Technical Reference Architecture

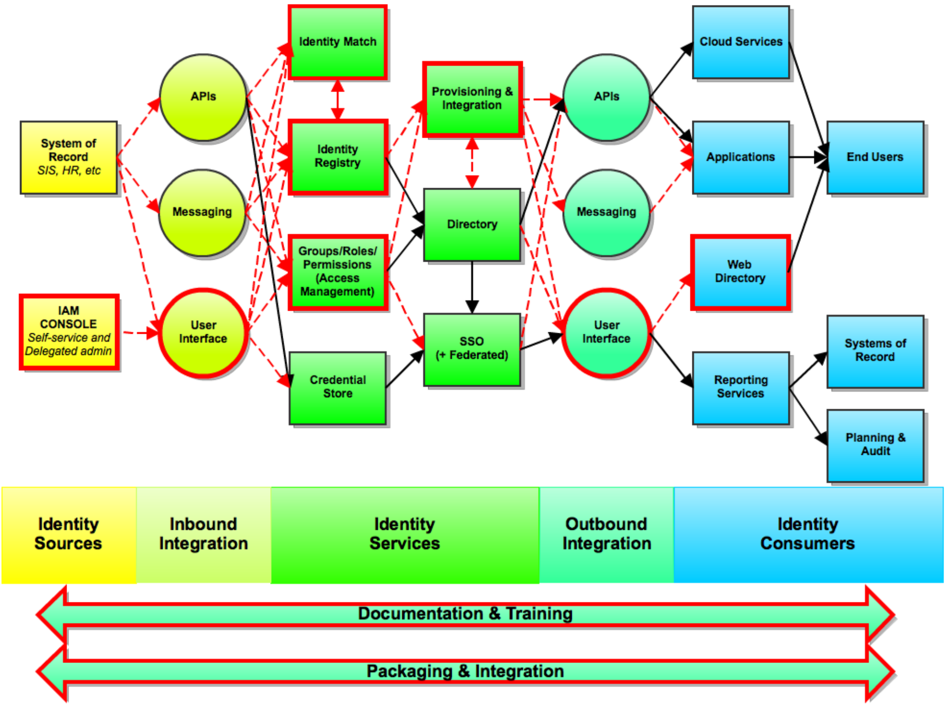
There are two ways of looking at the CIFER Reference Architecture. One is to highlight function and flow between identity services and other components of the IT ecosystem. The other is to put capabilities in the foreground and map those capabilities onto the workstreams identified by the CIFER teams.

- Function and Flow View of CIFER Reference Architecture
- Capability and Component View of CIFER Reference Architecture

Click links above to jump to the corresponding view.

Function and Flow View of CIFER Technical Reference Architecture

(draft)



In the above diagram, Thick borders and dashed lines (both in red) are potential areas of significant CIFER work.

Component	Description	Status
System of Record	Authoritative source of a person's identity at an enterprise. Example SORs include HR, SIS, etc.	*(Out of scope)*
Delegated and Self Service via "Identity Portal" or "Console"	A pluggable/configurable user interface providing end users and functional administrators access to identity services (backed by any compatible product). Potentially integrated services include: • Identity Enrollment and Maintenance • Credential Management • Group Management • Access Management WorkflowIntegration is not necessarily restricted to JV-endorsed OSS components.	Potential Initiative See Also: PWM, Syncope
Identity Match	A component that can operate stand-alone or as part of an Identity Registry that is responsible for reconciling identities from multiple sources into a single identity. May also assign identifiers.	Potential Initiative • ID Match Strawman • OpenEMPI • OYSTER (U Ark Little Rock) • FRIL

