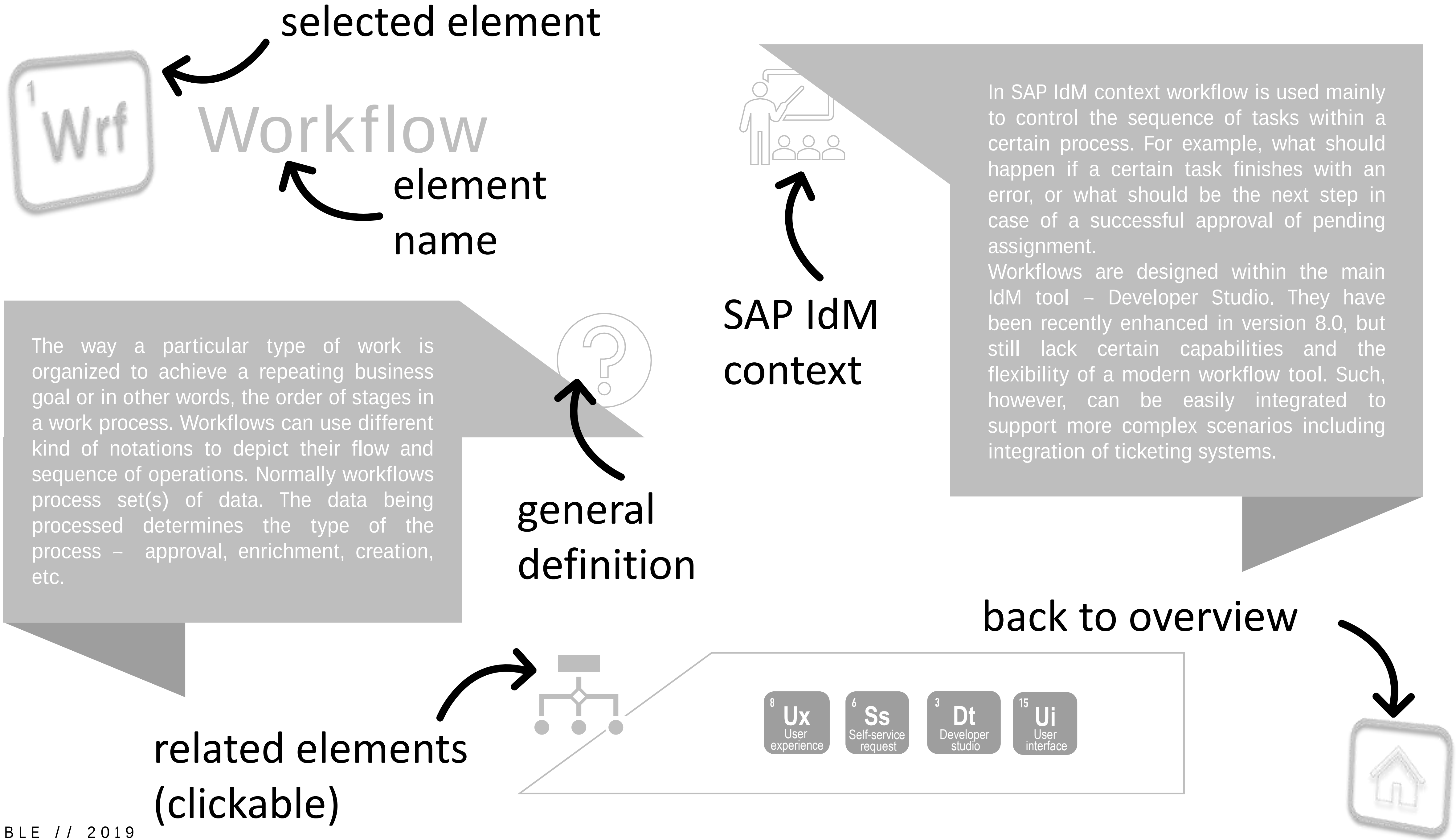
ROIABLE Periodic Table of SAP IdM

element number — 26 — Id — symbol
short name — Identity

- 🟧 user experience
- 🟥 building blocks
- 🟦 HR actions
- 🟥 common terms
- ▨ technical terms
- 🟦 landscape
- 🟦 security
- 🟩 others
- 🟪 compliance
- 🟧 HR terms
- 🟩 master data
- 🟫 main processes

1 Wrf Workflow																	2 Sst Single source of truth
3 Dt Developer studio	4 H Hire											5 Ea Emergency access	6 Ss Self-service	7 Wd Web Dynpro	8 Ux User experience	9 Os Organizational structure	10 Dq Data quality
11 Db Database	12 Cp Change position											13 Re Reports	14 At Authentication	15 Ui User interface	16 Va Validations	17 Hjp HR job/position	18 M Monitoring
19 Dbp Database procedure	20 Rh Re-hire	21 Q Queue	22 Jb Job	23 Ds Dispatcher	24 Ag Assign-ment	25 A Access	26 Id Identity	27 P Privilege	28 An Admin	29 Sc Source	30 Tg Target	31 Sh Scheduling	32 Az Authorization	33 Pw Password management	34 De Derivations	35 Ex External	36 Rd Role design
37 Ipk IdM package	38 Lta Long-term absence	39 Ma Mass actions	40 U User	41 Ast Asset	42 Ids Identity store	43 Gr Group	44 Br Business role	45 Sr Script	46 Cx Context	47 Fu Future actions	48 Rp Repository	49 Tp Transport	50 Ate Attestation	51 2fa 2-factor authentication	52 Idp Identity provider	53 Idl Identity lifecycle	54 Gp GDPR
55 Aon Add-on	56 Rlt Return from absence	57–71 * Tt	72 Ac Account	73 Uid Unique identifier	74 Dg Dynamic group	75 Io Initial load	76 Y MSKEY	77 Att Attribute	78 F Form	79 Et Entry type	80 Yv MSKEY-VALUE	81 En Email notification	82 Ar Archiving	83 Tsl Translation	84 Sv Service provider	85 Lu Lock/unlock	86 Di Data integrity
87 Icp IdM components	88 T Termination	89–103 ** L	104 Sta Staging area	105 Mr Manual repository	106 Su System users	107 Ap Attribute mapping	108 Lm Line manager	109 Ro Role owner	110 Ar Automated repository	111 Rc Reconciliation	112 Co Constants	113 Sd Segregation of duties	114 Pi Provisioning	115 Ra Risk analysis	116 Dpi De-provisioning	117 At Audit trail	118 Au Authorization matrix
			119 Cl Containers and leaves	120 Qn Qualified name	121 Al Access control	122 Ey Encryption	123 St Search results	124 Tk Tasks	125 Ps Passes	126 Rs References	127 Dl Delta	128 Mi Mitigation	129 Ev Events				
		*	57 So SSO	58 Api API	59 Vd VDS	60 Pr Protocol	61 Sq SQL	62 Ue UME	63 Cu CUA	64 Sl SAML	65 Si SCIM	66 R1 REST v1	67 Sp SOAP	68 Js JSON	69 X XML	70 R2 REST v2	71 Oa OAUTH
		**	89 Cn Connector	90 Ad Active directory	91 Hr HR system	92 Hl Hybrid landscape	93 Iag IAG	94 Im IAM	95 Sy System	96 G GRC	97 Ne SAP NetWeaver	98 Cs Cloud systems	99 Fi SAP Fiori	100 Hc Heterogeneous landscape	101 Ias IAS	102 Ips IPS	103 Cc SAP Cloud Connector

ROIABLE // 2019



selected element

Workflow

element name

The way a particular type of work is organized to achieve a repeating business goal or in other words, the order of stages in a work process. Workflows can use different kind of notations to depict their flow and sequence of operations. Normally workflows process set(s) of data. The data being processed determines the type of the process – approval, enrichment, creation, etc.

general definition

SAP IdM context

In SAP IdM context workflow is used mainly to control the sequence of tasks within a certain process. For example, what should happen if a certain task finishes with an error, or what should be the next step in case of a successful approval of pending assignment.

Workflows are designed within the main IdM tool – Developer Studio. They have been recently enhanced in version 8.0, but still lack certain capabilities and the flexibility of a modern workflow tool. Such, however, can be easily integrated to support more complex scenarios including integration of ticketing systems.

back to overview

related elements (clickable)

1 Wrf

Workflow

The way a particular type of work is organized to achieve a repeating business goal or in other words, the order of stages in a work process. Workflows can use different kind of notations to depict their flow and sequence of operations. Normally workflows process set(s) of data. The data being processed determines the type of the process – approval, enrichment, creation, etc.

In SAP IdM context workflow is used mainly to control the sequence of tasks within a certain process. For example, what should happen if a certain task finishes with an error, or what should be the next step in case of a successful approval of pending assignment.

Workflows are designed within the main IdM tool – Developer Studio. They have been recently enhanced in version 8.0, but still lack certain capabilities and the flexibility of a modern workflow tool. Such, however, can be easily integrated to support more complex scenarios including integration of ticketing systems.

8 Ux User experience

6 Ss Self-service

3 Dt Developer studio

124 Tk Tasks

2 Sst

Single source of truth

SSOT is fundamental for SAP IdM, since the system is seen as the all-seeing-eye of every landscape and it comes quite naturally to be aware of every bit of information that runs across it. During the design phase it should be taken into consideration how SAP IdM can become the SSOT for the organization not only in terms of access/privileges, but also when it comes to employee/externals master data.
Second, but not less important is when SSOT is established to keep it intact. This is not always easy, especially if edit mode is still enabled in the target systems, for which SAP IdM is seen as master.

The single source of truth, shortly SSOT, is the practice of structuring information models and associated data schemas in such a way that every data element is mastered (or edited) in only one place. In other words SSOT is a concept that an organization can apply as part of its information architecture to ensure that everyone in the organization uses the same data when making business decisions.

86 Di Data integrity

35 Ex External

30 Tg Target

10 Dq Data quality

Developer studio

Developer studio is an integrated development environment (IDE) for most of the Java-based modules of SAP. The IDE was always based on Eclipse releases, but only since the recent releases it is utilizing clean Eclipse builds and implementing the concept of plug-ins, which delivers the needed toolset for developing various enterprise applications like BPM, BRM, PI, Portal, SAPUI5, etc.

Developer studio is the design-time tool for SAP IdM. Most of the artifacts can be created and maintained only there, including forms, processes, entry types, idm packages, etc.

The studio replaces the outdated console, which was available with releases prior to SAP IdM 8.0.

It is important to keep the patch level of the SAP IdM plug-in for Developer studio aligned with the patch levels of the other relevant SAP IdM components to avoid any cross-component communication issues.

Developer studio is using the attached SAP NetWeaver UME for authentication.

87 Icp IdM components

62 Ue UME

32 Az Authorization

97 Ne SAP NetWeaver

4 H

Hire

Hire is an HR process of reviewing applications, selecting the right candidate(s), assessing them and choosing between them to make the hiring decision. Selected candidates are sent an offer, that if accepted, starts an internal company hiring procedure. Last, but not least it triggers an onboarding process that should enable the new employee to fulfill their job according to the job definition.

The hiring process in SAP IdM context normally starts in the moment when a new employee is registered in the company's human resources management system (e.g. SAP HR, SuccessFactors, etc.). During that process, the new employee is registered for the first time in SAP IdM and receives their unique identifier and pre-defined access according to their job position. To speed up the process of onboarding, it is a good practice to run certain processes before the actual hire date, in order for the employee to be be fully empowered to do their job on Day One. Such process could be the assignment of a hardware (laptop, mobile device) to the new employee.

47 Fu Future actions

91 Hr HR system

17 Hjp HR job/ position

53 Idl Identity lifecycle

5 Ea

Emergency access

Emergency access is critical during when crisis happens. For example, during fire, timing and quick response are essential to save lives and property. Effective emergency access ensures that fire trucks can reach a building in time to extinguish the fire. Pertinent facilities and equipment remain available and unobstructed at all times to ensure effective fire detection, evacuation, suppression, and response.

Emergency access is equally important in IT. Imagine a breach or a critical bug that has just occurred in a productive system and is obstructing your business of functioning correctly. Thousands, if not millions of dollars could be potentially running down the drain and this must be stopped immediately. The worst thing that could happen is if your most skilled rescue personnel has the proper knowledge to solve the problem but does not have the needed access to actually put the solution to work. SAP IdM can provision the needed access just for the needed time interval. Proper monitoring of all actions can be facilitated with SAP GRC.

96 G GRC

14 At Authentication

32 Az Authorization

115 Ra Risk analysis

6
Ss

Self-service

Self-service is a type of electronic support (e-support) that allows customers and employees to access information and perform routine tasks over the network, without requiring any interaction with a representative of an enterprise. In other words self-service means offering customers and employees tools and information so they can find answers to their questions and have a better experience with a product or service.

After the onboarding process has been finished and the initial employee privileges and roles based on their position have been assigned comes a time, when additional access for a side project is needed. Such access can be requested by the employee using self-service. Other self-service tasks could include password change, change of own master data or even some custom tasks defined during the implementation.

The self-service process is vital for SAP IdM, since it removes the burden of IT taking care of everything and gives the control in the hands of the end users.

8 Ux User experience

15 Ui User interface

99 Fi SAP Fiori

7 Wd Web Dynpro

Web Dynpro

Web Dynpro (WD) is a proprietary web application technology developed by SAP SE that focuses on the development of server-side business applications. One of its main design features is that the user interface is defined in an entirely declarative manner. Web Dynpro applications can be developed using either Java (Web Dynpro for Java, WDJ or WD4J) or ABAP (Web Dynpro ABAP, WDA or WD4A) flavor.

SAP IdM utilizes the Web Dynpro Java technology for its standard user interfaces. The interesting thing here is that Web Dynpro forms are generated from scratch using a form configuration in Developer Studio. This makes the approach extremely flexible and easy to adapt.

Unfortunately, Web Dynpro is already quite outdated as web technology. That is the reason why, more and more, you would see SAPUI5 as leading UI technology for new applications, even such running on SAP IdM. Thankfully, there are many frameworks available that transform the standard UI of SAP IdM into a more appealing Fiori UI.

3 Dt Developer studio

99 Fi SAP Fiori

8 Ux User experience

15 Ui User interface

8 Ux

User experience

User experience refers to the singular and accumulated experiences that occur for users as a consequence of them interacting with an object in a given context. True user experience goes far beyond giving customers what they say they want or providing checklist features. Providing high-quality user experience includes services of multiple disciplines, including engineering, marketing, graphical and industrial design, and interface design.

SAP IdM was acquired by SAP at the time when SAPUI5 had not seen light yet. This has determined the UI course for the product – Web Dynpro. Already building the first UI for the product was a challenge, so migrating it from one UI technology to another was out of the question. The user experience topic is pretty much influenced by the web appearance of the product, but there are also other aspects where much can be expected. This really niche topic is thankfully addressed by a number of add-ons that exist, which help raise the product adoption and popularity among end users.

15 Ui User interface

7 Wd Web Dynpro

99 Fi SAP Fiori

1 Wrf Workflow

9 Os

Organizational structure

Organizational structure is a system used to define hierarchy within an organization. It identifies each job, its function and where it reports to within the organization. This structure is developed to establish how an organization operates and to assist in obtaining its goals to allow for future growth. Such structure is illustrated using an organizational chart.

