

Progress Report
of the
Gateway Rollout Working Group

April 15, 2013

Introduction

The *Gateway Rollout Working Group* is a subgroup of the *Social Identity Working Group*.

The group's goal is to integrate Google login with both the InCommon Ops Federation Manager and the Internet2 Spaces Wiki.

The resulting gateway solution was developed by *Cirrus Identity*, an Internet2/InCommon Ops business partner.

Work in Progress

Two threads of work in progress:

Work Effort #1: Leverage social identity to enhance internal apps (FM and Spaces)

Work Effort #2: Extend gateway technology to the InCommon community

Work Effort #1

- **Goal:** Leverage social identity to enhance internal apps (FM and Spaces)
- **Phase 1 (beta)**
 - SOW executed
 - Legal is reviewing contract
 - Internal funding is secured
 - Technology is partially deployed and well understood
- **Phase 2 (production)**
 - Deploy remaining gateway technology
 - SLA and production service contract needed
 - Funding sought for ongoing maintenance/support

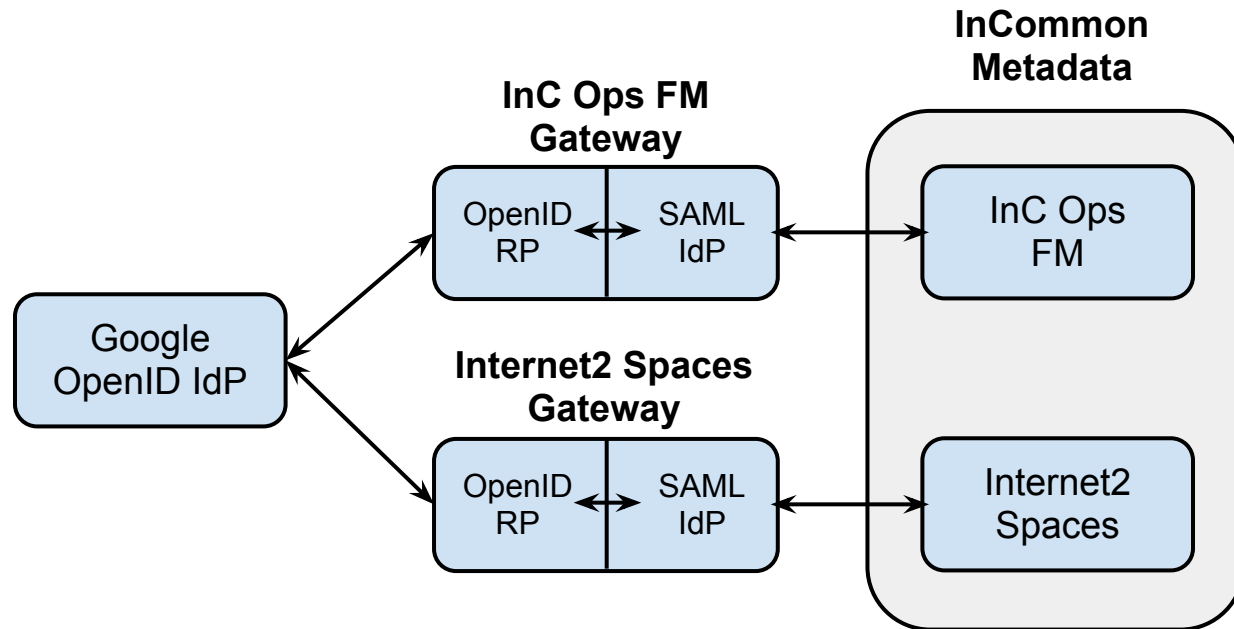
Phase 1 (beta)

Status: Two gateway instances deployed:

1. Google OpenID Gateway for Internet2 Spaces Wiki
2. Google OpenID Gateway for InCommon Operations Federation Manager

The above gateway instances will be demoed at the Internet2 Annual Meeting and will be in production by end of June 2013 pending completion of Phase 2 (SLA and production service contract).

Gateway Architecture Phase 1 (beta)



Why Google OpenID?

The Google OpenID IdP is:

- mature and relatively stable
- [FICAM LoA-1 certified](#) by OIX
- [FICAM OpenID 2.0 Profile](#) conformant
 - asserts Private Personal Identifier (PPID)
 - requires user consent

Google also supports OpenID Connect (an emerging profile of OAuth2) but it is not stable.

