v1.0 | 16 01 2019

White Paper IAM

FLEXIBLE MANAGEMENT OF IDENTITIES, USERS AND RIGHTS

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INDEX

INTRODUCTION

TOOLS4EVER'S IAM

WHERE DOES TOOLS4EVER EXCEL?

CONCLUSION

FOREWORD

The management of business information is rapidly becoming more complex. End users are demanding increasing flexibility and require access to company data and applications from anywhere, on any device, for both cloud as well as on-premise applications.

Due to the workforce's continued decentralization, 3rd party arrangements, and need for flexibility (e.g. contingent labor: self-employed, temporary/contract staff, freelancers, external consultants), more individuals than ever access company networks – from within and outside the organization. Organizations deploy these users in various manners and locations throughout their operations. Regardless of employment type or job function, all employees are increasingly fulfilling expanded roles in their organization that encompass duties beyond their core tasks.

Further, these changes occur in an environment of continually stricter laws and regulations regarding the security of information (e.g individuals' Personally Identifiable Information (PII), government contracts, financial or health data). The government sets increasingly demanding requirements and confronts more and more organizations with annual audits. Meeting these requirements while remaining an agile, decisive, and secure organization has become so difficult that manual management of all this data is impossible.

Identity Governance & Administration (IGA) solutions provide the necessarily technology to rapidly manage your information resources at the speed today's business world requires while providing your organization the tools to ensure security and regulatory compliance. Choosing the right IGA investment enables optimal responses to the latest technology trends (e.g. increasing flexibility, cloud usage, virtualization, Bring Your Own Device (BYOD)). In this heterogeneous technological environment, Tools4ever's Identity and Access Management (IAM) solution offers the ability to manage and control the identities and access rights within the organization. In this case, IAM is part of the total IGA concept and primarily focuses on the management of the identities and users and their accompanying rights.

We can identify the following topics within IGA, whereby IAM focuses on Administration and Authorization:

- Administration is about the creation and management of the identities and the corresponding user accounts. Correctly creating, managing and disabling according to the life cycle processes forms the foundation of this component.

- The goal of Authorization is to ensure the appropriate assignment of rights to a person so that they can access the correct applications and information in order to perform their work activities. Authorization also involves withdrawing these rights when they are no longer needed.

- Authentication concerns the identification of the user relative to the network and logging in. Username and password credentials traditionally accomplished such, but many organizations now increasingly incorporate Multi-Factor Authentication (MFA) via access passes, one-time passwords (OTP), smartphones, biometrics and other means.

DEFINITION OF IDENTITY AND ACCESS MANAGEMENT

This white paper is about Identity and Access Management (IAM). IAM comprises the technology for managing identities and the associated rights to resources across multiple systems and platforms. This white paper presents the IAM solution according to the vision of Tools4ever.

Tools4ever distinguishes the following main components within IAM:

1. **Identity Vault:** To be able to manage all identities, it is necessary to have one location where they can be stored. The IAM Identity Vault offers this ability. Identities from multiple sources can be stored in the Vault and linked to the various users in the different target systems. This allows for the creation of complex links between multiple identities and multiple users. The Identity Vault is a standardized database that is based on Tools4ever's years of experience in connecting source systems (such as HR and Education systems) with target systems (such as ERP, ECD/EPD, and Service Management applications).

2. **Identity Lifecycle Management (ILM):** ILM involves the creation, modification and disabling of user accounts in linked systems and applications – the Administration part of IGA. ILM automates the various processes that, often, are still manually completed. Links with a Source and/or Service Management System are very common here. The topic of Administration in IGA is, in this context, also regularly referred to as automated provisioning and comprises the entire automation of the user account management process.

