Knowledge Brief

Quadrant Knowledge Solutions

KeyScaler by Device Authority is a Leader in SPARK Matrix: IoT Identity and Access Management (IoT IAM), 2023

Quadrant
Knowledge Solutions

2023
SPARK MATRIX
LEADER

IoT Identity and Access
Management (IoT IAM), 2023

An Excerpt from Quadrant Knowledge Solutions
“SPARK Matrix: IoT Identity and Access Management (IoT IAM), 2023”

KeyScaler by Device Authority is a Leader in SPARK Matrix: IoT Identity and Access Management (IoT IAM), 2023

Even as the Internet of Things (IoT) has emerged as the most widely embraced technology has found its way into numerous sectors, including consumer businesses, industrial applications, energy and utilities, building and facilities management, mobility, infrastructure, and more, this widespread adoption is also enhancing the associated security concerns. These concerns encompass a broad spectrum, ranging from global geopolitical tensions to the security of smart home devices. Consequently, organizations of all sizes have made it a top priority to safeguard IoT devices against threats like hacking, data breaches, and privacy issues. This push for security measures is driven by both efforts within companies and the enforcement of strict regulatory frameworks, such as the General Data Privacy Rule (GDPR) and the California Consumer Protection Act (CCPA). In response to the growing cybersecurity challenges, numerous technology vendors have embarked on the development of Identity Access Management (IAM) solutions. These IAM systems are designed to seamlessly integrate with both legacy and modern IoT devices, providing comprehensive coverage for IoT security concerns.

Conventional Identity Access Management (IAM) systems tailored for IoT have traditionally centered on human identities, making it difficult to accommodate devices and other identity types. Standard IAM measures, such as multi-factor authentication (MFA) or even traditional authentication methods like user IDs and passwords, may not directly apply to these entities. Therefore, IoT providers must utilize various protocols like MQTT (MQ Telemetry Transport), CoAP (Constrained Application Protocol), XMPP (Extensible Messaging and Presence Protocol), and others to enable entities to authenticate themselves. However, despite the availability of these established authentication options, vendors are encountering significant challenges when attempting to implement them comprehensively across all IoT entities. This is primarily due to IoT necessitating an entirely different approach to identity classification.

In modern IoT Identity and Access Management (IAM) strategy, the focus extends to encompass people, devices, and applications, all sharing similar interaction requirements. Recent developments in IoT IAM platforms primarily address fundamental challenges to facilitate IoT adoption and realize envisioned benefits.

These benefits include establishing and managing device identity for trust, integrating with data trust policies, ensuring end-to-end data security, enhancing operational efficiency, and automating IoT scalability. Various vendors now offer SaaS-based platforms with proven technologies like PKI scanners.

According to Quadrant Knowledge Solution's research findings, the widespread adoption of IoT-based smart devices is reshaping traditional, people-centric IAM solutions. These solutions are evolving to include identities of diverse entities, such as people, services, and objects, all within a unified IAM framework. Given the multifaceted nature of IoT entities, defining relationships between them, such as between a device and a human or between a device and an application, becomes crucial. This is where the concept of Identity of Things (IDoT), an extension of IAM, comes into the picture to define these relationships.

Quadrant Knowledge Solutions' SPARK MatrixTM: IoT Identity and Access Management (IoT IAM), 2023 research includes a detailed analysis of the global market regarding short-term and long-term growth opportunities, emerging technology trends, market trends, and future market outlook. This research provides strategic information for technology vendors to better understand the existing market, support their growth strategies, and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

The research includes detailed competitive analysis and vendor evaluation with proprietary SPARK MatrixTM analysis. SPARK MatrixTM includes ranking and positioning of leading IoT IAM vendors with a global impact. The SPARK MatrixTM includes an analysis of vendors, including Device Authority, DigiCert, Entrust, ForgeRock, Global Sign, HID Global, Keyfactor, Okta, Palo Alto, Ping Identity, Sectigo, and Trustwave.

Market Dynamics and Technology Trends

The following are the key market and technology drivers as per Quadrant Knowledge Solutions' IoT Identity and Access management (IoT IAM) strategic research:

- IoT IAM providers offer a comprehensive and robust security framework by combining the Zero Trust and SBOM approaches. The Zero Trust approach offers continuous assurance by authorizing devices, users, and applications.

