**IJCTA,** 9(30), 2016, pp. 105-117


# Analysis of security identity and access management systems

**Pavel Sergeyevich Ptitsyn* Dmitry Vladimirovich Radko** and Alexey Vasilevich Skrypnikov*****

***Abstract :*** Security Identity and Access Management systems provide centralized access and identity control of users and resources and monitoring security risks. The aim of this study was to determine the effectiveness of existing security identity and access management systems in terms of achieving main key performance indicators. These indicators included the flexibility of managing user identity and accounts, the integration into the information landscape of the organization, the capabilities for configuration, management and administration of security infrastructure. The study contains analysis and evaluation of modern security identity and access management systems. The evaluation was performed by the following functional criteria: authentication and authorization methods, user registration methods, user rights management and delegation of the user rights, management user requests, monitoring and reporting, configuration and customization. The performed research identified the main advantages and disadvantages of existing security identity and access management systems, and identified the most advanced systems, which provide a complex platform build on open security standards, including the related Web Services, SOA, OGSA specifications.

***Keywords :*** Security infrastructure, user identity management, user access management.

## 1. INTRODUCTION

In today's business world, information security is often a prime factor of success. However, the needs to safeguard business critical information and other sensitive data should be balanced with providing necessary access to information and resources across your organization's technology environments. To complicate matters, this balancing act must also adhere to strict compliance requirements [1, 2].

Security Identity and Access Management solutions are designed to provide you with centralized visibility and control, allowing you to actively measure and monitor the risks inherent in a system that must match up users and resources. Security Identity and Access Management solutions refers to a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources [3]. Security Identity and Access Management solutions fall under the overarching umbrella of IT security. Identity and access management systems not only identify, authenticate and authorize individuals who will be utilizing IT resources, but also the hardware and applications employees had to access. Identity and Access Management solutions have become more prevalent and critical in recent years as regulatory compliance requirements have become increasingly more rigorous and complex [4, 5].

Security Identity and Access Management solutions provide the following set of services: Compliance Manager, Lifecycle Manager, Identity Intelligence, Governance Platform, Integration Modules, User Provisioning [6].

The aim of this study is to determine the effectiveness of existing security identity and access management systems, and define the weak and strong sides of given systems.

* Research Institute of Semiconductor Engineering, JSC Russian Federation, 394033, Voronezh, Leninsky Prospekt, 160a

** Voronezh innovation and technology center, LLC Russian Federation, 394033, Voronezh, Leninsky Prospekt, 160a

*** Voronezh State University of Engineering Technologies Russian Federation, 394036, Voronezh, Revolyutsii Prospekt, 19

## 2. METHODS

**From the marketing analysis of the security identity and access management systems, the most popular systems are the following [7, 8]:**

- IBM Security Identity and Access Manager (IBM Corporation, USA).
- Oracle Identity Management (Oracle Corporation, USA).
- NetIQ Identity Manager (NetIQ Company, USA).
- Microsoft Forefront Identity Manager (Microsoft Corporation, USA).
- RSA Identity and Access Management (EMC Corporation, USA).
- SailPoint IdentityIQ (SailPoint Company, USA).

The security identity and access management systems have a wide range of security features. To determine the strengths and weaknesses of the systems, we consider in more details each of them.

### 2.1. IBM Identity and Access Manager

IBM Identity and Access Manager provides centralized and automated procedures for creating, modifying and deleting user accounts and applies policies of user identity [9, 10].

**IBM Identity and Access Manager provides the following functionality :**

- Intuitive web-based administration console.
- Role-based security models for delegating administrative authority.
- Web-interface and self-service request/response.
- Built-in workflow for automatically sending user requests for approval and implementation of the approved requests.
- Built-in automation to perform administrative inquiries.
- A set of tools for managing applications that extends the management model to include emerging environmental protection and special purpose.

