Identity Management Product Feature Details

DRAFT to be reviewed during meeting in the mid November 2016 and by email.

Legend

Advantage. The product is significantly better than competing products.

Average. The product has an average quality.

Disadvantage. The product is slightly worse than competing products.

Warning. The product has a serious disadvantage that can be critical for deployments.

The points are awarded in accord with the evaluation methodology.

	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**
Project information						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**
License	Proprietary	Proprietary	Apache 2.0			Apache 2.0
Evaluated version			3.1		2.3	1.2.2
Date of evaluation						
Primary supporters	Sailpoint	Fischer International	Evolveum & Partners			
Suitability						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**
Enterprise: Employee **Management of enterprise employees. Requires good RBAC, support for complex organizational structures and entitlements, excellent provisioning capabilities, reasonable reporting and governance.**						

Enterprise: Customers **. Management of enterprise customer identities. Requires scalability and good provisioning capabilities. Organizational structure and RBAC are much less important. Governance is usually only an obstacle here.**						
Cloud **Use of IDM inside cloud service deployments, e.g. integrating applications in SaaS clouds or directly exposing functionality as IDaaS. Requires scalability. At least basic support for RBAC and organizational structure is also required. Multi-tenancy is critical.**						
Public Sector **Management of identities in the public sector. Usually a good support for organizational structures is required to model organizational structure of public agencies, hierarchy of regions/provinces for citizen identities, etc. Also reasonable support for RBAC, good authorizations and at least a basic governance is required. Public sector seems to be shifting to open source preference therefore a clean open source strategy is also important.**						
Academia **Mgmt. of Identities in the in Higher Education. Requires all types of identities: teachers, students, employees, visitors, researchers, collaborators, visitors etc., Usually support for very complex and parallel organizational structures is required. Ability for a parameterized membership in many organizational units is critical. As is the support for temporal conditions to limit student and visitor access) Clean open source strategy is also crucial.**						
Architecture						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHatKeyCloak**	**ApacheSyncope**
Overall System Architecture How good is the software architecture from the software engineering point of view. Is the system well divided into subsystems and components? Are there proper abstractions in place (such as interfaces)? Is the structure of the system appropriate and understandable?						
Platform **Platform on which the system runs. E.G. specific operating system or hardware-independent platform**						
Structural Framework **Framework (or other method) which is used to 'wire' the system together. Framework that binds the components together and forms the basic structure of the system.**						
User Interface						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHatKeyCloak**	**ApacheSyncope**
Framework *What is this?* **Programming framework that was used to build GUI. This is crucial as the framework is very difficult to change. It usually means re-writing the entire GUI.**						
Usability *What is this?* **How easy is to use the system, how easy is to understand it. Is the system flooding user with information? Does it spread the information in a thousands of confusing tabs? Ergonomy, etc.**						
Completeness *What is this?* **Does the user interface provide access to all functionality available in the system?**						
Speed *What is this?* **How quickly the GUI reacts to user actions.**						
Customization *What is this?* **How easily can be the GUI fuctionality be customized.**						
Role-Based Access Control (RBAC)						

