Securing the Exploding Identiverse

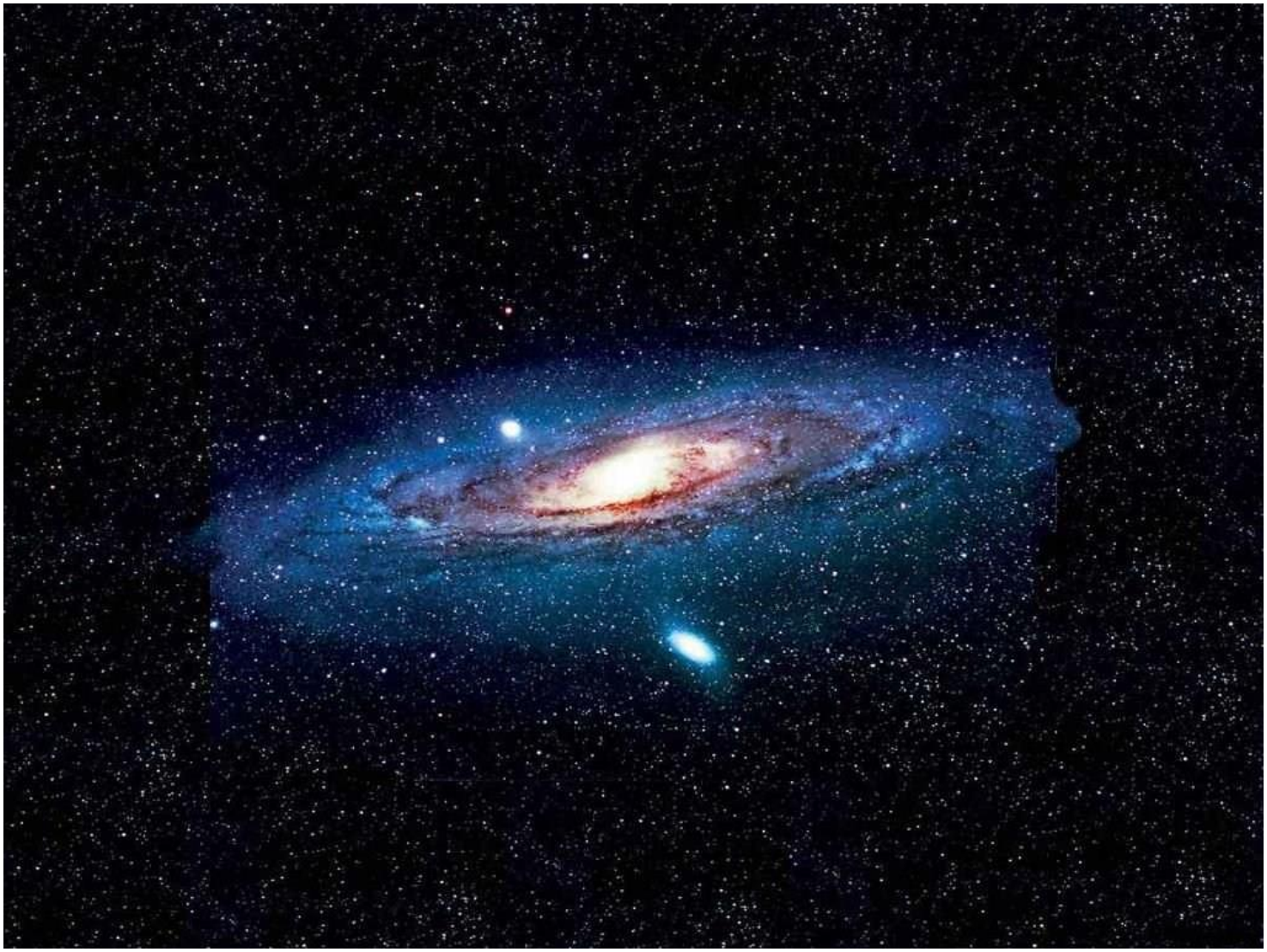
David Gorton, Platform Product Manager
Ping Identity
Aug 2013

The Identity Security Company™

What is the Identiverse?