The SBOM approach helps provide transparency and visibility into the software assets and enables better vulnerability and risk management.

- Within a Zero Trust framework, Machine identities are being established with Role Based Access Control (RBAC), and policies or guidelines are set to regulate the lifecycle of identities. Continuous verifications are being done to ensure that only the required data is being accessed by the devices and avoid unauthorized access.

- Information Technology and Operational Technology convergence has become an important aspect of IoT as it involves using IT security practices to safeguard the OT devices, policies, protocols, and management strategies. It helps protect organizational IoT infrastructure against cyber threats and vulnerabilities to offer an integrated and secure operational environment. This approach provides improved visibility and control over IoT devices with a single view of the entire IoT infrastructure and helps implement security information and event management (SIEM) solutions, through which data on suspicious activities are identified and collected.

- IoT IAM providers are offering IAM for cloud services as well. They achieve this by integrating IAM platforms with cloud tools and ensuring that only authorized users or devices access the resources in the cloud. This also helps automate provisioning and identity creation.

- AIoT is a market driver in the IoT market, as it involves AI's integration with IoT security. This approach allows advanced threat detection, predictive analysis, and faster response mechanisms. This integration also enables protection against emerging threats and streamlining operations within the IoT environment.

- Crypto Agility is an important trend in the IoT security market. It refers to the capacity to adapt to new encryption standards and involves investing in PQC-ready features within certificate authorities (CA), toolkits, and cryptographic lifecycle management (CLM) systems without overhauls or disruptions.

- IoT IAM platforms adopt TPM (Trusted Platform Module), a specialized hardware component for device integrity and secure cryptographic operations. It securely stores sensitive information like encryption keys, certificates, and measurements of the device's state. It helps verify that the device hasn't been tampered with or compromised. It also performs cryptographic operations such as generating, storing, and managing encryption keys. This ensures secure communication and data protection within the IoT ecosystem.

SPARK Matrix Analysis of IoT Identity and Access Management (IoT IAM) Market

Quadrant Knowledge Solutions conducted an in-depth analysis of the major IoT Identity and Access management (IoT IAM) vendors by evaluating their product portfolio, market presence, and customer value proposition. Metadata management market outlook provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK MatrixTM. SPARK Matrix analysis offers a snapshot of key market participants and a visual representation of market participants. It offers strategic insights on how each vendor ranks related to their competitors based on their respective technology excellence and customer impact parameters. The evaluation is based on primary research, including expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall metadata management market.

