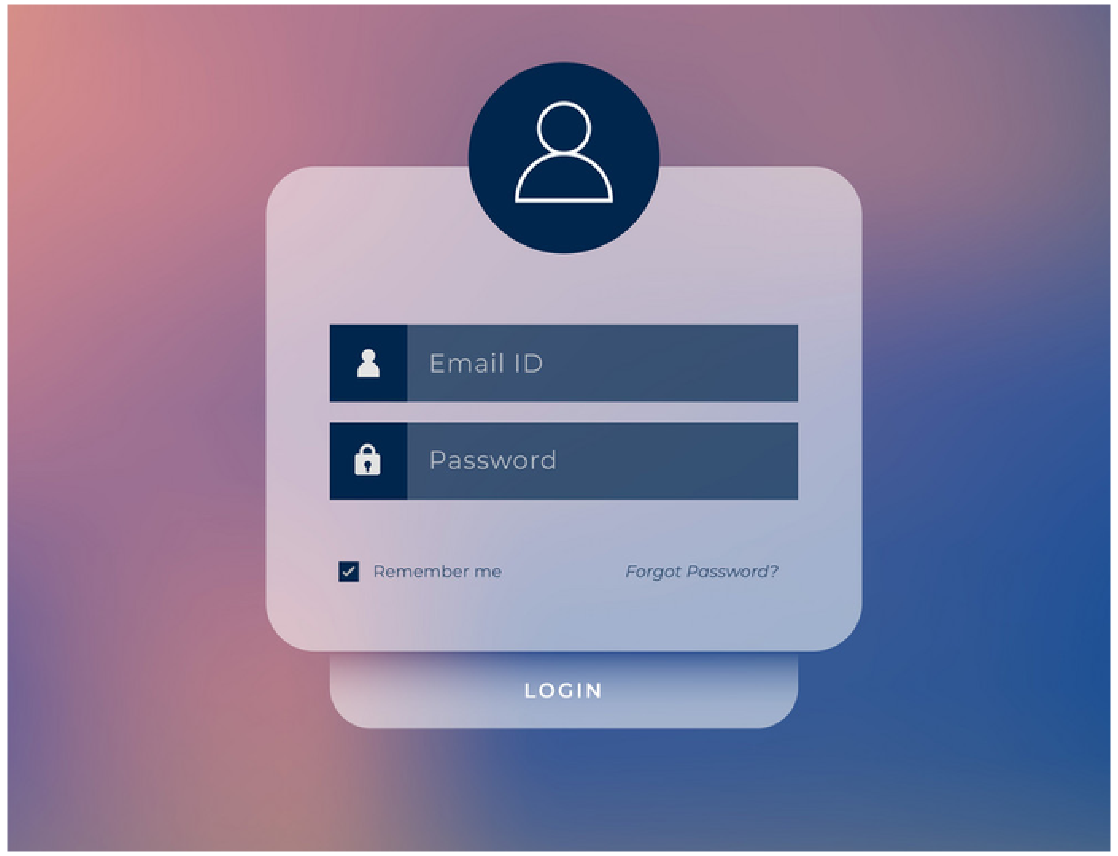
Passionate about Unraveling the Why and How

HOW IDENTITY HAS EVOLVED?