- Everything has an Identity
  - People
  - Devices
- Those things need to securely interact
- Identity is the key

State of the Identiverse



Stable Identity Infrastructure

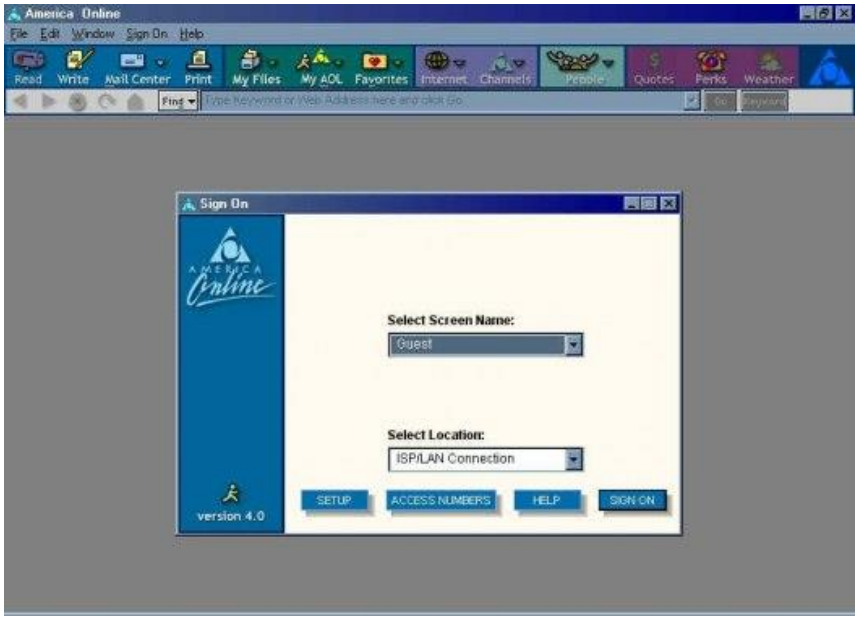
- Your directories “just work”
- Web Access Management infrastructure manages internal applications
- Federation connections growing
- SOA infrastructures are maturing

Identiverse Explodes!

The Next Big Bang –Mobile Apps, Devices & REST

Mobile Apps, devices and REST APIs are exploding across the enterprise

REST Security Is Back to the Dark Ages (mid 1990's)



- PASSWORDS are being cached on devices and passed with each API call
- Identity data is passed back and forth between client and server

