Identity Governance Using FastFed

Presented by: Matt Domsch

The FastFed Working Group is meeting at IIW on Thursday at 1pm. This presentation covers one topic for discussion. Comments made today will be incorporated for that discussion.

What is FastFed?

FastFed is a working group of the OpenID Foundation, whose goal is to make it simpler, quicker, and less error-prone to onboard a new target Application to an existing Identity Provider for Single Sign-On.

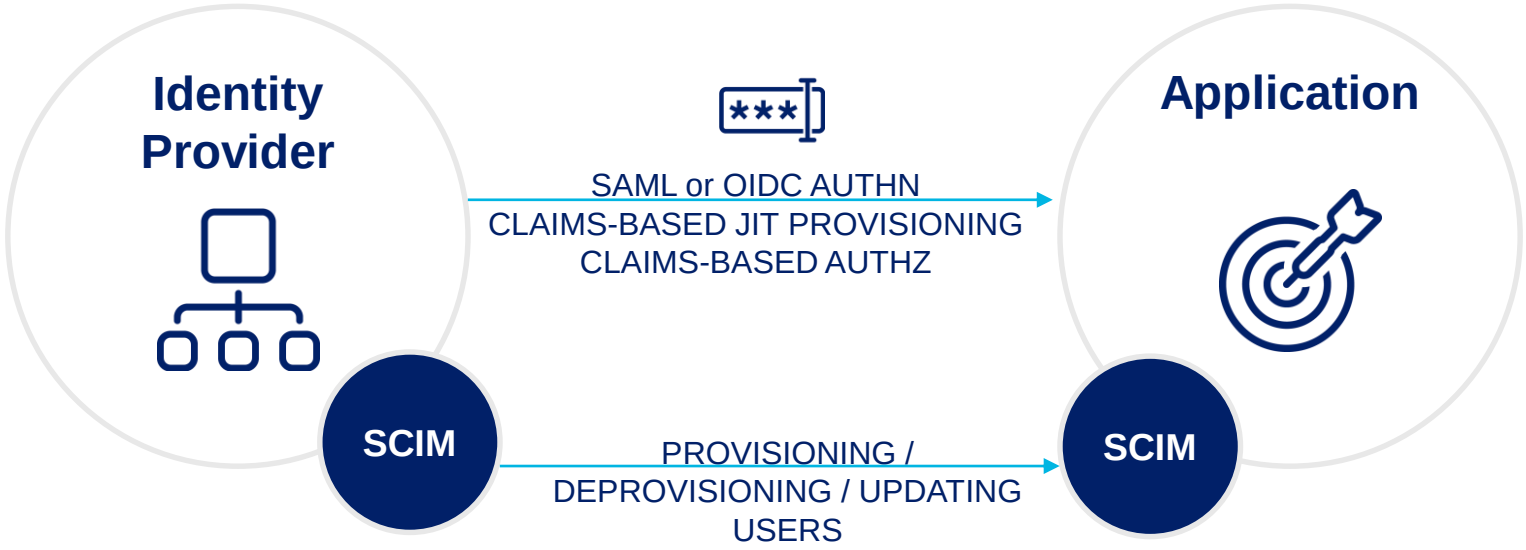
Builds on existing standards:

- OpenID Connect Authentication & Authorization, metadata exchange
- SAML Authentication & Authorization, metadata exchange
- SCIM Identity Governance protocol & schema
- WebFinger discovery

Participants: Oath, Google, AWS, SalesForce, Okta, Microsoft, Auth0, SailPoint

SailPoint

FastFed 1.0 Draft



- IDP Discovery protocol
- App / IDP trust relationship handshake
- Standardized SAML & OIDC Claims
- SAML & OIDC to SCIM mapping