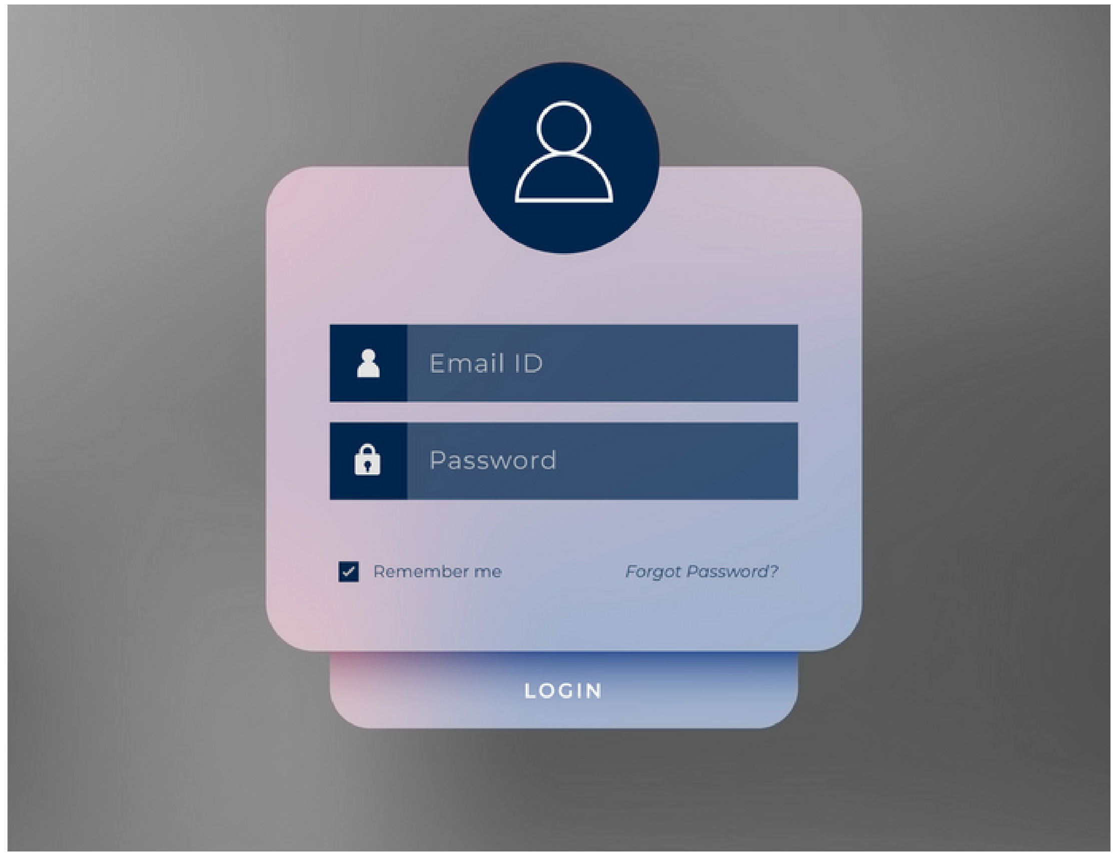
Centralized

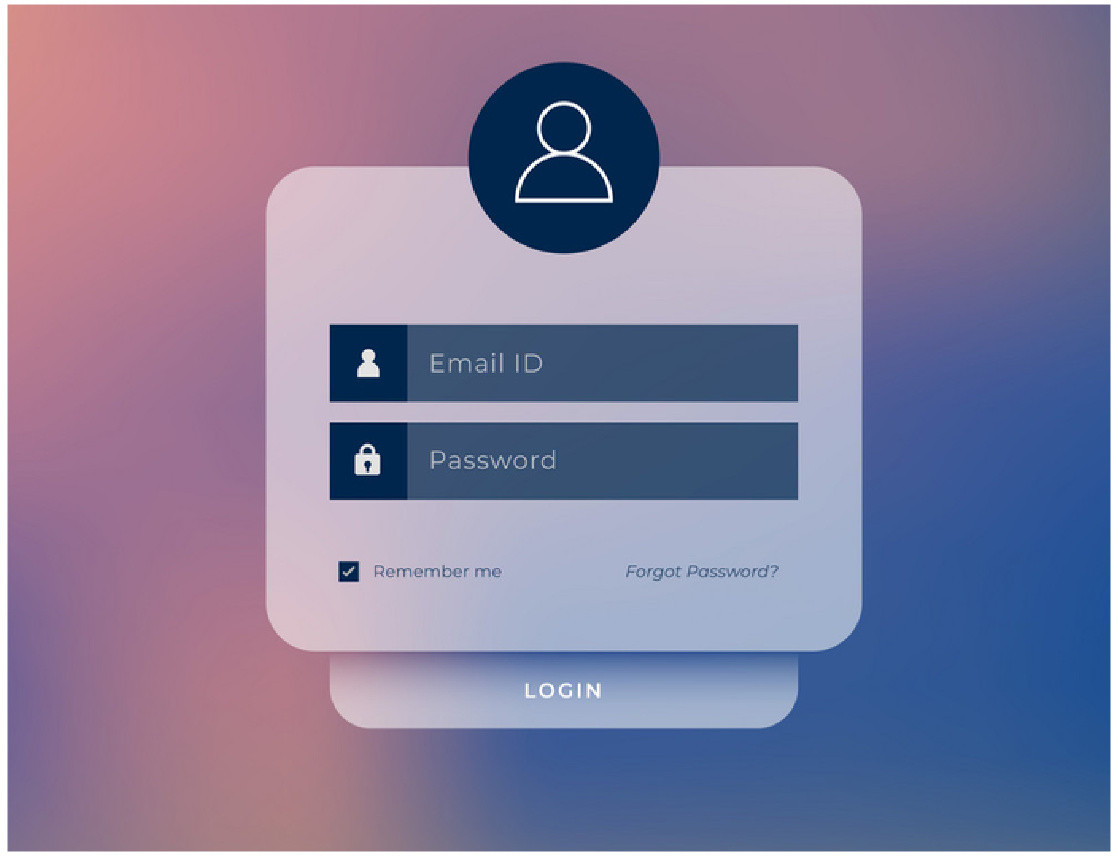
Federated

Decentralized



ZOHO

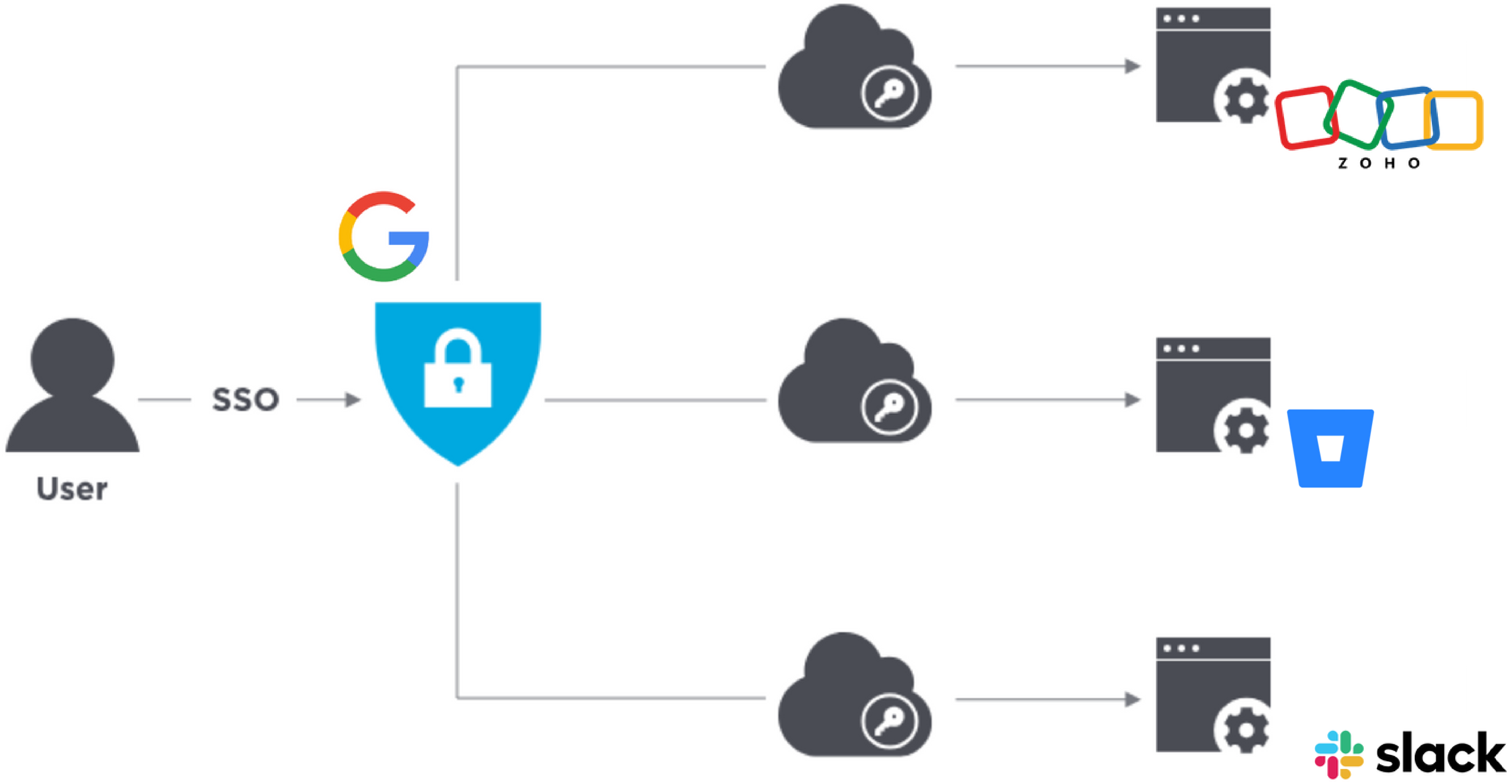




slack

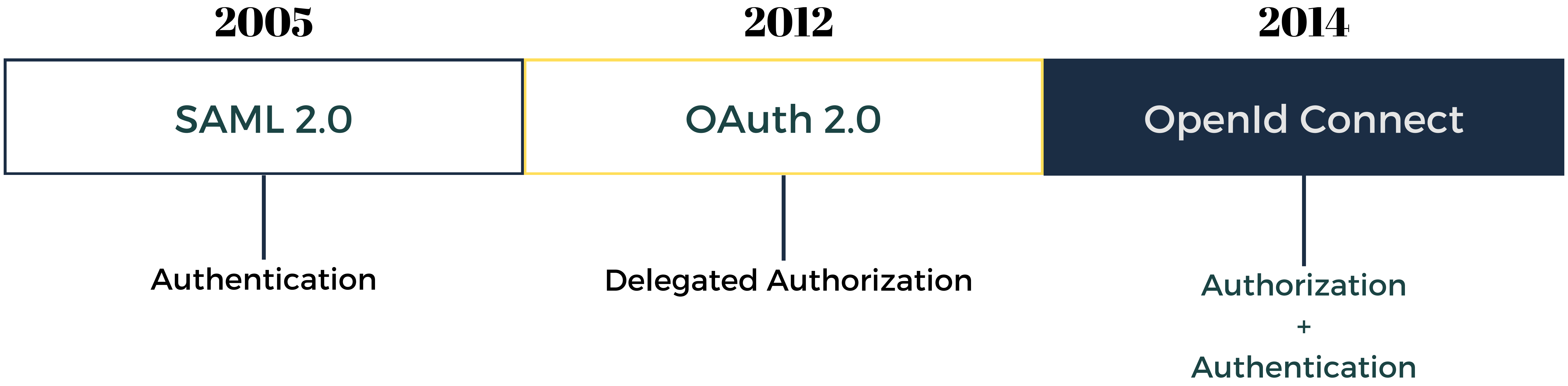
- Password Fatigue
- Administrative Burden
- Increased Security Risks
- User Frustration and Productivity Loss

SINGLE SIGN ON



- Improved User Experience
- Enhanced Security
- Ease of Management
- Scalability