Enter OAuth 2.0

Written for API clients to securely interact with APIs on behalf of users

OAuth 2.0 Details – Tokens & Scopes

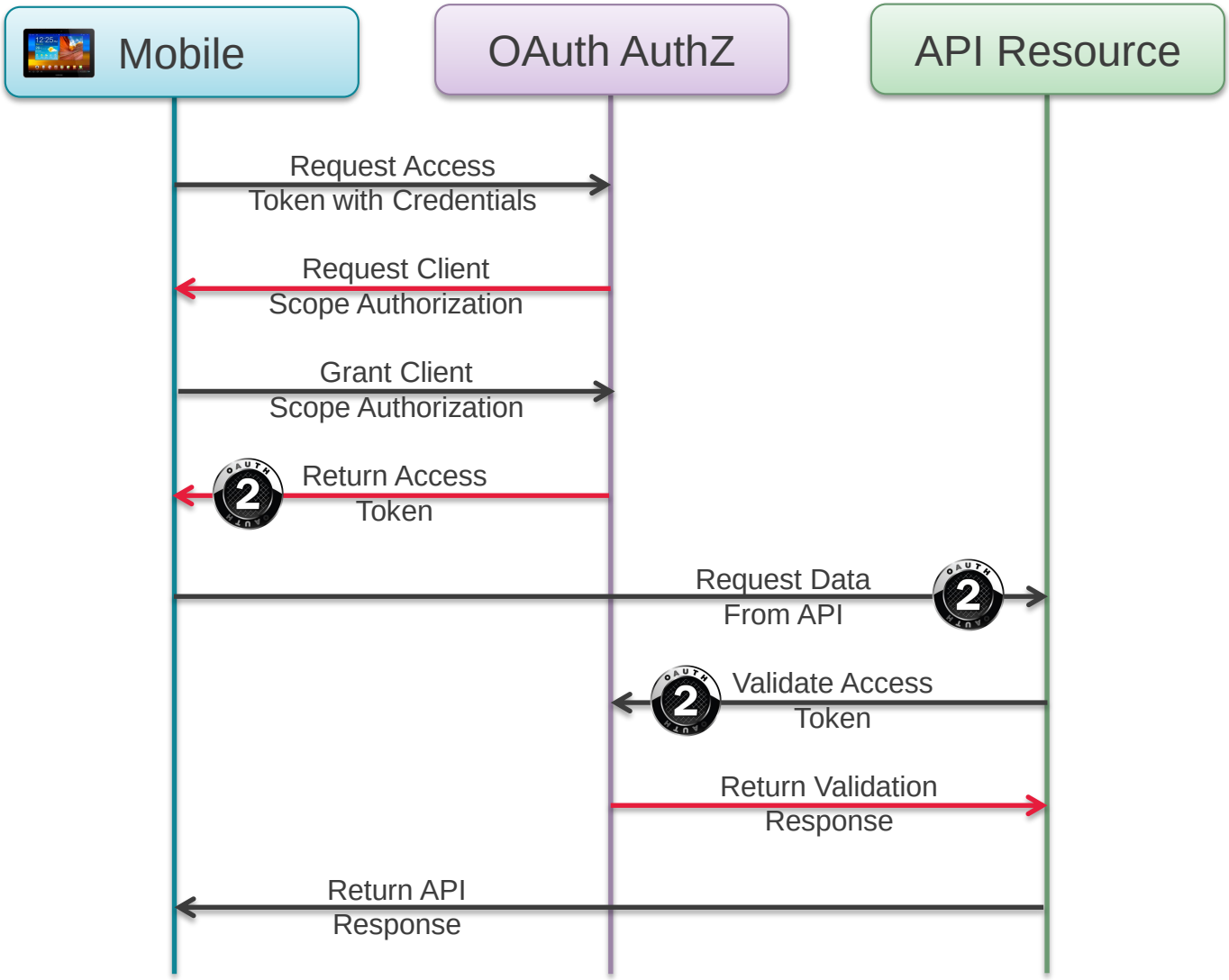
- "Authorization Server" runs the show
  - Issues Tokens with Scopes
- Scopes
  - Tiny capabilities related to API usage
  - Could be activities like "read-invoices"
  - Could be a role like "manager"
- Security Policy Enabled by Scopes
  - "read-invoice" authorized for GET on /invoice API but not for POST

OAuth 2.0 Details – Users, Clients & Tokens

- Client Requests a Token with a Scope
  - User Authenticates
  - User Authorizes Client for a Scope
- Access token returned that represents a scope for the authenticated user for use by the client

Multiple flows (profiles) exist based on the trust between the client, server, and user.