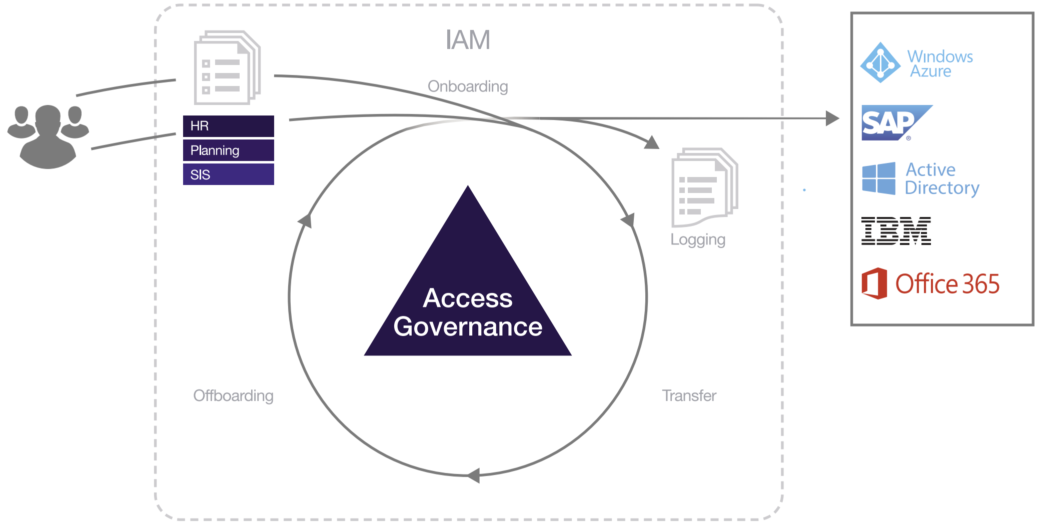
3. **Access Governance:** The primary goal of Access Governance is to ensure users only have access to those applications and resources that are strictly necessary for them to be able to perform their function within the company. Access Governance (AG) contains the techniques and processes to ensure that the access rights are and remain correct. These techniques and processes requiring extra attention include: establishing and managing the authorization matrix, having deviations be approved and checked by the responsible managers, supporting audits, etc. Roles and rights within AG can be assigned both automatically and via a self-service portal. This offers organizations greater ranges of flexibility in properly deploying this functionality.

4. **Workflow and Service Automation:** To make employees self-sufficient and to relieve the service desk, it is possible to have users and managers request roles and rights themselves via the self-service module. The module's execution is automated because these user and manager roles are often the respective requesters and owners.

5. **Logging:** This component keeps track of what takes place in IAM, especially the external actions executed on the target systems. Because the infrastructure often lacks this logging component, IAM offers the ability to perform various activities within the solution in such a way that they can be logged and monitored. This is valuable information that enables audits to check any exceptions occurring outside the processes.

TOOLS4EVER'S IAM

The IAM solution from Tools4ever consists of various components. The correlation among the components is displayed in the following diagram.



GENERAL

The organization provides the authoritative data as the input for the IAM solution. The organization determines, in detail, which IT resources a given individual requires for their role in supporting business processes. Whereas an IAM solution automates the processes ensuring that employees maintain proper access to resources, its absence requires complicated chains of manual processes. Source systems already store individuals' important "who-what-why" data. Source system examples include HR systems or a Student Information System (SIS).

An organization comprises many dynamic processes. Each individual who fulfills a role in a process most likely requires some access to data, applications, facilities and/or other means to perform their duties. Those individuals performing these duties change regularly: people are added, people leave, or people will perform other tasks. The organization of these work activities also changes, albeit less frequently, and includes modifications in departments or learning groups, fusions, reorganizations and changes in compliance laws and regulations (audits).

Individuals in the organization can have different identities, which are often stored as separately within IAM (e.g. employee, student, teacher, caretaker or flex worker). Based on these different identities, IAM can create and manage different user accounts. Source systems still provide all of these identities' information, but do not assist with their proper management. An IAM solution makes managing all of these complex links between identities and users possible.

