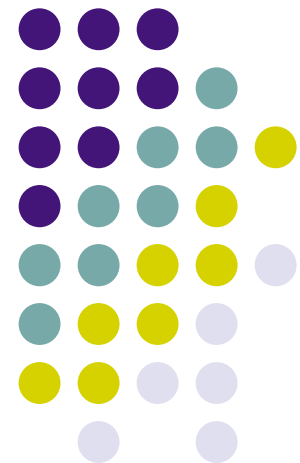July, 18 2011

OpenID Implementation

Intel® Expressway Cloud Access 360

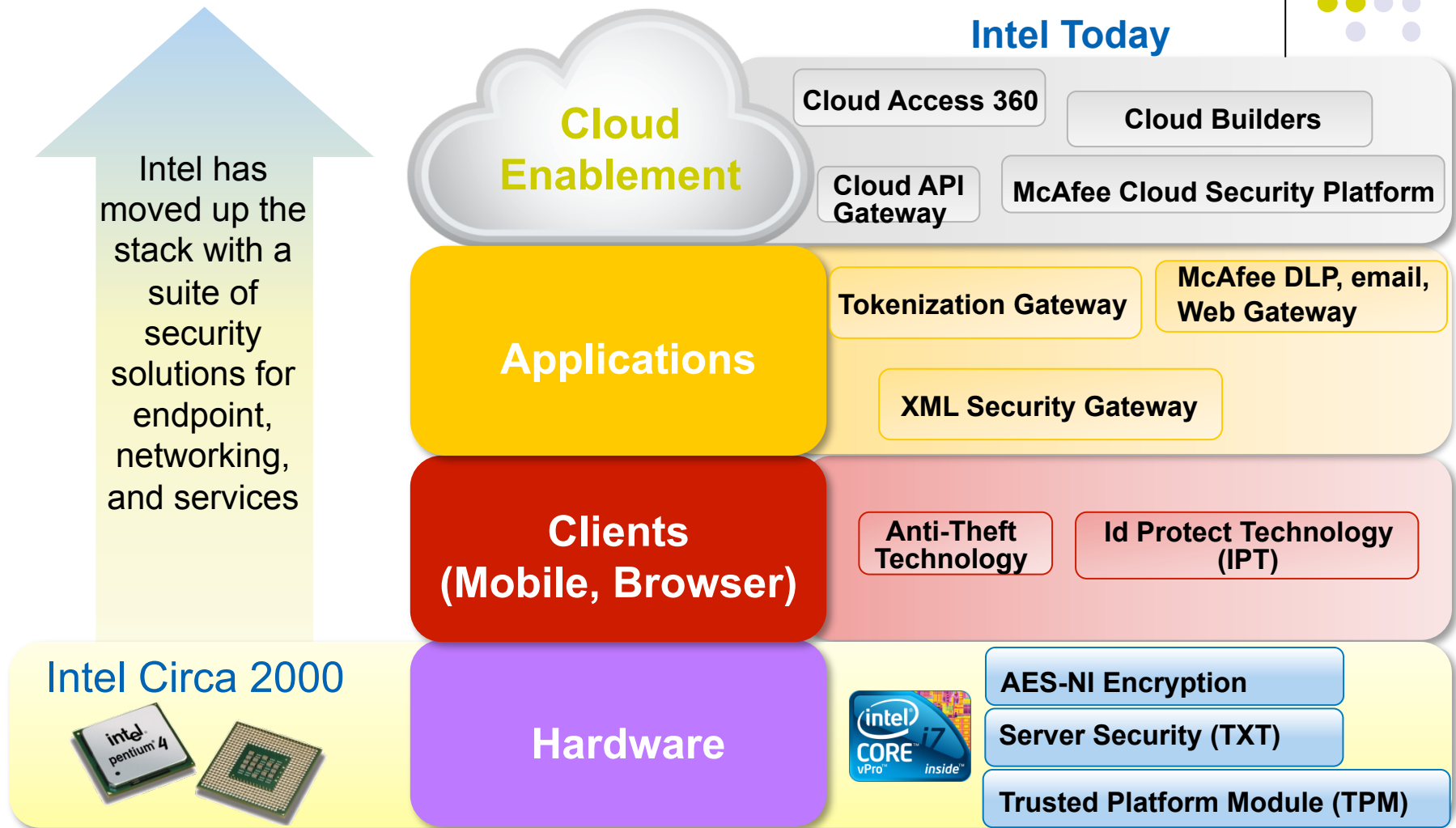**Go Beyond SSO with Strong Auth & Provisioning**