The organizational structure of the enterprise plays a very important role during the design and implementation of an SAP IdM system. A lot of information can be derived from the way the structure is defined. For example line manager rules can be extracted from the org. structure and assigned automatically in IdM. This would also automate any changes that might appear – e.g. a manager leaving the company would automatically re-assign all existing employees to the new manager. Additionally systems like Active Directory could be directly dependent on the org. structure, thus making it a key component during provisioning and de-provisioning.

114 Pi Provisioning

116 Dpi De-provisioning

108 Lm Line manager

90 Ad Active directory

10 Dq

Data quality

Data quality is a perception or an assessment of data's fitness to serve its purpose in a given context. The quality of data is determined by factors such as accuracy, completeness, reliability, relevance and how up to date it is. As data becomes more intricately linked with the operations of organizations, the emphasis on data quality gains greater attention.

As any other system dealing with important employee data, SAP IdM makes no exception in terms of data quality metrics. Especially if the concept of SSOT (Single Source Of Truth) is implemented, then the system is regarded as the master for any information related to the identities that reside in it. Any kind of inconsistency when it comes to the accuracy, completeness, reliability, relevance or actuality of the data can be categorized as a critical issue. Therefore, one of the most important aspects during the design and implementation of the system is to make sure that data quality is always preserved .

2 Sst Single source of truth

86 Di Data integrity

26 Id Identity

54 Gp GDPR

11 Db

Database

A database is a collection of information that is organized so that it can be easily accessed, managed and updated. Computer databases typically contain aggregations of data records or files, containing information about transactions or interactions with specific counterparts. Databases vary according to their structure and internal operations – e.g. Relational DB, In-memory DB, noSQL DB, etc.

The database is the most important component of an SAP IdM system. There is a simple explanation to that – every important piece of information – from the configuration of the display forms, through the assignment of the privileges, the audit trail, the values, the logs, even things invisible to the human eye – are persisted in the IdM database. In case of a disaster – it is absolutely essential to ensure that you have a recent backup of the database to restore operations as fast as possible. Although being a relational database, SAP IdM DB is offering a serious amount of flexibility due to its column-based tables structure.

87 Icp IdM components

27 P Privilege

24 Ag Assign-ment

117 At Audit trail

12 Cp

Change position

Change position is an HR process that happens whenever an employee is moving from one department to another within the organization or changes their job description due to internal reorganization in their department. Often position changes are directly related to the way an employee moves on their career ladder. This might or might not be associated to any pay raise or more responsibilities.

The change position process within SAP IdM is one of these having the least standardization. This is because every enterprise has its own internal procedures about how things should happen during such an organizational change. Some prefer hard conditions – e.g. remove all previous access from the old position, assign new access for the new position, while others prefer a more smooth transition, where the employee would still have access to their old roles/privileges for a certain period of time so they can coach or help a potential new signing with their tasks on the new position until they are able to perform on their own.

1 Wrf Workflow

114 Pi Provisioning

116 Dpi De-provisioning

25 A Access

13 Re

Reports

A document (electronic/paper) containing information organized in a narrative, graphic, or tabular form, prepared on ad hoc, periodic, recurring, regular, or as required basis. Reports may refer to specific periods, events, occurrences, or subjects, and may be communicated or presented in oral or written form. Reports are often following a specific format depending on the audience to which they will be presented.

Reporting within SAP IdM plays an important role in informing the security owners on how the system is performing its job, whether any adjustments are needed and of course if any inconsistencies exist that need addressing.

Reports are often requested by auditors to trace assignments of critical privileges to individuals. Those should include the reason why the access was requested and the belonging approvals that led to the actual assignment.

SAP BW and Lumira have established themselves as the standard reporting tools for SAP IdM. Overnight jobs sync the data to those tools and reports are generated there.

22 Jb Job

10 Dq Data quality

25 A Access

86 Di Data integrity

Authentication

Although authentication is not carried out directly by SAP IdM, the system has an important role in the process, which precedes the authentication itself. Alongside IdM, SAP is also delivering an identity provider service that could actually carry out the authentication. The IdP is running on SAP NetWeaver Java and supports SAML 2.0 assertion authentication requests. Logically, in order to verify an identity, it should first know of its existence. Check is done against the underlying UME of SAP NW. Here comes the role of SAP IdM that should provision the user to the respective UME before an authentication request is started.

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if user's credentials match the credentials in a database of authorized users or in a data authentication server. The process only verifies the identity but does not provide any explicit privileges/roles checks.

15 Ui

User interface

In IT, the user interface (UI) is everything designed into an information device that a person may interact with. This can include display screens, keyboards, a mouse and the appearance of a desktop/tablet/mobile. It is also the way through which a user interacts with an application or a website. The UI is one of the components that has a direct impact on the user experience of the complete product/solution.

SAP IdM standard user interface relies on Web Dynpro. An UI technology that is long-time outdated, unintuitive and mobile un-friendly. Unfortunately, replacing the standard UI with another technology is not a trivial task due to the high complexity and flexibility of the current user interface. Following the configurations of the IdM UI forms, the runtime UI is rendering respective fields, entry types and assignments on the screen. The selected approach, although smart, makes the re-creation of the UI a tough task. Thankfully, SAP partner companies have found a way to break the tradition and generate fully functional SAPUI5 interfaces.

8 Ux User experience

7 Wd Web Dynpro

78 F Form

79 Et Entry type

16
Va

Validations

Assessment of an action, decision, plan, or transaction to establish that it is correct, complete, being implemented (and/or recorded) as intended and delivering the planned outcome. Validations can be automated, manual or guided. Clearly, it is preferable to implement fully automated validations to simplify the input of the end user, but this is not always possible. In those cases it is considered a good practice to at least provide a guide on how the end user can perform a manual validation.

Due to the complexity and flexibility of the SAP IdM solution, validations are built throughout its user interactions to ensure error-free input and illogical operations.

Although the validations give a helping hand, they do not show you one "best way" to do a certain thing, neither would they object if you try to create an endless loop of connected jobs.

The human factor in implementing SAP IdM still cannot be neglected and the requirements of the companies are only getting more complex. That is why sometimes it is necessary to build your own validations that make sure the system runs stable and according to the specifications.

8 Ux User experience

34 De Derivations

22 Jb Job

6 Ss Self-service

17 Hjp

HR job/position

An HR job/position is a written narrative that describes the general tasks, or other related duties, and responsibilities of an employee. It may specify the functionary to whom the position reports, specifications such as the qualifications or skills needed by the person in the job, information about the equipment, tools and work aids used, working conditions, physical demands, and a salary range.

At the end an HR job/position can be broken down to the attributes that are maintained in the human resources management system. For example if an employee has to work in a certain plant, then the plant number will be assigned to their personnel record giving indication about the above. A close analysis of the HR record of each employee can give us a lot of valuable information, which can be put to work with SAP IdM. Using an Authorization Matrix it is possible to create a mapping between important attributes of the employee and the access that they need in order to carry out their duties according to the HR job/position they currently have.

9 Os Organizational structure

118 Au Authorization matrix

91 Hr HR system

77 Att Attribute

18 M

Monitoring

Supervising activities in progress to ensure they are on-course and on-schedule in meeting the objectives and performance targets is defined as Monitoring. In IT monitoring is regarded as low-qualified, but high-importance task. Sometimes this contradiction is leading to false alarms or in the worst case late notification to more qualified personnel. For a proper monitoring, it is critical to monitor the correct controls and have a proper automated notification in place.

Since SAP IdM is relying for its operation on the underlying database, it is quite clear that one of the main monitoring targets for the system would be exactly the database itself. However, metrics like throughput, remaining free table space, buffers state, speed of SQL query execution, etc. may not provide answers to questions like – why my provisioning runs slow, why is my SAP IdM system at a standstill, etc. Those can only be answered if important parameters in the IdM specific tables are monitored and proper thresholds are established. Thankfully, you do not need to know all those, since several companies are already providing a solution to the problem that runs out-of-the-box.

11 Db Database

55 Aon Add-on

114 Pi Provisioning

61 Sq SQL

19 Dbp

Database procedure

A stored procedure is a set of Structured Query Language (SQL) statements with an assigned name that are stored in a relational database management system as a group, so it can be reused and shared by multiple programs.
Stored procedure can access or modify data in a database, but it is not tied to a specific database or object, which offers a number of advantages.

It is no wonder that in a database-driven solution, such as SAP IdM, database procedures play an extremely important part. Repeatable operations that run on DB level are implemented as procedures to simplify and streamline the product development. However, this comes at a cost. The product supports various database vendors and those do not have an aligned SQL language syntax. This means that procedures should be written as generic as possible and the result is sometimes complex and hard to understand SQL statements. On top comes the fact that the same DB was used for previous releases like 7.2. So old and new database procedures should live next to each other in harmony. Easy, right!?

11 Db Database

61 Sq SQL

20 Rh

Re-hire

Re-hire is an HR process of an ex employee/external returning to the company, where they used to work before. The employee most often is recovering their previous employee id and record, while being assigned new job position, responsibilities and chain of command.
Apart from the above differentiation, a re-hire process is much like a regular hire from HR perspective.

A re-hire process is not the most common HR action that happens in one company and therefore it is often neglected during the implementation of SAP IdM. However, due to its complexity, automating exactly this process can avoid a lot of headaches later. Although often compared with a hire, the re-hire process has its own specifics and those must be obeyed. For example, a returning employee has already an existing record within SAP IdM and there would be no need to generate a new unique identifier, but maybe the person has married and would require a new email address and their new position maybe requires new system provisioning.

91 Hr HR system

4 H Hire

114 Pi Provisioning

73 Uid Unique identifier

21 Q

Queue

A queue is a list of work items that are awaiting to be processed. When a job is sent to a queue, it is simply added to the list of jobs. Computer programs often work with queues as a way to order tasks. For example, when the CPU finishes one computation, it will process the next one in the queue. Often queues might have priorities that distort the sequential order of the processing, where higher prioritized items are processed first.

SAP IdM is an asynchronous processing system and as such it needs to have an order in which it should process its work items. As mostly everything, this order is stored and determined on database level. Unfortunately, it is not very easy to predict the exact sequence in which jobs will be executed. Even though in version 8.0 it is not recommended to start more than one thread of your dispatcher, it is still hard to say which job/task will follow.

When executing processes, synchronization can be achieved using “Wait Tasks” that wait for all child processes spawn from the parent to finish before continuing. This is applicable on entry level.

22 Jb Job

1 Wrf Workflow

23 Ds Dispatcher

11 Db Database

22 Jb

Job

A job refers to units of work or set of instructions that need to be executed. A job includes all the activities involved in completing it end to end. It may include small programs or large processes, depending on the task at hand. Normally jobs are then scheduled using a job scheduler to run on particular intervals of time or at specific times during the day.

The units that need to be executed within one job are known as passes in SAP IdM. There are two main categories of passes – to- and from-passes. Both can be configured in different setups to read/write data both from source/target repositories, a temporary database table or the Identity Center database itself. This makes them extremely useful for any kind of task and once we add also the complex possibilities for scheduling and nesting, the jobs become one of the main building blocks of any SAP IdM implementation. Do not forget that they also need good maintenance and, of course, always a running dispatcher to execute them.

11 Db Database

23 Ds Dispatcher

31 Sh Scheduling

125 Ps Passes

23 Ds

Dispatcher

The dispatcher in SAP IdM context represents a Java service/program that runs on the runtime IdM component of the system. Normally the dispatcher pools the IdM database for any scheduled jobs to be processed. The pooling interval can be configured to optimize performance. Additionally, tasks from the queue will also be processed by an available dispatcher. One SAP IdM system may have more than one dispatcher, but the recommendation is not to have more than one dispatcher per IdM runtime component. Thus, if you need more than one, you should install it on a separate IdM runtime component.

A worker/service whose job is to receive instructions and organize those appropriately for execution. The most important aspect of a dispatcher is their availability and workload processing speed (e.g. how fast they process certain instruction). Another important feature would be the possibility to self-reset in case of error, thus not blocking the processing queue and continuing from where it stopped before the error.

87 Icp IdM components

11 Db Database

22 Jb Job

21 Q Queue

24 Ag

Assignment

The simple definition of assignment would be something that has been assigned to someone. However, if we dig deeper, there are more aspects to it. Such would be the period for which the assignment has been assigned, by whom was it assigned, who requested the assignment, etc. It does not end with the current state of the assignment – equally important is also to know its history, e.g. has it been assigned in the past?

Assignments in SAP IdM can range from business roles, technical privileges, employees, to dynamic groups, custom entry-types and company addresses. Practically anything that is an entry-type can be assigned to another entry. Most common assignments, of course, are those where an employee is assigned a business role, a technical privilege or a manager with all its accompanying information – from when, till when, who made the assignment, why (reason) and who requested it initially. A detailed audit trail is constantly available to track down all historic movements of those assignments.

79 Et Entry type

27 P Privilege

44 Br Business role

117 At Audit trail

25
A

Access

In general, access refers to the permission to use. If you've been given the rights to use a computer or service, you have an authorized access usually granted by entering your username and password or using a certificate. Access can also be a channel of communication that is opened with a software or hardware device such as computer drive, modem, or printer. If the appropriate access is not obtained, the user receives “access denied” or other similar error message.

Access in the SAP IdM vocabulary is mostly used in two aspects. First, for permissions related to the usage of the IdM system itself – e.g. access for the role administrator. The other, more common meaning is when we are talking about the permissions a specific employee/external has in a target connected system – being represented by business roles or/and technical privileges. If particular access is only available in the target system without SAP IdM having knowledge about it, then we are talking about a breach in the SSOT paradigm and a proper reconcile process should be started to sort this inconsistency.

2 Sst Single source of truth

111 Rc Reconciliation

27 P Privilege

44 Br Business role

26 Id

Identity

Shortly, this could be the distinguishing character or personality of an individual. The longer description varies depending on the area of application. Generally in IT, identity is accepted as a term, when we would like to abstract from properties irrelevant for the information processing. Such could be – gender, physical state, hair color, clothing, etc. Although abstracted, each identity must be uniquely identifiable among others, even though sharing same attributes.

The identity is the one of the main reasons why SAP IdM exists. It is its main processor, primary controller and safe-keeper. Identities in SAP IdM vary from employees, through 3rd party contractors, to seasonal workers. All of them are seen as equal identities before IdM. They all need to be catered by the system. Organized in identity stores the identities evolve during their life in SAP IdM representing their identity lifecycle in the company. Each identity must be unique to SAP IdM and therefore each has a unique identifier. That might not be any meaningful peace of information but should be good enough to distinguish one identity from another.

42 Ids Identity store

53 Idl Identity lifecycle

73 Uid Unique identifier

40 U User

27 P

Privilege

A privilege is the smallest possible entity that can give access to a particular functionality in SAP IdM or any connected target system. Privileges are normally loaded from target systems and should be refreshed regularly to maintain consistency. Privileges from different target systems are regularly combined in meaningful business roles to simplify self-service requests and streamline access control. Privileges are stored in a dedicated entry type called ‘MX_PRIVILEGE’. Although it is enough to store only the ‘MSKEYVALUE’ and the ‘Display Name’ in the entry type, it is highly recommended to build privileges with richer information.