TRENDS

The most important source of data for IAM is typically the HR system, which maintains information on all relevant persons within the organization. More and more organizations are opting to use the HR system as the core registration system for employees. In other words: if an employee is not included in the HR system, this employee will not receive provisions in the company - lacking an access card, a desk, a laptop, login details, a telephone, etc. This core HR system maintains all of an organization's active individuals (e.g. permanent employees, external staff, volunteers and other contingent workers). Increasingly strict laws and regulations bear some responsibility for prompting these practices.

Another interesting trend seen in IAM systems is that the supplier's HR system continues to add self-service components and that these are implemented as such by organizations. People can view information and implement modifications themselves. For example, employees can immediately see in an HR system such information as salary, days off, function and department. Students can complete relevant data themselves in a Student Information System. This trend results in the source system data being more complete, more current, less contaminated and, thus, of a higher quality. An important side effect is that responsibilities for maintaining accurate data are shifting toward the organization.

Another trend for IAM systems is that many organizations are busy reorganizing their job matrix (number of roles/function profiles). The HR system's more central role makes clarifying the job matrix increasingly important. This means maintaining a small set of roles corresponding to department structures and company hierarchy rather than giving every individual their own customization. This leads to the need for other source systems to supply the correct, detailed information for IAM. An example of this is a scheduling system often used in the healthcare sector. This system includes extra information about which persons work, when and in which location/department. IAM can use this information to arrive at a better assignment of rights as well as to withdraw old, unnecessary rights.

The interface between the source system and the IAM system is an important component of Tools4ever's IAM solution.

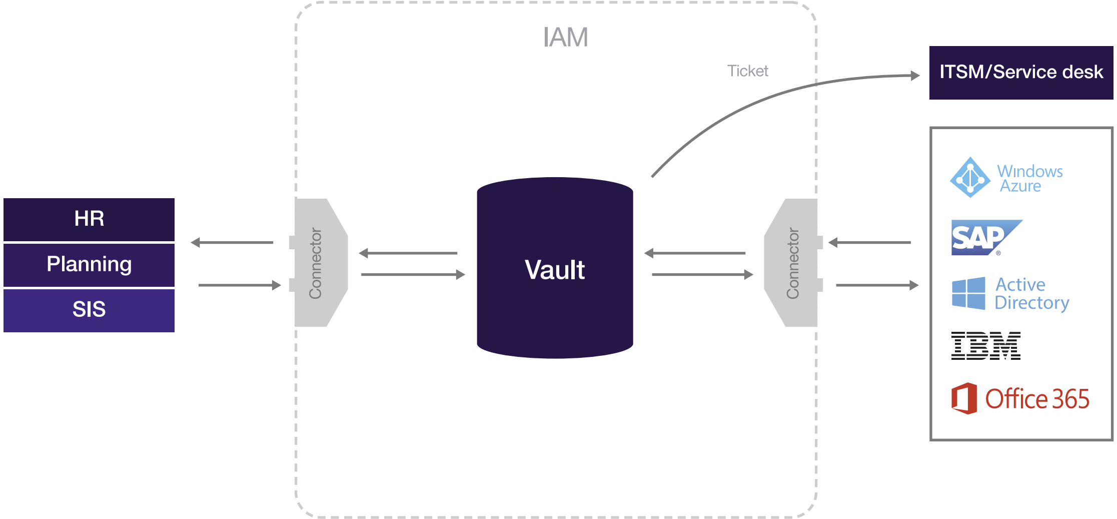
IDENTITY VAULT

The Identity Vault provides the central storage of all identities for all connected systems. The Vault contains identities, rights, relationships and ID references to source and target systems. The Vault is object-oriented and scalable - capable of easily managing tens of thousands of objects. By way of a powerful standard in this database, it is possible to respond to any requirement/wish for attribute sharing between systems in the Identity domain. Using standard connectors, the data can be loaded from many different source systems. The type of source system depends on the organization's industry: an HR system that contains employees, a SIS for students, a scheduling system with data regarding flex-schedule workers, or a combination of multiple systems. Basic identity data is stored in the source system, such as starting and ending dates, function, department, location, and grade level or graduation year.