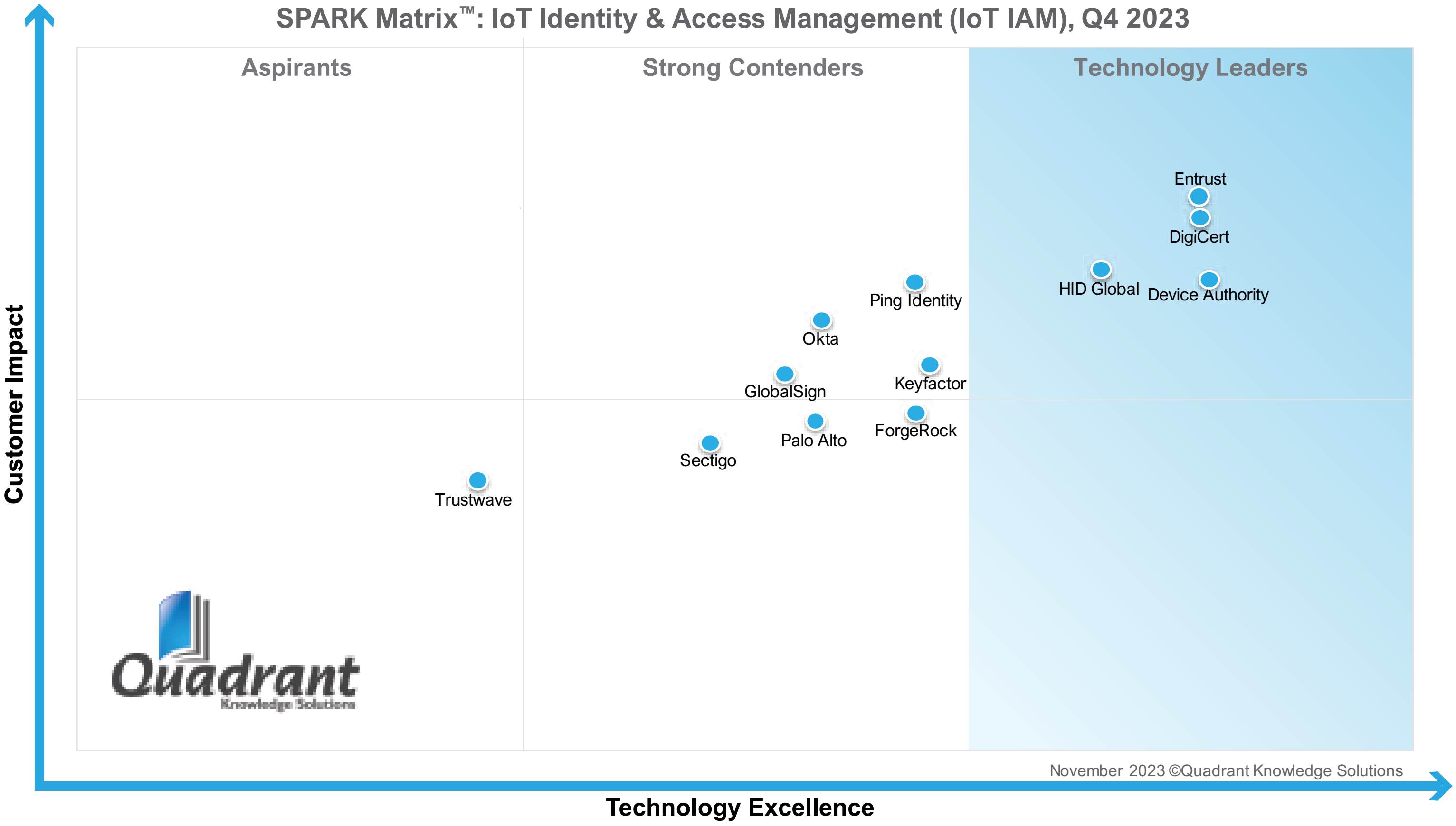
According to the SPARK Matrix analysis of the global IoT Identity and Access management (IoT IAM) market, "KeyScaler by Device Authority, with its unique enterprise-grade IoT IAM solution, has secured strong ratings across the performance parameters of technology excellence and customer impact and has been positioned as a technology leader in the 2023 SPARK Matrix of the IoT Identity and Access Management (IoT IAM) market."

Technology Excellence	Weightage	Customer Impact	Weightage
Device authentication and authorization	20%	Product strategy and performance	20%
Certificate and key management	20%	Market presence	20%
Device lifecycle management	15%	Proven record	15%
Scalability	15%	Ease of deployment and ease of use	15%
Device Security	10%	Customer service excellence	15%
Policy management and compliance	10%	Unique value proposition	15%
Analytics and reporting	5%		
Vision and roadmap	5%		

Figure: 2023 SPARK Matrix™

(Strategic Performance Assessment and Ranking)

IoT Identity and Access Management (IoT IAM) Market



KeyScaler by Device Authority

URL: https://www.deviceauthority.com/

Company Introduction

Founded in 2016 and headquartered in Reading, UK, Device Authority is a provider of Identity and Access Management (IAM) solutions for the Internet of Things (IoT). Device Authority provides a device-centric IAM platform titled KeyScaler that offers automated devices and data security in a connected device environment.

Product Introduction

Device Authority offers a SaaS-based security automation platform with full Edge orchestration and AI & ML-based device and data trust titled KeyScaler. KeyScaler includes comprehensive capabilities to secure device registration and provisioning and provides end-to-end data encryption, automated certificate management, automated password management, tokenized authentication, secured IoT device software and firmware updates, and network access control functionality.

Technology perspective

Following is the analysis of Device Authority's capabilities in the global IoT Identity & Access Management market:

- Device Authority's IoT Identity and Access Management (IoT IAM) platform, KeyScaler offers advanced features for the deployment and administration of Public Key Infrastructure (PKI) of IoT devices. The platform offers a highly adaptable Life Cycle Management solution that aids in safeguarding, accelerating, and overseeing IoT devices. KeyScaler manages the complete identity lifecycle, encompassing device registration, integration with enterprise security, linkage with IoT/Cloud applications, compliance with security policies, and the revocation of device identities in cases of theft, ownership transfer, or device retrieval.