Privilege, in the context of computer security, is the concept of allowing users to do only certain things. For example, an ordinary user might be prevented from changing certain data, while a system administrator is typically permitted to do so. A user privilege may be maintained manually or through the IAM system. Manual maintenance hides risks of security breach and thus it is highly recommended to be avoided.

94 Im IAM

80 Yv MSKEY-VALUE

30 Tg Target

79 Et Entry type

28
An

Admin

An administrator or shortly admin is a person who ensures that a system operates in a correct and efficient way. The specifics of their duties vary depending on the type of system they look after, but in general, they are the first to be contacted if something does not look good or behaves strange.

Often admins have more privileges and access than a regular user and that is why they are most often being audited for any irregular activities or misuse of authority.

The admin in SAP IdM has a very important role. It is crucial not to forget their password, since it may prove very hard to recover. Admins were irreplaceable in the old 7.2 release of IdM, but thankfully in 8.0 a proper user access has been introduced alongside the Developer Studio. Although the default owner of each package is its creator, it is possible to assign also other users to the package access. However, the limitation remains that only one user can checkout a package at the same time and if we take into consideration the forced check-in feature, the whole new constellation leads to a better structured development process.

3 Dt Developer studio

37 Ipk IdM package

25 A Access

27 P Privilege

29 Sc

Source

Following the classical definition, a source could be a place, person, or thing from which something originates or can be obtained. In IT terms this is most often some kind of code, system or service, which is designated as source, because particular data is obtained from it. It is common that multiple sources co-exist to feed enough information to a central system, which after formatting can supply it to a target for further processing.

The term source is most often used in SAP IdM when we are talking about source systems. We call them 'source' for short. Source systems are those systems, which play the role of feeders of information to SAP IdM. Such could be for example a Microsoft Exchange Server, which can be used as the source for the attribute 'email'. Proper definition of the source systems connected to SAP IdM is an important task, which needs to be performed carefully. In order for SAP IdM to play its SSOT role properly, it has to be fed with the most actual and proper information at the very moment it appears at the source.

95 Sy System

77 Att Attribute

2 Sst Single source of truth

10 Dq Data quality

30 Tg

Target

Following the classical definition, a target could be a place, person, or thing that is the aim of an operation. In IT terms this is most often some kind of code, system or service, which is designated as target, because it accepts specifically formatted data for further processing. If target is connected to a SSOT system, then often they are multiple and are being fed with the most actual information from the source to keep them up-to-date.

The term target is most often used in SAP IdM when we are talking about target systems. We call them 'target' for short. Target systems are those systems to which provisioning of data and access is made. A system may be both a source and a target, depending on the setup. For example, an HR system may be target due to an update of its email field from SAP IdM, but also plays the role of a source, since the personnel number of the employee is updated from SAP HR to SAP IdM. Normally proper triggers are set in place, so that whenever fields or access updates in SAP IdM happen, they are immediately sent to the correct targets.

91 Hr HR system

2 Sst Single source of truth

114 Pi Provisioning

29 Sc Source

31 Sh

Scheduling

Scheduling is a functionality that was natively built in the old management console of SAP IdM 7.2. It allowed users to define job executions using different options like specific times, reoccurring slots and even build chains of job executions. Unfortunately, this functionality lost its end user interface during the migration to v. 8.0. The new Developer Studio provides only a few pre-defined options for scheduling jobs and those options can run out very quickly. Thankfully, the backend functionality in the database was kept intact and following the SAP Note 2729037 it is possible to create your own rules. The other option would be to use the free add-on from ROIABLE.

Scheduling could have different meanings, but for our purposes let’s adopt this one - determining when an activity should start or end, depending on its duration, predecessor activity (or activities), predecessor relationships, resource availability, and target completion date of the project. Each mature IT system should provide means of creating scheduling rules, which could significantly simplify its operation and monitoring activities.

22 Jb Job

3 Dt Developer studio

11 Db Database

55 Aon Add-on

32 Az

Authorization

Authorization is a security mechanism used to determine user/client privileges or access levels related to system resources, including computer programs, files, services, data and application features. Authorization is normally preceded by authentication for user identity verification. During authorization a system verifies an authenticated user's access rules and either grants or refuses resource access.

Authorization, same as authentication, is not carried out directly by SAP IdM. The system has an important role in the process, which precedes both security mechanisms. Authorization is normally carried out by the service provider following specific rules. Often those are calculated by the presence or absence of a particular role assigned to an already authenticated user. Here comes the role of SAP IdM, which should provision the proper roles for the user so that the authorization is successful. In web applications absence of the role being checked leads to 403 HTTP Forbidden responses, which obstruct the user from accessing the requested resource.

84 Sv Service provider

14 At Authentication

114 Pi Provisioning

25 A Access

33
Pw

Password management

Passwords are a set of characters provided by users during authentication. Although they remain as one of the most often used methods of authentication, they are subject to security threats when mishandled. Password management is a set of principles and best practices to be followed by users while storing and managing passwords in an efficient manner to secure them as much as possible in order to prevent unauthorized access.

SAP IdM offers password management for all connected systems through the so-called password hooks. The mechanism allows setting both productive and temporary passwords. Respective settings should be configured both in SAP IdM and the target system to allow secure operations. One general drawback of the standard password management is the absence of any kind of progress feedback and the fact that only one password can be defined for all systems/accounts of the currently logged-in user. Thankfully, there are add-ons that can solve this challenge and drastically improve the user experience of the end users.

8 Ux User experience

55 Aon Add-on

30 Tg Target

72 Ac Account

34 De

Derivations

The action of obtaining something from a source or origin following specific guides/rules. In order to make sense, derivations are mostly automated. Their main purpose is to reduce as much as possible the manual input by the end users of data, which can be computer calculated. Even when such derivation is not 100% determinable, it is still regarded as useful to show a set of possible options for the user to choose from.

Derivations in SAP IdM are often hidden for the human eye, since they happen in the background. For example, a simple request for a role/privileges generates a number of objects in the database, which are derived from the events that appear throughout the whole process. That is why sometimes it is very hard to track everything happening in the product for a non-skilled person.

The human factor in implementing SAP IdM cannot be neglected and the requirements of the companies are only getting more complex. That is why sometimes it is necessary to build your own derivations that make sure the system runs stable and according to the specifications.

16 Va Validations

11 Db Database

6 Ss Self-service

25 A Access

35 Ex

External

Externals, although being regular identities from SAP IdM point of view, have a special status in most organizations. They are often not part of the corporate human resources system (e.g. SAP HR) and therefore do not fit out of the box in all established processes within IdM. Most companies have outsourced the management of those identities to a third-party system (e.g. AD). Unfortunately, this by itself does not solve the problem related to the fact that externals also need proper handling in IdM. Typically they have expiring contracts, special conditions, more regular permission changes and sometimes urgent requests for access.

When recruiting externals businesses source candidates outside of the organization. Most often those are hired for temporary projects or to fill in for a position. Sometimes big enterprises hire externals to fill in a new technology knowledge gap as mentors, advisors and tutors. It is healthy for an organization to keep a good ratio between internal and external employees, in order to avoid too much dependency on external resources.

5 Ea Emergency access
26 Id Identity
91 Hr HR system
90 Ad Active directory

36 Rd

Role design

Proper role design is very important to facilitate the so-called role-based access control (RBAC). It is probably the most used method in enterprises and that is why roles need proper definitions. Often a good principle to follow would be to build the role with the least access possible and then enrich it gradually as requests come in. Another very effective method to build proper roles is role mining. However, it requires a good amount of history transactions in the system.

SAP IdM offers a great opportunity to build the so-called business roles. They are cross-system and often represent certain position or function within a company. Since IdM is the SSOT, it knows about all available privileges within all connected systems, thus making their combination in meaningful business roles easier. A drawback of this approach is that there should be a person who is pretty well aware of what each position is responsible for and, most importantly, which privileges from which system are needed in order to fulfill their job. Business roles can be loaded also from external tools like SAP GRC, where risk analysis has already taken place.

2 Sst Single source of truth

96 G GRC

44 Br Business role

27 P Privilege

37 Ipk

IdM package

A package is a collection of configuration information, such as constants, scripts, repository types, processes, forms and jobs. It is the smallest part of the configuration that is maintained as a unit. This could be a connector for a repository type or a collection of utilities that are used by other packages. Users are granted access to different packages that allows multiple users to work on the configuration and transport separately.

Packages are a new addition to v. 8.0 of SAP IdM. They streamline the configuration and transport activities within Developer Studio. There are packages delivered during installation by SAP and others that the enterprise can create to customize, develop and enhance the solution further. A package contains two version numbers, a major version and a minor version. Those are used to track the changes within a package. A previous version of a package can be restored and unsaved (not checked-in) changes reverted. Objects within a package defined as public can be called from other packages. Processes, scripts and forms can be public in a package.

3 Dt Developer studio

78 F Form

120 Qn Qualified name

48 Rp Repository

38
Lta

Long-term absence

Long-term absence is an HR process of an employee/external being on absence that spreads longer than a regular vacation or normal sick leave. Most often such is related to maternity/paternity leaves that could extend sometimes to a year or two. Others that fall in this category could be long-term sickness or sabbatical leave. In both cases proper actions are needed to make sure that security remains intact within the organization.

The long-term absence differs quite a lot from other HR processes, since it is neither creating, nor terminating any access/account in the connected systems. Most often actions taken during this HR action are related to locking accounts, which will not be used by the employee/external during their long-term absence. Depending on the case, it could happen that the employee still needs access to their email, so a global lock might not be the best solution. Additionally, reflecting this HR action in SAP IdM needs to take into account that it is expected at some point of time the employee to return to their regular job.

91 Hr HR system

72 Ac Account

25 A Access

85 Lu Lock/unlock

39 Ma

Mass actions

An action involving operations with large volumes of information that belongs to different identities, can be categorized as mass action. Obviously, such actions are available to save time when, for example, the department of multiple identities needs to be updated to one and the same new value due to an organizational change. Other type of mass actions could include assignments of privileges/roles or even locking/unlocking multiple identities.

Mass operations are a critical functionality for every organization with large number of identities in SAP IdM. Expectations are that changing multiple users following a simple filter criteria should be a simple and non-problematic task. While an agreement may be reached with regards to the simplicity, the non-problematic aspect is an issue. Within the standard solution mass actions are handled by uploading CSV files using custom jobs. This is an extremely error-prone approach, which should be executed only by professionals. Luckily, there are add-ons that make things much easier and reduce significantly the risks.

26 Id Identity

10 Dq Data quality

22 Jb Job

9 Os Organizational structure

40 U

User

Entity that has the authority to use certain application, equipment, facility, process, or system, or one who consumes or employs a good or service to obtain a benefit or solve a problem. This is probably the most universal definition of the word ‘user’. However, in the security context users are not necessarily the people operating a solution or solving problems. Often a user in this context is pointing to the identity loaded in the system.

In SAP IdM users can be split in 4 categories – administrators, who have access to most critical functionalities of the system and are able to configure and operate it; key/power users who have more knowledge about the system than a regular user and thus can execute certain jobs/operations which require skilled supervision; system users being technical entities used for communication purposes between connected systems; end users – all identities loaded in the SAP IdM system irrelevant if employees or externals. They all share the same self-service tasks and use the system to simplify their daily lives in terms of security.

6 Ss Self-service

22 Jb Job

26 Id Identity

28 An Admin

41 Ast

Asset

An asset is a piece of software or hardware within an information technology environment. Tracking of assets within an IT asset management system can be crucial to the operational or financial success of an enterprise. Assets are integral components of the organization's systems and network infrastructure. In a broader sense an asset could also be a person, but for the purpose of this definition we will limit it only to non-living objects.

Normally assets are not stored/managed within SAP IdM. There are specialized systems for managing assets and the best practice would be to connect those to IdM and store only a reference of items related somehow to an employee/external. However, when such external systems are not present or their integration requires significant effort, it is possible to maintain assets in IdM. Adapted workflows can even make sure that, for example, laptops and phones are pre-ordered on time so that they are on the desk of the new employee on their first day at the office. One way or the other, assets are important aspect for the 360-degree view of the SSOT.

1 Wrf Workflow

2 Sst Single source of truth

26 Id Identity

53 Idl Identity lifecycle

42
Ids

Identity store

An identity store is a central repository for managing identity information, such as employees, departments, roles, privileges and groups. The information in the identity store can then be used for provisioning and synchronization purposes. An Identity Center may contain one or more identity stores, but only one can be connected to the user interface in SAP NetWeaver Java. The identity store is attribute-based and offers a lot of flexibility during the setup.

The identity store within SAP IdM is the safekeeper of the identity store schema. It is the blueprint about the existing entry types and attributes – both standard and custom. From a job, the identity store can be updated using a To identity store pass. On the other hand, an identity store can be used as a source in all To-passes. For provisioning tasks the identity store is always the source, which automatically means that any information sent to a target system should first be persisted there. This is a good practice that helps achieve the SSOT paradigm without worrying that something might get lost in IdM after being sent to the target system. There could only be one main identity store and multiple others called staging areas.

104 Sta Staging area

2 Sst Single source of truth

22 Jb Job

114 Pi Provisioning

43

Gr

Group

A collection of entities, being persons, roles or privileges, which are considered together as being related following some business rules/meaning. Grouping, if done right, is a concept that simplifies the management and operation of any large enterprise security. Instead of assigning multiple single privileges to a person each time they need to do a particular task, a group can be assigned once and reused later when needed. In this line of words business roles also represent a kind of grouping.

The group concept in SAP IdM has a bit of a different meaning. It could be used as a group of privileges representing certain backend functionality, most often used by Microsoft AD. Other option could be that groups are simply a set of users read from an SAP NetWeaver Java repository, thus representing a number of identities grouped together. Respectively, from the above explanation, the entity type MX_GROUP, which represents groups in IdM, can have assigned objects from the following two entity types -> MX_PERSON and MX_PRIVILEGE. AS ABAP repositories do not support the group concept.

79 Et Entry type

90 Ad Active directory

44 Br Business role

97 Ne SAP NetWeaver

44 Br

Business role

A business role is a semantic group of privileges, normally from different source systems, which build up the required access for an individual to do their job based on certain HR criteria – job description, position in org. structure, etc. Business roles can follow a flat architecture where they do not overlap, but sometimes stacking business roles can help reduce their count and simplify management.

Although business roles are crucial for every SAP IdM implementation, there is no proper user interface for their maintenance. The simplest option would be over the old Web Dynpro interface that however offers maintenance for only one business role at a time. This could be extremely time consuming within large enterprises and therefore an additional option with an upload of CSV file is provided. This option, however, does not provide critical validations of the file and could potentially mess up the data in the system irreversibly. The Authorization Matrix concept comes into play here to help structure and maintain all the business roles properly.