Phase 2 (production)

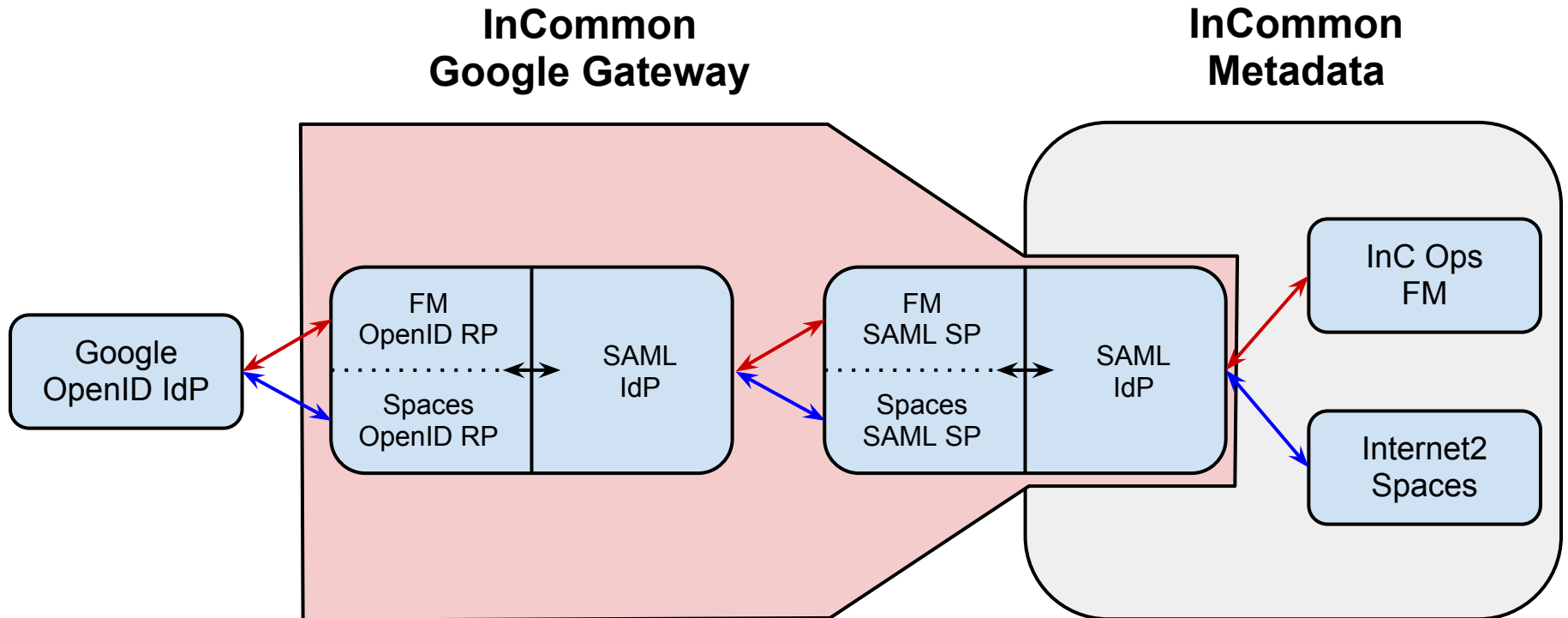
To bring the internal project to production, we need:

- Service Level Agreement
- Production Service Contract
- Funding for long-term maintenance and support

Additional work covered under Phase 1 SOW:

- SAML-to-SAML gateway abstraction layer
- Gateway Manager

Gateway Architecture Phase 2 (production)



Gateway Manager

The Gateway Manager (GM) allows site administrators to manage gateway instances. (the GM is not shown in the previous diagram)

Gateway Manager features:

- Enable/Disable access to gateway instance
- Set gateway name displayed on user consent page
- Determine how ePPN and ePTID are constructed
- View OpenID to MACE-Dir SAML attribute mapping
- View usage stats (e.g., hourly, daily, etc.)

Work Effort #2

- **Goal:** Extend gateway technology to the InCommon community
- **Things to do:**
 - Elicit requirements
 - Define SOW
 - Develop timeline
 - Identify and address scaling issues
 - Determine funding model
- **Align with NET+**
 - Identify early adopters
 - Find a path forward to "General Availability"

Alignment with NET+

NET+ Service Phases:

1. Inquiry
2. Evaluation
3. Service Validation
4. Early Adopter
5. General Availability

The first three steps may already be complete.