KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert

February 11, 2021

HID Global Authentication Platform

HID Global offers robust and highly secure solutions for identity and access management, including physical access controls, smart identity card manufacturing and credential issuance, biometric authentication, and mobile/remote identity proofing. HID Global's Authentication Platform combines each of these elements into a packaged service that is suitable for B2B, B2C, B2E, and G2C use cases.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

Many organizations across both the public and private sectors are looking for modular authentication services to augment and modernize their existing IAM infrastructures. With the occurrences of data leaks and fraud on the rise, risk-adaptive and multi-factor authentication are capabilities that can help improve security postures on multiple fronts. Authentication is a pre-cursor to enterprise access control: one of many possible inputs to authorization systems. Properly implemented authentication can allow for personalization in consumer and government-to-citizen use cases, while respecting privacy as mandated by regulations via consent management.

Authentication has been one of the areas within IAM that has experienced the most technical advancement. Researchers and vendors have sought to address the inherent weaknesses of password-based authentication and have thus developed many different kinds of authenticators and protocols to increase assurance levels. Biometrics on mobile devices, out-of-band applications, mobile push notifications, and a variety of hardware tokens are visible examples. Authentication processes have also been improved by invisible measures such as the evaluation of user attributes, history, and behavioral analysis; behavioral biometrics; device identity, history, and health; and environmental context, including request types and history, locations, and networks. The unobtrusive means can operate as required in the background, only interrupting users with explicit need for input when deviations from their established baselines occur, leading to continuous, risk-adaptive authentication.

Regulations written with the goal of improving cybersecurity across various industries have taken effect in multiple jurisdictions. In the EU, the European Banking Authority's (EBA) Revised Payment Security Directive (PSD2) requires Strong Customer Authentication (SCA), which is defined in the common way of two or more factors plus risk evaluation mechanisms. This regulation has been a driver for authentication upgrades at banks, financial institutions, retailers, and other businesses across the continent. In the US, legislation such as the New York SHIELD Act imposes penalties of up to $250,000 per incident for organizations that allow unauthorized access to personal information. Therefore, stronger authentication controls are on the radar for many organizations that hold the personal data of New Yorkers.

Organizations with older IAM stack solutions in place sometimes find that they are not equipped to meet these regulatory and security challenges or take advantage of newer technologies. Modular authentication services, whether deployed on-premises or from the cloud are increasingly popular alternatives to full IAM stack upgrades or replacements.

Authentication services are important threads in Identity Fabrics, which are gaining traction in industry today. An Identity Fabric is an architecture that can be composed of disparate data sources and capabilities delivered as discrete services. Identity Fabrics permit organizations to add and upgrade segments of their infrastructure or contract with service providers to meet business objectives in a more agile manner. Given the widespread availability and adoption of cloud-hosted services running the gamut from IaaS to PaaS to

SaaS, more vendors are packaging their solutions in containers such that they can provide the same types of functions regardless of deployment models. This means that on-premise software ships as images or virtual instances that can be deployed on most of the common operating systems or IaaS/PaaS platforms or made available as micro-services via the vendor or managed service providers.

Use cases can be grouped into several major categories: Business to Employee (B2E), Business to Business (B2B), Business to Consumer (B2C), and Government to Citizen (G2C). In heavily regulated industries, strong and/or MFA may have been in place for employees and even contractors and partners for years already, but generally based on hard or soft tokens. B2C and G2C use cases where MFA is present or planned are more often served by having smartphones act as the MFA facilitator. This has spurred development of mobile app-based authenticators and secure SDKs that allow customers to create their own integrated apps. Authentication solution providers that serve all these market segments must provide a range of options that satisfy customer expectations and improve security.

Consumer IAM (CIAM) use cases are typically solved with a common set of features including self-registration, ability to deploy multiple types of passwordless MFA and account recovery mechanisms, analysis of risk factors within authentication contexts, ability to present consumer portal to manage consent, and various reporting facilities, including inbound and outbound API access for third-party identity and marketing analytics tools. SaaS delivery of CIAM services is trending upwards and will likely remain the default choice for most organizations.

2 Product Description

HID Global is a subsidiary of ASSA ABLOY Group AB of Stockholm. HID Global's US headquarters is in Austin, TX. HID Global has IAM solutions, and also makes physical access controls systems, RFID tags and readers, biometric readers, smart cards, passports and some national identity cards, card readers, and mobile apps capable of remote identity verification. Their intersection of IAM, biometrics, and SDK allows them to perform identity card issuance for a number of organizations.

HID Global Authentication Platform includes support for a plethora of authenticators, an adaptive risk engine, account recovery mechanisms, identity vetting, credential provisioning methods, and consent management. Their focus is on B2C use cases in the finance and healthcare industries, and providing G2C solutions for government agencies around the world.