SINGLE SIGN ON STANDARDS



2005

SAML 2.0

Authentication

2012

OAuth 2.0

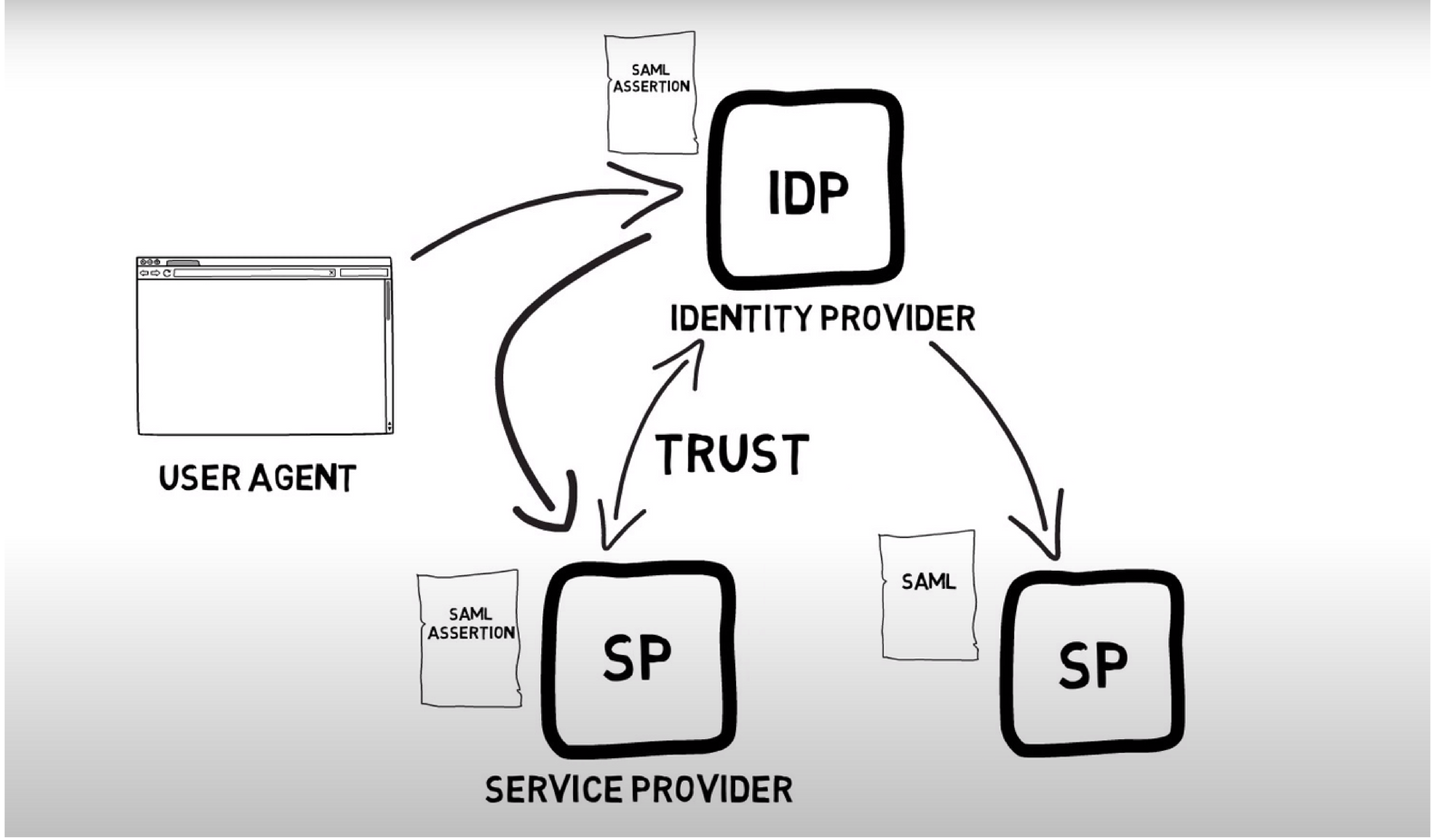
Delegated Authorization

2014

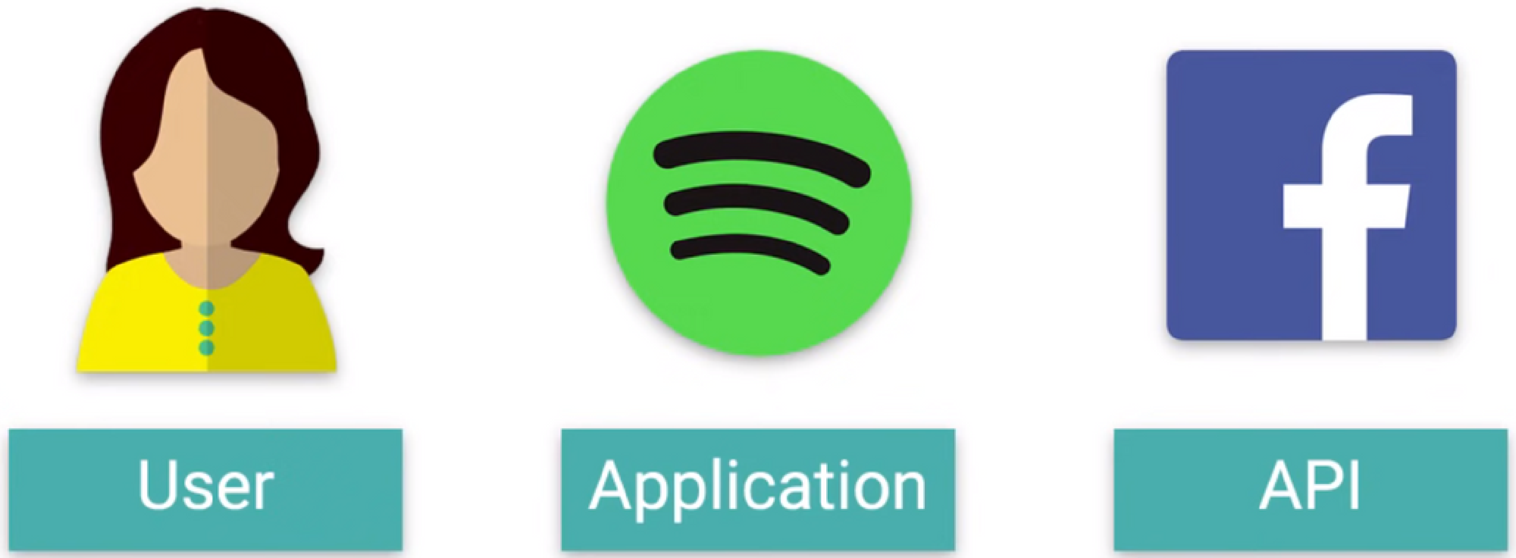
OpenId Connect

Authorization
+
Authentication

SAML :