9 Os Organizational structure

118 Au Authorization matrix

7 Wd Web Dynpro

27 P Privilege

45 Sr

Script

A script is a program or sequence of instructions that is interpreted or carried out by another program rather than by the computer processor. Scripts are gaining serious momentum within SAP nowadays since they are easier to learn, simpler to debug and are very undemanding when it comes to consumption of hardware resources. Some of the popular script languages are JavaScript, Python, Ruby, Perl, etc.

The official scripting language for SAP IdM v. 8.0 is JavaScript. In previous releases other scripting languages like Visual Basic were supported, but not anymore. Although JavaScript is rated as one of the most prospering script languages, it is bogged down in IdM due to a very old version support of the runtime. Because of that most of the innovative features of the language have to be re-created in an old-school fashion. On the bright side, there is practically nothing that cannot be achieved using scripts in SAP IdM, including calling Java functions, which by itself opens a wide range of possibilities.

107 Ap Attribute mapping

3 Dt Developer studio

16 Va Validations

34 De Derivations

46 Cx

Context

A context can be defined as the situation within which something exists or happens and that can help explain it. In our IT meaning it is possible to add a reference to a given context that limits the validity of the assignment to a specific context. Such, for example may be a region, a project or an organizational unit. The purpose is to reduce the number of roles needed to depict all possible combinations of the attribute values.

Contexts in SAP IdM should be created in a separate entry type. Then the newly created entry type should be defined as a legal context type in the entry type to which it can be assigned. This is then reflected automatically in the user interface and the inherited assignment of roles and privileges. Conditional context assignments are also possible. They are executed only if the value of the context attribute matches a pre-defined value (list of values) in the parent object. Default contexts are also a useful feature for person entities, where the attribute MX_CTX_AUTO_VALUES contains the default contexts for each context type.

79 Et Entry type

24 Ag Assign-ment

27 P Privilege

44 Br Business role

47
Fu

Future actions

Future actions in SAP IdM are often represented as pending values that are applied when the time comes. The right time for that is determined based on their validity attributes and more precisely on “valid from”. Its value makes the difference, if the attribute will be applied immediately or on a certain date. If the “valid from” attribute is attached to a person, then we are talking about the so-called “future action”. An often-used approach, when we need to hire someone in the future, but we already have the required data in HR upfront and the sync is delivering needed information to SAP IdM. This method is useful also when certain processes need to be started in advance – e.g. request for laptop, phone, etc.

When we talk about the future in IT context, we tend to focus on upcoming technologies and breakthrough innovations. However, if we focus in the area of IAM, the future is something that is not so distant and often related to a period of a couple of weeks, maximum a month. It identifies with the time when a person is entering the IdM system, but certain attributes and/or roles/privileges have future dates and therefore won’t be applied immediately.

77 Att Attribute

91 Hr HR system

41 Ast Asset

94 Im IAM

48 Rp

Repository

In order to use the new provisioning framework delivered by SAP IdM v. 8.0 the proper repository types should be assigned to the repositories. The old repository approach from v. 7.2 won't work with the new framework. The type of the repository is also the decisive element that defines what type of system we are connecting. Most common repository types being connected are on-premise systems like SAP Business Suite, Microsoft Active Directory and cloud platforms like SAP Cloud Platform. From the cloud hybrid scenarios are possible using services like IAS and IPS.

In general terms, a repository can be viewed as a place where information may be stored. For our context, this information could range from connection details through system specific constants to repository type. All this also defines the behavior of the repository, the available parameters and provisioning options. Repositories may be enabled, disabled, copied, exported, imported, created and deleted.

101 Ias IAS

102 Ips IPS

114 Pi Provisioning

95 Sy System

49 Tp

Transport

Transport is the procedure that includes moving software packages from one system to another (e.g. from Development to Quality). Packages are the only unit that can be transported, and they follow a strict version release, which is changed depending on what is updated within the package since it was last checked-in. The check-in process is equally important for the transport, since open packages (not checked-in) cannot be transported.

The transport procedure is built from two steps -> an export and an import. Both can be executed only using the Developer Studio. The export part is easier to handle, since it simply gathers the existing data from the source transport system (each package separately). On the other hand, the import part of the two-step process has certain prerequisites and could go one way or another depending on the content of the target IdM system. A hard condition for a successful transport is that the name of the dispatcher, used within the package being transported, is one and the same in both IdM systems.

37 Ipk IdM package

3 Dt Developer studio

23 Ds Dispatcher

50 Ate

Attestation

Attestation is the process that periodically confirms users' access rights to critical resources. There could be multiple reasons for the periodic check, but the two most repeating ones are manual assignment of critical access, which has not been time-limited, and temporary assignment of access directly in the target system, which is then later identified during comparison with the IdM system as an outcast. Options here allow for access review, which lead either to permanent assignment or removal.

There is no standard attestation process delivered out-of-the-box with SAP IdM. However, building one is dully documented and should be no problem for a skilled professional. The verification itself is done by executing the mentioned process for each role or privilege that needs to be reviewed. For every assignment there could be only one attester, who sees only the assignments for which they are responsible. Logically for such important process, all attestation operations are logged and available in the audit trail. Once the process is triggered, the so-called attestation task is generated in the To Do list of the assigned attester.

1 Wrf Workflow

24 Ag Assignment

117 At Audit trail

25 A Access

51
2fa

2-factor authentication

2-factor authentication (2FA) is a security process in which the user provides two different authentication factors to verify themselves as a result protecting better both the user's credentials and the resources that can be accessed. Two-factor authentication provides a higher level of assurance than authentication methods that depend on single-factor authentication (SFA), where the user provides only one factor – typically a password or passcode.

Logically, since SAP IdM does not play a direct role in the authentication security process, it is even less involved in providing 2-factor authentication. However, same prerequisites apply for both authentication and authorization processes. A user should be provisioned in the system where they are trying to use or setup 2FA. SAP NetWeaver Java offers options for 2FA as part of another SAP solution – Single Sign-On. Often it is installed together with SAP IdM, but neither of the two products should be seen as a prerequisite for the other. They can exist fine as stand-alone solutions, however some features are more streamlined when used together.

57 So SSO

97 Ne SAP NetWeaver

14 At Authentication

32 Az Authorization

52 Idp

Identity provider

An identity provider (IdP) is a system that creates, maintains, and manages identity information for principals, while providing authentication services to registered and trusted service providers. Identity providers offer user authentication as a service. The most often consumer of such service are web applications through SAML2 protocol. In a cloud environment IdPs play a very important role eliminating the need for the user to re-authenticate with every app.

SAP IdM by itself does not provide the functionality to serve as an IdP. However, part of the installation package contains an IdP that can be installed on SAP NetWeaver Java and serve authentication requests to web applications in the landscape. In hybrid scenarios SAP IdM can be seen as the source of the identities master data, which is then loaded in the cloud, for example, in the Identity Authentication Service. IAS is the cloud IdP of SAP and can serve requests to every web application in the cloud, or any on-premise web application with Internet access. Such hybrid solutions are common nowadays before complete IT is moved to the cloud.

14 At Authentication

84 Sv Service provider

64 Sl SAML

101 Ias IAS

Identity lifecycle

An identity lifecycle represents the full cycle of an identity and its access in a given enterprise. From the moment when the person was hired to the moment when they retire or leave the business. In between there could be multiple changes in the identity status like position changes, pay raises, maternity/paternity leaves, etc. All those account to the history of the user, or the so-called identity lifecycle.

The main reason why enterprises integrate IAM solutions in their landscapes is to handle properly and in timely manner the identity lifecycle of their employees – both external and internal. SAP IdM is no different here. Its main priority is to keep the access of the users according to specified rules, update those when next step in the identity lifecycle occurs and respectively terminate as soon as possible any system access, when the user is no longer part of the enterprise. All other features and functionalities of the product are seen as secondary, even if definitely useful and important.

54 Gp

GDPR

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). Since the Regulation applies regardless of where applications are based, it must be heeded by all that target European citizens, even if they don't specifically market goods or services to EU residents.

GDPR defines a set of principles, which form the legal framework. Those also have impact on the so-called rights of an individual. Such are the right to be informed, right of access, right to rectification, right to erasure/to be forgotten, right to restrict processing, right to data portability, right to object and rights in relation to automated decision making and profiling. With most of those, if not with all of them, SAP IdM can help a lot by putting order in the inevitable informational chaos of a heterogeneous landscape. Crucial here is that the SSOT paradigm should be intact. It will guarantee that the information in SAP IdM is actual.

2 Sst Single source of truth

100 Hc Heterogeneous landscape

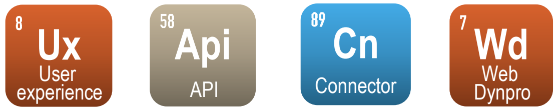
25 A Access

77 Att Attribute

Add-on

An add-on is a software extension that adds extra features to a product. It may extend certain functionalities, add new ones, or simply improve their usability. The concept is popular from leading browsers, which allow add-ons to bring various new functionalities to their products. An add-on should never alter the original functionality of the product. It may provide alternative means of doing the same thing but should never change the original product.

SAP IdM has reached maturity. Certain enhancements and stability fixes are planned for the near future, but its existing functionality won't change dramatically. However, the product has APIs and a connector framework that allow customers and partners to extend and continue developing the solution according to their needs. For example one of the biggest drawbacks to date is the user experience for end users, which is also one of the main showstoppers during adopting. Thankfully, here SAPUI5 can easily come in play with an add-on and deliver an alternative to the old Web Dynpro interface having more user-friendly, mobile-enabled experience.



56
RIt

Return from absence

Return from absence is an HR process of an employee/external joining back after long-term absence such as maternity/paternity leave or longer sick leave. Normally, in such cases all actions taken during the long-term absence should be reverted, so that the person can go back to their regular duties. Sometimes, there are more complicated cases, where during the long-term absence the position was taken by a substitute or the role of the absent employee has changed.

The return from absence can be seen as the opposite of the long-term absence HR process. In most cases, the locked accounts are being unlocked in order to revive the user in all target systems, where they had access before the long-term absence. Partial unlock might be needed, if during the initial lock not all systems were under a global lock. Respectively, such partial lock should be handled with a partial unlock. Critical here is that we do not generate new accounts for the user, or we would overwrite any preferences/settings they have in the target systems. A good practice is to reset the password and send it again to the user.

38 Lta Long-term absence

85 Lu Lock/unlock

95 Sy System

72 Ac Account

57 So

SSO

Single sign-on (SSO) is a session and user authentication service that permits an end user to enter one set of login credentials (such as a name and password) and be able to access multiple applications. In general, SSO can be achieved with different means. Focusing on SAP, the most common ones based on the authentication method are logon tickets, X.509 certificates and Kerberos (SPNEGO).

Within SAP, SSO is introduced through a product with the same name – SAP Single Sign-On. The solution supports on-premise and hybrid scenarios for simple and secure authentication setup. Alongside the single sign-on, two additional important functionalities are introduced – the multiple sign-on, which could be required for critical business applications, and the multi-factor authentication, where the user must provide at least two different authentication factors to verify themselves. A pre-requisite for the SAP SSO product is the availability of SAP NetWeaver Java server, where the solution runs and reuses a number of services already available on the platform.

51 2fa 2-factor authentication

97 Ne SAP NetWeaver

14 At Authentication

64 Sl SAML

API

A set of functions and/or procedures allowing the creation of applications that access the features or data of an operating system, application or other service is called an API. The short abbreviation stands for application programming interface and can be categorized depending on if the APIs are provided or consumed by the product/solution in question. APIs can be programmed in different languages, but the important thing for their consumption is the design pattern used.

SAP IdM is both providing and consuming a number of APIs. On the provider side the most common ones are the REST v. 1 and REST v. 2 interfaces, which expose a large portion of the product functionalities. They are very useful when building new web applications. The REST v. 1 is the predecessor and was popular before the release of SAP IdM v. 7.2 SP8. After that the REST v. 2 protocol is the more often used and the one that will be enriched in future releases. On the consumer side IdM uses a number of BAPIs from SAP Business Suite as well as SAP HR. Through VDS two additional protocols are supported – LDAP & SPML.

59 Vd VDS

66 R1 REST v1

70 R2 REST v2

91 Hr HR system

59 Vd

VDS

A virtual directory server (VDS) offers options to visualize data between applications, directory servers or data stores that are fundamentally incompatible. The virtual directory server is a kind of software operating as a middleware application. It can abstract back-end data from client software applications thus allowing dynamic change of how the data is visualized. In other words, it can offer a unified virtual view from several systems that appear as one.

The VDS delivered together with the SAP IdM installation can provide important features like namespace conversion and schema adaptations to enable a flexible solution that can continually grow and change to support demands from current and future applications without changing the underlying architecture and design of data stores like databases and directories. Commonly VDS is used when connecting to SAP HR through the standard LDAP export. Another interesting usage for VDS would be, if it is connected to the user store of SAP NetWeaver Java – UME. Then the user interface of the user management can be used to browser and create new users in SAP IdM.

62 Ue UME
91 Hr HR system
97 Ne SAP NetWeaver
11 Db Database

60 Pr

Protocol

A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed. The standard framework of the Internet is TCP/IP and the most famous protocols that operate within include UDP, HTTP and FTP. In terms of security protocols - SPML and SCIM are used for identity provisioning.

SAP IdM supports both SPML and SCIM protocols, whereas SCIM is the one that is establishing itself as standard. While SPML relies on XML, SCIM supports an API that speaks REST and the data can be either formatted as JSON or XML. From communication point of view SAP IdM has certain prerequisites in order to support part of its functionalities. For example, the consumption of its REST APIs is possible only if https protocol is used. Same applies if you would like to change the productive password of a target system (e.g. SAP or AD). In those cases secure communication protocol should be established between the system and IdM.

61 Sq

SQL

Structured Query Language (SQL) is a computer language for relational database management and data manipulation. SQL could be used to query, insert, update and delete data. SQL syntax may vary between the different database vendors, referred to as Native SQL, but there are a number of commands that are unified and should be executed in the same manner irrelevant of the DB vendor.

SQL for SAP IdM is like ABAP for SAP Business Suite. If you are good at it, there is nothing you cannot do with the system. Apart from all the job passes and configuration options, where SQL is used within Developer Studio, a lot can also be achieved directly on a database level. It is absolutely forbidden to manipulate data directly in the IdM database, but this goes exactly the other way around, if you only want to retrieve information from there. If you know yourself around the DB schema, you can get some amazing reports in no time. As a DB-based solution SAP IdM also has a serious amount of database procedures, which can be reused.

11 Db Database

19 Dbp Database procedure

3 Dt Developer studio

13 Re Reports

62 Ue

UME

The user management engine (UME) is a centralized user management for all Java applications. It can be configured to source its user data from multiple data sources like ABAP, LDAP or VDS. It is seamlessly integrated in SAP NetWeaver Java as its default user store and can be administrated using its administration tools. UME has a very extensive Java API, which can be used to build additional extensions or add-ons.

UME plays an important role for SAP IdM in a couple of aspects. First of all, since the user interface is running on SAP NetWeaver Java, this also automatically means that UME is the central place to assign UI related roles for SAP IdM. Second, the Developer Studio is connecting to the database using an Application resource again from SAP NetWeaver. On top SAP SSO is also based on SAP NetWeaver Java. Third and last, UME can be connected to a VDS to act as a browser or/and initiator of creation for new identities within the SAP IdM identity store. Not to forget is also that UME is one of the standard supported target systems that SAP IdM can provision to.