**IBM Identity and Access Manager has the following core features:**

- Empowering end-users using the technology of centralized logon (SSO).
- Simplifying administration of security in the inter-company business processes.
- Providing integrated security management built on the rules for web-services in a SOA-environment.
- Support for open standards and specifications, including the LDAP, SAML, WS-Federation, WS-Security and WS-Trust.
- Supply adapters for: IBM AIX, IBM OS/400, Microsoft Windows Active Directory, Novell NetWare, Sun Solaris, Oracle, IBM OS/2, HP-UX, Red Hat Linux, IBM RACF, Lotus Notes, LDAP V3 Compliant Directory Servers, SAP R/3.

The business logic module is implemented as J2EE-application, which is hosted by the IBM WebSphere Application Server. This module implements web-console user and the system administrator. IBM Identity and Access Manager provides a complete solution to manage access in more than 150 different information systems (OS, Microsoft Active Directory, database, LDAP-catalogs, e-mail servers, business applications and so on). IBM Identity and Access Manager provides custom adapters using IBM Directory Integrator.

### 2.2. Oracle Identity Management

Oracle Identity Management provides management of the rights and privileges of each user, as well as automatic compliance to protect information. Service-oriented architecture provides a single point of control for all enterprise applications [11].

Oracle Identity Management helps the organizations to manage the full lifecycle of the identity of the users as a resource within the security perimeter, and outside it, no matter what kind of applications are used in the organization. In other words, the approach of Oracle Identity Management, focused on serving the needs of the application, enables customers to clearly separate business logic from security and resource management [12].

**Oracle Identity Management provides the following basic functions:**

- Creating and maintaining a single repository of credentials.
- Providing automatic creation of accounts for employees in accordance with their duties.
- Providing automatic control of credentials of users in all target systems.
- The identification of unused user accounts.
- Administrators to control the actions of target systems and to prevent unauthorized changes to the access rights.
- Delegation of various administrative functions.
- Reducing total cost of ownership for enterprise systems.
- Providing security audit.
- Matching the requirements of the legislation, including the storage of personal data.

**Oracle Identity Management has the following core features :**

·Full range of essential services, including the management of identity and roles; the delivery of credentials and their coordination; control access to Web-based applications and Web-based services; single sign-on and federated identity; fraud detection; multifactor authentication and risk management; optimization of corporate roles and analysis of identity data, auditing and reporting.

- Oracle Identity Management provides integration with Oracle applications, like PeopleSoft, Hyperion, Siebel, and components of Oracle Fusion Middleware, such as SOA, WebCenter, and Business Intelligence.
- Oracle Identity Management components can be used in heterogeneous environments from different vendors, including a variety of operating systems, web-servers, applications servers, directory servers, and database management systems.

### 2.3. NetIQ Identity Manager

NetIQ Identity Manager is a solution for account management, which automates the provision of resource users and password management throughout the life cycle of users, providing new employees immediate access to the system [13].

NetIQ Identity Manager provides a powerful foundation for creating accounts, single sign-on, self-service, authentication, authorization. It helps to integrate, manage and monitor a distributed identity information by providing the right resources to the right users.

**NetIQ Identity Manager provides the following basic functions :**

- Automates the management of user profiles and passwords.
- Customers with the ability to self-service.
- Self-registration of users.
- Automates the process of issuing permits.
- Ensures adherence to the rules of the password.
- Performs two-way password synchronization.
- Administration of role base models.
- Create and deploy processes without programming.
- Create and test rules without risk to production.
- Automates the paperwork to simplify regulatory compliance.

**NetIQ Identity Manager has the following core features :**

- Support for open standards and specifications, including the SAML, WS-Federation, WS-Security and WS-Trust.
- Supply adapters for: BEA WebLogic Server, Citrix XenApp, Dell OpenManage, HP OpenView, IBM Tivoli, IBM WebSphere Application Server, Lotus Domino, Microsoft Active Directory, Microsoft Exchange, Microsoft IIS, Microsoft SharePoint Server, Microsoft SQL Server, Microsoft Windows Management Instrumentation (WMI), Microsoft Windows OS, Oracle databases, UNIX-Linux OS, VMware.