The connectors provide the centralized transition of data between the source system, the Identity Vault and the linked target systems. Tools4ever has developed more than 200 connectors as part of its support program; if target or source systems are modified, Tools4ever updates the connectors. Tools4ever has standard connectors for the most widely used HR and SIS systems, cloud applications, standard on-premise applications, virtualized applications, email environments, databases, operating systems and directories.

In addition, Tools4ever has links with service management systems such as TOPdesk or Zendesk. Application owners may receive tickets from the linked service management system containing employee information, facilitating user account management in target applications. This provides the ability to link external applications without setting up a specific connector for that purpose. This can be a first step in informing application managers about in-service and out-of-service actions taken by individuals. This saves time and money, but it remains partly manual work.

A common setup is one that in the first phases of an Identity Management implementation, target applications are linked via an ITSM product based on tickets. Later on in the project these links are replaced by fully automated API connectors. Such a setup can clearly indicate when an employee is starting employment or, more importantly, when they terminate their employment. This often provides substantial value to the organization. The reasons for choosing such a link are: fewer than 200 employees are using the application, there is no available yet API for linking, there is no clear way to directly control the application, or the link can only be realized in a later phase. This is completely dependent on the desired plan.



IDENTITY LIFE CYCLE MANAGEMENT

Identity Lifecycle Management (ILM) takes care of the management of identities within the digital environment. This concerns the creation, modification and termination of user accounts within the IT infrastructure and target systems. The IAM solution’s configurable triggers and processes control these actions. An assortment of fields and values, relevant to the particular organizational need, are monitored for changes. These values may include items like hire or termination dates, preferred name values, or organizational data like department, title, phone number, etc.

When changes to those values occur, the IAM trigger monitoring such initiates an associated process to manage the changes according to organizational logic and need. Standard components of the ILM processes are Triggers, Processes, Notifications and Name Generation. These are constructed so that they are able to support the specific customer processes in a standard manner.

The ILM processes form the foundation of IAM and determine for whom and when a user account is created, modified and disabled. These processes are designed within and then automated by the IAM solution, according to the organization’s need. A very common process is one where the accounts and mailbox for an individual are already created prior to his or her first working day so that they are known in advance. This enables email delivery, appointment-planning, or sending tickets before the employee actually commences their employment.

HELPDESK SUPPORT

Supporting helpdesk tasks that cannot be automated remains an important IAM solution component. IAM offers the ability to implement specific service desk tasks regarding the provision of rights or management of accounts via the IAM Portal. This helps the current Administrator assign or revoke rights in the infrastructure.

ACCESS GOVERNANCE

GENERAL

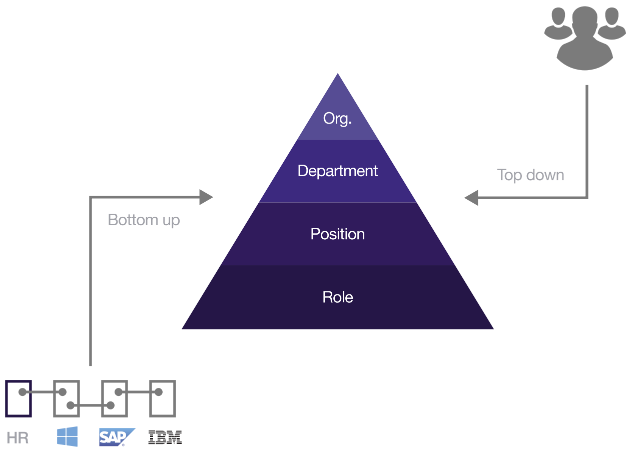
Access Governance (AG) is an important part of Tools4ever's IAM. The objective of AG is to ensure that employees have access to the network resources they need in order to be able to perform their duties. In recent years, AG has become increasingly important due to the tightening of laws and regulations (GDPR, FISMA, HIPAA, SOX, NEN7510, etc), the strong rise in the computerization of work processes, and the proliferating complexity of IT infrastructure (cloud, virtualization, outsourcing and the establishment of shared data centers). Traditionally, Access Governance was primarily the domain of financial institutions and large international companies. These days, it is becoming more and more the realm of care institutions, mid-sized companies (300-5,000 employees) and other commercial organizations.