Presented by:

Todd Cramer, Director Product Marketing

Intel Application Security and Identity Products

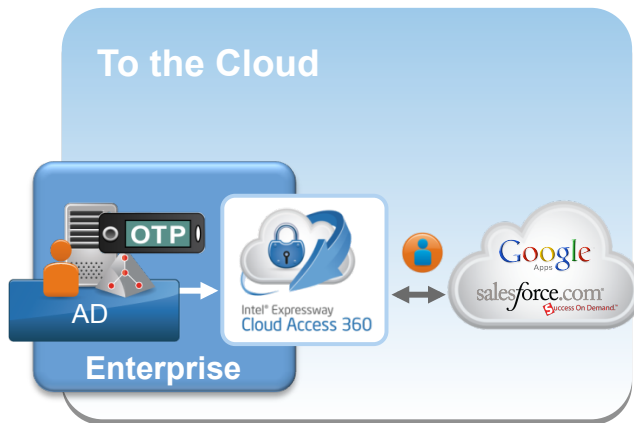# Intel - Security as 3rd Strategic Pillar

Intel has moved up the stack with a suite of security solutions for endpoint, networking, and services

Intel Today

Cloud Enablement

- Cloud Access 360
- Cloud Builders
- Cloud API Gateway
- McAfee Cloud Security Platform

Applications

- Tokenization Gateway
- McAfee DLP, email, Web Gateway
- XML Security Gateway

Clients (Mobile, Browser)

- Anti-Theft Technology
- Id Protect Technology (IPT)

Intel Circa 2000

Hardware

- AES-NI Encryption
- Server Security (TXT)
- Trusted Platform Module (TPM)