### 2.4. Microsoft Forefront Identity Manager

Microsoft Forefront Identity Manager (FIM) is a solution that provides identity management of users. FIM manages user accounts and user access to information resources of the company. FIM provides the most strictly secure access as a "cloud" services, as well as to domestic corporate resources from virtually any location connected to the Internet and using different types of devices [14].

FIM simplifies identity and access management through a self-service web-portal, and provides a set of tools for administrators. FIM automates common tasks for managing user accounts, passwords, groups and mailing lists, as well as users of digital certificates [15].

FIM is a flexible platform that provides capabilities for integration with custom solutions, and has the potential to scale to large and medium-sized businesses. At a basic level, there are many built connectors to the LDAP-directories, e-mail systems, ERP systems and other decisions leading vendors. When deploying SharePoint service, FIM provides convenient administration interfaces for management and defines a variety of business processes.

FIM includes agents to identification services of the following systems: Active Directory Domain Services, Active Directory Lightweight Directory Services, IBM Tivoli Directory Server, Novell eDirectory, Sun ONE Directory Server, IBM Directory Server, Microsoft Exchange Server, Lotus Notes, Microsoft SQL Server, IBM DB2 Universal Database, Oracle Database, SAP - R/3 Enterprise, mySAP, Microsoft Office services; Microsoft Sharepont.

FIM was developed using SOA-architecture and related open web-services standards, which provide mechanisms for integration into the information landscape of the enterprise. FIM supports the following functions:

- Providing integrated security management is built on the rules for web-services in a SOA-environment.
- Support for open standards and specifications, including SAML, WS-Federation, WS-Security and WS-Trust.
- Support for communication services of Windows Communication Framework.

### 2.5. RSA Identity and Access Management

RSA Identity and Access Management is a software providing securely access Web applications in external and internal networks. RSA Identity and Access Management provides authentication and access control for physical, virtual and cloud infrastructures. Integrated management of secure access to corporate resources is implemented through a centralized administrative console. RSA Identity and Access Management exposes safe user interaction and information systems using verification of authentication data, which increases the overall level of confidence in the information assets of enterprises [16].

**RSA Identity and Access Management has the following features for access management :**

- Access control – provides access to confidential data for authorized users.
- Centralized policy management - reducing cost of policy management authentication and authorization across multiple applications. Rapid assessment of the level of regulatory compliance and reducing the cost of the audit.

- Unified Access Control - the unified access control across multiple applications. Reducing the complexity of the IT infrastructure and administration costs by centralizing and eliminating redundant infrastructure.
- Detailed access control - reducing risks due to access rights, depending on the selected parameters such as the position held and duties.
- Incorporated web entry system - improved quality of interaction with users: employees, customers and partners of your organization now needs only once to sign in to your web portal.
- Delegating management responsibilities - allocation of responsibilities for the management of users and access policy.
- Authentication, taking into account the context - the protection of resources, high-risk, from unauthorized use through a combination of unified login authentication.

**RSA Identity and Access Management has the following features for identity management :**

- Service attributes - control over which attributes should enter each user, and management methods of sharing and secure exchange of such information.
- Binding to the account – providing a link between user accounts and data requests.
- Support for multiple protocols - simple interaction with the products of partners using different integration standards.
- Profile sharing attribute X.509 - help in making access control decisions in real-time through dynamic retrieval of user attributes.
- Tools of quick installation - automation installation using the setup wizard, combining large amounts of data, cloning policies and other automatic functions.

RSA Identity and Access Management includes agents for access to the following services identification systems: Microsoft Windows Server, Red Hat Enterprise Linux, IBM AIX, SUSE Linux Enterprise Server, VMWare ESX, Sun Solaris, Active Directory Domain Services, Microsoft SQL Server, Oracle Database, Oracle Directory Server, Sybase Adaptive Enterprise Server, Sun Directory Server, BEA WebLogic Portal, and IBM WebSphere Portal.

RSA Identity and Access Management supports for web services standards, including the OASIS Web Services Federation (WSFED), Protocol Simple Object Access Protocol (SOAP), and a markup language Security Assertion Markup Language (SAML 1.1 and 2.0). It makes it easy to integrate, customize and extend the safe identification.