With Access Governance, Tools4ever supports the various forms of collecting and recording information pertaining to rights. Tools4ever offers a uniform storage method where the identities and associated rights can be correlated with each other. Data storage is a sensitive issue in organizations because this type of information is stored in multiple systems under various IDs and in different formats. However, only one unique ID per identity is needed for synchronization and analysis.

The Board of Directors, Management and Security Managers must be in control of who has access to what. One big disadvantage of manually identifying the rights structure within an organization is that it is incredibly complex, time-consuming and comprehensive. Many organizations are at the immature stage of managing rights and do not have the necessary approach and software. Rights are issued based on sample users (copy user, because 'Jolanda will do the same work as Marion'), template users (available at the organizational or departmental level), spreadsheets and small self-developed applications. These methods manage the assignment of rights to some extent, but the most important action – the withdrawal of rights – is often poorly safeguarded.

With Access Governance in the IAM suite, Tools4ever offers the ability to establish the rights model using a phased approach. Access Governance gradually brings organizations from their current maturity level to a professional platform that manages rights in a controlled manner.

The diagram below provides an overview of Tools4ever's approach to Access Governance.



INVENTORY OF RIGHTS

AG's starting point is the inventory of the current state of rights in the network and the related organizational information The current status can be determined in two ways:

Top Down: this term refers to information that is known by the service desk or by company managers or security managers. There are always several "birthrights" to which (almost) everyone is entitled or requires to be able to perform his or her work activities. Sometimes a (partial) inventory has been done that provides an overview of the most important or critical rights. This method is described as 'top down' because policy or regulations already determine who should be included. Examples are folders and distribution lists for each department and the group memberships that everyone receives, such as Citrix and Intranet. In addition, there are critical applications for which access is very known in the organistion; this will be a select group, and it is important that only those persons may access the applications.

Bottom Up: this description refers to obtaining and merging information from the HR system (beginning with the job matrix and the roles that employees have in the organization) and the actual rights issued in the relevant systems (Active Directory, Exchange, SharePoint, ERP and Data Storage/Shares). This method is often termed 'role mining'. The roles are derived from the current network. A separate analysis must be conducted here to ensure that roles are not contaminated.

The approach of Tools4ever focuses first on the commonly used rights in order to spare the service desk or system manager and to safeguard access to critical applications and critical data. With a phased approach, these rights can be quickly accelerated and managed while other rights first require more extensive inventory and analysis.

In addition to IAM, Tools4ever also has simulation software that can measure the actual rights used in the file system over a certain period. This step results in a sanitized rights structure on a file system that can be set up and maintained in the model.

ROLE DESIGN

In this step, the rights information from the previous step is converted and housed in a role model. By translating system rights into business roles, it becomes much easier for (supervisory) managers to assess rights and be able to assign them to employees. There are a number of types of roles within AG so that the role model can be constructed modularly. This is an important step and becomes the foundation of the Access Government model. The roles that are specified must be independent of department/function/location so that modifications in the organizational structure will have limited impact on the role model.

This assures that the time spent on designing a role model does not have to be spent again when a new organizational change presents itself. This is also true for linking the rights in IT systems. When the role model is set up properly, the management impact can be minimized, with the model even used to control the rollout from or to new software packages.