Bringing Trust to all layers of the computing stack

Intel® Expressway Cloud Access 360

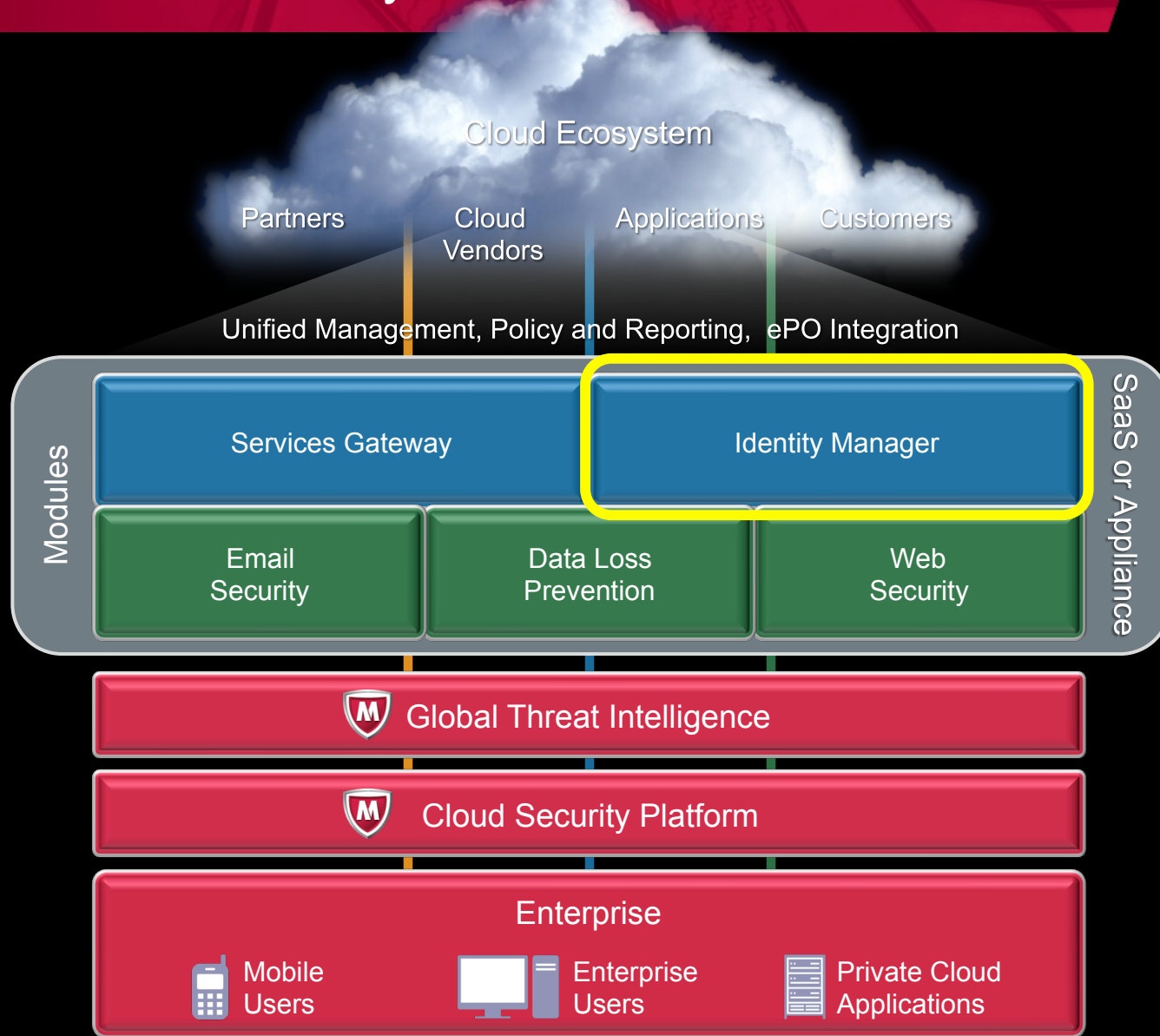**Enterprise to Cloud SSO**

Securing Custom or SaaS Apps

To the Cloud

OTP

AD

Intel® Expressway Cloud Access 360

Google Apps

salesforce.com
Success On Demand.

Enterprise

In the Cloud

SAML

OTP

Intel® Expressway Cloud Access 360

Apps
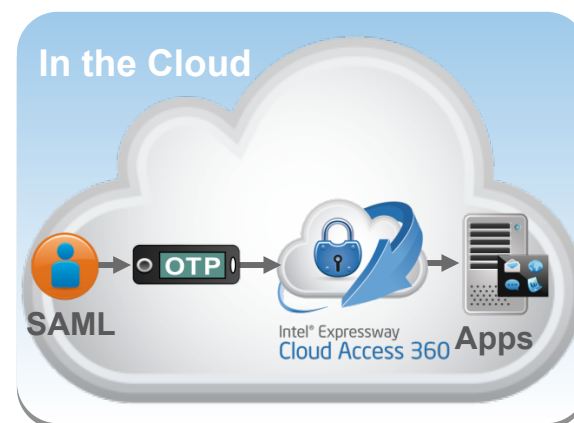
Combining Enterprise Class Strong Auth with SSO

Provision Access

- Provision/de-provision user accounts
- AD integration
- Sync Id Profiles

Adaptive Strong Auth

- Selectively apply 2nd factor OTP AuthN
- Variety of software AuthN methods & devices- mobile devices, SMS, email

OTP
Log In

Secure SSO

- Federate windows/AD log in
- To popular SaaS like Salesforce & Google Apps

Regulatory Compliance

- Rich audit trail of user login showing AuthN level
- De-provision & orphan account reports