### 2.6. Sail Point Identity IQ

Identity IQ is a solution for managing identity and access to distributed enterprise information systems. Identity IQ helps users to take an active part in the processes for managing identity and access - using the automatic certification of the rights of access, policy management, access requests, password management, and analytics. Together with resource connectors as a part of the base platform, it provides integration between different applications running in the data center or the cloud [17].

**Identity IQ consists of the following functional subsystems :**

- Compliance Manager - organizes the implementation of compliance procedures and increases efficiency by automatically auditing certification and access policy management.
- Lifecycle Manager - combines independent inquiry to access and password management with automated lifecycle management events to simplify the creation, modification and revocation of access privileges.
- Identity Intelligence - converts the technical identification data of users in various corporate systems, or in the cloud, in a centralized, easy to understand and relevant business information;

- Platform Management (Governance Platform) – centralizes identity, provides a single space modeling roles, policies and risks in order to maintain compliance with the organization's processes. It includes more than 80 connectors to enterprise management and cloud resources.
- Modules integration (Integration Modules) - provides flexible options for integration with solutions from other developers for data collection and organization changes.

IdentityIQ includes the following connectors to application, system, and specialized software: BEA WebLogic Server, CA Unicenter NSM Connector, HP Systems Insight Manager, IBM Systems Director, IBM Tivoli Connector, IBM WebSphere Application Server, IBM WebSphere MQ, Lotus Domino, Microsoft Active Directory, Microsoft Cluster Server, Microsoft Exchange, Microsoft SharePoint Server, Microsoft SQL Server, Microsoft Windows Management Instrumentation (WMI), Microsoft Windows OS, Oracle Database, RIM BlackBerry Enterprise Server, SAP ERP.

Also IdentityIQ supports for system integration using an application programming interface which is implemented in accordance with the standards of Web services SOAP \ REST.

### 2.7. Methodology of testing security identity and access management systems

The evaluation of security identity and access management systems was performed using the methodology, which is represented below.

The expert examines each of the selected systems. Then, based on the knowledge and experience of their usage, the expert evaluates given system by the appropriate functional assessment criteria [18, 19].

In the process of testing and evaluation four staff members were involved, two of them were employees of the research organization and two were the independent consultants.

The expert studied each of the systems by working with trial versions, and the examination of relevant technical documentation, including the description of the system, administration and user guides.

The expert carried out evaluation of the systems by related criteria. These criteria grouped into logical functional groups. The description of the functional groups and the relevant criteria presented in Section 2.8.

The evaluation of the systems by each criterion *was* performed by a five-point scale. Table 1 presents the degrees of compliance with functional capabilities of systems.

**Table 1. The degrees of compliance with functional capabilities of systems**

| ***Degree*** | ***Value*** |
|---|---|
| 0 | Absence of related functionality. |
| 1 | Does not satisfy the requirements. |
| 2 | Partially satisfies the requirements. |
| 3 | Satisfied, but there are serious drawbacks. |
| 4 | Satisfied, but there are minor drawbacks. |
| 5 | Fully satisfies the requirements. |

The result of the evaluation is the sum of estimates for all functional criteria.

The averaged overall rating, exhibited by the group of experts, is determined by the following formula: Sum of final ratings of all experts divided by the number of experts.

### 2.8. Evaluation criteria of security identity and access management systems

For testing and evaluation, the list of functional criteria was formed. The criteria reflect the features and the most important aspects of security identity and access management systems [20, 21]. Table 2 presents the list of given evaluation criteria.

