KuppingerCole Report

EXECUTIVE VIEW

By Peter Cummings | October 2013

EmpowerID 2013

By **Peter Cummings**
pc@kuppingercole.com
October 2013

Content

1 Vendor Profile

EmpowerID was founded in 2005 and is based out of Dublin, Ohio. EmpowerID was previously known as a niche player, with products like the Active Directory (AD) Self-Service Suite, which provides web-based white pages and password reset for AD.

At EIC 2013[1], EmpowerID announced the general availability of EmpowerID 2013. This new release shows a respectable attempt to unify the approach to Identity and Access Management in a single tool. EmpowerID now offers User Management, Provisioning, Access Governance, Cloud Single Sign-On (SSO) and access management in one product. EmpowerID 2013 is workflow-based, highly configurable and customisable, while paying attention to the current issues in Identity & Access Management, such as Cloud services and the need for extreme scalability.

Workflow is extremely useful for organizations that do not want to perform a high degree of customization, but rather want to rely on out-of-the-box functionality. EmpowerID ships with more than 400 ready-to-use workflows and significant coverage from user provisioning to Cloud SSO. The workflow engine in EmpowerID allows an organisation to implement virtually any business process in a consistent way without requiring a large number of resources.

It should however be noted that for provisioning, while EmpowerID has deep functionality with AD, there are a fair number of platforms to which it can provision out-of-the-box. EmpowerID offers full AD support, mailbox provisioning and provisioning to other Lightweight Directory Access Protocol (LDAP) compliant directories. While EmpowerID supports connectivity to major systems such as AD, LDAP etc. with native connectors, they also have an OEM partnership with IdentityForge for several other platforms, including mainframe systems. The latter is a valid approach other vendors take as well. However, customers should ensure that they can access experienced support resources in case they want to rely on the OEM connectors.

EmpowerID also features simplified SSO and access management for Cloud and on-premise web applications. This is a feature that is normally implemented in a separate product to the provisioning and governance functionality, but with EmpowerID all three solutions are available in one product. The new Web Access Management functionality can enhance existing SSO capabilities to enforce corporate security policies. This enables protection against unauthorised access to enterprise resources while enabling SSO for web applications that do not support Security Assertion Markup Language (SAML). Another useful feature of EmpowerID is the built-in multifactor authentication service which can service to reduce or eliminate the costs associated with 3rd party tokens, as the authentication service supports Open Authentication (OATH) compliant tokens, thus giving the organisation a choice between hardware and software tokens as well as smartcards and one time password or a combination of them.
As should be expected from an access management solution EmpowerID offers federation using open standards like SAML, WS-Federation, WS-Trust, OpenID and OAuth as well as centralised authentication using a built-in LDAP and Remote Access Dial-In User Service (RADIUS) server.

[1] European Identity and Cloud Conference, www.id-conf.com

With the Microsoft centric background, EmpowerID presents a credible approach to the otherwise seemingly cumbersome task of managing large SharePoint sites by adding inventory and access request workflows for SharePoint sites and Group as well as SharePoint user profile synchronization.

2 Product Description

2.1 Single Sign-On

EmpowerID offers a complete solution for SSO, Federation and Mobile Identity Security. By using an SSO dashboard EmpowerID have user experience in mind. The dashboard allows the user to login into EmpowerID once and from there have access to all configured SSO applications. A huge benefit with the dashboard it that is has been designed for mobile compliance, meaning that the SSO dashboard will also work on mobile devices, effectively BYOD-enabling your organisation.

The federation functionality of EmpowerID supports most of the standard identity protocols such as SAML, OpenID, WS-Trust, WS-Federation and OAuth. Furthermore the server includes a Security Token Server and an OAuth Server supporting OAuth 2.0. The very broad reaching federation capability allows an organisation to facilitate SSO to virtually any system, be it in the Cloud, on-premise or hosted by a 3rd party.

For applications that do not support federation, EmpowerID comes with a feature called Web Access Management. This feature facilitates SSO with the use of agents running on Java and .NET based application servers. This method allows authorization to be granted by role-based and attribute-based authorization policies.