Go Beyond SSO with Strong Auth and Provisioning

3

OpenID Implementation

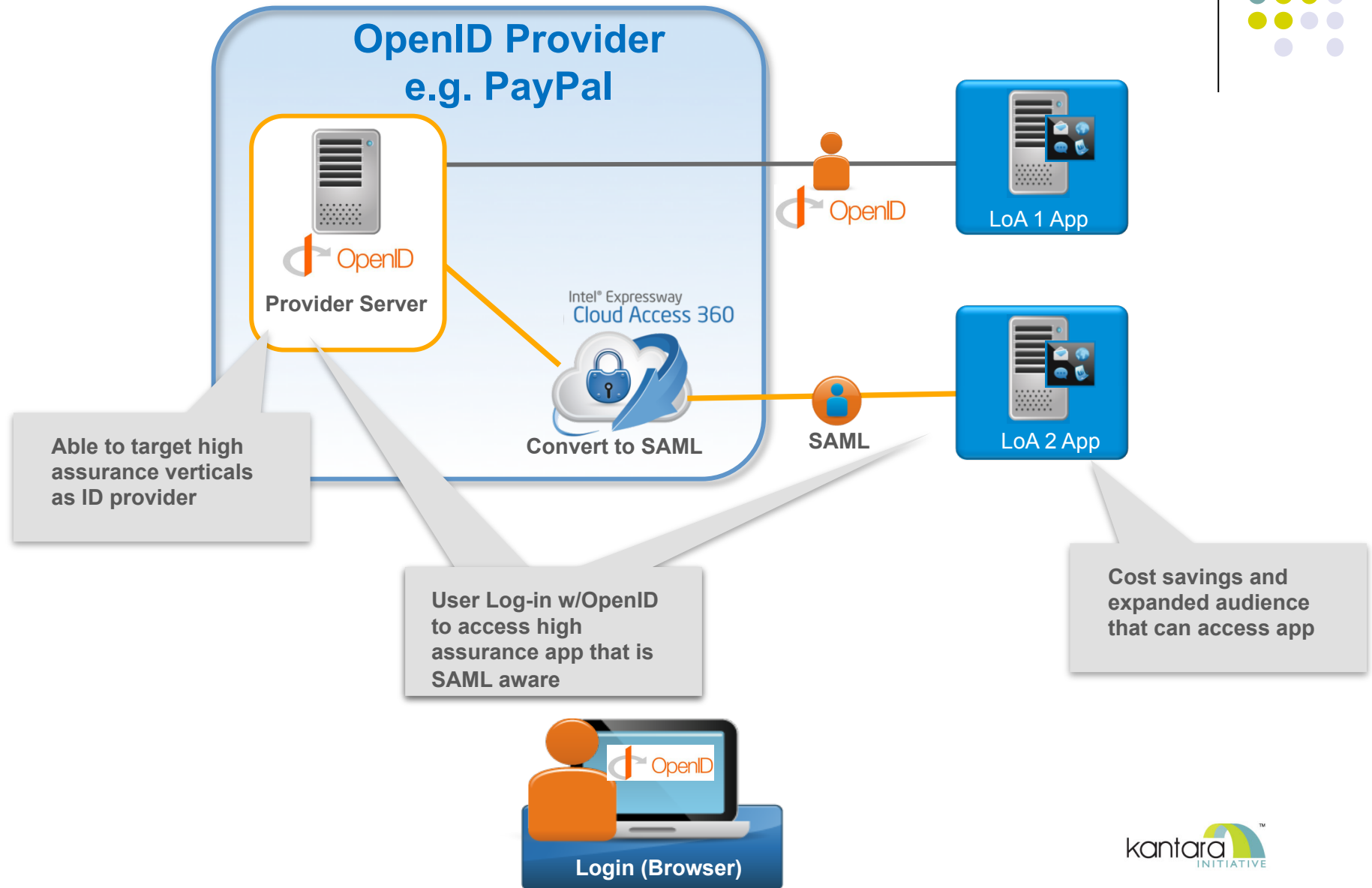# ICAM Trust Frameworks