**Table 2. The list of evaluation criteria of security identity and access management systems.**

| # | *Group of criteria* | *Description of criteria* |
|---|---|---|
| 1. | Methods for user authentication and authorization. | 1.1 Authentication with the reusable passwords.<br>1.2 Authentication with the one-time passwords.<br>1.3 Authentication with the PIN-code.<br>1.4 Strong authentication with symmetric algorithms.<br>1.5 Strong authentication with asymmetric algorithms.<br>1.6 Biometric user authentication.<br>1.7 Hardware authentication (smart cards, USB-keys, RFID). |
| 2. | Support for single sign-on. | 2.1 SSO Kerberos.<br>2.2 SSO LDAP.<br>2.3 SSO Microsoft Active Directory Federation Services.<br>2.4 SSO SAML.<br>2.5 OpenID.<br>2.6 OAuth. |
| 3. | User registration. | 3.1 the registration templates for different categories of users and organizations.<br>3.2 Setting up the mechanisms of activation of the user account.<br>3.3 Protection against automatic registration of users. |
| 4. | User rights management. | 4.1 Manual entry of employee data into the system.<br>4.2 Role-based access control.<br>4.3 Support for role hierarchy.<br>4.4 Workflow of role processes (creation, approval, change, delete).<br>4.5 Monitoring SoD-conflicts.<br>4.6 Certification (revision of access rights).<br>4.7 The control system changes made to bypass IDM.<br>4.8 Monitoring user activity in the target systems.<br>4.9 Risk control of user access.<br>4.10 Support for multiple accounts for the employee in the same system.<br>4.11 Management of service accounts.<br>4.12 Access control functions (setting of functional roles).<br>4.13 Separation of the scope of the rights and roles (who, what may request).<br>4.14 Separation of user interface visibility including forms and their fields.<br>4.15 Resetting the password by control questions.<br>4.16 Resetting the password at the entrance to the OS. |

| # | *Group of criteria* | *Description of criteria* |
|---|---|---|
| 5. | Delegation of the rights. | 5.1 Setting delegation policy for users, services, organizations.<br>5.2 Support for uniform registry service for delegation rights.<br>5.3 Support for writing scenarios using scripting languages.<br>5.4 Unload policies in XML-format.<br>5.5 Delegation on the proxy certificates.<br>5.6 Delegation on the temporary tokens. |
| 6. | Management user requests. | 6.1 Creating requests for additional rights.<br>6.2 Request rights for definite time.<br>6.3 Request rights like other employee.<br>6.4 Request rights using configured templates.<br>6.5 Request more employees multiple roles in a single application.<br>6.6 Approval of requests.<br>6.7 Approval of a part of requests.<br>6.8 Bulk approval of requests.<br>6.9 The ability to split the requests into its constituent parts to separate negotiation and collect them in a single request.<br>6.10 Digital Signature requests.<br>6.11 The delegation of coordination requests for the holiday period.<br>6.12 E-mail alerts.<br>6.13 Assigning requests to execute manually. |
| 7. | Reporting. | 7.1 Formatting of reporting forms.<br>7.2 Reporting on the state of the rights to a certain date in the past.<br>7.3 The use of charts and graphs in reporting forms.<br>7.4 Generating reports in different formats (PDF, XML, Excel, Word).<br>7.5 Preparation of reports in the context of: day, week, month, year.<br>7.6 The collection and accounting of the resources for the organization and domain.<br>7.7 The collection and accounting of user resources.<br>7.8 The collection and accounting of system resources. |
| 8. | Configuration and customization. | 8.1 Design reports.<br>8.2 Changing the form of employee.<br>8.3 Changing the form of requests.<br>8.4 Add custom forms and entities.<br>8.5 Individual layout of interface.<br>8.6 Tools for constructing a role model (Role Mining). |

| # | Group of criteria | Description of criteria |
|---|---|---|
| 9 | The quality of the documentation and the technical support. | 9.1 Completeness of the documentation. |
| | | 9.2 The quality of learning materials (demo examples, case studies). |
| | | 9.3 The quality of technical support. |

## 3. RESULTS AND DISCUSSION

### 3.1 Overall evaluation results of testing the security identity and access management systems

Functional testing and evaluation of the security identity and access management systems had been made on study of their flexibility of managing user identity and accounts, the integration into the information landscape of the organization, the capabilities for configuration, management and administration of security infrastructure.

Table 3 presents the results of testing and evaluation of the security identity and access management systems by related evaluation criteria (Table 2).

