KNOWLEDGE BRIEF

Device Authority is Leader in SPARK Matrix™: IoT Identity & Access Management (IoT IAM), 2020

KNOWLEDGE BRIEF

BY

Quadrant Knowledge Solutions

Device Authority is Leader in SPARK Matrix™: IoT Identity & Access Management (IoT IAM), 2020

IoT Identity & Access Management (IoT IAM) market consists of vendors that offer a scalable solution for deploying and managing security keys and certificates to enable device identity and integrity to be cryptographically proven and validated throughout its lifecycle. Securing IoT devices require a purpose-built device-centric IAM solution as traditional employee-centric IAM or customer IAM (CIAM) solutions are not capable of addressing IoT-specific challenges. Traditional IAM systems were designed to enforce access control policies for the users and their access to enterprise networks, applications, and data. These systems are not capable of handling billions of IoT devices, their identities, and communications with other entities, including other devices, people, and applications on the network. A purpose-built IoT IAM solution capabilities, include massive scalability & availability to handle a wide variety and volume of IoT devices, secure device registration & provisioning, end-to-end data encryption, device authentication, compliance management, and centralized policy management. The unique capability required in IoT IAM is device-bound assurance for both identity and data as one cannot apply traditional IAM methods of multi-factor, user or another entity involvement for trust in typical IoT M2M interactions at scale. The scope of IoT IAM needs to extend the model throughout the device journey starting from secure-by-design, which global government organizations are already enforcing regulations around. In March 2018, the UK government published a report titled “Secure by Design: Improving the cyber security of consumer Internet of Things Report”

As part of the research “SPARK Matrix™: IoT Identity & Access Management (IoT IAM), 2020” Quadrant Knowledge Solutions conducted an in-depth analysis of major IoT IAM vendors by evaluating their products, market presence, and customer value proposition. Based on the analysis, the study provides competition analysis and ranking of the leading vendors in the form of SPARK Matrix. The evaluation is based on the primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall IoT IAM platforms market. The SPARK Matrix evaluation examined Device Authority and ten other vendors, including Blue Ridge Networks, DigiCert, Entrust Datacard, ForgeRock, GlobalSign, KeyFactor, Mocana, Ping Identity, Rambus, and Rubicon Labs.

Quadrant Knowledge Solutions research analyzes market dynamics, growth opportunities, emerging technology trends, and the vendor ecosystem of the global market. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendor capability, competitive differentiation, and its market position.

Driven by the impact of Covid-19, the global economy, along with industries, is facing significant challenges and negative growth. While Covid-19 has impacted the market for overall digital transformation projects and associated IoT security solution, the overall growth outlook looks promising for IoT IAM market. IoT IAM market is currently in the nascent stage with the presence of multiple vendors marketing their traditional IAM solutions to support the requirement of IoT IAM solution. Additionally, the specialized IoT IAM vendors are currently engaging with numerous small scale and pilot projects to establish the authenticity and effectiveness of a purpose-built IoT IAM solution. However, the widespread adoption of IoT analytics and edge analytics platform is driving the need for a purpose-built device-centric IoT IAM solution.

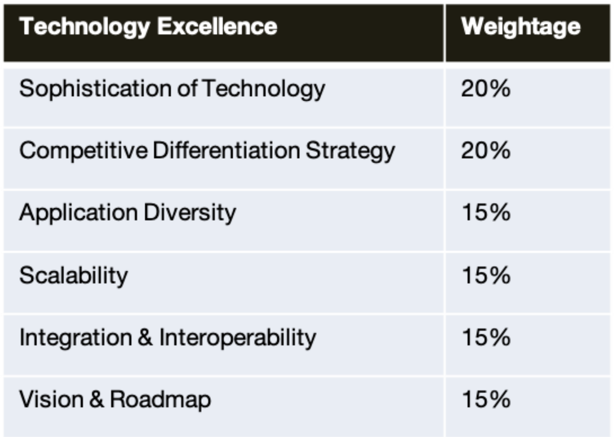
Despite the economic recession and negative impact on technology investments, the IoT IAM market is expected to continue its growth momentum in 2020, and during the forecasted years of 2020-2025. However, the forecasted growth rate for the year 2020 is significantly lower than our last year forecast for the same year. Quadrant analysts believe that from the year 2021 onwards, the technology investments will rise again mainly driven by the pent-up demand and economic recovery for the key industrial, energy, automotive, healthcare, connected cities and infrastructure market.

The primary drivers for the IoT IAM market growth include continued emphasis and investments on digital transformation projects across industry sectors and geographical regions; increasing frequency of IoT-specific cybersecurity attacks, including DDoS, malware, spoofing, data breach, and others; growing confidence of purpose-built IoT IAM solutions with multiple successful demonstrations through pilot projects as well as full-scale deployments; continued investments by IAM leaders to their product strategy, marketing messaging, and technology innovation budgets to provide scalable IoT IAM solution; increasing partnership with IoT analytics and edge analytics platforms; growing popularity of next-generation of wireless technologies, such as LP-WAN, 5G, and Gigabit LTE; and such others. From a long-term trend perspective, IoT IAM market is expected to evolve towards an integrated IoT security solution to include the integrated solution for root-of-trust, device-centric identity and access management, end-to-end data security, comprehensive device visibility and granular access control, and such others.