3 Dt Developer studio

57 So SSO

97 Ne SAP NetWeaver

59 Vd VDS

CUA

CUA or central user administration is an ABAP based resource for managing centrally large number of users that exist in multiple ABAP systems within the SAP landscape. Although limited to only ABAP-based systems, it is useful for complex landscapes with a lot of manual maintenance. Since the release of SAP IdM, CUA has been an outcast, although there are scenarios, where both solutions can work in parallel.

SAP IdM has been named the terminator of CUA, but that neither happened, nor will it happen in the future. The reason for that is quite simple – both solutions more complement themselves rather than competing against each other. If CUA is already implemented and working in a rather homogeneous SAP landscape, there is nothing easier than connecting SAP IdM directly to CUA, instead of every individual SAP system. On top CUA definitely knows better how to distribute an ABAP privilege the right way, it just needs the proper command from the central mind – SAP IdM, in order to do so.

40 U User

27 P Privilege

114 Pi Provisioning

116 Dpi De-provisioning

64
Sl

SAML

Security Assertion Markup Language, shortly SAML, is an open standard for exchanging authentication and authorization data between parties, in particular between an identity provider and a service provider. SAML is an XML-based markup language for security assertions. It is one of the most common used languages for web applications and is widely supported by multiple vendors, among them also SAP.

SAP IdM has a web-based part and this is its user interface (not based on Developer Studio). A whole IdM component being deployed on SAP NetWeaver Java is responsible for the rendering of the dynamic Web Dynpro UI. These web applications as well as any new SAPUI5 apps, built using the REST APIs of SAP IdM, can take advantage of SAML authentication/authorization. The SAP NetWeaver Java server is fully capable of delivering this functionality and can even act as Identity provider for other web apps through the additional IdP component delivered as part of the SAP IdM installation package.

52 Idp Identity provider

84 Sv Service provider

97 Ne SAP NetWeaver

87 Icp IdM components

65 Si

SCIM

System for Cross-domain Identity Management, or shortly SCIM, is a standard for automating the exchange of user identity information between identity domains or IT systems. It is becoming a kind of enterprise standard for web applications that are open to being controlled from outside identity providers. Within the SAP portfolio SCIM is supported by the following security-related products: SAP IdM, SAP IAS and SAP IPS.

Since SAP IdM v. 8.0 SP5, there is a new standard connector for SCIM 2.0. It allows for seamless communication and provisioning of identities from on-premise to other (cloud or on-premise) systems that support the standard. The hybrid security scenario is based on this connector. It establishes a link to SAP IPS that is used to provision to multiple target cloud systems. This way the information within SAP IdM is reused also for the cloud landscape of the enterprise without exposing the information within to the outside world. If however the scenario requires data to be stored in the cloud, SAP can connect to IAS, which also supports SCIM.

52 Idp Identity provider

92 HI Hybrid landscape

102 Ips IPS

101 Ias IAS

66 R1

REST v.1

Representational State Transfer (REST) is a software architectural style that defines a set of constraints to be used when creating Web services. Web services that conform to the REST architectural style, called RESTful Web services, provide interoperability between computer systems on the Internet. Most often data transmitted with REST services is either JSON or XML formatted.

REST v. 1 is the old web API exposed by SAP IdM until v. 7.2 SP8. Up to that release this was the only option to use services to build custom web applications. For those who are used to the new REST v. 2 API, the old one may look awkward and it is incompatible with the new one. REST v. 2 is not a real successor of REST v. 1, rather a completely rewritten API that initially used odata4j library and lately switched to Apache Olingo due to supportability issues. REST v. 1 is limited with regards to the supported HTTP methods, covering only GET and POST. It doesn’t offer expanding and the only supported data format is JSON (non-ODATA compliant).

70 R2 REST v2

68 Js JSON

69 X XML

58 Api API

67 Sp

SOAP

Simple Object Access Protocol, or shortly SOAP, is a messaging protocol specification for exchanging structured information through web services in computer networks. Its purpose is to provide extensibility, neutrality and independence. It uses XML for its message format and relies on application layer protocols, most often Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.

SOAP is probably one of the few messaging protocols that are not integrated and supported in SAP IdM by default. To consume SOAP services you would need VDS. Alternatively, because of the openness of the SAP IdM product, it is possible to build your own SOAP connector that can consume mostly any kind of SOAP services. There are even add-ons on the market that allow you to generate the structure of the input/output directly in Developer Studio to reduce the time needed for the integration. Popular solution that uses SOAP for example is Success Factors.

69 X XML

59 Vd VDS

3 Dt Developer studio

58 Api API

68
Js

JSON

JavaScript Object Notation, or shortly JSON, is an open-standard file format that uses human-readable text to transmit data objects consisting of attribute–value pairs and array data types. It is a very common data format used for asynchronous browser–server communication used by both REST and ODATA services.

JSON is somehow not directly related to SAP IdM. Rather their relation comes through the available APIs – REST v. 1 and REST v. 2. Both support JSON as format for transmitting data between the IdM server and the browser making the call. Lately, JSON has been preferred instead of XML due to a number of reasons like faster parsing, readability of the raw data (better formatting) and less volume due to less tags needed. Of course, XML has its own advantages in some cases, for example it is better supported by desktop applications. For web applications built with JavaScipt like SAPUI5, JSON is the preferred choice.

58 Api API

69 X XML

66 R1 REST v1

70 R2 REST v2

69 X

XML

EXtensible Markup Language, or shortly XML, is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is a common data format for asynchronous browser–server communication used by both REST and ODATA services.

XML is more popular within SAP IdM than JSON. Apart from being used also for the available APIs – REST v. 1 and REST v. 2, it is in the roots of how VDS builds its data representations. Additionally, the new IdM transport packages also use XML to describe their contents. Somewhat hidden, but important functionality like 'jobs' is using XML to store its information in the database. Understandably XML is much better supported by desktop applications than JSON and this is an area, where its usage is predominant. Another benefit of using XML is that we can apply XSLT transformations, which are popular among developers.

58 Api API

59 Vd VDS

22 Jb Job

37 Ipk IdM package

70 R2

REST v.2

Representational State Transfer (REST) is a software architectural style that defines a set of constraints to be used when creating Web services. Web services that conform to the REST architectural style, called RESTful Web services, provide interoperability between computer systems on the Internet. Most often data transmitted with REST services is either JSON or XML formatted.

If we talk about REST v. 2, we cannot uniquely identify which release of SAP IdM we exactly refer to, because the interface itself is available already with SAP IdM v. 7.2 SP8, but its completeness and implementation differ significantly from the latest release at the moment, which was posted with SAP IdM v. 8.0 SP6. Alongside the change of the used library from odata4j to Apache Olingo, a lot of additional functionality was exposed like for example the option to create new objects. With the latest additions the API has become a standard for building web applications that need to exchange data with SAP IdM.

58 Api API

68 Js JSON

69 X XML

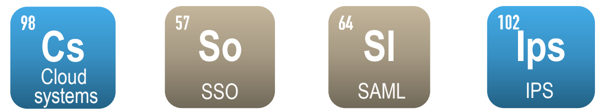
66 R1 REST v1

71 Oa

OAUTH

OAuth is an open standard for delegated authorization. One of the main differences to SAML is that OAUTH does not deal with authentication. Its main usage is with mobile scenarios or it's also popular when consuming ODATA services from SAP Gateway. The good news is that OAUTH and SAML can be applied together where the SAML Assertion is used as an OAuth Bearer Token getting the best of both standards.

The scenario involving OAUTH authorization is a bit distant to an enterprise environment, where one would configure single sign-on between the required systems and be done with it. In a cloud setup however, things look different. Very often the provided resources are not hosted by one and the same organization and such SSO is not possible. In this case OAuth ensures that only permissions for the requested resources are granted to user and application, but access to other resources is denied. Similarly, SAP IdM can use OAUTH to get access to the cloud IPS, but not to the other services available on the SAP Cloud Platform.


98 Cs Cloud systems

57 So SSO

64 Sl SAML

102 Ips IPS

72 Ac

Account

An account is an established technique for connecting a user and an information service and/or computer network. User accounts determine whether a user can connect to a computer, network or similar. User account is one of the methods to authenticate to a system and receive the necessary access to resources of that system. A user technically is not limited to only one account per system.

Accounts in SAP IdM play a very important role in the access provisioning and de-provisioning processes. An identity within IdM has as many accounts as connected target systems where this identity has access or is created as a user. Often each account represents a combination of important parameters that identify the user in the respective system as unique. For AD it could be the SAMaccountname, for SAP just the logon name, for other third-party systems it could be the email address. In the best-case scenario accounts can be disabled, enabled, locked and unlocked separately without having to go over a global lock or global disable process.

26 Id Identity

114 Pi Provisioning

30 Tg Target

90 Ad Active directory

73 Uid

Unique identifier

A symbolic identification code that is attached to an item or business entity, which is exclusive to that particular entity. Often, this can be a serial number or similar identification. In this case we need the unique identifier to be able to tell one identity from another within SAP IdM. Thus the unique identifier can be practically anything that does not duplicate among identities.

Although a sequenced numbering of the identities within SAP IdM is often used approach, it is not necessarily the best and most suited one for every purpose. It may work well, if the complete landscape is created from scratch with IdM being available from its first operational days. This, however, is actually a quite rare situation. Most of the companies introduce IdM only when the complexity of handling multiple users and systems gets unbearable to be operated manually. For such cases picking such unique identifier that can easily match identities across multiple systems could be a life saver during the initial load.

26 Id Identity

40 U User

95 Sy System

75 Io Initial load

74 Dg

Dynamic group

Dynamic groups are such, where identities falling into the group are not predefined in advance but are determined dynamically (in real time) based on certain attribute values. Although any set of attributes can be used, often attributes like plant, location, manager are used to create those dynamic groups. They have their own entry type, which is called MX_DYNAMIC_GROUP.

As mentioned, members of a dynamic group are determined at the time of resolving a group. The attributes MX_TARGET_FILTER and MX_TARGET_DEFINITION are used to define the members. The following two are seen as the most common usages for dynamic groups: using them as a source for a job to define a selection of entries to be processed at the same time or using them as a constraint for a role. In this case any entries matching the filter for the dynamic group will be defined as members of the role. The same approach can be used to define members that are either allowed or not allowed for a role.

77 Att Attribute

79 Et Entry type

22 Jb Job

44 Br Business role

75 Io

Initial load

The first step when connecting a target/source system, which contains identity data, to SAP IdM is performing an initial load. It represents loading relevant identity data from the source/target system into the Identity Store of SAP IdM. Before IdM can control any identities and assign them roles/privileges it should know about them, so this step cannot be omitted and if executed improperly could lead to an inconsistent state of the IdM system.

Before actually running an initial load in SAP IdM there are a number of things that should be thoroughly checked. Each synced attribute should know its leading system, initial passwords generation should be defined, and a test initial load should be executed before running it productively. During the initial load, the mapping of the attributes should be carried out carefully and identities with the same unique identifier should be merged into the Identity Store, not created as new. Once all systems are initially loaded, we have a snapshot of the current state of the system landscape. This snapshot should be regularly updated to keep SAP IdM a verified SSOT.

2 Sst Single source of truth

30 Tg Target

29 Sc Source

26 Id Identity

76
Y

MSKEY

Although you won’t find the term mskey in common solutions, its actual usage is widely spread in relational databases. Mskey is a key column in a table that is auto-generated with an ongoing increment of one (e.g. 101, 102, etc.). This approach makes sure that every entry in a table will have at least one unique identifier. Additionally, such key is quite handy when we need to operate with complex SQL statements/joins due to its numeric value.

Within SAP IdM the mskey has a bit more important role than just being a key for a particular entry. It is the only attribute that can be considered unique across all identity stores in an SAP IdM installation. Apart from that it mostly inherits all the benefits of a regular relational database auto-increment key and it is often preferred for complex SQL joins and views. Once assigned during creation the mskey remains unchanged in the database unless a physical deletion is performed. Inactive entries also retain their original mskey. All object relations (references) in IdM are built based on mskey.

11 Db Database

61 Sq SQL

77 Att Attribute

42 Ids Identity store

77 Att

Attribute

The IdM definition of an attribute is not much different than the original with some additions. Apart from the obvious properties like name, description and type, there are three additional – a definition if the attribute is single or multi-value, a mapping value for target/source system, if such is maintained, and a freestyle comment. There are also some special attribute types like task and entry reference. The task reference can be addressed either with the TaskID (numeric) or with the Task GUID (string), while the entry reference is always defined using mskey. It is allowed to create custom attributes in any of the identity stores.

In computing an attribute is a specification that defines a property of an object, element, or file. It may also refer to or set the specific value for a given instance of such. For clarity attributes should more correctly be considered metadata. An attribute is frequently and generally a property of a property. However, in actual usage the term attribute can and is often treated as equivalent to a property depending on the technology being discussed.

76 Y MSKEY

42 Ids Identity store

79 Et Entry type

104 Sta Staging area

78 F

Form

A form is a window or screen that contains numerous fields or spaces to enter data. Each field holds a field label so that any user who views the form gets an idea of its purpose. A form is considered more user friendly than free text input because it can guide the user and validate their input. Forms can also include a lot of browser coding, which can make them extremely sophisticated and appealing.

Forms in SAP IdM were previously known as UI tasks. Their old name was probably more self-explanatory, but it was replaced in recent releases of the product. A form, in practice, is a dedicated user interface that is targeting a certain entry and can either view, create or maintain it. A form usually contains the needed attribute definitions (what user sees on the screen), the execution access control (who is allowed to access the form) and some other UI configurational elements (e.g. sections, tabs, etc.). For a quick start SAP delivers predefined forms as a standard package, but it is a common practice that customers also define such themselves.

79 Et Entry type

77 Att Attribute

15 Ui User interface

121 AI Access control

79 Et

Entry type

An entry type is the representation of the identity data according to the schema in the identity store. While SAP delivers a significant number of predefined entry types like MX_PERSON, MX_ROLE, etc., a customer is free to either extend the available ones or build their own entry types. If entry types are defined as searchable, they would also appear in the Manage tab of the SAP IdM user interface thus letting end users search entries from that type and perform different operations using forms. By default the MX_PERSON entry type is set as the identity entry type, but this can be changed using the configuration in Developer Studio.

An entry type is not a very common term when it comes to general IT systems. The closest to it would be something like a predefined type or a user-defined type. The idea is that the simple types provided in most systems are not enough for the IdM scenario. Therefore complex, more metadata-rich types are delivered already by the product out-of-the-box. Customers can also extend those or create brand new ones.

15 Ui User interface

3 Dt Developer studio

78 F Form

26 Id Identity

80
Yv

MSKEYVALUE

Within SAP IdM the mskeyvalue is treated specifically. It is an attribute that is unique within one identity store across all entry types. If we talk about a person, this attribute normally contains something that uniquely identifies the person – e.g. email, employee number, etc. The mskeyvalue is also the username used for logging on to Identity Management user interface and must therefore match the name of the user in SAP NetWeaver Java UME. An additional usage is during provisioning, where the mskeyvalue is used as the main identifier. That’s why there is a prefix recommendation for those entry types mskeyvalues – e.g. ROLE:, PRIV:, etc.