Identity Registry	The "Source of Truth" about a person's identity as assembled from one or more Systems of Record.	Several in-progress initiatives, including for enterprises: • KIM • OpenRegistry • Penn State Registry and for VOs: • COmanage Registry
Groups/Roles /Permissions Registry	A repository of authorization information associated with people identities.	• Grouper • KIM
Credential Store	A repository of authentication information, such as passwords, tokens, or certificates.	• MIT Kerberos • See also: Directory Servers • Mobile-OTP
Provisioning and Integration Engine	A component responsible for maintaining identity information consistency between registries, applications and other consumers in order to ensure, for example, that people have access to exactly the services to which they are entitled.	• OpenIDM* • UNC-Chapel Hill SPML Toolkit
Provisioning Connectors	Plug-ins for a Provisioning Engine that know how to talk to specific target systems (such as LDAP servers, SPML targets, mainframes, etc).	Potential in-progress initiative: • OpenICF*
Directory	A public or semi-public directory of identities, generally read-only or read-mostly.	• 389 Directory Server • ApacheDS • OpenDJ* • OpenLDAP
SSO & Federated Auth	A component responsible for web-based authentication, single sign-on, and federated authentication.	• CAS • OpenAM* • Shibboleth
Web Directory	A web-based frontend to an enterprise's public directory (typically an LDAP server).	Potential in-progress initiative: • COmanage Directory
Reporting Services	Tools for providing data analyses to various business units.	*(Reporting tools are considered out of scope, though see "Additional Potential Work" below.)* • OpenXDAS (possibly stale) • OSSIM
APIs	Standards for exchanging data between applications.	Potential initiatives: • SOR-to-IDMS • Identity Match • Groups • website: SCIM (on this wiki: SCIM)
ESB	Enterprise Service Bus: A message passing infrastructure used for sharing notifications across an enterprise.	*(Out of scope)*
Packaging & Integration	Packaging & Integration refers to endorsed collections of specific version of products known to work well/be compatible, assembled together in a way to facilitate deployment ("suites"). (eg: download archives, VMs, cloud instances). Independently, products must also be packaged in a way to facilitate deployment, and to integrate with other endorsed components.	
Documentation & Training	Documentation and Training resources refer both to suite-level packages as well as products independently.	

**Denotes a former Sun product forked by ForgeRock*

Additional Potential Work

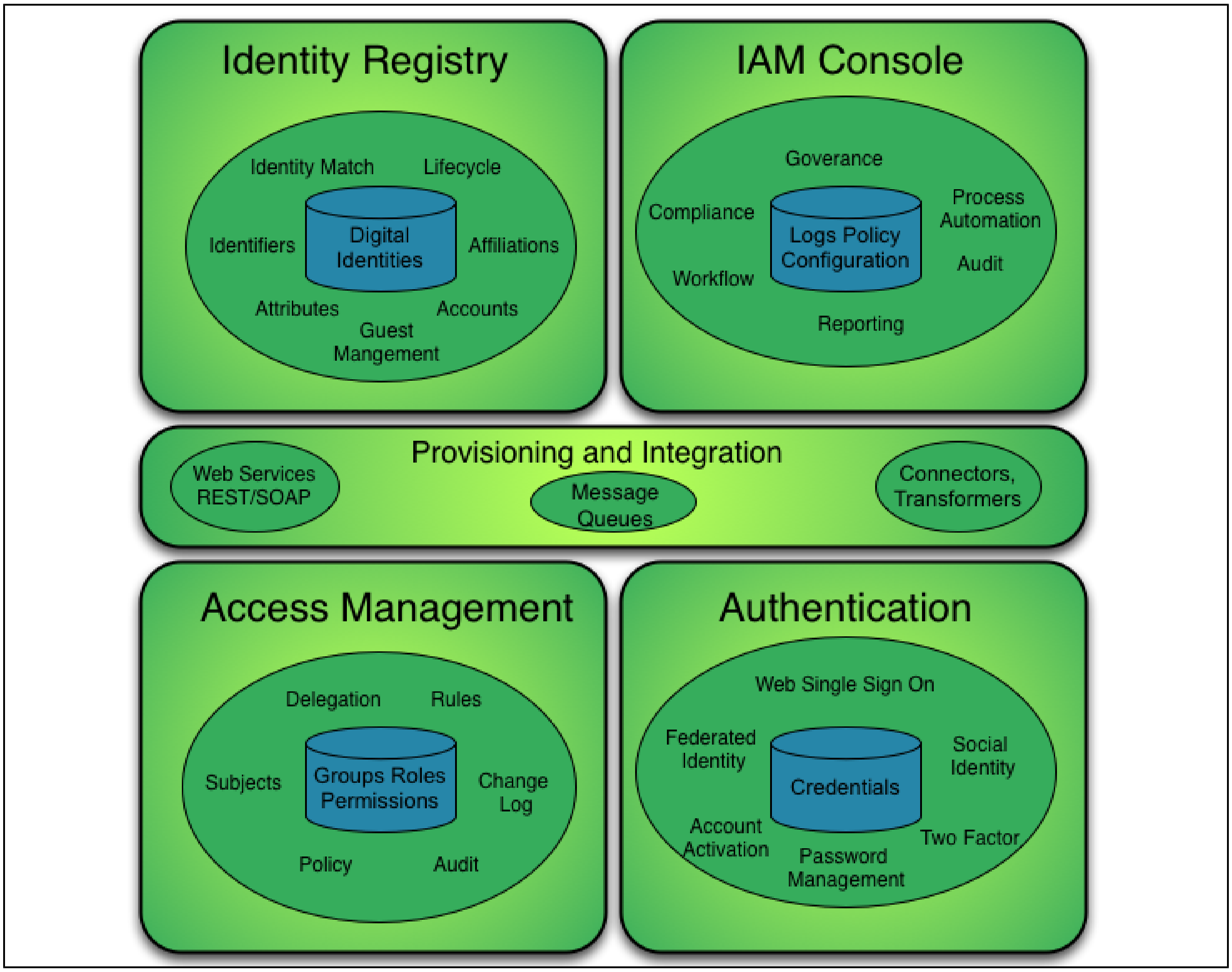
These items are more about enhancements to existing products, but might be of general interest to the community:

- Single Log Out
- CAS SAML support
- "Out-of-the-box" common reports for OSS reporting tools

- Credential Management/Password Quality tools
- Multi-Factor integration
- Client/Server PKI

Capability and Component View of CIFER Reference Architecture

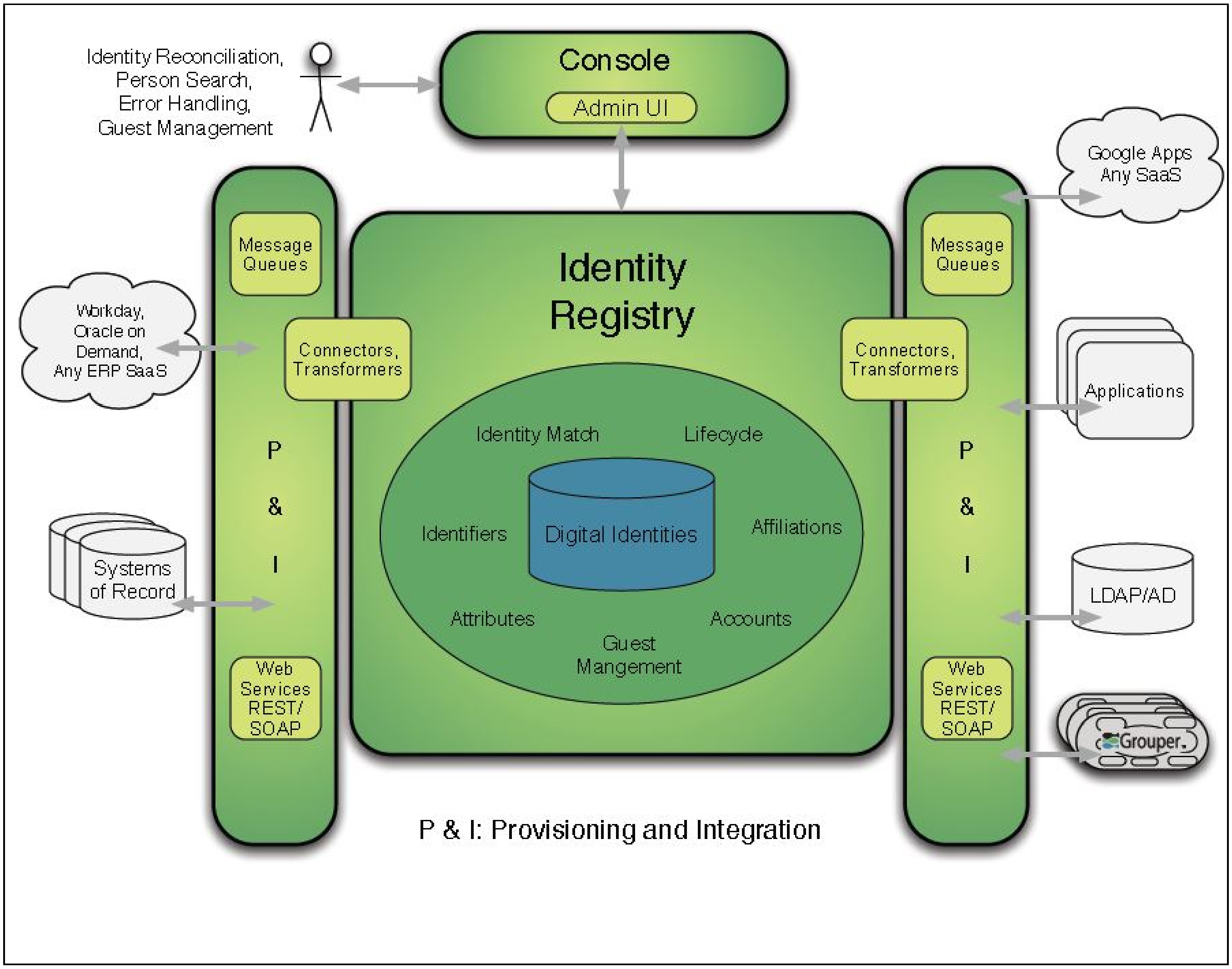
CIFER Overview



Suggested Improvements:

- Need an overall label at center top of diagram. Something different than just CIFER Overview. Something that ties back to the 5 major workstreams proposed in our marketing material.
  - 5 Overarching CIFER Areas?
  - 5 Major CIFER Focus Areas?
- Provisioning and Integration label should be same size and bolded as each of the other major areas.
- Put REST/SOAP in parentheses underneath web services label in all diagrams.
- Put commas between concepts in blue database drums and include etc. (i.e. Groups, Roles, Permissions, etc.) (Logs, Policy Configurations, etc.)