SECURITY ASSERTION MARKUP LANGUAGE



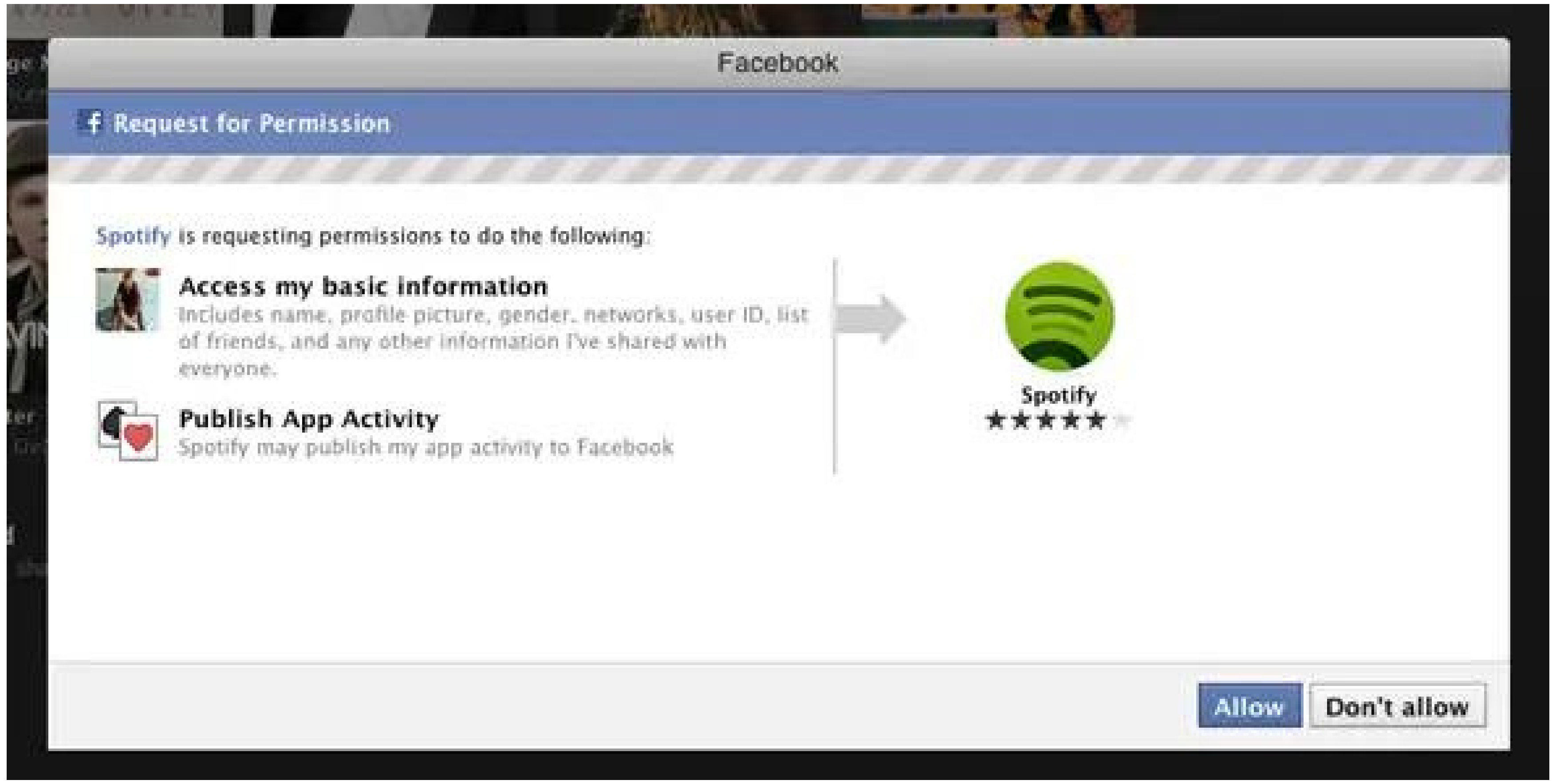
OAUTH :
OPEN AUTHORIZATION



User

Application

API



Facebook

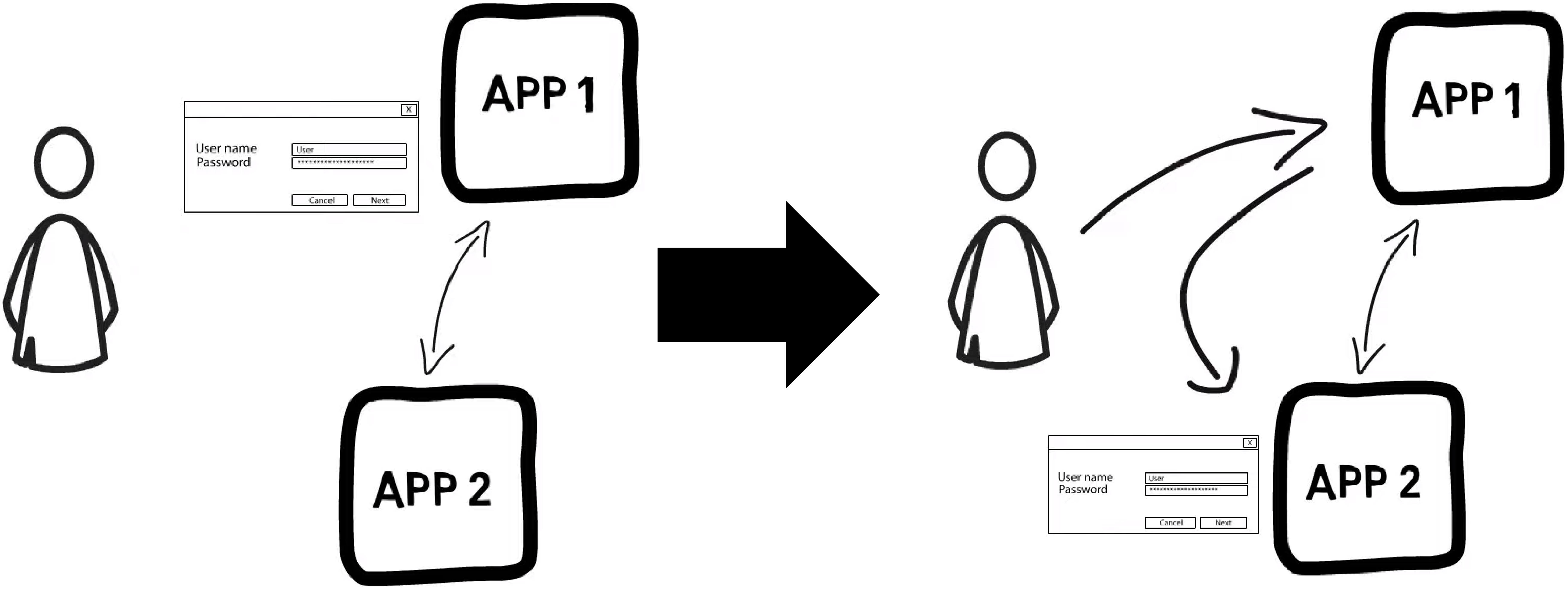
Request for Permission

Spotify is requesting permissions to do the following:

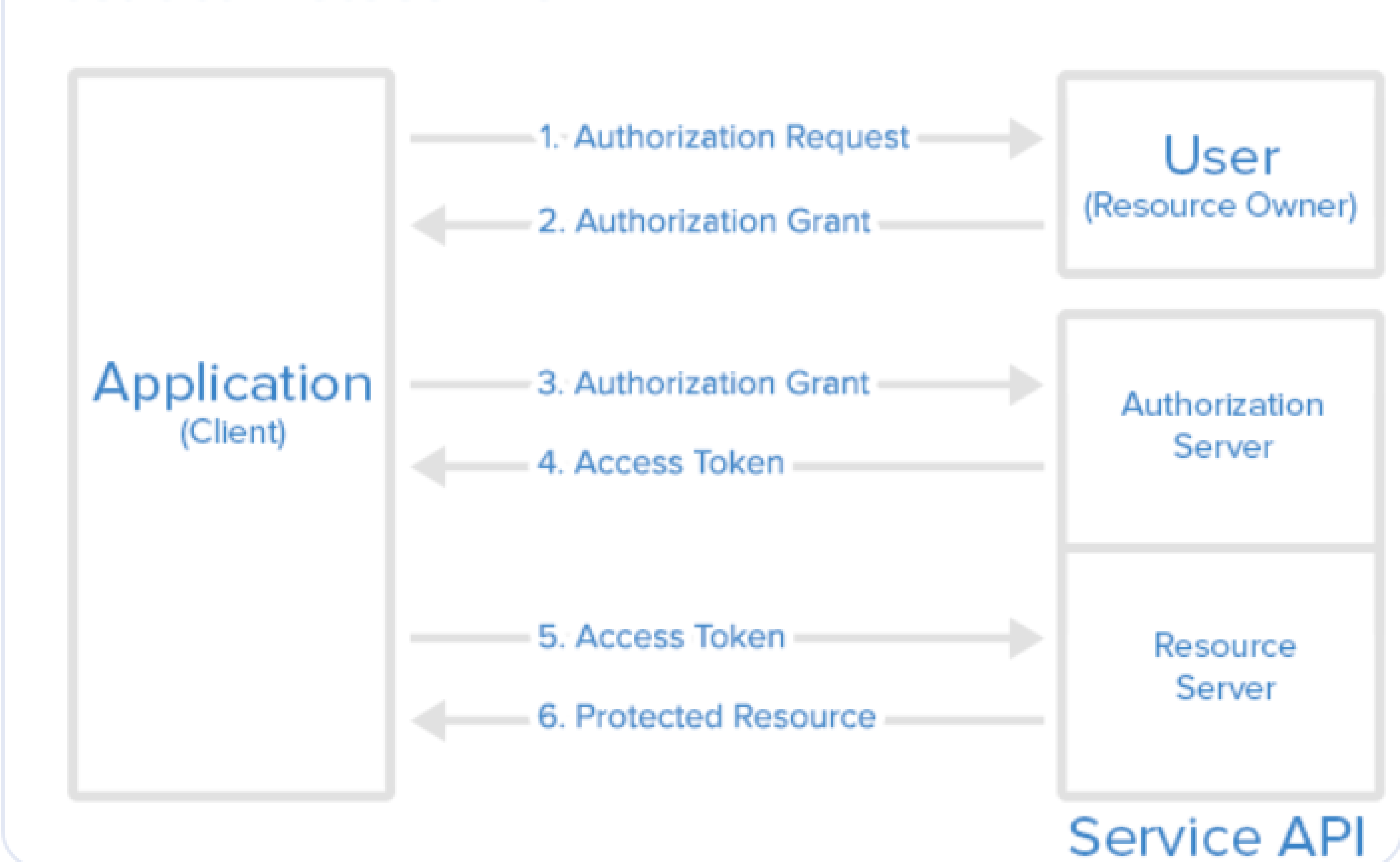
Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone.

Publish App Activity
Spotify may publish my app activity to Facebook

OAUTH :
OPEN AUTHORIZATION



OAUTH :
OPEN AUTHORIZATION



Application
(Client)

1. Authorization Request

2. Authorization Grant

3. Authorization Grant

4. Access Token

5. Access Token

6. Protected Resource

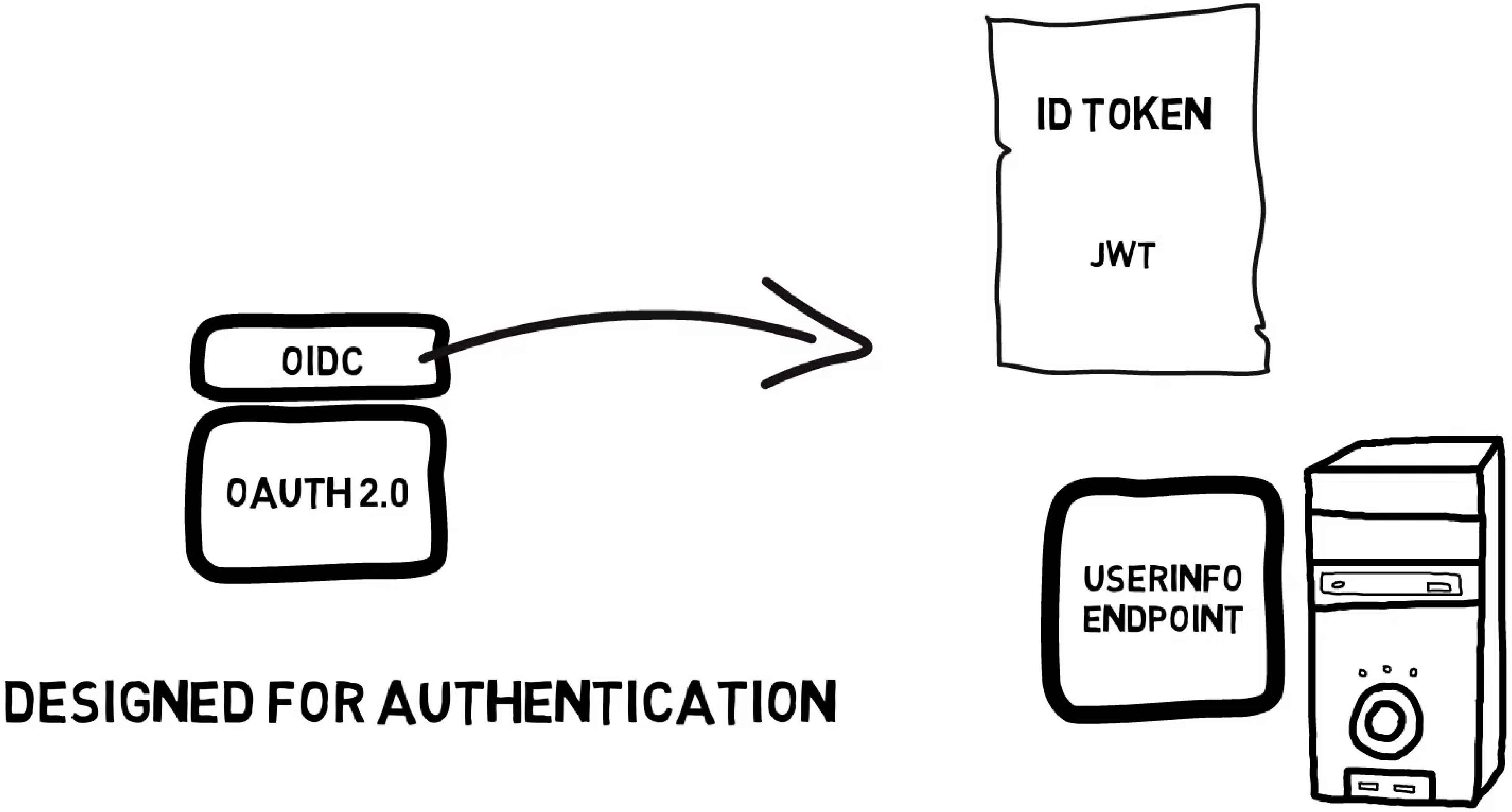
User
(Resource Owner)