Similar to mskey, mskeyvalue is not found very often in common solutions. Mskeyvalue can again be seen as a unique identifier, but it is not auto-generated, rather defined by the developer (e.g. HOUSE101, HOUSE102, etc.). It can be referred to as a readable mskey, with the exception that it might not be unique in the whole database. This might happen if multiple companies are using the same database for the same application, but different identities (e.g. multi-tenancy).

76 Y MSKEY

62 Ue UME

114 Pi Provisioning

79 Et Entry type

81
En

Email notification

Nowadays emails are an established way of communication between people, but also from machine to a person. The latter are sometimes referred to as automated email notifications since they do not involve any human interaction and are often used to notify a person about the appearance of certain event. A very basic form of such emails are newsletters. Although their content might be prepared by humans, the actual send out is automated.

Email notifications play an important role in SAP IdM being the easiest way of informing a person about what is happening inside the system. A very common use case is to send messages from the SAP provisioning framework. To use email notifications you would need the standard notifications package, which delivers the notification process and prebuilt templates to cover the most common cases. If those are not enough for your use case, you can always build custom notifications using JavaScript and sending them with the function uSendSMTPMessage. Since SAP IdM is open to integrations, using other means of notifications is also possible.

114 Pi Provisioning

37 Ipk IdM package

45 Sr Script

55 Aon Add-on

82 Ar

Archiving

Data archiving is the process of moving data that is no longer actively used to a separate storage for long-term retention. Archived data consists of older data that remains important to the organization or must be retained for future reference or regulatory compliance purposes. In the best-case scenario data archives should be indexed and have easy search capabilities.

The process of archiving is especially important for IAM systems due to the large amount of historical data, which they store. The data dictionary of the database is built using column-based instead of row-based approach. The first is the reason why the solution is so flexible, but also brings to the table the important question of data volumes and performance. To gather all information for a particular person in a column-based table, you need to join it with itself as many times as the number of attributes you would like to select. This operation is extremely costly if the table contains too much historical data that is no longer relevant for the enterprise.

11 Db Database

77 Att Attribute

94 Im IAM

26 Id Identity

83 Tsl

Translation

With a very long list of supported languages we can say that SAP IdM is an international-ready software. Using a special annotation for translated texts (whenever a text has translations in different languages, its presentation label is prefixed by “#”, e.g. #MX_DISPLAYNAME) SAP IdM can output the proper label according to what is defined within the UME property for user language. Automated translation is not possible out-of-the-box and if you define any new attributes, entry types, etc. then you need to take care of translating the visible texts on the screen to the supported languages according to your use case.

The most common definition for translation can be summarized as the process of translating words or text from one language to another. When we talk about it in the IT context, most of the time we are not referring to an actual person who is given one word in a language and they simply output the same word in another language. Often translation is fully or semi-automated, using services that automatically scan the text and output it in the selected language.

77 Att Attribute

62 Ue UME

79 Et Entry type

15 Ui User interface

84 Sv

Service provider

A service provider is a vendor that provides IT solutions and/or services to end users and organizations. This incorporates all IT businesses that provide products and solutions through services that are on-demand, pay per use or using a hybrid delivery model. Sometimes service providers build also identity services to cover the needs of authorization and authentication for their products and services. However, it is often the case that external identity providers are used.

SAP IdM can be seen as a service provider, since it offers a wide range of services for identity access and management. As part of the SAP IdM installation package there is also an identity provider service that runs on SAP NetWeaver Java and can close the cycle without the need of integrating an external IdP. If we look at a broader hybrid scenario including the cloud, there we also have two services - SAP Provisioning Service and SAP Authentication Service – one acting as the service provider, while the other providing authentication and authorization functionality.

94 Im IAM

92 Hl Hybrid landscape

101 Ias IAS

102 Ips IPS

85 Lu

Lock/unlock

The term is popular mainly as a secure mechanism of obstructing operational system access on a device (e.g. mobile, laptop, etc.) by requesting a user to enter again their credentials (e.g. user/password, biometrics, etc.). However, in software terms, lock/unlock could mean more. For example you might have access to your computer/OS, but not be able to access your SAP software in the same time, because your account is locked there.

The term lock/unlock has established itself as a key process within SAP IdM. Apart from being integrated in at least two important HR actions – Long term absence (Lock) and Return from long term absence (Unlock), it can also be used as a self-service for managers and administrators. Sometimes without any HR action there might be a need to lock somebody from accessing the underlying IT infrastructure. MX_DISABLED attribute can be used for that purpose. If set, it will trigger a global lock to all systems where the user has a registered account. Partial system locking is also possible but requires additional custom development.

38 Lta Long-term absence

56 Rlt Return from absence

6 Ss Self-service

91 Hr HR system

86
Di

Data integrity

Data integrity is the overall completeness, accuracy and consistency of data. As you can imagine, if this integrity is broken, then the system credibility is undermined. You cannot rely any more on the data there and until the integrity is restored you are prone to making wrong decisions based on incorrect/incomplete data. Even though this applies to most of the IT systems, it is particularly important for those, acting as a single source of truth.

Data integrity is paramount when it comes to SAP IdM. Acting as a 360-degree single source of truth, it is always expected that data within the solution is complete, actual and consistent. This applies not only to the master data, but also to the access of each single user in the database. Unfortunately, if certain best practices are not implemented, it is easy to break the data integrity of SAP IdM. A simple example is manipulating a user's access directly in the target system without using the provisioning mechanism of SAP IdM. The newly assigned role in the target system is not visible to SAP IdM and thus data integrity is broken.

2 Sst Single source of truth

114 Pi Provisioning

10 Dq Data quality

40 U User

87 Icp

IdM components

Obviously, the term has no meaning outside of the IdM area, but we will focus here on the definition of components as a general term. A component is a functionally independent part of any system. It performs some function and may require input or produce output. A component in software is often represented by classes. Components sometimes communicate with each other in order to produce the expected result for the end user.

SAP IdM can be roughly broken down in 4 components. Those would be the IdM runtime, IdM user interface, IdM database and IdM developer workspace. Each of those play an important role in providing the final product experience/functionality. A regular user would have the most interaction with the IdM UI, while for example an IdM admin will often use the Developer studio, which is part of the developer workspace. The other two components, however, are the real heart of the solution. All configuration and operational data is stored in the database, while the runtime makes sure that those jobs and tasks are executed on the proper environment using a dispatcher.

3 Dt Developer studio

23 Ds Dispatcher

28 An Admin

15 Ui User interface

88 T

Termination

Termination in HR marks the end of an employee's contract with an employer. Irrelevant if it was voluntary or due to the employer's initiative, the end effect is that the employee would no longer need their access to the enterprise IT landscape and respective processes must be triggered. This would also be applicable independent of the fact if the leaving employee was an internal or external hiring (e.g. contractor).

The termination process in SAP IdM context normally starts in the moment when an appropriate HR action is received from the company's human resources management system (e.g. SAP HR). It is also possible to trigger a termination in the future. During that process, an existing employee (internal or external) will be terminated/removed from any existing accounts in the company's landscape. The access is removed permanently, but the master data of the user is not deleted. It is simply marked with the attribute MX_INACTIVE, since it might happen that the same person might be rehired again in the future.

20 Rh Re-hire

91 Hr HR system

72 Ac Account

40 U User

89 Cn

Connector

A connector is usually known as part of a cable that plugs into a port or interface to connect one device to another. In order to bring this knowledge into our context, we might just as well say that a connector is an interface that supports several operations, which are enough to connect one system to another for a specific purpose (e.g. identity management). Connectors use underlying protocols like SCIM, REST, ODATA, SOAP, etc. to transport data between systems.

The more standard connectors an IdM system has to its target repositories the better is the connectivity of this system within a heterogenous landscape. SAP IdM provides a number of connectors out-of-the-box for standard SAP and non-SAP software like Business Suite, Active directory, AS Java, etc. In order for a connector to be fully operational in IdM context, it should support several operations like user creation, modification, deletion, disable/enable, assign/unassign roles and setting up passwords. In the last years a protocol has established itself as a standard – this is the System for Cross-domain Identity Management or shortly SCIM.

65 Si SCIM

67 Sp SOAP

90 Ad Active directory

100 Hc Heterogeneous landscape

90 Ad

Active directory

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.

Active directory plays a very important role in SAP IdM context, since it drastically expands the reach that SAP IdM can have across multitude of applications, which simply support AD out-of-the-box. Having a standard connector for AD, SAP IdM can easily provision users and roles to the directory service, which then can be used to operate other solutions via AD as their main identity directory. It is even possible to split the individual applications within AD as separate repositories in SAP IdM, but this requires a bit of custom development. It is worth the investment, since then you would have truthful reports as to what access is assigned in which applications and not one common repository – e.g. AD.

48 Rp Repository

114 Pi Provisioning

13 Re Reports

89 Cn Connector

HR system

A human resources (HR) system or often also referred to as human capital management (HCM) system is a software that combines a number of processes to ensure easy management of human resources as well as the attached business processes and data that go along with. Such often are employee data storage, manage payrolls, benefits administration and attendance records.

HR is the main source system for SAP IdM. SAP or non-SAP, it is the starting point for any identity lifecycle trigger, no matter if it is new hire, change position, termination, etc. When SAP HR is the main source for employee data, then it can be connected using a standard connector to SAP IdM over VDS and delta sync mechanism can be enabled to reduce the data traffic between the two systems. Apart of this role, HR can also be a target system for SAP IdM. For example if a new employee needs first to be created in Microsoft Exchange to get an automatically generated email address, then this email will be provisioned back to HR from SAP IdM for completeness of the employee record.

29
Sc
Source
59
Vd
VDS
53
Idl
Identity lifecycle
114
Pi
Provisioning

92
HI

Hybrid landscape

Hybrid landscapes in computer terms are those combining two or more different types of environments in order to grasp the best of both worlds. Specifically in SAP context, hybrid has established itself as a best practice, where you can still operate your on-premise investments, but in parallel go forward with innovations in a very agile and rapid-moving cloud environment.

When talking about SAP, the cloud is always the topic that is pushed forward and the one that is developed actively. However, often the question is – how do we secure the new cloud applications. If we would like to integrate those new applications and systems the way we used to do it in the past with on-premise, then the answer is to go for a hybrid approach. Since SAP IdM is an on-premise solution, it can remain the single source of truth for your employees and externals but connecting it to services in the cloud like SAP IAS and SAP IPS opens a new horizon of opportunities with cloud applications.

2 Sst Single source of truth

35 Ex External

101 Ias IAS

102 Ips IPS

93
Iag

IAG

The general business definition of Identity and Access Governance (IAG) sometimes overlaps with Identity and Access Management (IAM). It is more precise, however, to use it in the specific context of assessment and mitigation of the risks related to User access. SAP IAG is a software solution that addresses cloud needs as for example Segregation of duties reporting, which normally are served by on-premise products like SAP GRC.

While IAG is not a one to one reproduction of SAP GRC Access Control in the cloud, it does have some overlapping areas and functionalities. Similar to SAP IdM, IAG can also build business roles and provision those using SAP IPS to different target systems. As a workflow the solution uses the established SAP Cloud Workflow service and SAP Cloud Business Rules. IAG offers also standard connectivity to on-premise SAP GRC to retrieve the risk rules and collections. One distinctive difference that comes up with IAG is that it can also address non-SAP systems, which is not so trivial task with on-premise SAP GRC.

96 G GRC

113 Sd Segregation of duties

44 Br Business role

114 Pi Provisioning

94 Im

IAM

Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place IT managers can control user access to critical information within their organizations. IAM products offer role-based access control that allows system administrators to regulate access to systems or networks based on the roles of the individual users within the enterprise.

Usually IAM solutions bundle additional components like single-sign-on and multi-factor authentication. With SAP those are separated in another product called SAP Single Sign-On. The two main solutions that take care of the fundamental IAM features are SAP IdM and SAP GRC. They contain the necessary information of users' master data and access. Often built as single source of truth, their data integrity is crucial for the correct operation and truthful reporting. One of the most important roles of an IAM system in the landscape it to take proper care of the identity lifecycle of an employee/external, so that they always have the proper authorized access to the IT landscape.

2 Sst Single source of truth

53 Idl Identity lifecycle

57 So SSO

86 Di Data integrity

95 Sy

System

In IT context system is a basic, complete and operational computer, including all the hardware and software required to make it functional for a user. It should have the ability to receive user input, process data, and with the processed data create information for storage and/or output. Systems nowadays can be situated in different environments (e.g. on-premise, cloud, private cloud, etc.), but this should not affect in any way their fundamental functionalities described above.

Looking at systems in SAP IdM context, they may be categorized in four types: source, target, proxy and manual. Source are the systems, regarded as the master for a piece of information, coming in SAP IdM. For example SAP HR is regarded as master for the employee's name, while Microsoft Exchange is the master for the employee's email address. Target systems are simply the receivers of the information stored in SAP IdM – be it master data or access that is being provisioned. Proxy is a special type of system common in hybrid landscapes (e.g. when SAP IdM needs to control a cloud service like SAP IPS). Manual are the systems that are not automatically provisioned by SAP IdM but are still controlled by the process.

29 Sc Source

30 Tg Target

105 Mr Manual repository

110 Ar Automated repository

96 G

GRC

Governance, risk and compliance (GRC) refers to a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations. We can think of GRC as a structured approach to aligning IT with business objectives, while effectively managing risk and meeting compliance requirements.

While SAP GRC has many functionalities, it is the Access control module that is most often connected with SAP IDM in order to achieve more holistic approach. The out-of-the-box integration delivers the needed Segregation of Duties check when assigning new roles to users. GRC ensures no major risks are active in the system and if such cannot be avoided that they have proper mitigation rules in place. Apart from the standard rules framework delivered by SAP, a customer can also expand and build their own custom rules for risk evaluation. The three most common rules sets are R3, Basic and HR based (often used as basis for GDPR).

113 Sd Segregation of duties

54 Gp GDPR

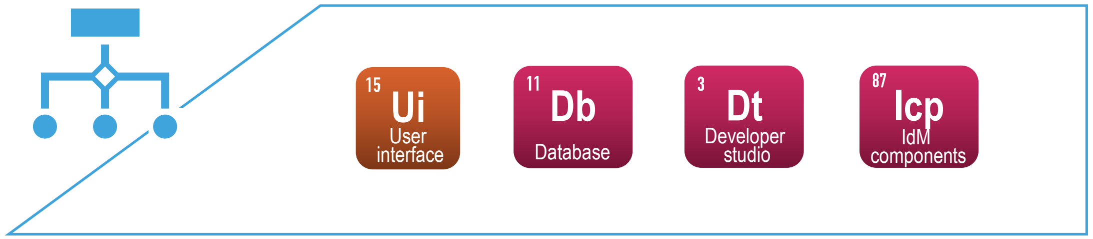
93 Iag IAG

115 Ra Risk analysis

SAP NetWeaver

SAP NetWeaver refers to a technological foundation (platform) acquired by SAP in the beginning of this century. Since 2003 when the first SAP version “NW 2004” was released up to the latest release “NW 7.5” the platform went through massive transformations, but almost 20 years later it still serves multiple use cases with numerous important software products, among which are SAP Process Orchestration and SAP Identity Management.