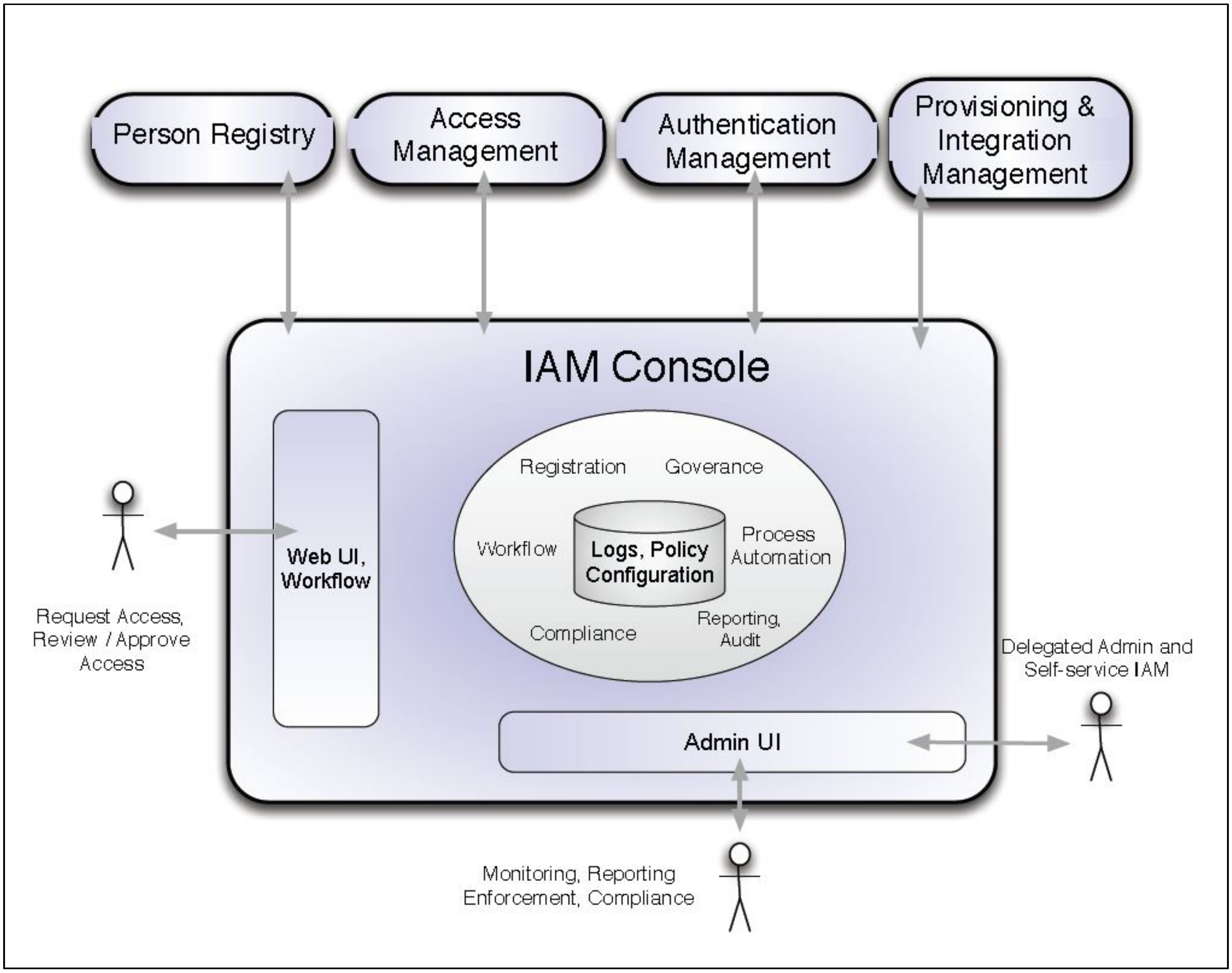
Identity Registry



Suggested Improvements:

- Put P & I: Provisioning and Integration as a footnote or legend at the bottom off to the right side of the diagram. As is it seems to be a label for the diagram. (i.e. P & I = Provisioning and Integration)
- Change Console label to IAM Console for consistency throughout all diagrams.
- Put overall label at top center of the diagram. CIFER Identity Registry Focus Area?
- Change stick figures to some modern 3d clip art for a person in all diagrams
- Remove Grouper reference and make it generic "access management" label on right side of diagram. Why is there stacked bubbles for this? Does it imply multiple grouper installations?
- Remove Admin UI sub bubble in the IAM Console bubble.

