KuppingerCole Report

EXECUTIVE VIEW

by John Tolbert | October 2019

Curity Identity Server

Curity AB delivers a software-based API-driven identity server for businesses that need help connecting identity infrastructure, digital services, and cloud applications. Their solution adheres to many identity standards, to promote interoperability and to make it easier for clients to deploy necessary new features while shielding users from complexity.

by **John Tolbert**
jt@kuppingercole.com
October 2019

Content

Related Research

Leadership Compass: Access Management and Federation - 71102

Leadership Compass: CIAM Platforms - 79059

Leadership Compass: Adaptive Authentication -79011

Leadership Brief: Prevent, Detect, Respond: The Changing Face of IAM - 71305

1 Introduction

Many businesses and public-sector organizations are finding that they must provide better digital experiences for and offer new services to consumers who are using their services. Organizations need support for secure and convenient ways to enable employees, contractors, partners, B2B customers, and consumers to securely access resources across their digital properties. Organizations are finding that they must provide a variety of authentication methods and assurance levels to address different kinds of use cases, risk adaptive authentication and authorization mechanisms to support policy-based access controls, comprehensive identity and attribute management for workforces, self-service identity management for consumers, and identity federation for partners and B2B customers.

Some organizations want a completely customizable IAM or CIAM solution. Some may have a preference for open-source or to build their own from components. Others only need limited functionality, such as wrapping a single consumer-facing application with an identity layer. In these cases, SaaS and fully packaged C/IAM solutions may not be the best fit. Dev-centric C/IAMs allow customers to build a modular solution around existing infrastructure or services, without having to buy more features and functionality than needed. Dev-centric C/IAM solutions typically provide on-premise or IaaS options, often supporting Docker or Kubernetes. As the name implies, in order to successfully deploy a Dev-centric C/IAM system, knowledgeable developers are required.

Trends in workforce authentication are increasingly away from passwords and toward strong and/or multi-factor authentication (MFA). For partners and contractors, identity federation is a must. On the consumer side, businesses need to accept social logins and mobile devices as authentication factors. For all kinds of users, risk-adaptive authentication, the ability to “step-up”, is a necessity depending on the type of access or transaction. Compromised credential, fraud, and cyber threat intelligence can help mitigate identity related risks.

For identity and access management, the ability to provision and de-provision users in a timely manner is critical, not only for business enablement but also to diminish the possibility of data loss when employment ends. Attribute assignment and management is a key to proper policy-based access control operations. For banking, retail, insurance, and similar industries, consumers need online facilities to register, edit their information, and give/withdraw consent.

Curity AB is a privately held IT security firm headquartered in Stockholm, Sweden. They launched their identity server in 2015 with an API-first strategy and a focus on authentication, token service, and user management modules. Their current offering, the Curity Identity Server, is a solution that can be deployed on-premises or hosted in IaaS. It provides robust federation options, advanced mobile authentication using the GSMA Mobile Connect standard, and can integrate with some European bank IDs and national e-IDs.

2 Product Description

The Curity Identity Server is designed to be run on-premise or in common IaaS environments. As such, it has a very straightforward licensing model. There are three options: Basic, Standard, and Enterprise. Basic has limited capabilities; Standard is full-featured and detailed below but limited to one company; while Enterprise can be used by affiliates, subsidiaries, etc.

The Curity Identity Server is composed of three major modules: Authentication, Token Service, and User Management. The solution runs on Linux and works with Docker and Kubernetes.

Authentication

The Curity Identity Server accepts a number of different authentication methods.

- Username/password
- Knowledge-based Authentication (KBA)
- TOTP hardware tokens, such as KeyFob or Yubikey
- Mobile push notifications
- SMS OTP
- GSMA Mobile Connect
- Social logins, such as Facebook, Google, Instagram, LinkedIn, Twitter, or Windows Live
- European national E-IDs, through partnerships with Criipto and Signicat
- Swedish Bank IDs

The solution does not provide native mobile apps or leverage mobile biometrics. FIDO is not supported. Curity recommends the use of AppAuth SDK from OpenID Foundation for mobile development. SSO between environments is possible due to support for OAuth, OpenID Connect, and SAML.