**Table 3. The results of testing and evaluation of the security identity and access management systems.**

| | *Criteria/Estimation of system* | *IBM Identify and Access Manager* | *Oracle Identify Management* | *NetIQ Identify Manager* | *Forefront Identify Manager* | *RSAIdentify and Access Management* | *Sail Point IdentityIQ* |
|---|---|---|---|---|---|---|---|
| 1. | Methods for user authentication and authorization. | 25 | 29 | 28 | 28 | 22 | 30 |
| 2. | Support for single sign-on. | 20 | 21 | 10 | 16 | 6 | 13 |
| 3. | User registration. | 15 | 15 | 12 | 15 | 13 | 15 |
| 4. | User rights management. | 72 | 77 | 56 | 76 | 73 | 72 |
| 5. | Delegation of the rights. | 19 | 29 | 15 | 29 | 25 | 24 |
| 6. | Management user requests. | 37 | 47 | 40 | 41 | 33 | 53 |
| 7. | Reporting. | 31 | 34 | 26 | 36 | 21 | 30 |
| 8. | Configuration and customization. | 14 | 14 | 11 | 22 | 8 | 20 |
| 9. | The quality of the documentation and the technical support. | 14 | 15 | 9 | 15 | 8 | 8 |
| | Total estimation | 247 | 281 | 207 | 278 | 209 | 265 |

**The following overall rating of security identity and access management systems achieved:**

- Oracle Identity Management (281 points).
- Microsoft Forefront Identity Manager (278 points).
- SailPoint IdentityIQ (265 points).
- IBM Identity and Access Manager (247 points).
- RSA Identity and Access Management (209 points).
- NetIQ Identity Manager (207 points).

**According to the results of testing and evaluation, the following leaders were determined :**

- Oracle Identity Management (Oracle Corporation, USA).
- Microsoft Forefront Identity Manager (Microsoft Corporation, USA).
- SailPoint IdentityIQ (SailPoint Company, USA).

These systems have the best functional and technical features among other security identity and access management systems. Each system gives different advantages and disadvantages, but in common, these systems represent the complex platforms, which provide management of security access and identity distributed applications. The platform implemented main features such as user registration, access management, identity management, configuration management, monitoring and reporting are built using open standards, and programming interfaces, which provide flexible integration mechanism with a wide range of system and enterprise software.

**However, it should be notice the significant disadvantages of security identity and access management systems:**

- The weakness in implementation of single sign-on features using open standards such as SSO SAML, OpenID and OAuth.
- Lack of the support PIN-code authentication functions.
- Lack of the user request management, in terms of support mechanisms and scenarios, coordination and execution of user requests.
- Lack of the functionality for delegating user rights using scripting approaches.
- Lack of the functionality for reporting and publishing of security access and identity data.
- The weakness in implementation of mechanisms for adjustment and adaptation, which provides the features to add custom entities and forms, the tools for building role models, as well as exposing programming interfaces.

### 3.2. The test results of Oracle Identity Management

**Oracle Identity Management is a leader of functional testing. However, this product have the following weak sides and disadvantages:**

- There are no features, which provide PIN-code authentication.
- Lack of SSO support, including OpenID and OAuth.
- Lack of WS-Federation and WS-SecureConversation.
- Lack of the user request management, in terms of support mechanisms and scenarios, coordination and execution of user requests.
- High cost of implementation and ownership.
- High dependence on Oracle software, including Oracle 10g database, Oracle SOA Suite integration platform).

### 3.3. The test results of Microsoft Forefront Identity Manager

**Microsoft Forefront Identity Manager is a leader of functional testing. However, this product have the following weak sides and disadvantages:**

- Lack of SSO support, including SSO SAML, OpenID and OAuth.
- Lack of functional for configuration and customization, in implementing the capability to add additional entities and user forms, the lack of advanced tools for building a role model.
- Lack of support security standards of messages XACML, SAML.
- High cost of implementation and ownership.
- High dependence on Microsoft software, including SQL Server database, OS Windows Server services, SharePoint Server services.