HID Global authentication platform is containerized and can therefore run on-premises on servers or as appliances, or in any supported IaaS. HID Global runs the solution in AWS in EU and North American data centers as managed SaaS for customers who prefer to consume it that way. The SaaS version is ISO 27001 and SSAE SOC 2 Type 1 accredited.

Users can be provisioned using LDAP and SCIM. HID Global supports OAuth, OIDC, RADIUS, and SAML, which can be used to facilitate interoperability with other IAM and IDaaS systems.

For workforce deployments, HID Global features hardware and software tokens, desktop biometric readers, mobile device biometrics, mobile push notifications (HID Approve), x.509, CAC/PIV cards, smart cards and virtual smart cards, and USB keys. HID Global's Crescendo® Key USB-A/C authenticators are FIDO 2.0 certified and can achieve NIST SP800-63 IAL 2/3 compliance. HID Global Authentication devices, such as the desktop fingerprint readers, can directly integrate with Microsoft Windows Hello for passwordless authentication. Users can associate multiple authenticators per account to make account recovery easier in the event of lost credentials.

For CIAM environments, HID Global supports username/password, Knowledge-based Authentication (KBA), email/phone/SMS OTP, and mobile push notifications. HID Approve™ is built on FIPS 140-2 certified asymmetric key cryptography. HID Approve™ can also be used for transaction signing. Support for SCA and transaction signing enables finance customers to satisfy EU PSD2 Strong Customer Authentication (SCA) and dynamic linking requirements without exposing PII.

HID Global works with a variety of system integrator partners in the finance industry. Some implementation partners OEM (package) HID Global to serve as the authentication component of their "bank-in-a-box" offerings.

The administrative interface is intuitive and allows customers to build risk-adaptive authentication policies. All features of the admin interface are available over APIs, and many customers choose to manage the

system via these APIs rather than using the HID Global utility. Risk factors examined include device registration and fingerprints, device health assessments (include software versions), checks for presence of malware, geo-location, geo-velocity, jailbreak detection, and user and device history. The product does not currently allow for analysis of external feeds of compromised credential intelligence.

HID Global is also in the identity assurance verification and credential issuance business. Government and enterprise customers can utilize HID Global for authoritative attribute lookups, remote document verification, and electronic credential assignment. In the case of remote document proofing, users utilize the smartphone app to scan and register the authoritative documents, take selfies, and perform real-time biometric matching. Remote identity verification can be used increase identity assurance levels for self-registering consumers. Remote identity proofing has rapidly gained acceptance and has become a requirement for many consumer-facing businesses as a result of the pandemic. Remote ID proofing also facilitates Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance for financial customers. The HID Approve SDK offers a low-code approach plus strong tamper resistance to allow customers to create their own mobile apps for citizen and workforce identities.

For consumer facing scenarios, HID Global Authentication supports OAuth and OIDC. Scopes can pass entitlements. Consumers can manage consent to personal information in the user dashboard.

HID Global Authentication platform provides secure APIs for developers, including REST and WebAuthn. Moreover, OAuth, OIDC, and SAML token exchange allows HID Global Authentication platform to act as a gateway for other applications, translating authentication events with extended attribute information such as identity and authentication assurance levels for downstream consumption. Customers currently pull most information out of the solution via reports, but additional access to customer identity analytics via APIs is planned.

3 Strengths and Challenges

HID Global has an excellent reputation for identity and access control products, including a wide range of hardware tokens, readers, and other devices, as well as software, SDKs, and services. Their solutions operate in high security environments and highly regulated industries. HID Global products and services trusted at multiple key points in identity lifecycle management processes: from identity vetting, through credential issuance, attribute assignment, and runtime authentication and authorization decisions.

Remote identity verification is a valuable feature that facilitates consumer onboarding and identity verification for compliance with KYC regulations. This type of functionality is not ubiquitous in authentication solutions today, but demand will certainly increase in the months and years ahead.
HID Global has obtained several important certifications, including FIPS 140-2, ISO 27001, and SOC 2 Type 1. SOC2 Type 2 status is planned for March 2021.

HID Global has been a strong player in government and enterprise workforce IAM for years and is moving more into consumer IAM. They have the technology that is well-suited for consumer authentication scenarios, especially mobile.

Strengths

- Wide range of MFA types
- FIDO 2.0 certification
- Strong support for relevant IAM standards
- Product suite designed to meet high security requirements
- Architected to help finance customers achieve compliance with AML, KYC, and PSD2
- Identity vetting and strong credential issuance, including support for remote document verification

Challenges

- Needs social network registration and logins for CIAM use cases
- Does not process 3rd-party intel sources
- Needs connectors for SaaS apps, IGA and PAM solutions

4 Related Research

Buyer's Compass: Consumer Identity and Access Management Solutions - 80111
Leadership Brief: 5 Steps to Consumer Identity and Access Management - 72549
Leadership Compass: CIAM Platforms - 80040
Leadership Compass: Consumer Authentication – 80061
Leadership Compass: Identity API Platforms - 79012

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, 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 back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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