- KeyScaler's patented trust anchor technology, Dynamic Device Key Generation (DDKG) validates the integrity of each device during every authentication process, involves a response mechanism and unique keys based on the device's hardware entropy, eliminates the possibility of device clones and other impersonation attempts and ensures that only valid devices are being connected or registered to the IoT environment.

- KeyScaler provides pre-established integrations built upon its core platform, harnessing PKI infrastructure, enterprise applications, cloud services, and threat intelligence. Through the EPIC framework, KeyScaler simplifies integration with third-party systems via MQTT or real-time connectivity, using KeyScaler's authorization service connector.

- KeyScaler Edge facilitates the convergence of IT and OT (Operational Technology), enhancing device visibility while keeping device identity records up to date at the cloud application layer. KeyScaler AI introduces native capabilities to organizations, enabling enhanced device discovery, detection of abnormal behavior, and the automatic generation of alerts and recommended actions, preempting potential breaches.

- KeyScaler's HSM Access Controller empowers administrators to manage connected Hardware Security Modules (HSMs), allowing for key generation, data signing, data encryption, and secure storage of public keys. Device Authority Secure Data Repositories offer centralized encrypted data storage for securely sharing data with authorized entities. Additionally, Device Authority provides automated password management, facilitating automatic configuration and control of device passwords. It also enables the enforcement of real-time security policies and access restrictions for unauthorized users. Furthermore, it provides client-side software development kits (SDKs) and libraries for seamless integration into both new and existing applications.

- Device Authority offers PKI Signature+ as an authentication option designed for low-power devices ineligible for Dynamic Device Key Generation. It eliminates the need for manual processes by automating the delivery of PKI security (keys and certificates) and associating them with physical or virtual devices on a large scale.

- The KeyScaler platform employs an Enhanced Platform Integration Connector for effortless integration with any Application Enablement Platform (AEP)/IoT platform and Hardware Security Module (HSM)/Certificate Authority (CA). Device Authority offers automatic secure updates for organizations, simplifying the management of code signing, delivery, and installation to ensure the reliable verification of IoT device updates.

- KeyScaler continually performs authorization checks, validates software versions, searches for vulnerabilities, ensures hardware integrity, verifies compliance with policies, detects behavioral anomalies, monitors device processes, and reports any identified threats.

- KeyScaler employs SBOM (Software Bill of Materials) automation for IoT device resilience to pack and update events related to connected devices within the SBOM assurance hub. Whenever a device connects, registers, or requires authentication, the KeyScaler authorization engine consults the SBOM assurance hub for compliance history. Access is granted, or devices are quarantined accordingly.

- The key differentiator of KeyScaler is it is offered as a Software-as-a-Service (SaaS) model, which ensures quicker deployments and increased adaptability with rapidly evolving requirements. KSaaS (Keyscaler-as-a-Service) centralizes data availability by supporting industry-specific AI models and enhancing protection levels. KSaaS was also awarded as 2023's Microsoft Partner of the year for rising Azure Technology.

- Device Authority's KeyScaler delivers device-specific identity, authentication, and data security, establishing trust for both devices and data at the application layer. It also covers code signing, security updates, zero-touch provisioning, and operational security. Additionally, it seamlessly integrates with cloud platforms, enterprise infrastructure, and PKI trust infrastructure, such as Hardware Security Modules (HSMs) and Certificate Authorities (CAs).

Market perspective

- From a geographical presence perspective, Device Authority has a strong presence in North America and EMEA, with recent expansion in APAC. From an industrial vertical perspective, the company's primary verticals include transportation/logistics, healthcare, energy/utilities, govt & public sector, manufacturing, retail, telecommunication, food & beverages, BFSI, eCommerce, and gaming.

- From a use case perspective, Device Authority's solutions cater to a wide range of use cases, including key management, storage & distribution, supply chain, edge device identity orchestration, automated device identity lifecycle management, end-to-end data encryption, and HSM Access control.

Roadmap

As a part of its technology roadmap, Device Authority is focusing on improving the control panel UI, Open DDKG & DDKG Lite for flexible KeyScaler-Ready solutions on any device, KeyScaler Edge feature support and post-quantum support for KeyScaler platform, device certificates, and DDKG.