	SailPoint	Fischer	midPoint	CoManage	RedHat KeyCloak	Apache Syncope
Provisioning Roles *What is this?* **Ability to specify which accounts to create when a role is assigned to a user. Ability to define attribute values.**						
Hierarchical Roles *What is this?* **Ability to include one role in another role.**						
Assignment parameters *What is this?* **Ability to customize each role assignment with parameters. E.g. specify a tenant for which the assigned role applies). The assignment parameters are not part of role definition and neither they are part of user data. The parameters must be part of user-role relation (assignment).**						
Parametric Roles *What is this?* **Use parameters from user assignment or from a super role in the role expressions. E.g. parametrize the assignment of role assistant with an organizational unit or locality to which it applies.**						
Conditional Roles *What is this?* **Ability to "switch on and off" each role based on an arbitrary condition. Ability to assign temporal validity constraints (role valid from or to a specific date).**						
Meta-roles *What is this?* **Roles that can be applied to roles themselves. E.g. ability to sort roles to groups or types (functional,business, IT,...) and specify the synchronization properties for each group using a unified policy (meta-role).**						
Role ownership *What is this?* **Assign a role owner who have more privileges over the role, e.g. ability to modify role definition.**						
Role lifecycle *What is this?* **Ability to guide the creation, modification and disposal of a role, e.g. using proper authorizations, workflow, approvals, etc.**						
Role synchronization *What is this?* **Ability to create groups (or other objects) in the target systems as a reflection of a role. Also ability to create roles as a reflection of arbitrary resource objects.**						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**
Organizational units *What is this?* **Ability to support object that model organizational units such as companies, divisions, departments, projects, workgroups, teams, ...**						
Organizational tree *What is this?* **Ability to organize organizational units to a tree-like structures, ability to display them and efficiently browse them.**						
Parallel organizational structures *What is this?* **Ability to maintain several independent organizational structures. E.g. maintain functional organizational tree and a parallel flat project-oriented structure. Ability to assign the same user to each of them independently.**						
Organizational structure synchronization *What is this?* **Ability to create organizational units (or other objects) in the target systems as a reflection of organizational structure. Also the other way around. Ability to transform flat structures to tree structures, ability to reconstruct tree structure from flat string attributes, etc.**						
Provisioning and Synchronization						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**
Propagation *What is this?* **Ability to propagate data from the IDM system to the managed systems (resources).**						

Real-time synchronization *What is this?* **Ability to synchronize data from managed systems to the IDM on an almost-real-time basis (delay in seconds).**						
Reconciliation *What is this?* **Ability to compare data records in IDM and in the managed systems.**						
Opportunistic synchronization *What is this?* **Ability of the IDM system to automatically trigger synchronization when needed. E.g. in case that an account is missing when IDM attempts to modify it, when existing account is present when a new account is being created, etc.**						
Attribute mapping *What is this?* **Ability to map attribute values between resource objects (object on managed systems) and the objects in the IDM system.**						
Uniqueness, iteration *What is this?* **Ability to enforce uniqueness of attribute values (on managed systems) and to iteratively find a unique value, e. g. by trying identifiers in the form of jack001, jack002, ...**						
Provisioning ordering and dependencies *What is this?* **Ability to enforce proper ordering of provisioning operations. E.g. if an application account depends on existence of operating system account. Also ability to properly pass attribute values between systems. E.g. create e-mail account first, pass the e-mail address value to user attribute, then create an AD account and properly set the e-mail address.**						
Provisioning notifications *What is this?* **Notifications that announce success or failure of provisioning operations. Used mostly to deliver initial credentials and to notify system administrators about problems. Support for various channels (e-mail, SMS, ...)**						
Resilience *What is this?* **Ability of an IDM system to recover from provisioning failures such as timeouts and retries, compensation mechanisms, transactional guarantees, etc.**						
Entitlements *What is this?* **Support for management of entitlements on the resource side (in managed systems) such as LDAP groups, AD groups, privileges, ACLs, etc. Ability to display and synchronize them. Also ability to manage membership or association of accounts and entitlements.**						
Connectors						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHatKeyCloak**	**ApacheSyncope**
Framework *What is this?* **Framework of mechanism used to manage and access provisioning connectors.**						
LDAP *What is this?* **Support for LDAP servers.**						
Active Directory *What is this?* **Support for Microsoft Active Directory.**						
Databases *What is this?* **Support for relational databases.**						
Generic connectors *What is this?* **Connectors that can apply to many types of systems. Flat files, CSV, XML, scripting connectors, etc.**						
Unix connectos *What is this?* **Connectors for UNIX-like systems such as Linux, Solaris, BSD, AIX, ...**						
HR connectors *What is this?* **Connectors for HR systems such as SAP HR modules, PeopleSoft HRMS, ...**						
ERP and business applications connectors *What is this?* **Connectors for ERP systems and various 'business' systems such as SAP ERP (R/3), Oracle applications, ...**						
Cloud connectors *What is this?* **Connectors for cloud-based services such as SalesForce, Google apps, Office 365, ...**						
Mainframe and mini connectors *What is this?* **Connectors for mainframe systems and 'minicomputers' such as z/OS, OS400, RACF, ...**						
Other connectors						
Connector compatibility *What is this?* **Can the connectors be used in other systems? Is there a support for legacy connector frameworks?**						
Connector development *What is this?* **How easy is to develop a new connector.**						
Customization						