Authorization
Server

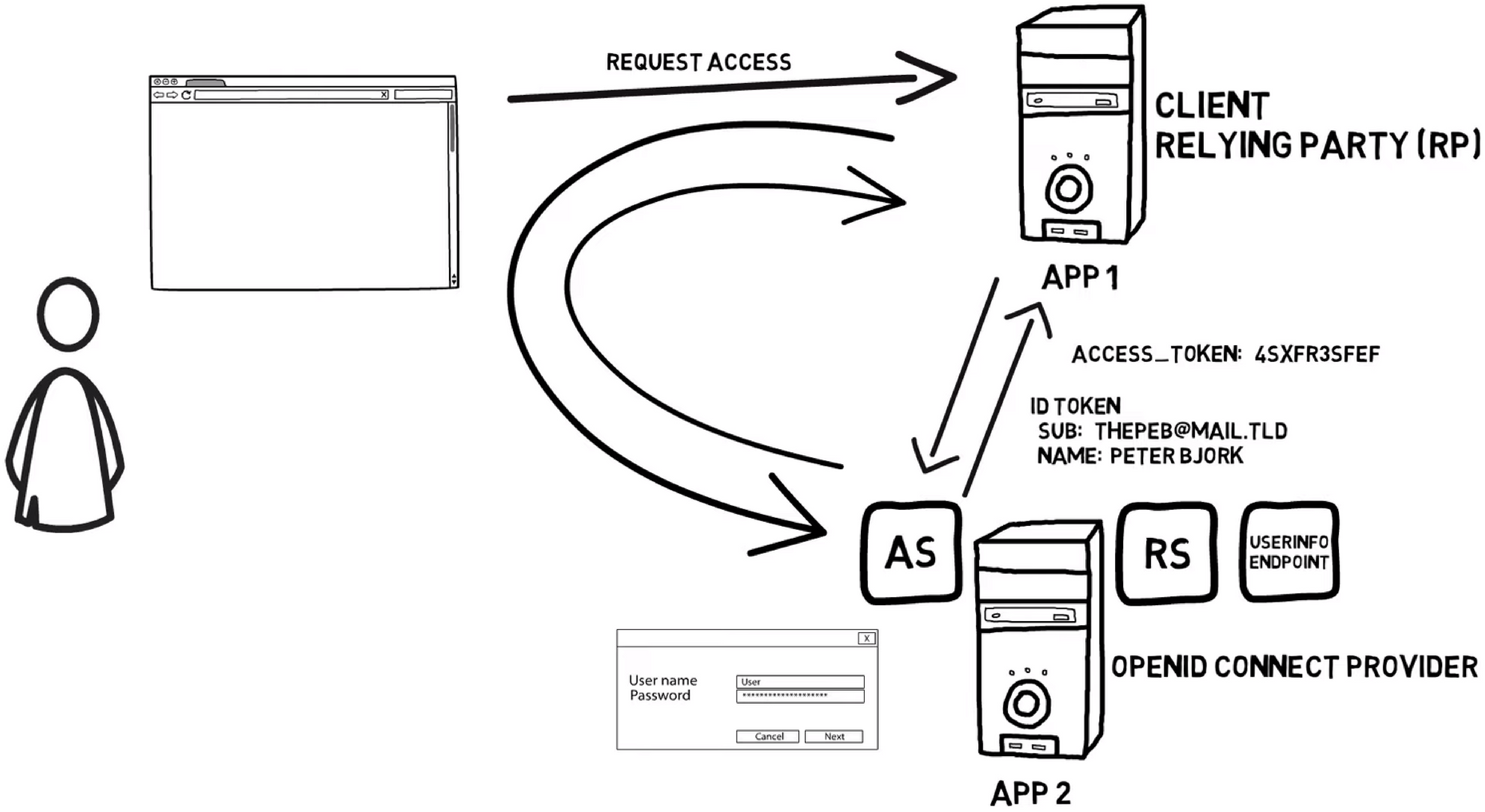
Resource
Server

Service API

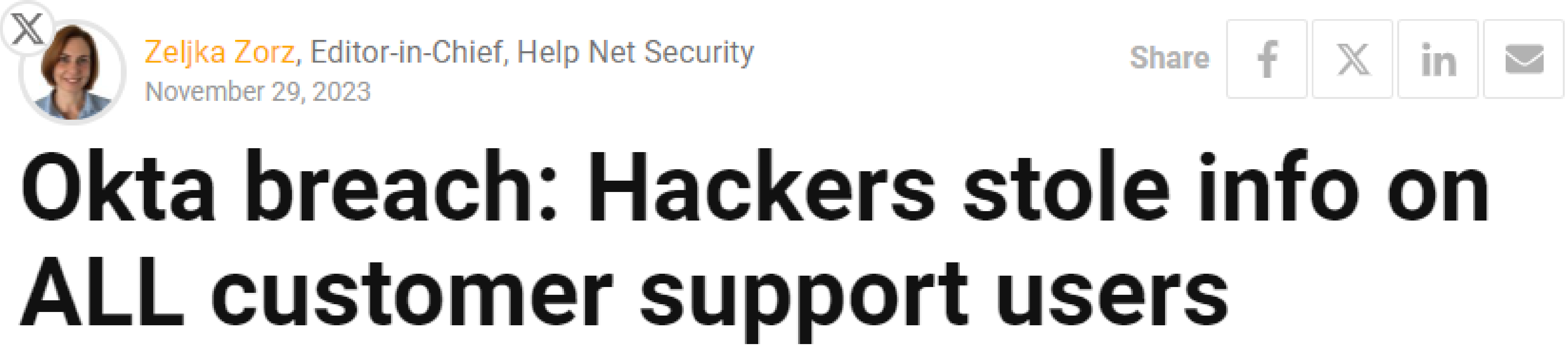
OIDC:
OPENID CONNECT



OIDC:
OPENID CONNECT

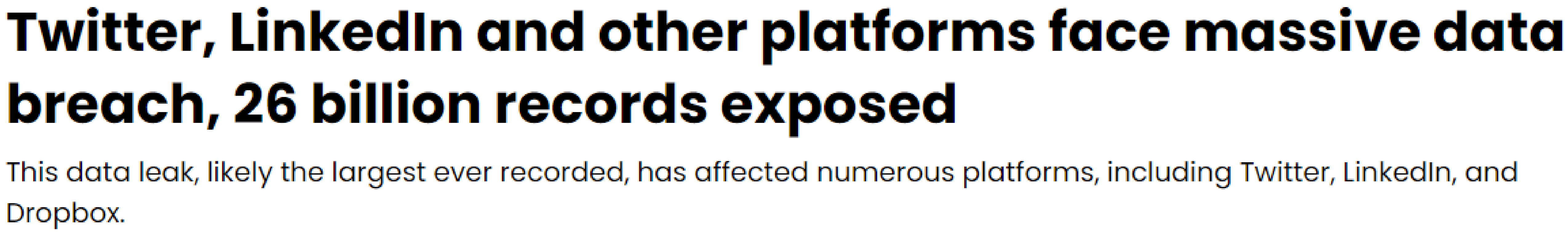


WHAT IF THE SOURCE IS BREACHED?



Zeljka Zorz, Editor-in-Chief, Help Net Security
November 29, 2023

Okta breach: Hackers stole info on ALL customer support users



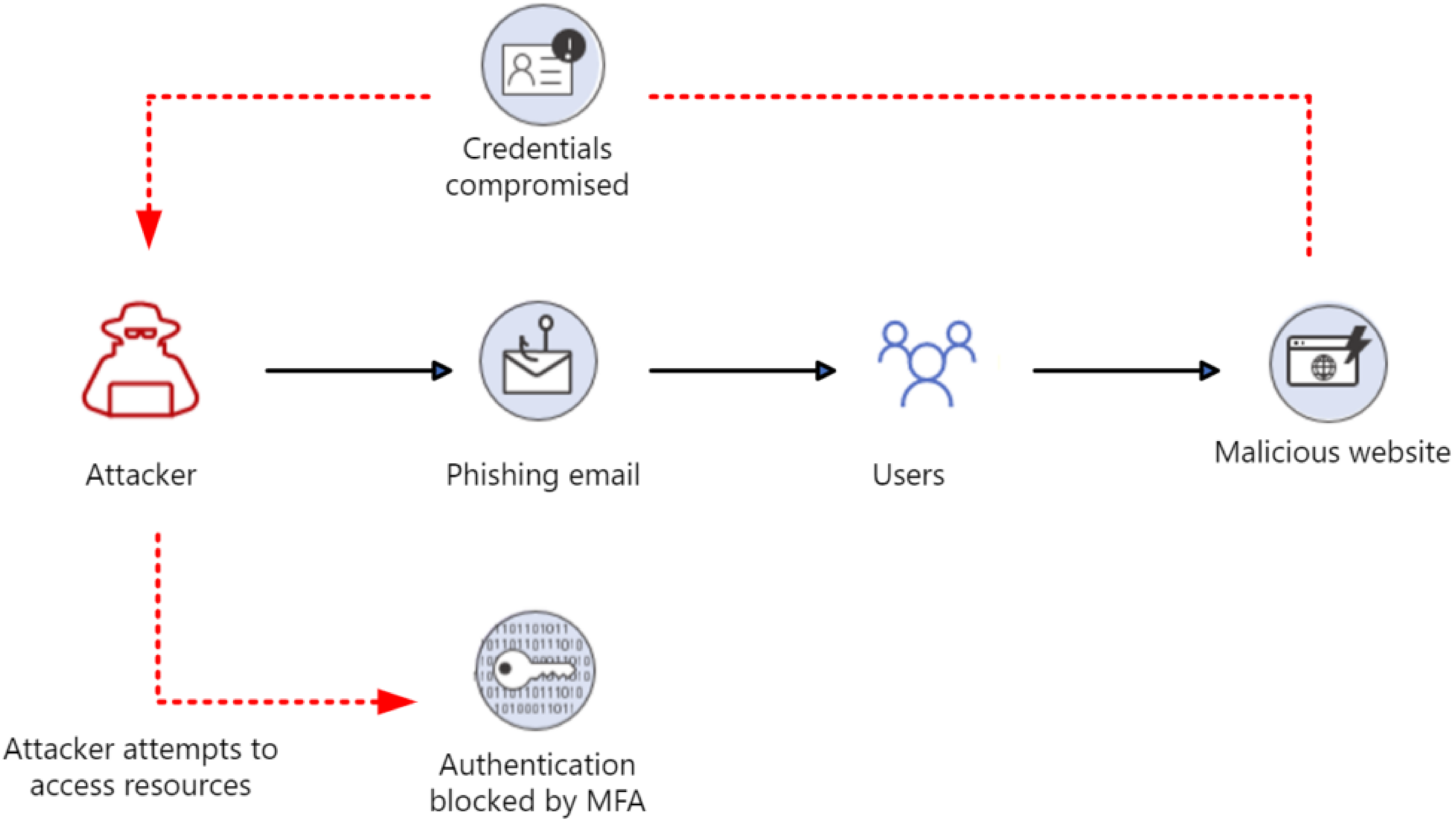
Twitter, LinkedIn and other platforms face massive data breach, 26 billion records exposed