Typical OAuth 2.0 Sequence



OAuth 2.0 Details – Message Protocols

OAuth 2.0 Access Tokens are independent of message format

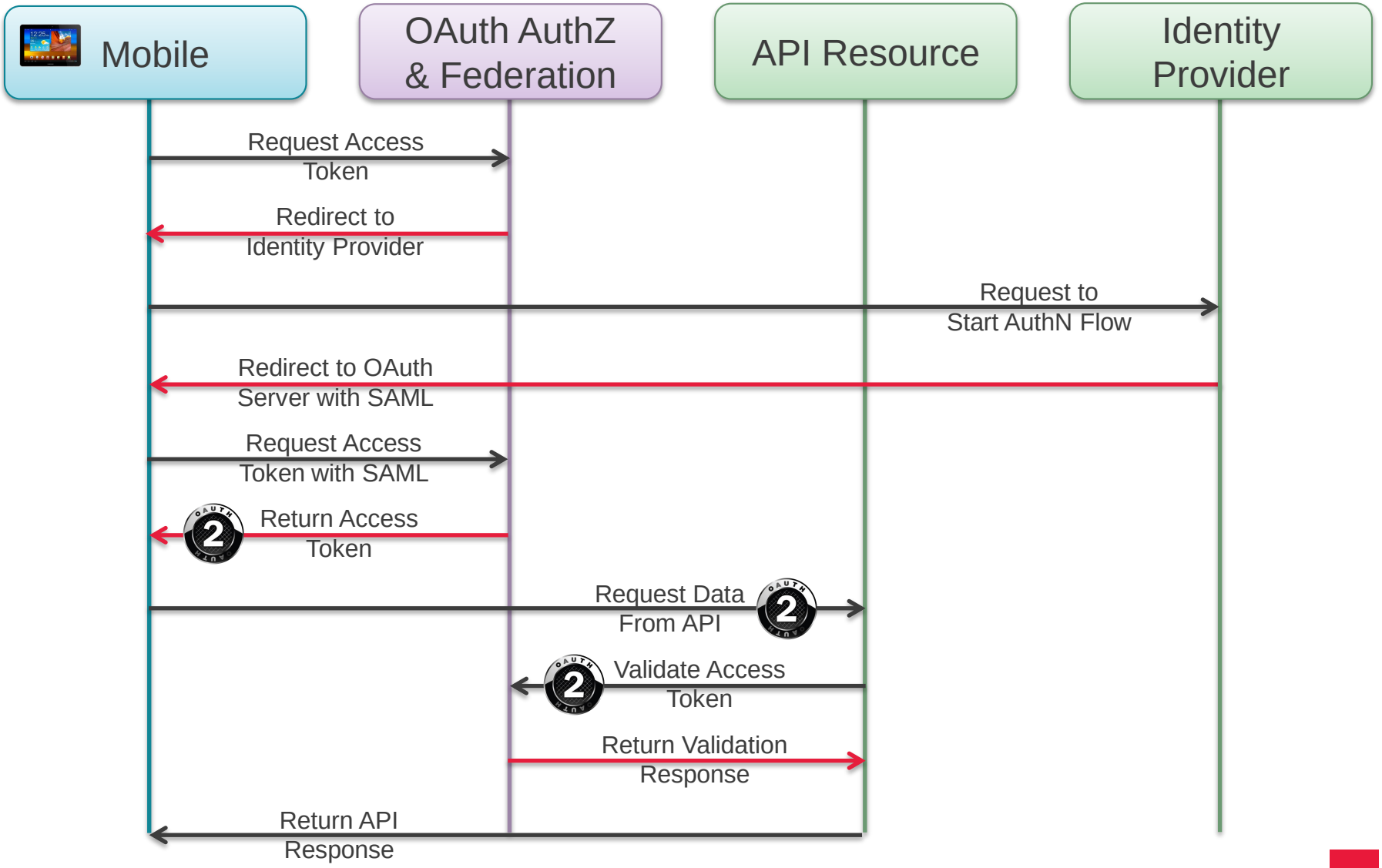
- Leverages HTTP Headers
- Message format can be SOAP, XML, JSON, or form data