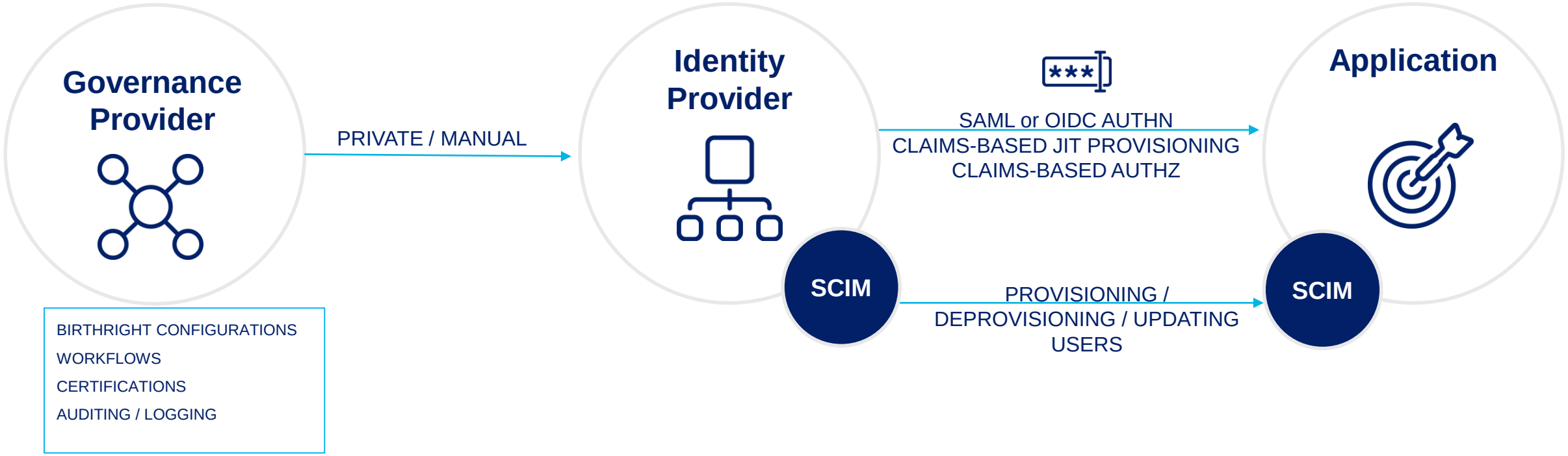
The Governance Provider Gap

FastFed expects that all governance is done by the Identity Provider. However, many traditional Identity Providers do not also play the role of an Identity Governance service. Example gaps:

- **ACCESS:** Which users within an IDP should have an account in the Application?
- **PERMISSIONS:** Which permissions within the target service should an individual account be granted?
- **WORKFLOW:** Does an individual require approval, by a manager or the application administrator, for requests to use the application?
- **LIFECYCLE:** When users joins, moves, or leaves, how do access and permissions change?

SailPoint

FastFed with Implicit Governance



“End-user administrators also want to establish governance when initially onboarding a new application, whenever possible, so as to have less to clean up after the ungoverned application has been in use for a while.”