Curity allows customer admins to write policies which can force step-up authentication as required by business policies. Policies can be exported/imported. Curity can call out to Axiomatics' XACML Policy Decision Points (PDPs). The authentication service has a risk engine which can evaluate various factors, including:

- IP address
- IP blacklists
- Date/time
- Device Type
- User attributes
- User history
- And more

It is possible to evaluate more advanced risk factors, such as geo-location, geo-velocity, device fingerprint, device health, behavioral biometrics, or user behavioral analysis by extending the product with its supported SDK. Likewise, Curity can accept fraud risk and cyber threat intelligence through feeds integrated with plug-ins built using the product's SDK. All operations within the authentication risk engine are accessible through the APIs.

Token Service

Functionally separate though supporting the authentication and user management modules, the Token Service is responsible for creating the appropriate token types for the other components to use. Curity supports many IAM standards, especially the OAuth family, for which they are OIDC certified. The Curity Token Service is an OAuth2 Server and OIDC Provider (OP).

The following specifications are handled by Curity's Token Service: OAuth2 Framework, Bearer Token, OAuth2 Token Revocation, OpenID Connect (OIDC), OIDC Dynamic Registration, OIDC Discovery, OAuth2 Device Flow, OAuth2 for Native App, JWT for OAuth2, JWT Response for OAuth Token Introspection, Proof Key for Code Exchange (PKCE), RESTCONF, SAML, and SCIM 2.0. The Token Services are all addressable via documented, standard-compliant APIs.

User Management

Curity allows in-provisioning over LDAP, RDBMS or SCIM. Users can be provisioned from Curity to popular SaaS apps using those standards or proprietary APIs. Some customers also utilize a consumer self-service feature for self-registration and password resets. Multiple accounts can be linked and used for account recovery when needed. Administrators can define and script name and attribute transformation for user data normalization between different domains.

Curity's User Management module is designed to integrate with existing customer portals and user data repositories, including no-SQL and SQL databases as well as LDAP.

3 Strengths and Challenges

Curity is a relatively young and growing company. They have engineered an API-focused IAM and CIAM solution based on the business requirements of their customer base. This approach aligns more closely with what KuppingerCole describes as Dev-centric C/IAM. This modularity is often attractive to companies that have existing C/IAM infrastructure that simply needs to be extended to cover new use cases, offer new services, or interoperate with partners and large customers. Curity's solution is also useful for those companies who are beginning their journey to the cloud.

Curity has comprehensive support for OAuth and OIDC, as well as SAML. They accept a number of different types of authenticators, including GSMA Mobile Connect, which will assist customers in meeting EU PSD2 Strong Customer Authentication requirements. More authentication options, particularly in the area of mobile, such as FIDO, are on the roadmap and will strengthen the offering.

Curity has a risk engine that can process some basic risk factors and allow administrators to customize workflows and step-up authentication. Additional risk factors and the ability to consume fraud risk and threat intelligence would be a benefit. The ability to call out to Axiomatics' PDPs is a useful feature.

Support for LDAP, RDBMS, and SCIM for provisioning adds flexibility. Possessing the capability to pull user attributes from both no-SQL and SQL sources is helpful for customers that store complex consumer profiles in those types of environments.

Strengths	Challenges
• Comprehensive OAuth and OIDC support • Mobile Connect authentication • Support for some bank IDs • National E-ID support for some European countries • Modular API-driven approach • Flat licensing models allow for easy growth • Enterprise license covers affiliates, subsidiaries	• Young but growing company • FIDO is not supported yet; limited mobile support • Risk engine processes a limited number of factors • Consumption of 3rd-party intelligence feeds only via SDK

4 Copyright

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 global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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

KuppingerCole Analysts AG.
WilhelmStraße 20-22
65185 Wiesbaden | Germany

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