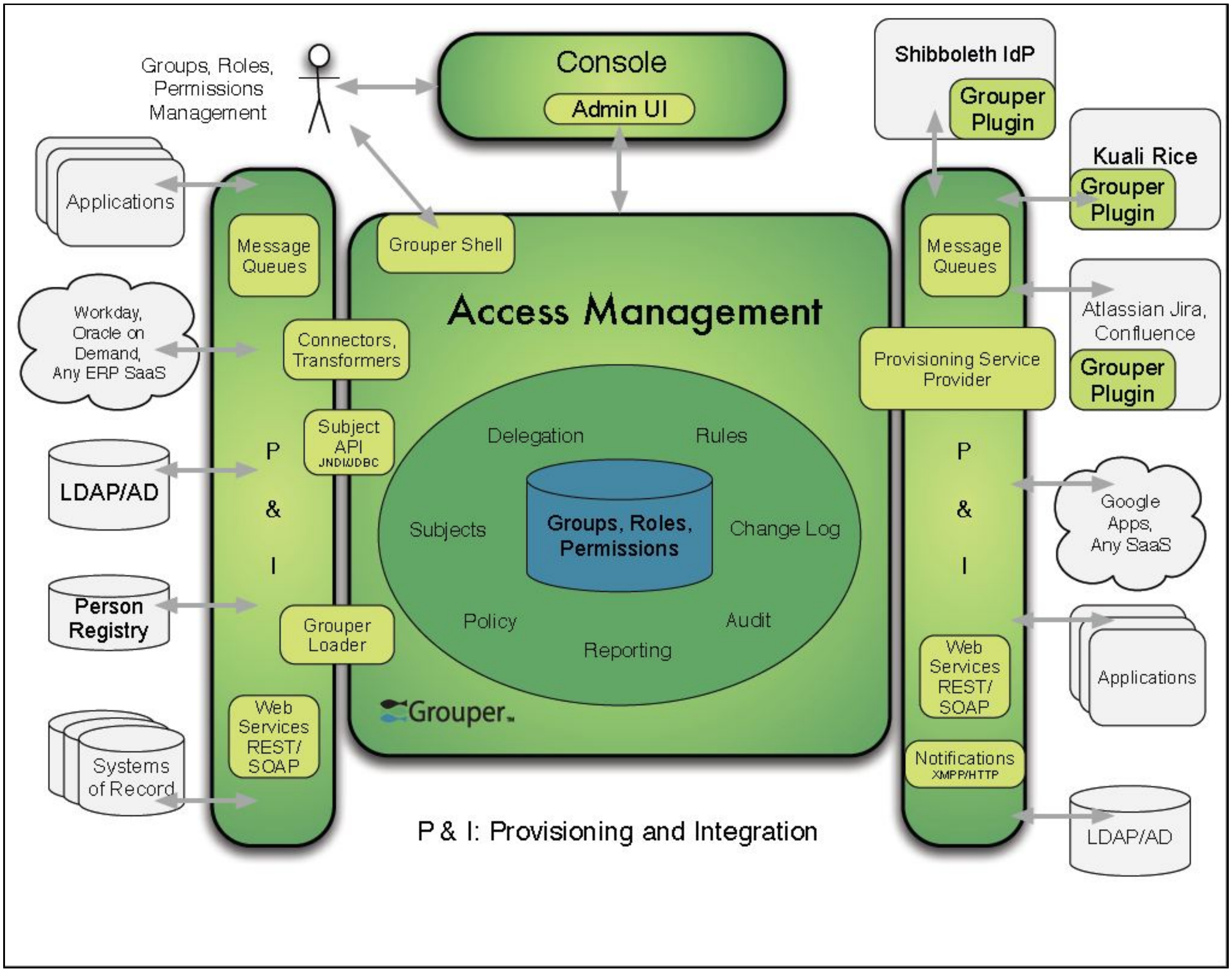
IAM Console


Person Registry
Access Management
Authentication Management
Provisioning & Integration Management
IAM Console
Web UI, Workflow
Registration
Goverance
Workflow
Logs, Policy Configuration
Process Automation
Compliance
Reporting, Audit
Request Access, Review / Approve Access
Delegated Admin and Self-service IAM
Admin UI
Monitoring, Reporting Enforcement, Compliance

Suggested Improvements:

- Put label in top center of diagram. CIFER Identity and Access Management Console
- I am fine with this color combination if others like it better than the green and blue orientation, but need to make all the diagrams consistent. I know it would take more effort but it would be good to have a separate color scheme for each of the 5 workstreams.
- Eliminate the Workflow under Web UI bubble. Workflow is already a capability around the database drum.
- Change Person Registry bubble to Identity Registry
- Since these stick figures represent different types of users might want to label each stick figure according to that type?
- Use a 3d stick figure clip art.
- The qualifier "Management" in each of the bubbles at the top and not just the P & I bubble.