### 3.4. The test results of Sail Point Identity IQ

**Sail Point IdentityIQ has strong functional capabilities, but it also has significant disadvantages, including:**

- Lack of SSO standards.

- Lack of security messaging standards.
- There are no features, which provide PIN-code authentication.
- There are no features, which provide synchronization of workflows and tasks in load balancing mode.
- Lack of functional user rights management, in terms of risk control of user access and accounts for the employee in the same system.
- Lack of functional user request management, in terms of providing capability of request coordination, and the ability to split the requests into its constituent parts.
- Lack of functional reporting, in terms of the provision of information in the form of charts and graphs.
- Lack of functional for configuration and customization, in implementing the capability to add additional entities, user forms, custom logic.
- Low quality of training materials.

### 3.5. IBM Identity and Access Manager

**IBM Identity and Access Manager has medium functional capabilities, including the following significant disadvantages :**

- Lack of PIN-code authentication and biometric authentication of the user.
- Lack of SSO, including OpenID and OAuth.
- Lack of functional for delegating user rights, in terms of customization logic using scripting languages, exchanging policies, and the ability to delegate rights using temporary tokens.
- Lack of digital signature.
- Lack of functional for configuration and customization, in implementing the capability to add additional entities, user forms, custom logic, reports, role models.
- Lack of OGSA architecture, including authentication & authorization services, data access control, monitoring and administration.
- High cost of implementation and ownership.
- High dependence on IBM software (DB2 database, WebSphere solution stack).

### 3.6. RSA Identity and Access Management

**RSA Identity and Access Management provides basic functional capabilities. This product has the following significant disadvantages :**

- Lack of support for one-time passwords and biometric authentications.
- Lack of SSO, including SSO Kerberos, SSO Microsoft Active Directory Federation Services, OpenID and OAuth.
- Lack of functions for delegating user rights, in terms of customization logic using scripting languages, exchanging policies, and the ability to delegate rights using temporary tokens.
- Absence of support for security standards Messaging Web Services Security, Web Services Resource Framework.
- Absence of support for message security standards SAML, XACML, REST.
- Lack of the user request management, in terms of support mechanisms and scenarios, coordination and execution of user requests.
- Lack of functional for configuration and customization, in implementing the capability to add additional entities, user forms, custom logic, reports, role models.
- Low quality of training materials.
- Low quality of technical support for international users.

### 3.7. Net IQ Identity Manager

**Net IQ Identity Manager provides basic functional capabilities. This product has the following significant disadvantages:**

- Lack of support authentication functions including one-time passwords and biometric authentication.
- Lack of SSO, including SSO Kerberos, SSO Microsoft Active Directory Federation Services, SSO SAML, OpenID and OAuth.
- Lack of user rights management, including support of the risk control of user access, differentiation visibility of interface forms and their fields, the ability to reset the password on the control issues and at the entrance to the OS.
- Lack of user request management, in terms of providing capability of request coordination, and the ability to split the requests into its constituent parts to the following coordination.
- Lack of functions for delegating user rights, in terms of customization logic using scripting languages, exchanging policies, and the ability to delegate rights using temporary tokens.
- Lack of functional for configuration and customization, in implementing the capability to add additional entities, user forms, custom logic, reports, role models.
- Low quality of training materials and technical support.

## 4. CONCLUSIONS

The object of analysis were security identity and access management systems, including their key features such as Authentication and Authorization methods, User registration. User rights management, Delegation of the rights, Management user requests, Reporting, Configuration and customization.

The main objective was to determine the effectiveness of existing identity and access management systems in terms of achieving the following key performance indicators: Functional characteristics in terms of the flexibility of managing user accounts, Functional characteristics in terms of integration into the information landscape of the organization, Capabilities for configuration, management and administration of security infrastructure.

**The achieved result identified the following leaders:**

- Oracle Identity Management (Oracle Corporation, USA).
- Microsoft Forefront Identity Manager (Microsoft Corporation, USA).
- SailPoint IdentityIQ (SailPoint Company, USA).