Apart from standard AD integration, EmpowerID offers deep integration with SharePoint. Large SharePoint installations are notoriously difficult to manage in large organisations. With EmpowerID much of this administration becomes easier, as organisations are now able to create an inventory of all SharePoint sites and groups. This enables centralized role and workflow-based access control, including access recertification and segregation of duties enforcement.

Other features in the EmpowerID SSO Platform include:

- Policy-Based Access Control
- Password Vaulting
- Metadirectory and Sync Services
- LDAP Virtual Directory

2.2 Provisioning

EmpowerID offers workflow based User Lifecycle Management and Provisioning. As expected, HR-driven provisioning is fully supported, however a good feature in this area is the ability to support multiple authoritative sources. This is particular useful for the many organisations that do not have one single trusted source of identities, but use multiple systems for contractors, partners and customers.
The same policies that would apply to normal employees can now be applied to the whole identity ecosystem, including external identity directories.

2.3 Mobile Identity Management

The ever-increasing use of smart mobile devices can be very hard to manage in a large organisation. Given the right approach however it can also encourage productivity from any location. EmpowerID embraces this and introduces a user interface (UI) specifically designed for mobile devices, resulting in a good user experience. EmpowerID allows linking, tracking, and management of multiple devices by user and at the same delivering role-based access to applications directly from the mobile device.

EmpowerID enables organisations to regain control over mobile access by allowing for the same access, governance and compliance policies to be used across all enrolled user devices. Furthermore, for added security, multi-factor authentication is also supported from mobile devices as a part of the package.

EmpowerID also offer an extensive application programming interface (API) supporting SSO, this enables application developers to use EmpowerID to manage access with applications using the most common formats including Representational State Transfer (REST), Windows Communication Foundation (WCF) and Simple Object Access Protocol (SOAP).

2.4 Governance and Compliance

EmpowerID is at the leading edge in terms of access control, offering both role and attribute-based access control (RBAC and ABAC). This allows for finer grained access control while enabling instant reporting on whom has access to what, and how the specific access was granted. Apart from this, EmpowerID also offers the standard detective controls such as a separation of duties (SoD) policy engine and access recertification and attestation.

Another interesting feature is the introduction of Rights-Based Approval Routing (RBAR). RBAR unifies RBAC and workflows to enforce real-time evaluation and routing of who can approve requests, based on the actual rights delegated to the current person relative to the target resource. Based on this, approvals are routed to the approver with the necessary privileges to perform the intended operation. A final feature worth mentioning is that EmpowerID supports time-based provisioning, for all assignments, out of the box. This allows for automatic expiration of access assignments based on policies defined by the organisation.

3 Strengths And Challenges

EmpowerID has delivered an all-in-one IAM solution, which covers all the traditional bases, while embracing future concepts such as Cloud identity management. This solution is one of the more complete offerings in the market, at the same time offering virtually unlimited configuration and customisation possibilities. This can be a downfall in some cases however, as there is the possibility to go down a route of customisation that can be hard to come back from, as many organisations realised previously with other customizing-heavy Identity Management tools. However, EmpowerID is mainly about customisation and less about coding.

That being said, in these days of "no-customisation" that we see in many organisations, EmpowerID seems to be set at the right level, with an extensive array of workflows already configured out of the box, allowing an organisation to get into the world of IAM very quickly and without the pain others have had to suffer.

The number of supported target platforms is limited, which could create issues in managing the legacy systems still prevalent in many financial institutions. This however has not prevented rapid take-up of the solution, including several Fortune 500 companies. It should also be noted that EmpowerID partners with IdentityForge[2], through this partnership a large numbers connectors are available extending the native capabilities of EmpowerID.

Strengths	Challenges
• An all-in-one IAM solution • Complete SSO capabilities both on-premise and Cloud • Advanced features in access control • Mobile Identity Management included • Easy to deploy • Everything in one place	• Significant numbers of connectors, but some from OEM partner • No Adaptive Access Management, this means no context aware access management • Can potentially be over-customised

4 Copyright

[2] http://www.identityforge.com/solutions/solutions-for-empowerid

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Am Schloßpark 129
65203 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com