	SailPoint	Fischer	midPoint	CoManage	RedHat KeyCloak	Apache Syncope
Flexibility *What is this?* **Overall flexibility of the product: ability to change its behavior to satisfy the requirements.**						
Popular scripting languages *What is this?* **Support for Groovy, JavaScript/ECMAscript or other popular scripting languages.**						
Other scripting *What is this?* **Support for other scripting languages.**						
Extensible objects *What is this?* **Ability to extend existing object types with custom attributes. Ability to use the custom attribute in the same way as built-in attributes. Also ability of the attribute to be properly stored, indexed, displayed in forms, etc.**						
Generic objects *What is this?* **Ability to define new object types beyond those that are provided by default. Also ability for these new object types to behave as a first-class citizens.**						
Generic synchronization *What is this?* **Ability to synchronize any object with any other object.**						
Hooks/triggers *What is this?* **Ability to place custom code to be executed at important points in request processing.**						
External interfaces (APIs)						
	SailPoint	Fischer	midPoint	CoManage	RedHat KeyCloak	Apache Syncope
Local native API *What is this?* **Local interface available in a primary language (e.g. Java). The goal is low overhead (local calls) and efficient development (e.g. use of callbacks, asynchronous invocation, etc.)**						
SOAP web service *What is this?* **Web service exposed by SOAP endpoint, WSDL definition, XSD schema, WS-Security support, etc.**						
REST *What is this?* **RESTful resource-oriented interface with proper structure according to REST architectural style (Fielding) and WWW architecture.**						
Client library *What is this?* **A stand-alone component that can be linked to an application code and can be used to conveniently access the IDM system over the network.**						
Data Storage						
	SailPoint	Fischer	midPoint	CoManage	RedHat KeyCloak	Apache Syncope
Commercial relational databases *What is this?* **Ability to store data in commercial relational databases such as Oracle, Microsoft SQL Server, etc.**						
Opensource relational databases *What is this?* **Ability to store data in open source relational databases such as PostgreSQL, MariaDB, etc.**						
NoSQL *What is this?* **Ability to store data in NoSQL databases.**						
Self-service						

	SailPoint	Fischer	midPoint	CoManage	RedHat KeyCloak	Apache Syncope
Self registration *What is this?* **Ability for anonymous user to fill out a registration form which creates a user record. Also ability to control which fields are required, field validation, CAPTCHA, etc.**						
Edit profile *What is this?* **A dialog that allows user to change some of their own user profile details. Also ability to control which fields are displayed, which fields are editable, etc.**						
Password change *What is this?* **Ability for a user to change his own password (when the user still knows the old password). Also ability to select/filter resources, apply policies, etc.**						
Password reset *What is this?* **Ability for a user to reset his own password when the old password is lost. Support for verification mail, security questions, etc.**						
Account summary *What is this?* **Simple page that provides easily understandable information about user's accounts, entitlements, group membership, etc.**						
Password agents *What is this?* **Agents that capture cleartext passwords and sent them to IDM for distribution. E.g. agents for Active Directory, LDAP servers, etc.**						
Other self-service functionality						
Security						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**
Authentication *What is this?* **Flexibility of authentication mechanisms, integration with SSO systems, etc.**						
Authorization *What is this?* **Ability to control who can do what. Overall authorization flexibility and architecture.**						
Fine-grained authorization *What is this?* **Ability to specify authorization policies on a fine granularity (e.g. on the attribute level)**						
Delegated administration *What is this?* **Ability to delegate administrative tasks to specific user groups. E.g. ability to specify administrators for individual divisions, ability to delegate some functions to he call center, etc.**						
Privilege delegation *What is this?* **Ability to delegate privileges of one user to another user. E.g. allow one user to take all the responsibilities of another user during a vacation.**						
Audit *What is this?* **Ability to record all the operations of the users and the system down to a very fine details.**						
Workflow						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**
Workflow engine *What is this?* **Whether the product contains built-in or default workflow engine and how good the engine is.**						
Workflow engine integration *What is this?* **How well is the workflow engine integrated into the system. Is it natural part of the system or was it added just as an afterthought? Are the workflow action items (such as approvals) reasonably integrated into the user interface?**						