This data leak, likely the largest ever recorded, has affected numerous platforms, including Twitter, LinkedIn, and Dropbox.

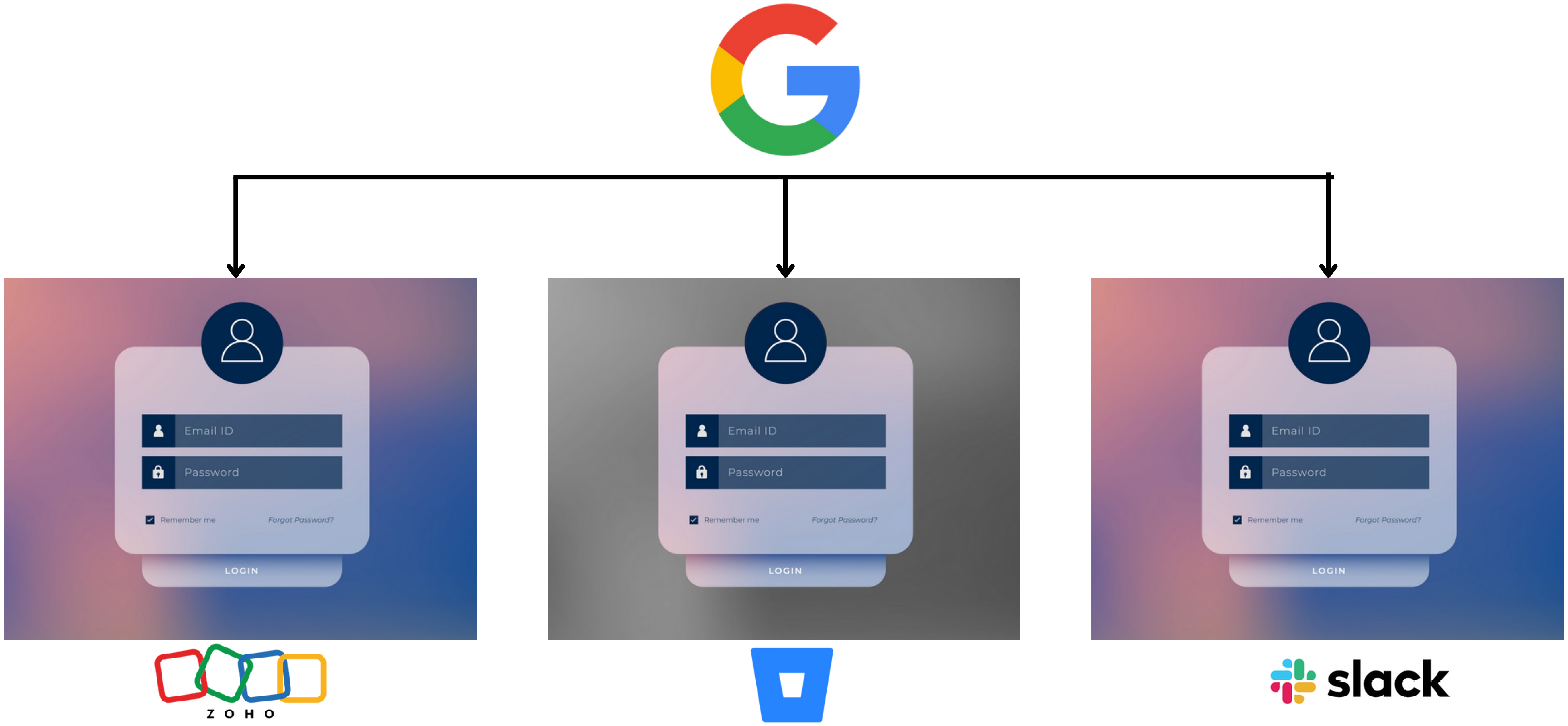
PRECAUTION IS BETTER THAN CURE!

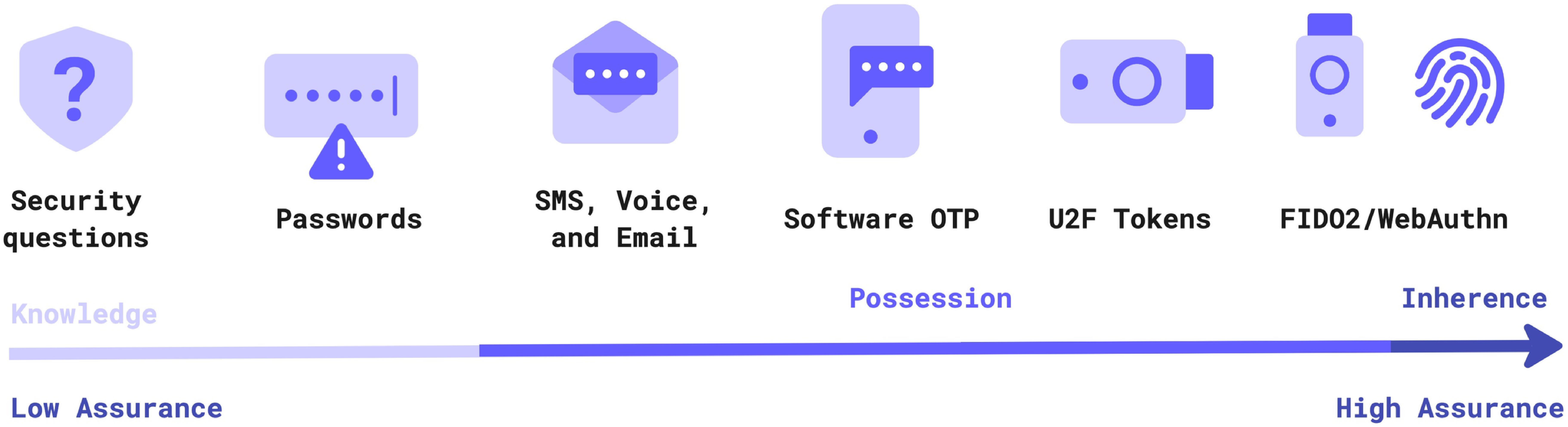
- Set Strong passwords.
- Secure the tokens used for authentication and authorization by employing strong encryption and tokenization methods.
- Implement strict access controls, granting users the minimum necessary permissions (least privilege principle) based on their roles and responsibilities.
- Adopt single logout capabilities to contain sessions.
- Ensure the accounts are secured by **MFA!**

How MFA can mitigate the risk?