ACTIVATION OF ROLE MODEL

In this step, the developed role model goes into production within Tools4ever's IAM and is actively applied to employees throughout their employment regardless of positional changes. The roles with the underlying entitlements are applied to the target applications.

Operational changes are processed by the model, and application of the role model occurs in three ways:

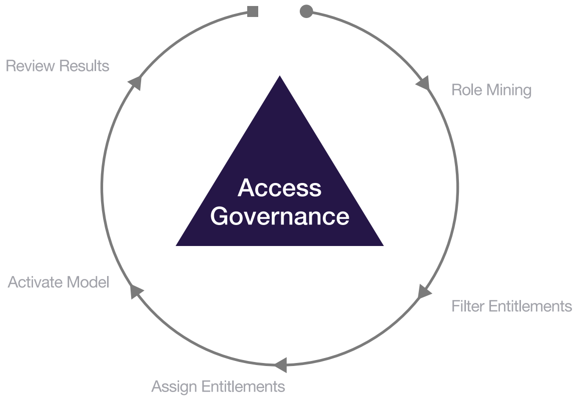
1. Role model application from the source system: as soon as a new person is added, it is clear which role/function this employee will fulfill within the organization. Promotions and changes in department, class and location that have been entered in the source system are also detected. The proper rights are assigned via the role model. When these elements are modified at a later date, any unnecessarily assigned rights will automatically be withdrawn. This prevents the accumulation of rights.

2. Role model application from a scheduled process: periodically in IAM, a process runs that assesses whether modifications in the model, in the Vault or in the underlying target systems have taken place. This process assigns the proper rights again and withdraws any assigned improperly for all persons in the model. This ensures that the model is always leading and that modifications are always applied.

3. Role model application via the Self-Service Shop: optional roles can be requested based on the model. These roles are not immediately assigned, but can be requested by the employee or the manager. Additional rights are immediately assigned by IAM as soon as the request is confirmed by the approver in the associated workflow. This also offers organizations the ability

to grant the relevant individual the ability to assign roles and rights. This prevents incorrect assignments by the Service Desk and offers the manager, for example, the ability to withdraw roles in order to keep the assignment of rights as clean as possible.

The phased approach of IAM offers customers the ability to quickly activate a part of the model to add value. By default, the role model will assign rights contained in the model and withdraw only those rights that have been administered by the model. In this way, the model can be used immediately and the contamination can be cleaned up later. This avoids having to first inventory and define all rights before the model can be activated. As a result, value is added from day one.