These systems provides the best functional and technical features among other security identity and access management systems. Each of these systems have different advantages and disadvantages, but in common, these systems provide the integrated platforms, which support open security standards, including related Web Services, SOA, OGSA specifications.

**The study identified the significant disadvantages of all security identity and access management systems, including :**

- The weakness of SSO implementation.
- Lack of the user request management, in terms of supporting mechanisms and scenarios, coordination and execution of user requests.
- Lack of the customization for delegation user rights using custom logic and rules.
- Lack of the functionality for reporting and publishing of security access and identity data.

## 5. ACKNOWLEDGMENTS

The Ministry of Education and Science of the Russian Federation supported the work (Agreement #14.576.21.0078, unique identifier agreement RFMEFI57614X0078).

## 6. REFERENCES


1. Whitman, M., & Mattord, H. (2013). *Management of Information Security*. Boston, MA: Course Technology.
2. Ptitsyn, P., & Radko, D. (2015). An analysis of technologies for building information security infrastructure of global distributed computing systems, *Journal of Theoretical and Applied Information Technology*, 82 (1), 1992-8645.
3. Rhodes-Ousley, M. (2013). *Information Security: The Complete Reference*. New York: McGraw-Hill Education.
4. Qing, L., & Clark, G. (2015). *Security Intelligence: A Practitioner's Guide to Solving Enterprise Security Challenges*. Hoboken, NJ: Wiley.
5. Osmanoglu, E. (2013). *Identity and Access Management: Business Performance through Connected Intelligence*. Rockland, MA: Syngress.
6. Omondi, P. (2014). *Identity & Access Management: A Systems Engineering Approach*. New York: CreateSpace Independent Publishing Platform.
7. Palat, W. (2015). *Identity and Access Management Solutions Review*. Woburn, MA: Solutions Review.
8. Merritt, M. (2015). *Balancing Customer Experience And Security With Customer Identity And Access Management*. Cambridge, MA: Forrester research.
9. IBM Redbooks. (2009). *Identity Management Design Guide With IBM Tivoli Identity Manager*. Springville: UT: Vervante.
10. IBM Redbooks. (2009). *IBM Tivoli Identity Manager 5.0 (Deployment Guide)*. Springville: UT: Vervante.
11. Marlin, B. (2008). *Oracle Identity Management: Governance, Risk, and Compliance Architecture.* Boca Raton, FL: Auerbach Publications.
12. Scheidel, J. (2010). *Designing an IAM Framework with Oracle Identity and Access Management Suite.* New York: McGraw-Hill Education.
13. Stont, V. (2014). *NetIQ Identity Manager Catalog Administrator.* Houston, TX: NetIQ Corporation.
14. Nordstrom, K. (2012). *Microsoft Forefront Identity Manager 2010 R2 Handbook.* Birmingham, United Kingdom: Packt Publishing.
15. Komar, B., & Kirsch, C. (2010). *Deploying Microsoft Forefront Identity Manager 2010 Certificate Management with Hardware Security Modules: Best Practices for IT Security.* New York: CreateSpace Independent Publishing Platform.
16. Griffiths, M. (2009). *RSA Access Manager 6.1.* Fairfax, VA: Corsec Security.
17. Booz, M., & Hamilton, L. (2015). *SailPoint IdentityIQ Supplemental Administrative Guidance*. Linthicum, MD: Cyber Assurance Testing Laboratory.
18. Wolter, K., & Avritzer, A. (2012). *Resilience Assessment and Evaluation of Computing Systems.* Berlin, Germany: Springer.
19. Mette, A. (2014). *Guide to Advanced Software Testing.* Norwood, MA: Artech House Publishers.
20. Kumar, M., & Rodrigues, P. (2010). A Roadmap for the Comparison of Identity Management Solutions Based on State-of-the-Art IdM Taxonomies, *Conference: Recent Trends in Network Security and Applications*, Chennai, India.
21. Perkins, E., & Gaehtgens, F. (2013). *Magic Quadrant for Identity Governance and Administration.* Stamford, CT: Gartner.