Credentials compromised
Attacker
Phishing email
Users
Malicious website
Attacker attempts to access resources
Authentication blocked by MFA

MFA


Email ID
Password
Remember me
Forgot Password?
LOGIN
Email ID
Password
Remember me
Forgot Password?
LOGIN
Email ID
Password
Remember me
Forgot Password?
LOGIN
ZOHO
slack



Security questions

Passwords

SMS, Voice, and Email

Software OTP

U2F Tokens

FIDO2/WebAuthn

Knowledge

Possession

Inherence

Low Assurance

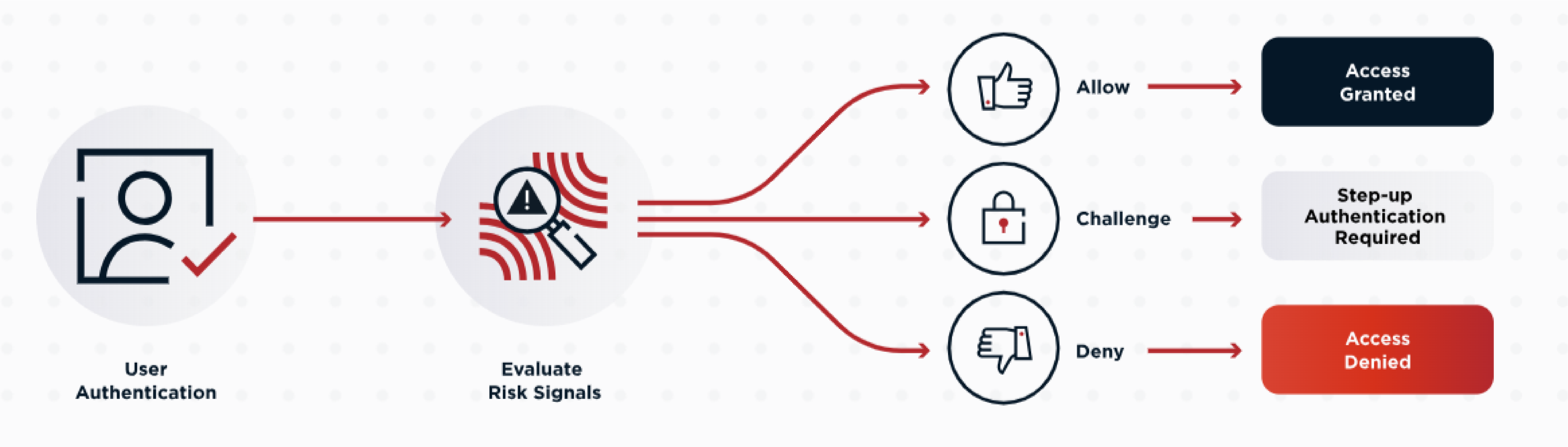
High Assurance

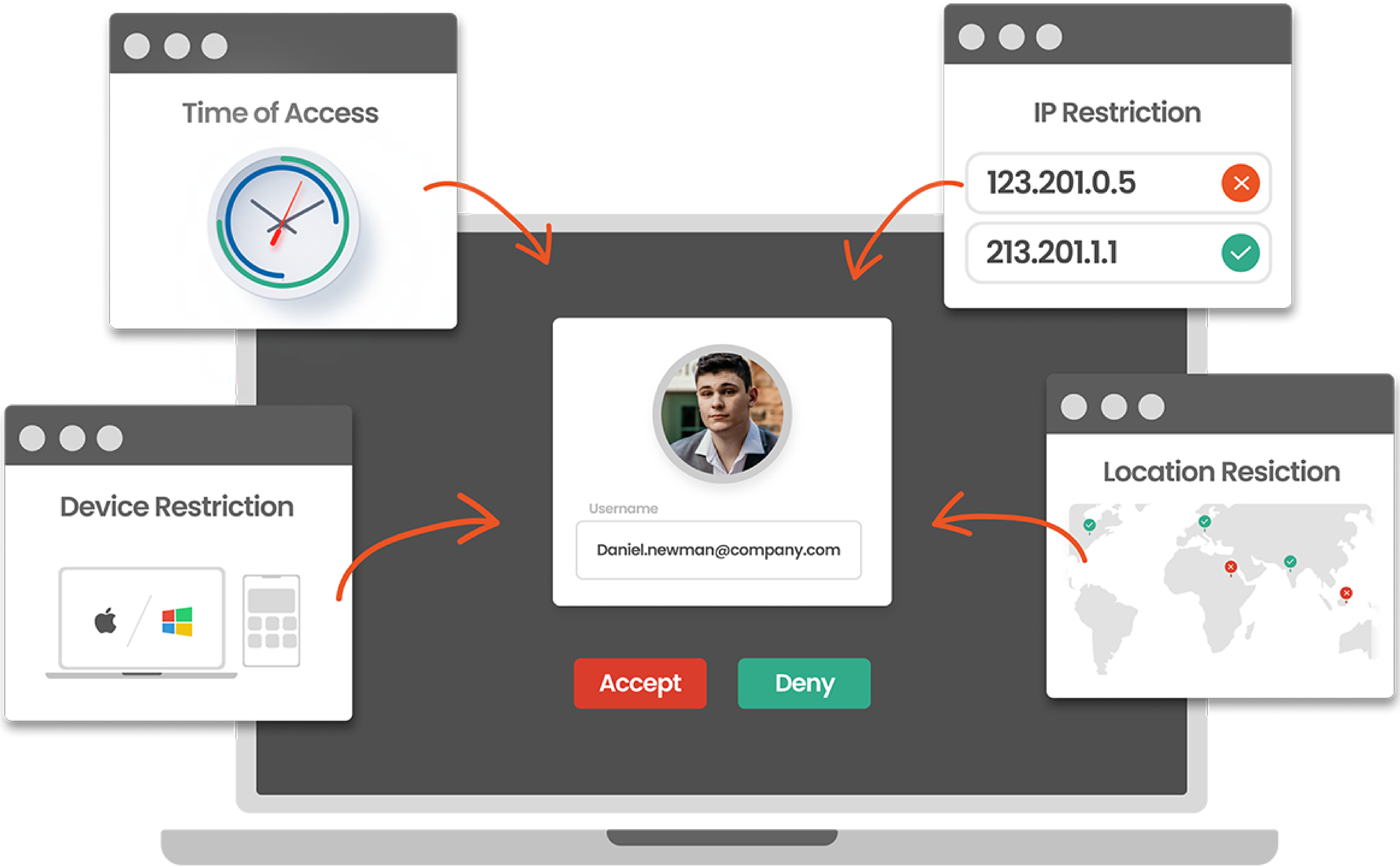
HOW MFA HELPS ?

- MFA adds multiple verification steps beyond just passwords
- Time-sensitive codes are harder for attackers to exploit.
- Even if passwords are compromised, MFA requires additional factors.
- MFA systems can spot suspicious login patterns, thwarting phishing.
- MFA implementation reinforces security awareness and verification practices.

MFA - Friction in User Experience!

DYNAMIC SAFEGUARDING - UNVEILING RISK-BASED AUTHENTICATION





Username

Daniel.newman@company.com

REFERENCES

- https://datatracker.ietf.org/doc/html/rfc7522
- https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
- https://datatracker.ietf.org/doc/html/rfc6749
-

Feedback!