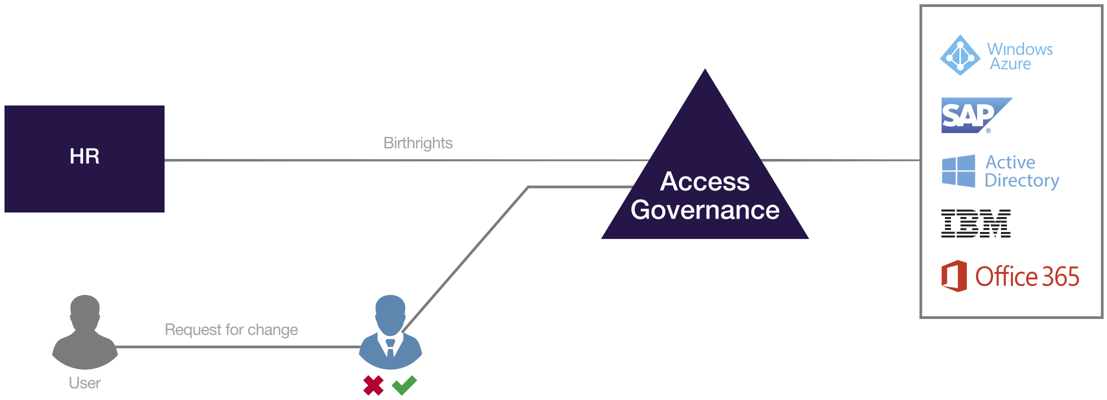
WORKFLOW AND SERVICE AUTOMATION

IAM’s Workflow and Service Automation modules give employees the ability to easily request or withdraw roles or rights via a web interface, with the IAM system executing any changes. These flexible request/approval processes align with contemporary business efforts to make employees and managers as self-sufficient as possible. Another reason for IAM’s Workflow and Service Automation module is to better define specific iterations of a more general job function. Consolidating functions within the job matrix better aligns similar employee roles for easier management, but it also means any individual distinctions for employees within more general functions disappear. Tools4ever’s IAM solution addresses this challenge by managing ad hoc requests through its self-service module.

In general, the standard rights via the HR system are sufficient for an employee to be able to initially work. However, the employee may be given extra tasks via his or her manager for which extra network resources (access to applications and data or shares) are also required. Here, too, Service Automation and Workflow Management offers the employee and/or manager the ability to request the extra rights (within the boundaries of the AG model).

The standard ULCM processes of IAM ensure that the manager of the new employee can already assign additional rights before the first working day. For example, management must provide the proper access to (cloud) applications, systems, data and email whenever a new employee comes onboard. The employee’s manager has an important role here. The manager makes requests for his or her employees and also approves requests. Depending on the type of request, more officers – such as the license manager, security manager and facility or ICT employees (in the role of Product Owner) – are involved in the approval process. After approval, requests are automatically processed in the IT infrastructure via IAM before the employee commences work; the employee can thus immediately start his or her work on the first day. This fits with the trend of self-service seen in the market and it relieves the Service Desk of all sorts of extra requests for additional rights.

Finally, a Service Automation and Workflow module makes it possible to maintain an accurate record of who has approved an access right for a certain employee, what that right is and when it was approved. In IAM, it is always clear who has approved what using an audit trail of the external systems. This prevents extra rights being assigned outside of IAM through the Service Desk without a trace.



LOGGING

Recording constant activity conducted within an environment is an important part of any IAM system. The Audit Log records what is being implemented in IAM and who modifies which items outside the standard IAM processes.

In this Audit Log, internal and external auditors can always locate which actions have been performed, when, and by whom - something not available in most Directories. This increases the monitoring of manual actions. Information about which actions have been conducted – such as the activation/deactivation of the account, the assignment of additional rights or groups, or resetting Active Directory passwords – can be retrieved on an individual basis. This enables compliance with the stricter laws and regulations regarding the security of business information.

WHERE DOES TOOLS4EVER EXCEL?

The IAM market is starting to become more mature and all parties agree on the functionality that IAM solutions must offer. Many suppliers offer solutions that seem suitable initially but lead to surprises or a great deal of extra work during the implementation phase.

The Identity and Access Management industry as a whole has developed something of a reputation for disappointing implementations that exceed expected effort and turnaround time. By contrast, Tools4ever offers a unique and innovative Enterprise IAM solution with a phased approach that quickly realizes value. Tools4ever's IAM ensures that organizations manage identities and rights in a controlled manner. Below is a list of issues where the IAM solution from Tools4ever is distinctive.

PHASED IMPLEMENTATION METHOD

When implementing an IAM solution, an organization will go through various phases of maturity regarding the professionalization of identity management. The focus here is certainly not just on IT, but increasingly on all the business processes (Provisioning, Workflow Management, Access Governance and Service Automation). To keep an IAM implementation manageable, Tools4ever strongly advises rolling out any IAM solution step-by-step.