-Source- Open Identity Exchange
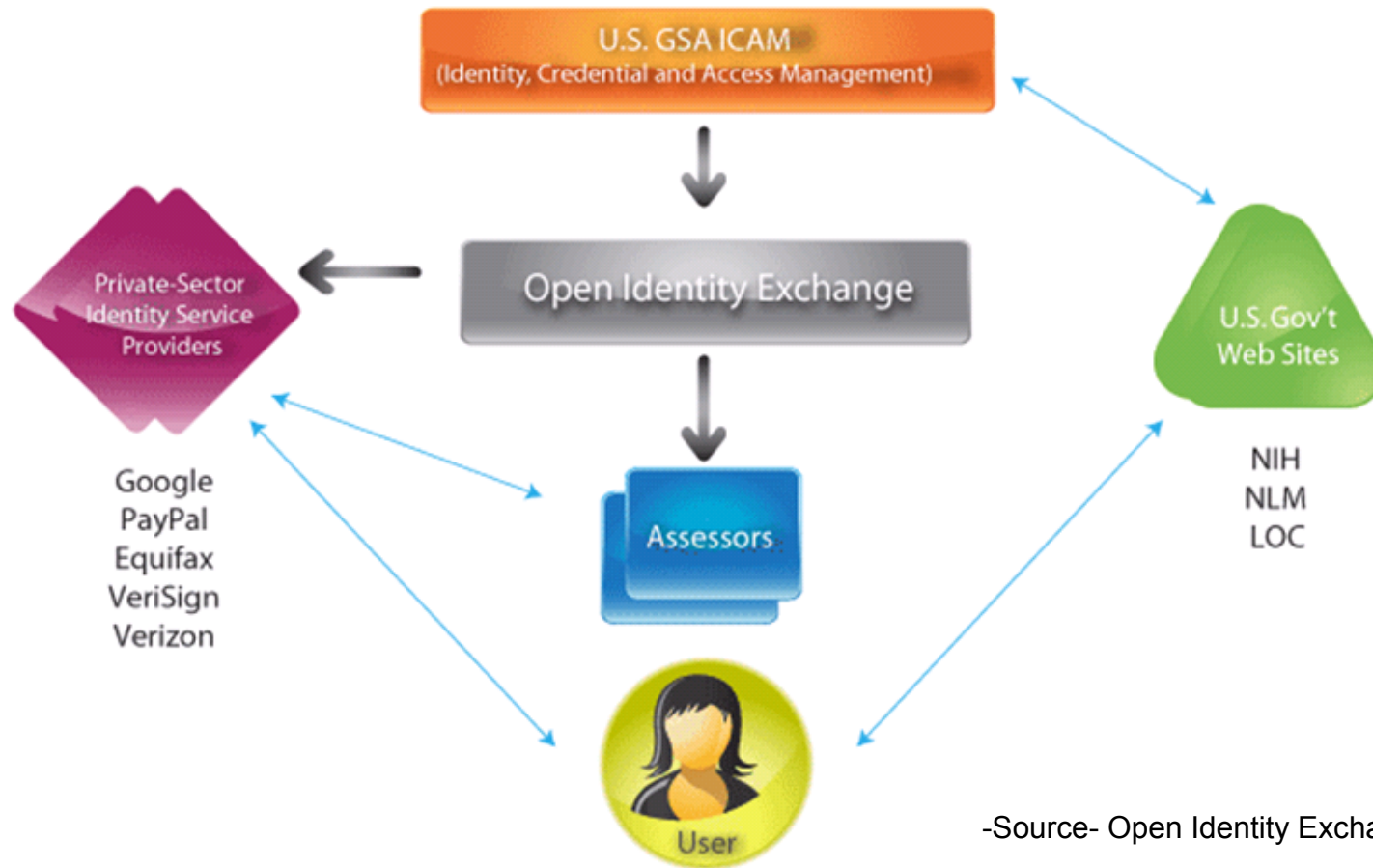
US ICAM LOA 1 trust framework enables U.S. federal agency websites to begin