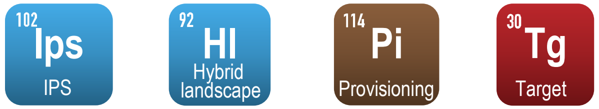
From version 7.3 SAP NetWeaver introduced a couple of new components that run on the platform from the SAP IdM portfolio. The user interfaces – both end user and admin, run on the platform and are accessible with the alias: /idm, or /idm/admin. With version 8.0 SAP IdM expanded even further the importance of the platform by making use of the standard data source resources to establish connections to the database for two purposes – one for the user interface and another one for the newly delivered Developer Studio. Respectively, the connection between the developer workplace and SAP IdM database is not direct, rather first going to SAP NetWeaver and from there to the database.



Cloud systems

A cloud system or cloud computing technology refers to the computing components (hardware, software and infrastructure) that enable the delivery of cloud computing services such as: SaaS (software as a service), PaaS (platform as a service) and IaaS (infrastructure as service) via a network (i.e. the Internet). Cloud systems are part of a model that shifts the computing workload to a remote location.

The most popular cloud systems from SAP are in the SaaS area: SAP S/4HANA and C/4HANA suites and all acquired applications like Fieldglass, Concur, SuccessFactors, etc. The popular PaaS services used to be two – the Neo and the Cloud Foundry platform, but recently SAP announced that strategically they are moving only with CF forward. With such rich palette of software it is no doubt that customers are asking questions about security integrations. SAP were capable to provide a solid answer to those questions with SAP Identity Provisioning Service. Running in a hybrid scenario with SAP IdM on-premise, it can provision to all those target systems in a similar fashion as it is typically done to on-premise systems.



SAP Fiori

SAP Fiori is a design language and user experience approach developed by SAP for use by SAP, its customers and its partners within business applications. The technology behind SAP Fiori is SAPUI5, which became quite popular in recent years and additionally has an open source version called OpenUI5 that can even be used in non-SAP scenarios. Currently SAP Fiori is on the market with its latest version – 3, whose main goal is to equalize the user experience across all SAP products.

Although Fiori is the targeted user experience for all SAP applications, there are some exceptions, which have grown historically with a very complex Web Dynpro auto-generated user interface. Pushing very hard to make big advancements in the Cloud, SAP decided to not invest resources in a challenging redesign of such products considered more or less mature. One of the impacted ones was SAP IDM. At the end it was the SAP partners that started offering an alternative to the customers through their own add-ons. Currently there are several solutions capable to transform the standard Web Dynpro UI into a beautiful SAP Fiori app. The 2 most popular approaches are to rework completely the old UI or to render the already built logic dynamically in Fiori.

100 Hc

Heterogeneous landscape

Heterogeneous landscapes are those built of different types of systems (e.g. vendors, interfaces, applications). Normally customers end up with such landscape trying to adopt best-of-breed solutions in different areas of their business, but even those that are very SAP minded have at least one Microsoft Active Directory that already helps with the heterogeneity.

Homogeneous landscapes are extremely rare nowadays. Proper IAM solutions should be able to tackle the challenges of a heterogeneous landscape without having to make compromises with the quality of service. Although IdM started mostly focused on SAP-based services and products, SAP expanded the portfolio significantly and now together with the cloud services like SAP IAM and SAP IPS they support numerous non-SAP systems like Google G Suite, Azure AD and actually any SCIM-enabled system. The single source of truth becomes even more important in such landscapes, where retrieving information from all systems is equal to a full-time job.

94 Im IAM

101 Ias IAS

102 Ips IPS

65 Si SCIM

101
Ias

IAS

SAP Identity Authentication Service is a cloud service for secure authentication and user management in SAP cloud and on-premise applications. It provides services for authentication, single sign-on, and user management. It is broadly used within SAP and popular there also under the name SAP ID service. SAP IAS can be very useful in hybrid scenarios, when authentication and authorization of end users still need to be re-routed to on-premise IdP, although the app is in the cloud.

SAP IAS can be used stand-alone as an IdP provider, but it has a lot more to offer if it is integrated with the other security offerings of SAP like IdM and IPS. On top SAP IAS also supports delegated authentication, making it ideal for hybrid landscapes and scenarios. Two-factor authentication and social login options allow for higher security and flexibility with customer facing applications. Further enhancements include logon overlay and custom design, self-registration with Google reCAPTCHA or phone verification, risk-based authentication and more. IAS can also enrich the existing information about an employee in order to enable them to use particular cloud services (e.g. additional group assignments in the cloud).

92 Hl Hybrid landscape

102 Ips IPS

57 So SSO

14 At Authentication

102 Ips

IPS

IPS is a cloud-based service from SAP providing robust identity management capabilities, including account creation, user authorization, de-provisioning, and more. It helps you optimize access management processes and meet corporate compliance standards. IPS is also the foundation for a landscape-wide single sign-on scenario in combination with SAP IAS. Additionally, it is an integral part of the hybrid approach together with SAP IdM.

SAP Identity Provisioning Service offers three use cases for connecting systems – source, which is usually the central user store of the enterprise; a target – could be on-premise or in the cloud; or a proxy, which is a special type of connector for hybrid landscapes. It allows to provision entities from one SCIM-based to another external non-SCIM system without making a direct connection between them. The actual provisioning is done through jobs, which can be ran on demand or scheduled. There is one further option for real-time provisioning, but it is available only if the source system is SAP Identity Authentication Service.

101 Ias IAS

65 Si SCIM

114 Pi Provisioning

92 Hl Hybrid landscape

103 Cc

SAP Cloud Connector

In common scenarios like integration between SAP IdM and IAS or/and IPS SAP Cloud Connector is not needed, since IdM establishes a direct connection to them. However, if we would like to expose an application that is implementing the REST v2 interface of SAP IdM in the cloud, then we should setup a Cloud connector, which first exposes the needed path to the APIs, and second connects to the right cloud account, where the app is running. The challenging part comes when we need to take care of the authentication of the end users. In the cloud we can achieve that using SAP IAS, but it should be connected to the same on-premise IdP, which SAP IdM is using in order to facilitate the single sign-on.

SAP Cloud Connector serves as a link between SAP Cloud Platform (Neo or CF version) and on-premise systems. It runs as on-premise agent in a secured network and provides fine-grained control over exposed on-premise systems and resources as well as the cloud applications using Cloud Connector. For productive scenarios it can be used in high-availability setup, which reduces the chance of interrupted communication.

101 Ias IAS

102 Ips IPS

57 So SSO

58 Api API

104
Sta

Staging area

An intermediate storage area between the source of the information and the actual place where it will be stored. Usually it is temporary, and its contents can be safely deleted after a successful transfer to the original target. It could be that the data undergoes certain transformations and validations before being transferred to its final destination. Often it can be used as an assembly point where data from multiple sources is gathered, processed and pushed to the productive area.

A staging area in SAP IdM is simply another identity store with its unique identifier (number) and its attached entry types, attributes, processes, etc. One implementation may have as many staging areas as needed. However, those sometimes add unnecessary complexity and they are not the solution to any data staging problem. A very common scenario where staging areas are used is during the sync with the HR system. Often the received data needs a number of validations and transformations and the staging area offers a very good option to execute those before moving the clean/verified data to the productive identity store.

42 Ids Identity store

16 Va Validations

91 Hr HR system

73 Uid Unique identifier

105 Mr

Manual repository

Manual repositories play a very important role during the initial architecture of SAP IdM. It is common in complex landscapes to be simply impossible to connect all systems to SAP IdM using standard or 3rd party connectors. Even if possible, maybe it does not make sense to invest so much for systems that are probably not updated so often. Here the answer would be to go for manual repositories. Their workflow reaches the important roles within the company for a particular system and gives them very detailed explanations about the access that needs to be granted. Once executed, the information is marked in SAP IdM as completed and the access is attached to the user.

The term manual repository could have multiple meanings, but the one that applies most to our context is: a target system that is connected to SAP IdM, but provisioning of users/access is not automated, rather running through an established workflow. Very often the initial loads for such systems are executed with files exported from the target system and imported in SAP IdM. For the end users the system appears as a regular IdM connected repository.

1 Wrf Workflow

114 Pi Provisioning

30 Tg Target

75 Io Initial load

106 Su

System users

System users are usually those used for machine to machine communication. Other name, which is often used, is technical users. Such are typically restricted from dialog logins and have non-expiring passwords and accounts. Even though there are no real people behind those users, they pose a similar or even sometimes bigger threat to the enterprise, if not managed properly. This is because system users have much more privileges than normal users, which makes them a hot target for a hacker attack.

Although system users do not have an identity lifecycle as most regular users, they can still be managed by SAP IdM. For that purpose, a separate cockpit is built, where such users can be monitored and handled from creation to termination. A best practice is to have at least one real person responsible for a system user and the moment it is not needed anymore, this user to be suspended and later terminated manually by its owner. System users do not simply need special accounts in IdM, but sometimes require completely new processes/branches due to their special status in the target systems. Because of that complexity they are often left out-of-scope for the first phases of an SAP IdM implementation.

53 Idl Identity lifecycle

72 Ac Account

40 U User

18 M Monitoring

107
Ap

Attribute mapping

Attribute mapping is the definition which target system attributes correspond to which identity store attributes. It's a predefined map that can be expanded with custom attributes as long as the connector allows it. Whenever this is not the case, then the connector needs to be extended or separate APIs can be implemented to have access to attributes not listed by default.

Within SAP IdM attribute mapping is delivered as a predefined template for each connector depending on the target system that needs to be connected to the identity store. Once imported those templates can be manipulated in order to achieve the expected result. A skilled consultant can add/remove attributes or even use attribute operators (e.g. {d}). Operators should be applied very carefully, since they are case-sensitive and could lead to drastically different results. Additionally, scripts written in JavaScript can be used for more complex transformations. Important is that every operation triggered by IdM (e.g. creation, modification, etc.) has its own set of attribute mappings, which need to be adapted.

77 Att Attribute

45 Sr Script

58 Api API

42 Ids Identity store

108
Lm

Line manager

A line manager is an employee who directly manages other employees and operations while reporting to a higher-ranked manager. They are responsible also for making sure that their subordinates have the proper permissions in the enterprise landscape to complete their job and achieve their goals. Respectively, an IAM system is a key asset for each line manager, helping them keep an eye on all employee permission requests and delivering them 360-degree reports about the existing access.

Line managers in SAP IdM are often synced together with the employee from the HR system. Normally they are determined based on the organizational structure of the enterprise. Most companies define a structure with only one responsible line manager per employee, but others rely on more complex rule framework, where two or more managers can be line managers for one employee depending on what area of their work is addressed. With standard approval workflows self-service permission requests are first approved by the assigned line manager before being processed to further approval levels or directly assigned to the target system.

9 Os Organizational structure

1 Wrf Workflow

6 Ss Self-service

94 Im IAM

109
Ro

Role owner

Role owner is a popular term with IAM solutions. It represents a person, who is responsible for a particular business role or a set of business roles. Since business roles require good knowledge in both security and business operations, the designated person should periodically review users attached to the role through attestation. They are also often included in the approval process when a self-service request is started for the business role they are responsible for.

The logic used to determine role owners differs from one SAP IdM implementation to another. It is why there is no standard algorithm to achieve that. The most common scenario is to open a form for maintaining role owners by hand or to assign them during the upload of the business roles. Often self-service permission requests include approvals from role owners, so that they are also informed about the ongoing access changes and can make more informed decisions in case they decide to update the business role or revise its assignments through an attestation process.

1 Wrf Workflow

6 Ss Self-service

44 Br Business role

50 Ate Attestation

110
Ar

Automated repository

The term automated repository could have multiple meanings, but the most applicable to our context is: a target system connected to SAP IdM with enabled automated provisioning of users/access. This requires a dedicated connector, which might not always be available and needs to be custom-developed. Connectors themselves and operations like initial load, creation, modification, termination are delivered as templates with the respective connector package.

Automated repositories are the key to the process automation that can be achieved with an SAP IdM system. The more target systems are connected as automated repositories, the higher the percentage of automation would be. However, in complex landscapes it is not common to connect all systems as automated repositories to SAP IdM using standard or 3rd party connectors. Even if possible, maybe it does not make sense to invest so much for systems that are probably not updated so often. That is why a good analysis needs to be executed before moving on with the implementation and only repositories with a lot of self-service requests and/or user/access changes should be fully automated.

105 Mr Manual repository

89 Cn Connector

75 Io Initial load

30 Tg Target

111 Rc

Reconciliation

Reconciliation is a popular term from the accounting world. Its standard definition however should be adapted in order to fit better to the IAM context. So, it is a process that compares sets of records to check that the data and the assignments are correct and in sync (e.g. not dirty). Items that are not consistent are marked with dirty and are then processed additionally by IdM in order to bring the system to an accurate and complete state.

Reconciliation in SAP IdM is executed following a scheduled procedure and ran through a dispatcher enabled for housekeeping. Entries that need to be processed are marked with a so-called “dirty” flag. Manual reconciliation is also possible using the internal function “uIS_PrivReconcile”. Reconciliation is applicable to roles and privileges and is most useful when large sets of assignments need to be recalculated and corrected. Performing it in one synchronous transaction could take very long time and put serious load on the system, thus preventing normal operations. This is unacceptable for a critical system as SAP IdM, so the operation is broken down into smaller asynchronous chunks.

23 Ds Dispatcher

27 P Privilege

44 Br Business role

24 Ag Assign-ment

112 Co

Constants

There are three types of constants in SAP IdM. Those would be repository, package and job constants. The first are normally defined in a template and their values are used to access the data source of a repository. The package constants are only available within the package where they are defined and can be called by jobs, tasks and scripts as long as those are part of the same package. A call from outside the package, though possible, requires a custom package script. Job constants can be used in any field in a pass definition. They are stored in the job definition. All of the above can be accessed using the function “uGetConstant”.

In computer programming a constant is a value that cannot be altered by the program during normal execution, i.e. the value is constant. When associated with an identifier, a constant is said to be "named," although the terms "constant" and "named constant" are often used interchangeably. This is contrasted with a variable, which is an identifier with a value that can be changed during normal execution, i.e. the value is variable.

37 Ipk IdM package

22 Jb Job

48 Rp Repository

45 Sr Script

Segregation of duties

Segregation of duties (SoD) is an internal control designed to prevent error and fraud by ensuring that at least two individuals are responsible for the separate parts of any process/task. SoD involves breaking down tasks that might reasonably be completed by a single individual into multiple tasks so that no one person is solely in control. A common segregation of duties for payroll is to have one employee responsible for the accounting portion of the job and someone else responsible for the payments.

