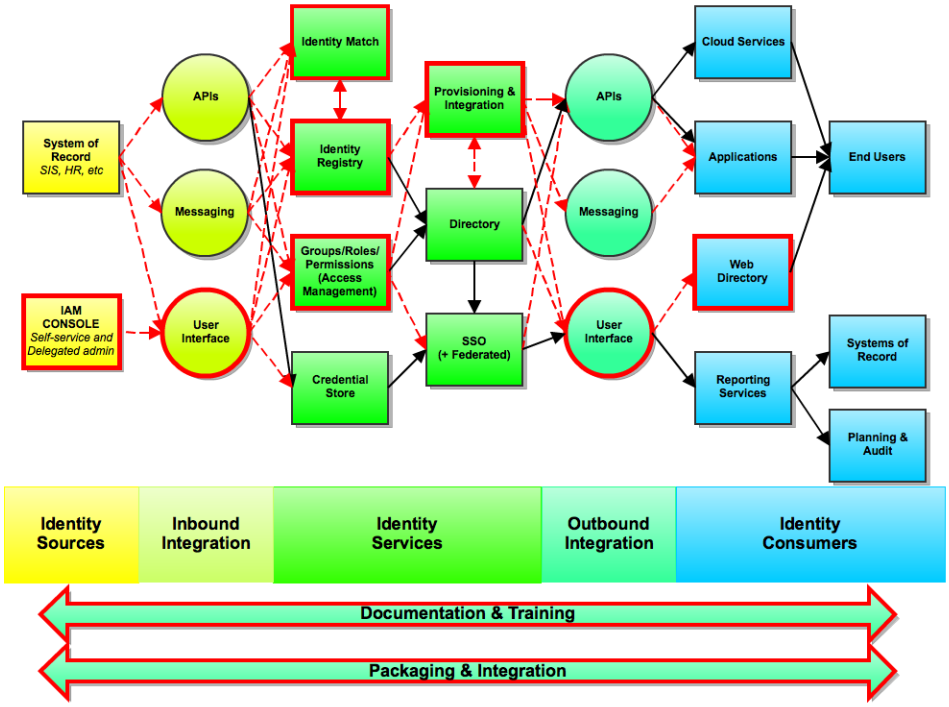
Technical Reference Architecture--Function and Flow

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