When a step has been successfully rolled out and accepted in the organization, the next step can be initiated. Complicated IAM steps that an organization must accomplish are: making policy decisions about the design of a core registration system for identities; the actual design of a core registration system; naming conventions and the harmonization of identities in various target systems; designing the Access Governance matrix; and the introduction and roll-out of a self-service portal in the organization. Tools4ever's experience allows each step to be implemented with reasonably little effort (in days and/or weeks), but the embedding of the solution within organization usually requires more effort. Tools4ever's implementation method coordinates seamlessly with the above-mentioned step-by-step process and has proven itself over the years. In doing so, Tools4ever offers the ability to quickly add value for the organization using small, focused steps.

MANY CONNECTORS

A familiar pitfall in IAM implementations is that connections with source/target systems are not available. The link is then developed as custom work by the IAM solution's implementation partner. Development takes time and is not always performed correctly by an expert party, while management, support and modification remain extra worries. Tools4ever is very skilled in the development of IAM-related connections and has already realized hundreds of connectors. All connectors are part of the IAM standard software and as such are also supported. All future modifications in the connections are part of the support contract and will be automatically applied and offered by Tools4ever.

If a desired connection is not yet available, it will subsequently be made a standard part of the Tools4ever IAM solution – with all the benefits that brings. In addition to the previously non-standard connections, Tools4ever IAM supports every conceivable interface method used in IAM implementations. Standard interface methods are: SOAP XML, OpenID, OAuth 2.0, SAML 2, SPML, ODBC, native Oracle, Progress, SQL Server and CSV.

IAM also offers the ability to establish a semi-automatic link using email or a service management system. In many cases, this can be an efficient solution.

COMPLETE PORTFOLIO

Although IAM supports a large number of processes, Tools4ever users other products to cover all components which Gartner indicates must be part of a total IGA solution in its Magic Quadrant for User Administration & Provisioning and Magic Quadrant for Identity Governance and Administration (IGA). Tools4ever offers an Enterprise-class Identity Governance & Administration solution so that an organization does not have to research and select various partial solutions. The organization also does not have to worry about integration complications. All software has been developed from scratch by Tools4ever itself, and thus has not been integrated together via mergers or acquisitions. This has been a growing trend for IAM suppliers in recent years - elevating concerns regarding whether these components integrate seamlessly.

SCALABLE

Tools4ever's IAM solution is suitable for the management of very large organizations with tens of thousands of identities, but is also appropriate for an SME organization starting at 300 employees. The IAM suite contains various components to easily support organizations from small to large.

CONCLUSION

FLEXIBLE, DECISIVE AND INNOVATIVE

Tools4ever has more than 10 years of experience with an impressive track record in the now mature market of Identity Governance & Administration. In the Netherlands, Tools4ever is the clear market leader, with more than 500 full IAM implementations. The IAM product portfolio of Tools4ever is more than complete and covers, for example, all topics that Gartner mentions in its reports on this subject. Compared to competing parties such as NetIQ/Novell, Oracle, Microsoft, Okta and SailPoint, Tools4ever is flexible, decisive and very innovative.

Over the years, Tools4ever has perfected its professional services. Using state-of-the-art software, a phased implementation method and very experienced implementation consultants, Tools4ever is able to produce successful turnkey IAM implementations in weeks instead of the usual months or years witnessed throughout the IAM market.

Above all, Tools4ever maintains a competitive pricing policy. The combination of a proven track record, a successful implementation method and very competitive pricing makes Tools4ever a party that is certainly worth being included in an IAM selection process.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER NEW YORK

Address	300 Merrick Road, Suite 310 Lynbrook NY 11563 USA
General	+1 866 482 4414
Support	+1 516 482 7525
FAX	+1 516 825 3018
Information	nainfo@tools4ever.com
Sales	nasales@tools4ever.com
Support	support@tools4ever.com

TOOLS4EVER WASHINGTON

Address	11515 Canyon Road E Puyallup WA 98373 USA
General	+1 888 770 4242
Support	+1 253 770 4823
FAX	+1 253 435 4966
Information	nwsales@tools4ever.com
Sales	nwsales@tools4ever.com
Support	nwsupport@tools4ever.com