SailPoint

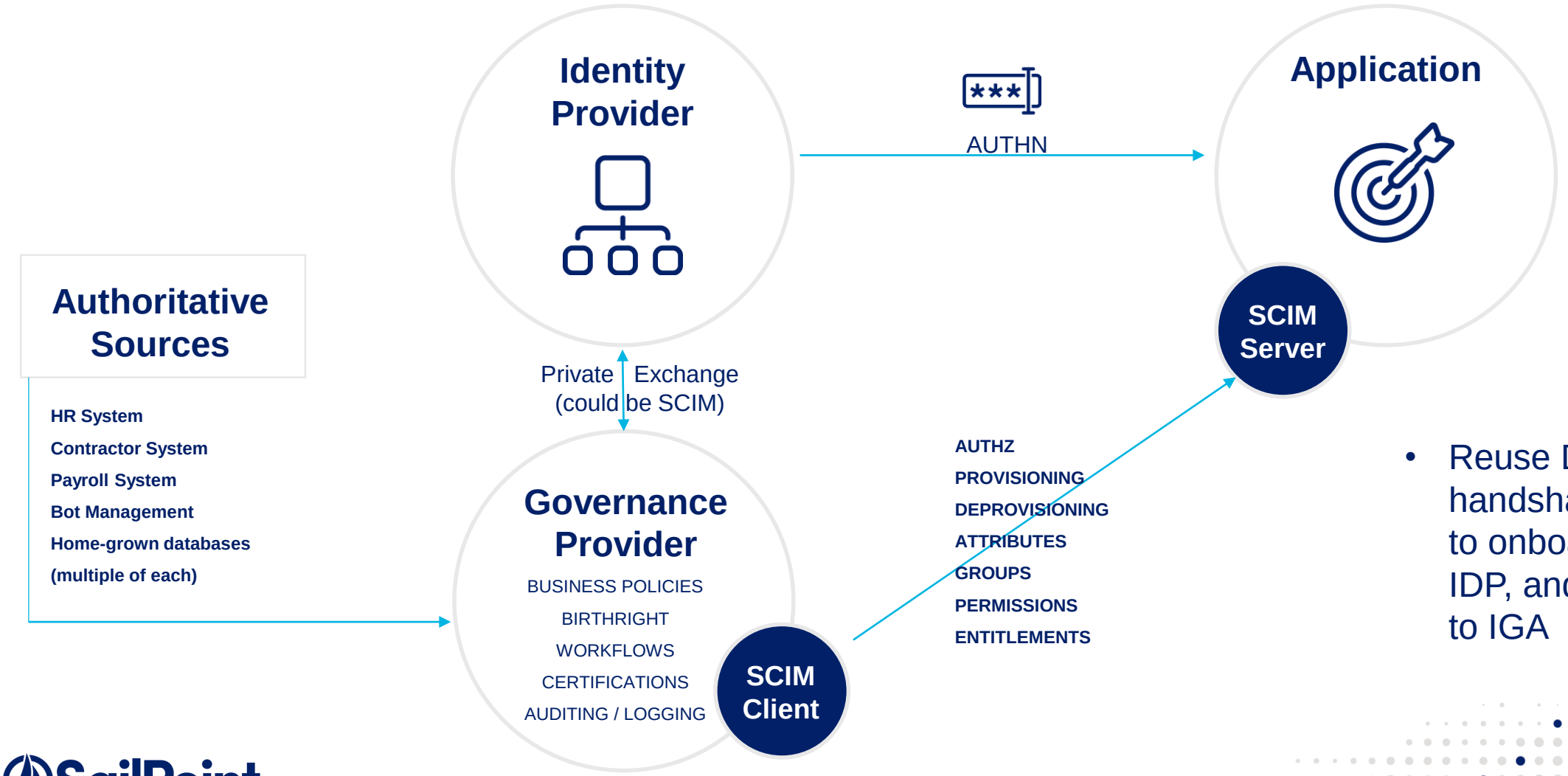
from

Onboarding with SSO

to

Onboarding with SSO & Governance

FastFed with Explicit Governance



- Reuse Discovery & handshake protocols to onboard IGA to IDP, and Application to IGA

FastFed with IGA = Governance from the Start

By splitting the FastFed concept of Identity Provider into two parts, the Identity Provider and the Governance Provider, we can allow a richer governance experience in the application.

Identity Provider

- User Authentication & SSO
- Claims-based Authorization
- User attributes routinely needed by applications
- Just-in-Time provisioning
- Identity Providers that also have Governance Provider features can continue to operate as a single system

Governance Provider

- Provision *and deprovision* accounts following a user's lifecycle
- Define user permissions based on applications' needs and user attributes the IDP may not know about
  - An IDP is just one of many attribute sources, including HR and other systems
- Enables business-defined request workflows and certifications
- Detailed auditing/logging records across all aspects of identity governance, including non-IDP related identity changes

SailPoint

FastFed has the right goal and approach. Treating Governance as a first-class participant makes FastFed more valuable. Including Governance in FastFed brings its benefits from the start. Adding Governance is a simple tweak to the FastFed draft and adds a critical component to the standard.

SailPoint

Other benefits

- FastFed 1.0 draft expects IDPs to push updates to users within 60 minutes, using SCIM. Most IDPs don’t push updates to connected applications today at all. Most IDPs don’t have SCIM clients today. IGA does both.
- FastFed use case #3 (pre-employment onboarding to a payroll service) cannot be accomplished if the end user does not have an account in the company IDP (which they do not). With IGA, this is possible within the usual lifecycle process of a user. HR provides a list of pre-employed user information, and when the user account is added to the IDP later, updates the payroll system.

Thank You