accepting OpenID and Information Card credentials from OIX certified private-industry providers.
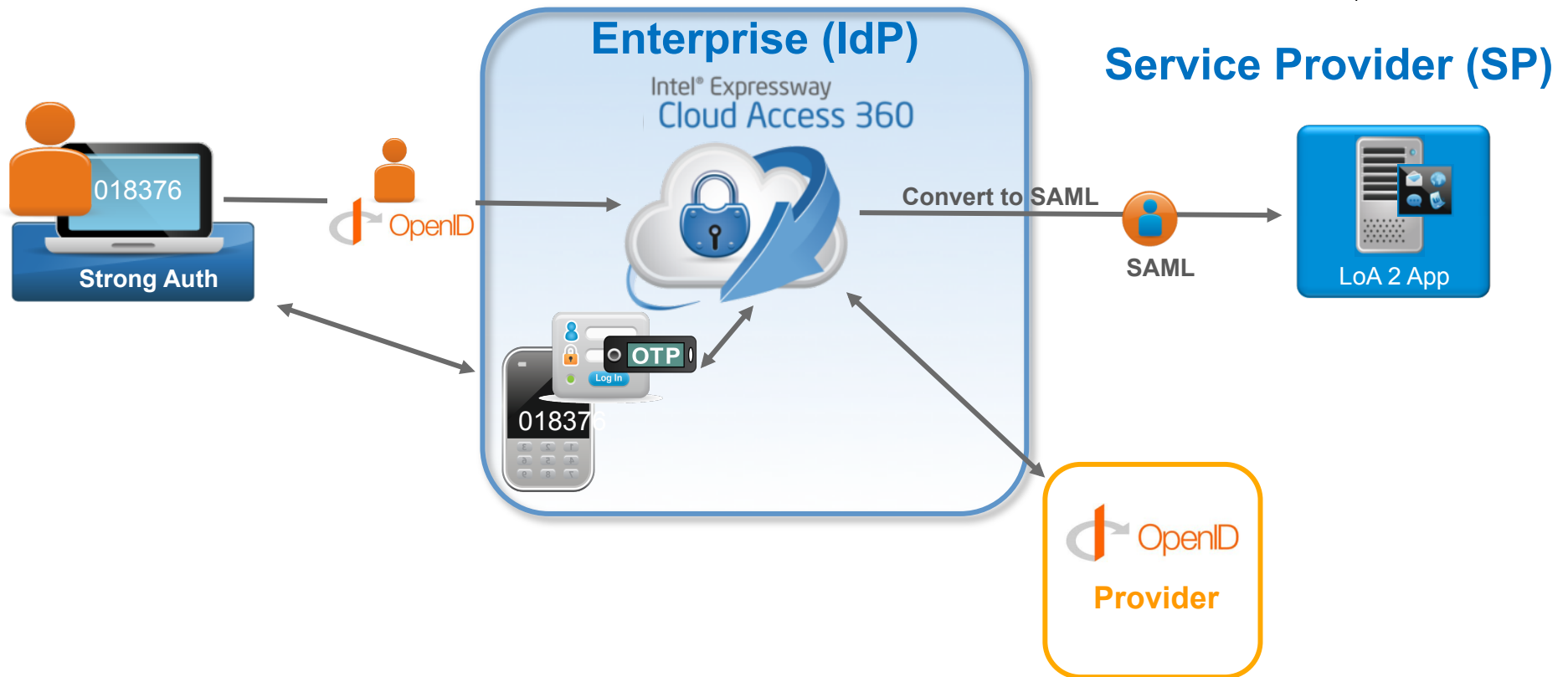
Background