OAuth 2.0 Details – Enhances SAML

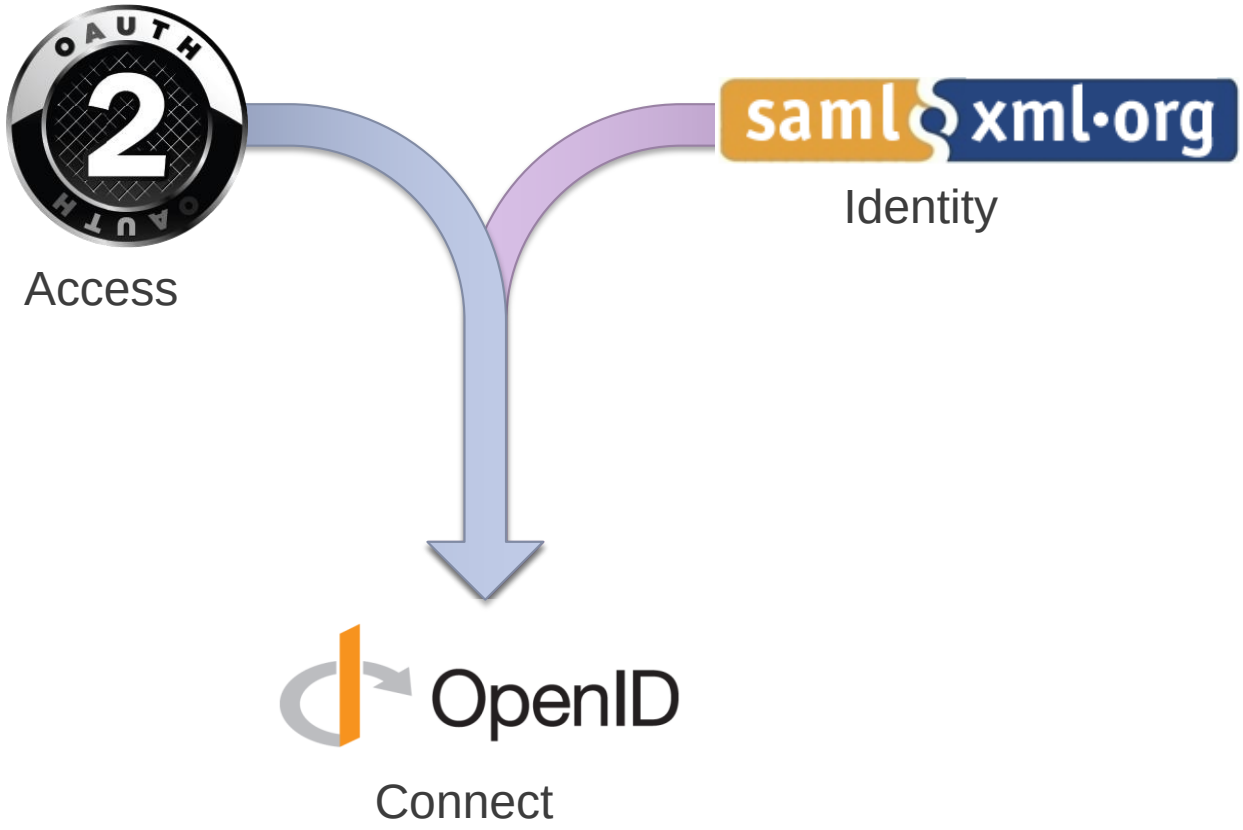
Layer OAuth 2.0 and SAML Together

- SAML handles Federation and Identity
- OAuth 2.0 handles Authorization

Typical OAuth 2.0 & SAML Sequence



Standards Converge – OpenId Connect



OpenID Connect Overview

- Authentication
  - Transmit Identity information (Token)
  - Request Additional Identity Information (REST)
- Authorization (OAuth 2)
  - Scopes
- Dynamic Client Registration
- Transport Layer Security (TLS) Required
- JSON Object Signing and Encryption (JOSE)

OpenID Connect Benefits

- One Specification for Authentication and Authorization
- Simplified Identity Token Format
- Supports Web and APIs
- Validates identity of user to the client
- Simplified Key Management

Choices to Secure the Expanding Identiverse

- OAuth 2.0 – Secure APIs with Tokens
- OpenID Connect – Extend OAuth 2.0 with Identity

Questions?

dgorton@pingidentity.com