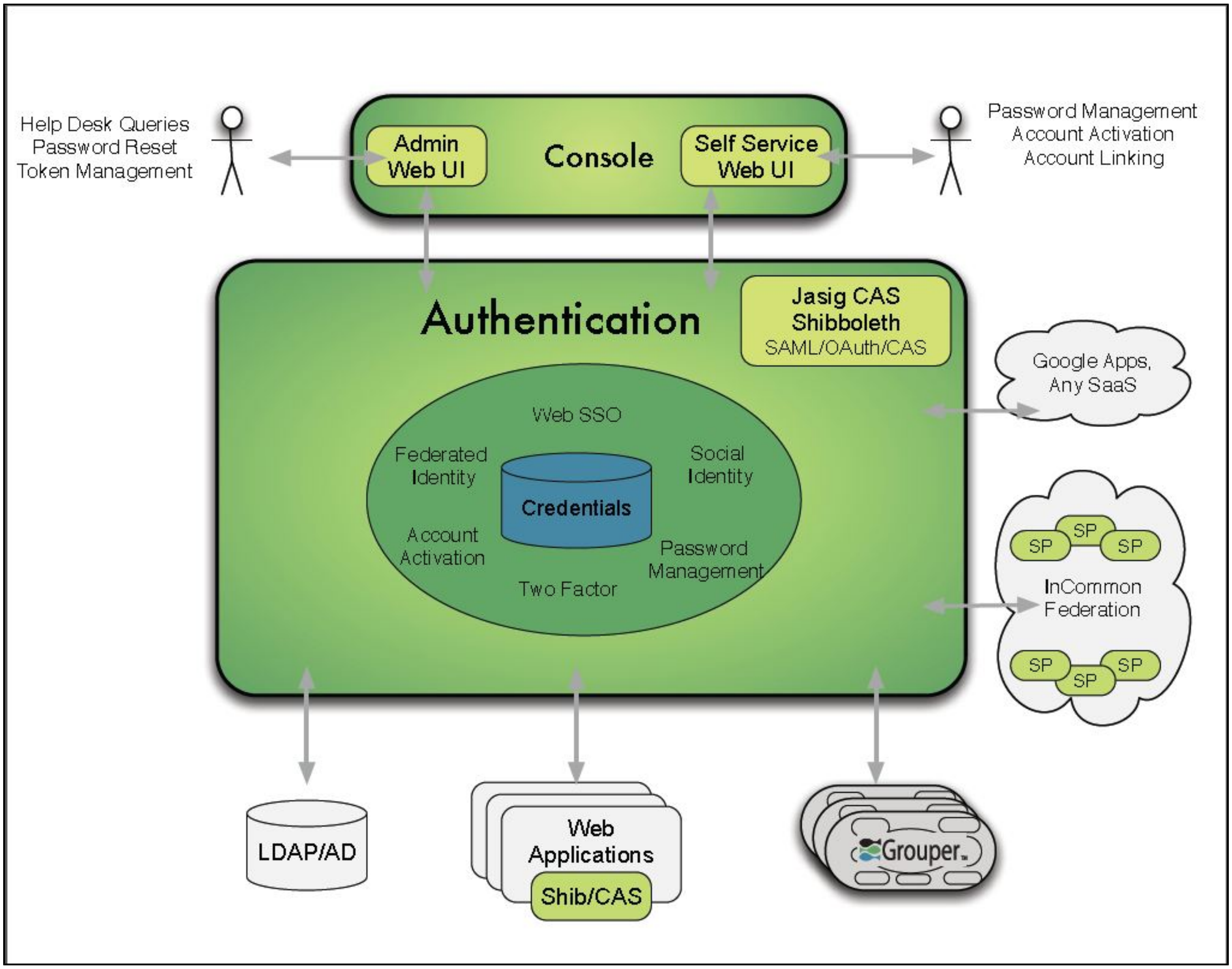
Access Management



Suggested Improvements:

- Put label in top center of diagram. CIFER Access Management Area of Focus
- Change Person Registry label in blue database drum to Identity Registry. Change color to blue to indicate a CIFER related database.
- Change all Grouper references to generic Access Mgmt reference
- Remove fine print acronyms under Subject API and Notifications. Or put them in parentheses.
- Not sure I understand Grouper Shell or Grouper Loader bubbles. Can these be changed to a generic Standard API reference? (i.e. Load Data API, User Interface API, etc.)
- Can Provision Service Provider be changed to Provisioning Service API?
- What is the Subject API? Subjects in the capabilities section around the middle database drum is something that does not resonate with me. Is there a better term to use?
- Simplify Grouper plugins in upper right to one generic rather than three separate. Use stacked bubbles, keep labels for each stacked bubble but indicate one Access Management Plugin.
- Remove Grouper label and icon from the middle of the green area and put as footnote at bottom of diagram indicating an "Implementation Option" for Access Management.

Authentication



Suggested Improvements:

- Put label in top center of diagram. CIFER Authentication Area of Focus
- Should this have a similar right and left hand side P & I orientation like the other diagrams?
- Spell out SSO like on the overall diagram
- Remove the bubble from the middle of the green area and keep as separate legend or footnote to the diagram. Label the Jasig CAS, Shib, etc. bubble as "Implementation Options" for authentication and make choices into a bulleted list. Why are there stacked bubles at the bottom for web applications and grouper?
- Is the term SP in the InCommon Federation cloud recognizable? I assume it stands for Service Provider? Can actual representative names be used instead?
- Relabel Console to be IAM Console
-