Built-in approval workflow *What is this?* **Whether the product contains built-in or default approval workflow and what are the capabilities. Approval process is a usual part of IDM solutions and it is not entirely trivial to implement.**						
Generic workflows *What is this?* **Can the workflow be customized? Can any type of custom workflow be plugged into the IDM processes?**						
Workflow standards *What is this?* **Does the workflow support workflow standards (such as BPMN)?**						
Pluggable workflow engine *What is this?* **How easily can the default workflow engine be replaced? Can the product use a different engine? Or can it invoke remote workflow system instead?**						
Governance, risk assessment, compliance and forensic						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**
Segregation of duties *What is this?* **Ability to exclude privileges or groups of privileges that cannot be assigned to the same identity at the same time.**						
Recertification (attestation) *What is this?* **Support for regular reviews and re-approvals of assigned privileges.**						
Role analysis *What is this?* **Support for automated analysis of privileges aiming at assisted design of RBAC structures. E.g. Role mining, role suggestions, etc.**						
Reporting *What is this?* **Support for producing a well-formatted human-readable reports (e.g in HTML or PDF) that contain information from the IDM system and/or the resources. Also ability to easily configure custom report, modify the report design, etc. (Simple data export from a database is NOT considered to be reporting)**						
History reports *What is this?* **Support for storage of historical data and ability to analyze them. E.g. ability to report who had a particular role 6 moths ago.**						
Operation						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**
Hardware resource efficiency *What is this?* **Systems that consume a lot of CPU, RAM or overload disks will have a low score here.**						
Reliability *What is this?* **Whether the system actually works, all the time, reliably, without strange bugs.**						
High availability *What is this?* **Ability to work in clusters, geoclusters or other distributed configurations.**						
Export/import *What is this?* **Ability to export all system data and import it to a different system. This is useful for configuration management, migrations (dev->test->prod), backup and restore, upgrades and variety of other reasons.**						
Bulk actions *What is this?* **Ability to efficiently execute operations on a selected objects in a batch mode.**						
Logging *What is this?* **Ability to control what information is logged, ability to log debug and tracing information, whether the log messages are easy to understand, etc.**						
Documentation						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHat KeyCloak**	**Apache Syncope**

Architectural documentation *What is this?* **Documentation of architecture, subsystems, components, dependencies, modules, UML diagrams, ...**						
Administration documentation *What is this?* **Documentation describing system configuration, administration and customization**						
Developer documentation *What is this?* **Documentation describing how the system is implemented, how to create plug-ins and other programming extensions, how to contribute to the project, etc.**						
Community						
	SailPoint	**Fischer**	**midPoint**	**CoManage**	**RedHatKeyCloak**	**ApacheSyncope**
Version control system ***What is this?*** **Where is the source code maintained? Is the history public? What are the technical obstacles to contribution?**						
Community support *What is this?* **Publicly shared information, e.g. in mailing lists, wiki, bugtracking, knowledge base, etc. Information that are only accessing for subscribers or behind a paywall are NOT considered to be community support.**						
Roadmap *What is this?* **Is project roadmap publicly available? Is product developemet planning transparent and predictable? Can roadmap be influenced by the community?**						
Contributions *What is this?* **Is the code a product of a closed team in a single company or is it a group effort? How many independent groups or developers contribute to the project? This is a crucial aspect because the companies behind open source projects tend to be small and there is still a risk of failure. However if the project has a broad community it is very likely that the product development will continue even if the project founder fails.**						
Openness *What is this?* **How much is the project open to the public? Is the product design and architecture discussed in public? The the planning done in public? Is everything done in a clean and transparent open source way?**						