SAP IdM is not capable of executing SoD checks on its own. Here an important role plays the integration with SAP GRC. It is a very common practice to run approval flows with integrated GRC step from within SAP IdM. This way not only the existing assignments are risk-free, but also any future assignment will first pass assessment in GRC and only then it can be assigned to the user in IdM. If risk cannot be eliminated, it should be at least mitigated with a proper mitigation control, which again can be set in SAP GRC. SoD is a very important process within public companies since it is a requirement for compliance with Sarbanes Oxley Act (SOX).

114 Pi

Provisioning

With SAP IdM provisioning can be defined by the creation of objects and setting of attributes in various repositories. It is based on setting number of tasks to perform given actions. Obviously one of the most important things for the provisioning is to have a consistent persistence state of the data. Event tasks on privileges can also trigger the provisioning process. During provisioning the audit trail is updated so that it is easier later to find who did what and when. Additional features like “wait for”, chaining tasks, context variables and possible rollbacks make the provisioning process quite comprehensive solution that can address even complex needs.

Provisioning is the process of coordinating the creation of user accounts, e-mail authorizations and others in the form of rules and roles as well as other tasks like provisioning of physical resources associated with enabling new users or modifying existing ones. To facilitate the provisioning identity management systems normally include a workflow component that moves the process from one step to the next.

77 Att Attribute

24 Ag Assignment

117 At Audit trail

1 Wrf Workflow

115 Ra

Risk analysis

Risk analysis is the process of identifying and analyzing potential issues that could negatively impact key business initiatives or critical projects in order to help organizations avoid or mitigate those risks. One of the common analysis that is available is the Segregation of Duties (SoD). Normally, solutions have a prebuilt set of rules available, but those can be modified and tailored to the specifics of the organization. The analysis includes the identification, mitigation and reporting.

Risk analysis is not performed with SAP IdM. For that purpose is used a module of SAP GRC Access Control called Access Risk Analysis or shortly ARA. Its main function is to perform SoD analysis and it was designed to identify, analyze and solve problems related to the topic. A nice addition is that simulations can be run in order to verify the organizational rules before they are applied productively. The reporting and analysis itself can be carried out on three levels – management, business and technical. This allows users from each area to dig into the details, which are of interest to them. Risks that cannot be completely omitted should implement mitigation controls.

96 G GRC

113 Sd Segregation of duties

128 Mi Mitigation

116
Dpi

De-provisioning

With SAP IdM de-provisioning operates quite similar to the provisioning process by actually modifying objects and setting attributes in various repositories. It is again based on setting number of tasks to perform given actions. Obviously one of the most important factors is to have a consistent persistence state of the data. Event tasks on privileges can also trigger the de-provisioning process. During de-provisioning the audit trail is updated so that it is easier to find later who did what and when. De-provisioning does not necessarily mean deletion in the target repositories. Sometimes data needs to be retained for a certain period and in those cases the users are only disabled, instead of physically deleted.

De-provisioning is the process of coordinating the removal of user accounts, e-mail authorizations and others in the form of rules and roles as well as other tasks like de-provisioning of physical resources associated with disabling users or limiting their access to a particular system. To facilitate the de-provisioning, identity management systems normally include a workflow component that moves the process from one step to the next.

77 Att Attribute

24 Ag Assign-ment

117 At Audit trail

1 Wrf Workflow

Audit trail

Audit trail, also referred to as audit log, is a security-relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. Audit records typically result from activities like financial transactions, scientific research and health care data transactions, or communications between individuals, systems, accounts, or other entities.

The standard audit trail of SAP IdM is stored in the database table mxp_audit, which has a long list of columns that help you identify important metrics about the particular audit - like the task that this audit record belongs to, date when the audit record was created, status of the audit record, reference to the parent audit ID, error message, general information, etc. Although each of these fields has its meaning, one of the most cryptic ones is the general information field – UserID. Its name is misleading, since it may contain information far beyond the userid – like task id, task name, attribute id, entry id, etc. Another approach to building custom audit trails is to store relevant data in custom entry types.

79 Et Entry type
77 Att Attribute
11 Db Database
124 Tk Tasks

118 Au

Authorization matrix

Authorization matrix is one or multiple lists of business roles with their attached privileges from all automated and manual repositories in SAP IdM. It helps keep an overview of what each business role provides as access to the users who have it. After an update to the authorization matrix normally a reconciliation should be executed in order to bring the roles and privileges assignments to a consistent state in the IdM system.

The standard way of building an authorization matrix with SAP IdM is by maintaining large CSV files with all the business roles and their belonging access across the system landscape. However, this approach is very error prone and always requires a skilled person, who will be responsible to upload the files, monitor their processing and potentially find any issues that resulted from the operation. Much better approach would be to have a proper tool, which is ideally web-based and allows you to have features like versioning, validation and collaboration. Thus you can enable your security team to be productive and not always rely on technical personnel.

110 Ar Automated repository

105 Mr Manual repository

27 P Privilege

44 Br Business role

119 Cl

Containers and leaves

Container is an object that can contain references to other objects. A leaf, on the other hand, is seen as an endpoint of a branch and cannot contain other objects. They are often used when hierarchies or assignments have to be designed within IT systems. Containers are characterized by the way they access their children/parents, the way those are stored and the way of traversing the objects within a container.

In SAP IdM context container and leaf objects refer to entry type classes. A leaf object is a single entry type that cannot have children. Such entry type, for example, is MX_PERSON. A container object is an entry type that can contain other entry types. Examples here could be MX_GROUP and MX_ROLE. Following this simple notation, it is very easy to define which attributes are available for use when making references between objects. The attribute MXMEMBER_<entry_type> is typical for containers, while the MX_REF_<entry_type> is used both with leaves and containers depending on the hierarchy we would like to build.

126 Rs References

79 Et Entry type

77 Att Attribute

44 Br Business role

120
Qn

Qualified name

With version 8.0 of SAP IdM a term qualified name entered the vocabulary. Already during install a base qualified name, which cannot be changed afterwards, is requested. It represents a system namespace that should be globally unique (e.g. com.<company>). The qualified name is used as identifier for a package. Public objects also have a qualified name, used when calling them from other packages. Repository types are similarly identified exclusively by qualified name and therefore if we move a repository type from one package to another, its qualified name changes. Same applies to processes. Their names should comply with the qualified name requirements.

In computer programming a fully qualified name is an unambiguous name that specifies which object, function, or variable a call refers to. Normally, the rules for building such qualified names should be part of the naming convention of each project. Often those define a certain prefix that always precedes the objects based on their type and location in the project. The dot notation is helpful to keep the path – e.g. com.sap.idm.processes.<Qname>

37 Ipk IdM package

1 Wrf Workflow

48 Rp Repository

121
AI

Access control

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental security concept that aims to minimize the risks for the business or organization. With IAM systems it is used to regulate the access internally for tools and user interfaces of the product. For example, administrators often have full access to all functionalities of the system, while end and key users have only a subset of the full admin access.

With SAP IdM when we talk about access control in 99% of the cases we mean form access control or who has access to execute certain form. The "on behalf of" options allow the following configurations: "everybody" means basically that this is a form visible to everyone without limitations; "user or identity store entry" can refer to one specific user, privilege, role or other entry type; the last one "relation" is one of the most complex since it supports 5 different modes: "self" for self-service; "<Entry>Manager" – entry for which the user is a manager; "<Entry>Owner" – entry for which the user is an owner; "<Entry>Member" – entry for which the user is a member and "Member of same" where the objects have the same entry assigned.

126 Rs References

78 F Form

79 Et Entry type

94 Im IAM

122
Ey

Encryption

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography. There are many different algorithms that could be used to encrypt a clear text, but some are considered not secure, so you always need to first check if the applied algorithm is still actual. For example 3DES is an algorithm that is no longer considered secure.

Encryption plays an important role in SAP IdM. Its usage comes with multiple aspects. On one hand it is used when encrypting secure attributes like passwords before storing them in the database. On the other hand it is used to encrypt the credentials used for establishing the connection to the database, for example for the dispatcher. The encryption keys should therefore be accessible to all components of an IdM installation. They are stored in a file called "Keys.ini", which could be stored centrally or distributed based on the setup. New keys can be generated on certain period, but it is critically important not to delete any old keys from the file, because this might render unusable all previously encrypted data.

11 Db Database

23 Ds Dispatcher

87 Icp IdM components

77 Att Attribute

Search results

Search results in SAP IdM can be found in the user interface on multiple occasions. The most used though is probably the one in the manage tab, where authorized users can search the available entry types. Others include for example searching for MX_ASSIGNMENTS (e.g. roles and privileges together). Interestingly, a search result is not configured, as some might expect, using a search form. The columns and the data displayed in the table of the search result are purely dependent on the listed attributes of the searched entry type. On the other hand the search form defines only the attributes over which the search query will be executed.

The list of results that a search returns in response to specific word or phrase query is called search results. Regularly, each listing includes some kind of a link that expands more information about the found result. Advanced search results might include a preview of the complete data behind the result as well as a semantic ranking, which helps the users find the best match for their search query quicker.

15
Ui
User interface
78
F
Form
79
Et
Entry type
77
Att
Attribute

124 Tk

Tasks

Tasks in SAP IdM are very useful for performing operations in the identity store or the target system. They always operate on entries such as entry types, attributes and assignments. They split in six types: action; conditional; switch; attestation; approval and wait tasks. Action task contains a reference to a job that is run after the task is executed. Conditional one executes subtasks based on the result branch that is followed as per some condition, evaluated as true or false. Switch tasks are similar to conditional ones, but the result can be any exact match and more than two exits are supported. Approval and attestation are human tasks and perform sub-flow based on result, e.g. approval. Wait tasks are used for synchronization of process branches.

A general definition of a task would be: the smallest identifiable and essential piece of work that can be performed. Important addition for the context we are in is that tasks can be used only as part of a process/workflow. They cannot be shared with other processes, neither can they be called outside of the process, where they were defined. Additional limitation is that they cannot be used as an event (e.g. onOK), for that purpose you need to use a process.

77 Att Attribute

24 Ag Assign-ment

79 Et Entry type

1 Wrf Workflow

125 Ps

Passes

A pass is an atomic unit that executes a piece of work. It could update or read from a repository but could also read from a source system or write to a target one. Depending on their configuration and type different options are available, but passes must always be part of a job and their execution is inevitably sequential within the job to which they are attached. A chain of passes is always executed completely, irrelevant if any of the passes has failed.

Often a collection of passes is responsible for some of the most important jobs within SAP IdM like initial loads, reconciliation or synchronization. Generally, there are two type of passes: “From pass” and “To pass”. The former reads from a source system or file and writes in a temporary database table. The latter reads from a database table and writes to a target system or to the identity store. During the pass execution attribute mapping and cleansing can be performed. A third type of passes is also available, but it is not as popular as the other two. It is “shell execute” – an extremely powerful pass, which can call any shell command, run scripts, start a program, etc.

29 Sc Source

22 Jb Job

30 Tg Target

127 Dl Delta

126
Rs

References

Reference is a relation between objects in which one object designates or acts as means by which to connect to or link to another object. The first object in this relation is said to refer to the second object. The second object is called the referent of the first object. Those relations within SAP IdM are depicted by the usage of two attributes MXREF_<ENTRY_TYPE> and MXMEMBER_<ENTRY_TYPE>.

References in SAP IdM can be bi-directional or unidirectional. The first are automatically created by IdM if two entry types are defined to have relation between each other. Such references are covered by the attributes MXREF_<ENTRY_TYPE> used for referencing a parent entry and MXMEMBER_<ENTRY_TYPE> used for referencing a child entry. The unidirectional references are between an attribute and an entry type. Examples here are many, but some of the standard ones are MX_APPROVERS, MX_MANAGER and MX_OWNER. All of them define a relation to the entry type MX_PERSON, but with different semantics.

119 Cl Containers and leaves

24 Ag Assign-ment

79 Et Entry type

77 Att Attribute

127
DI

Delta

Delta is an incremental approach to load data that only syncs up blocks, which have changed after the first full load or the previous delta run. The differences are recorded either in files or within database tables as hashes. The process involves examining the stored deltas and locating the blocks that have changed since the last load. Changed data, rather than the entire set, can then be sent to the target, which saves computing power and additional network traffic.

Deltas in SAP IdM are commonly used when loading data from connected systems (e.g. for syncing the privileges from a system). The process first marks all loaded entries as "not processed" and before it writes them to the target generates a hash of every record to be written. This is compared to a delta table (if such already exists). If the hash is missing or different, then the entry is written to the target and the new hash is stored in the delta table for future comparison. If hash is already in the table, the entry is skipped. Delta-enabled passes can be useful, but also very dangerous if not configured properly, since they might delete all entries from the target, if for some reason the connection to the source fails and returns an empty result.

125 Ps Passes

30 Tg Target

27 P Privilege

11 Db Database

128
Mi

Mitigation

The elimination or reduction of the frequency, magnitude, or severity of exposure to risks, or minimization of the potential impact of a threat or warning is defined as mitigation. Mitigation controls are used when you want to make certain functionality available to specific users or roles although there are risk violations associated with it.

Mitigation controls are available with SAP GRC and could perform functions like identifying SoD as a known risk, establishing a period of time during which this risk may exist (if monitored) and associates a list of monitors with the control. Mitigation is available for users, roles, profiles and HR objects and it is an important toolkit to move the business forward with well-calculated and monitored risks. Without mitigation controls most of the SoD risk checks can establish a blockage of any assignments, which may delay important business operations and decisions.

115 Ra Risk analysis

96 G GRC

113 Sd Segregation of duties

40 U User

129 Ev

Events

Events allow objects to notify other objects about important activities. Events are in the heart of the SAP IdM clockwork. They trigger the execution of important processes like modification, deletion, provisioning, de-provisioning, etc. Events can start only processes. During that default event context variables are created in the framework. Such context variable for example is #MxEventType, which points to the event type that has started the process.

Events in SAP IdM can be attached to forms, entry types, attributes, repositories, processes and identity stores. Respectively, there are many event types: add – when an entry is added; modify – when an entry is modified; delete – when an entry is deleted; onOK – executed when the outcome of a task is ok; onError – executed when the outcome of a task is error; provision and de-provision – triggered on a repository for respective process to be started; validate – used for starting approval processes; submit – when submitting an UI form; notify – for raising alerts; and last but not least, request complete – triggered when a request is completed in a particular identity store.

77 Att Attribute

114 Pi Provisioning

79 Et Entry type

1 Wrf Workflow

[1] Some references, inspirations and quotes for the general definitions have been used from the following sources:

Websites: sap.com; cio.com; wikipedia.org; techtarget.com; dictionary.cambridge.org; businessdictionary.com; techterms.com; computerhope.com; kissflow.com; study.com; fss.txstate.edu; uxdesign.cc; smallbusiness.chron.com; techopedia.com; zoho.com; investopedia.com
Authors: Neil Miller, Caglar Araz

[2] All names and trademarks of software products and services mentioned herein are owned by their registered owners

[3] This material is provided by ROIABLE for informational purposes only and does not guarantee against any errors or omissions with respect to the material

ROIABLE

sales@roiable.com
+1 (929) 235-9560
+359 (899) 954-027
www.roiable.com