- **Background -** PayPal & Intel implemented a POC to prove how an OpenID provider can enable access to SAML aware apps

- **Challenge -** ICAM community requires LoA2 certification- to be an IdP to high assurance apps. This requires support for SAML

- **Solution -** OpenId to SAML bridge

- **Benefit -** Enables users to leverage private sector credential to access federal apps

kantara
INITIATIVE

OpenID Provider

OpenID Provider
e.g. PayPal

OpenID
Provider Server

Intel® Expressway
Cloud Access 360

Convert to SAML

OpenID

LoA 1 App

SAML

LoA 2 App

Able to target high
assurance verticals
as ID provider

User Log-in w/OpenID
to access high
assurance app that is
SAML aware

Cost savings and
expanded audience
that can access app

OpenID

Login (Browser)
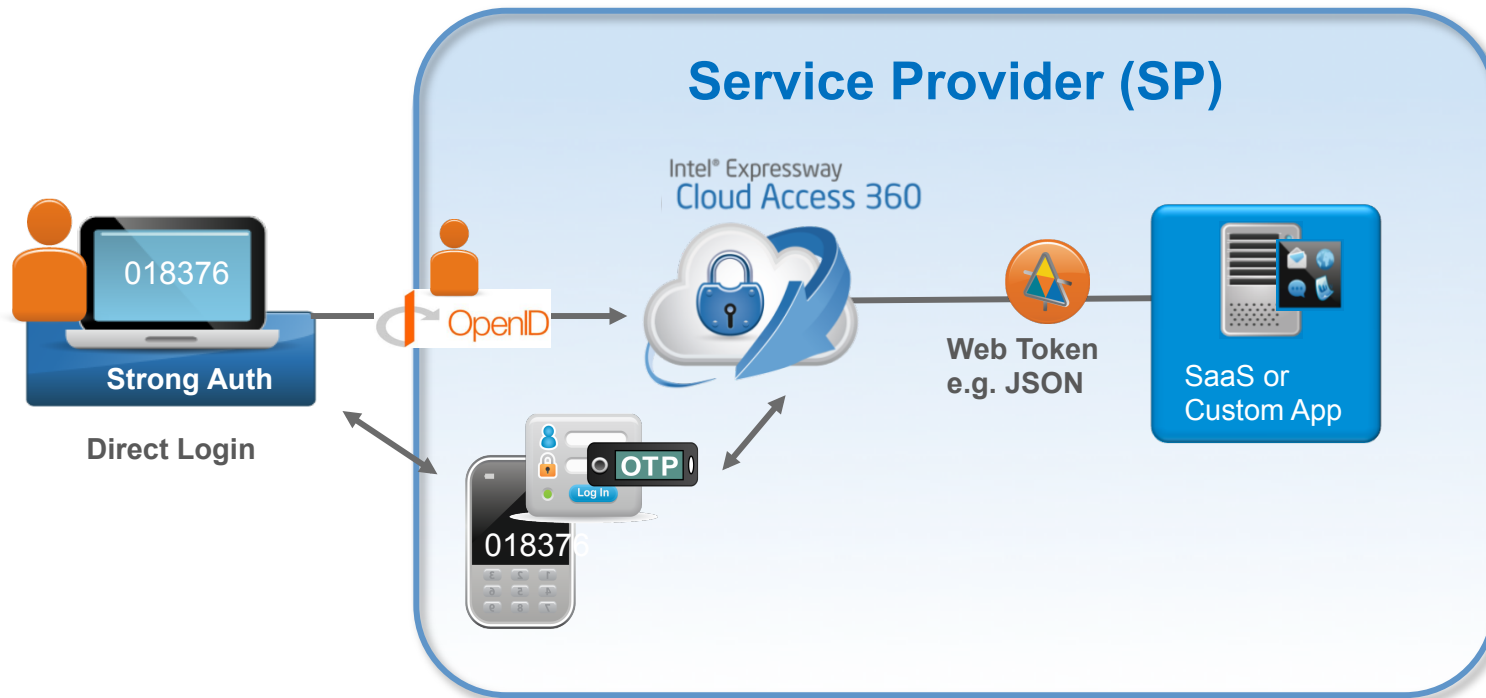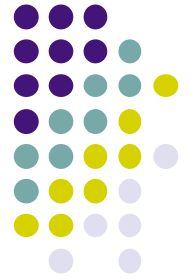
kantara
INITIATIVE

Enterprise Leverage OpenID w/Strong Auth

- Leverage OpenID over internal AD (e.g. Contract workers or affiliates)
- Add 2nd factor authentication to OpenID
- Convert to SAML for accessing LoA 2 level apps

Service Providers - Who want to Accept Open Ids w/Strong Auth

Service Provider (SP)

Intel® Expressway
Cloud Access 360

018376

OpenID

Strong Auth

Direct Login

OTP

Log In

018376

Web Token
e.g. JSON

SaaS or
Custom App

- Have applications accept both direct login and federated authentication
- Add 2nd factor authentication

kantara
INITIATIVE ™

More Info

www.intel.com/go/identity

Cloud ID Jam Session

2 Webinars with FORRESTER®

*Strong Auth
*Provisioning
July 27 & 28

Demos

kantara INITIATIVE™