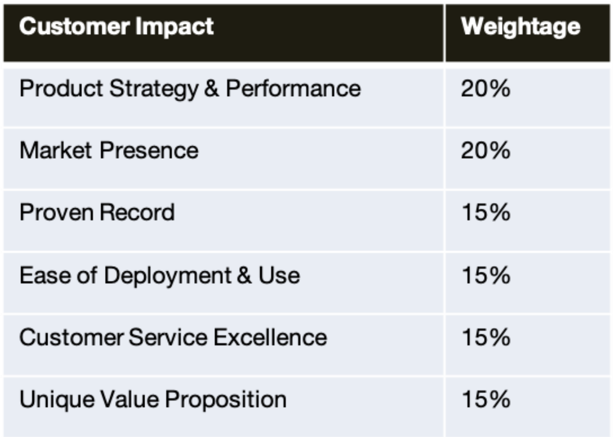
SPARK Matrix™ Analysis of the IoT Identity & Access Management Market

Quadrant Knowledge Solutions conducted an in-depth analysis of the major IIoT platforms vendors by evaluating their product portfolio, market presence, and customer value proposition. The IoT identity & access management research provide competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK MatrixTM.

SPARK Matrix analysis provides 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, concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision makings, such as finding M&A prospects, partnership, geographical expansion, portfolio expansion, and similar others. The evaluation is based on the primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall IoT IAM market.



Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%

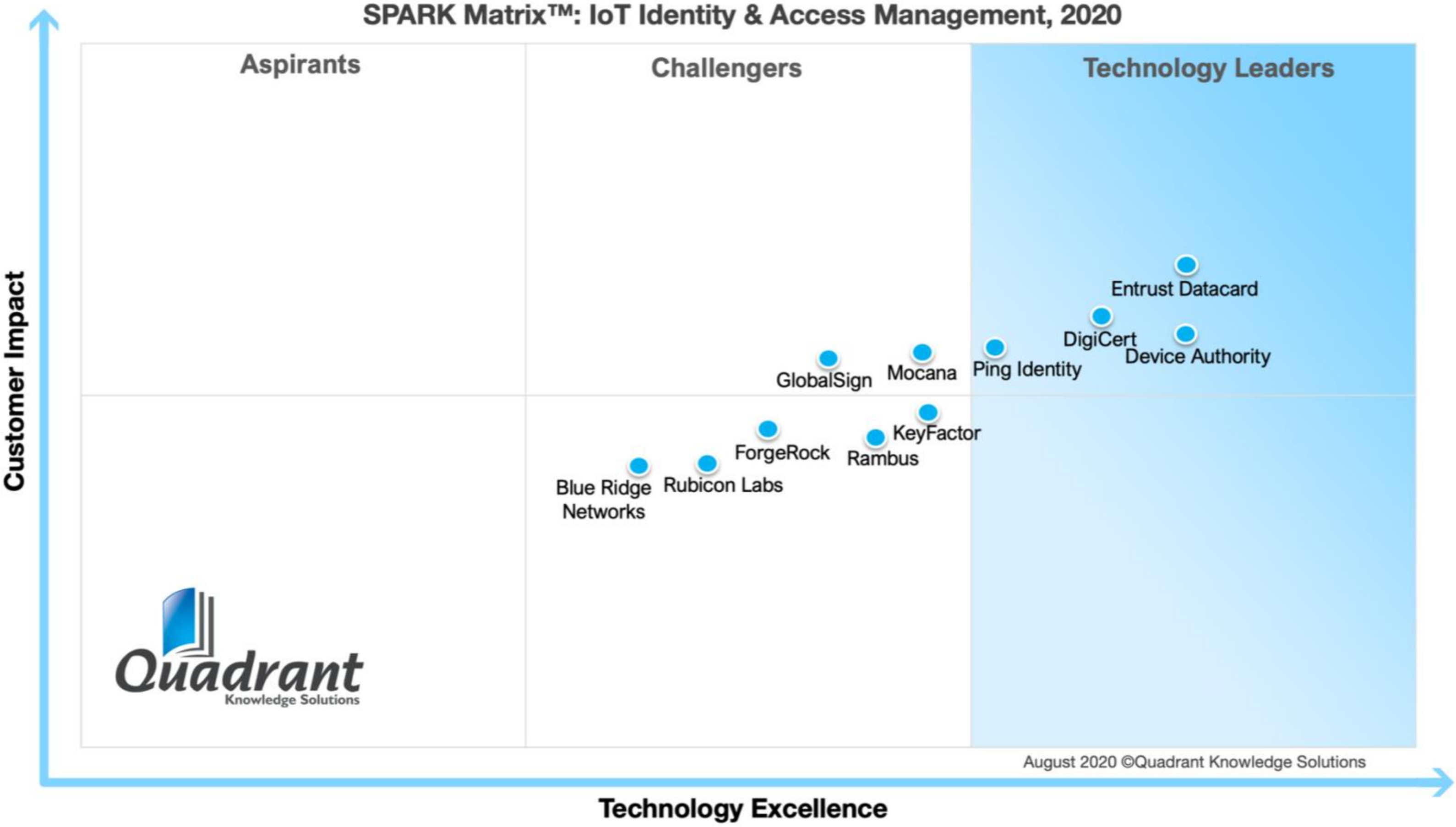


Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

Figure: 2020 SPARK Matrix

(Strategic Performance Assessment and Ranking)

IoT Identity & Access Management (IoT IAM) Market



Device Authority Capabilities in the Global IoT IAM Market

Founded in 2016 and headquartered in Reading, UK, Device Authority is the provider of identity and access management solutions for the Internet of Things (IoT). KeyScaler is the device-centric IAM platform from Device Authority that offers device bound data security for IoT devices.

KeyScaler offers comprehensive IoT security solution with capabilities for secure device registration and provisioning, end-to-end data encryption, automated certificate management, automated password management, tokenized authentication, secure updates of software and firmware on IoT devices, network access control functionality, and such others. KeyScaler provides secure & automated provisioning and onboarding of IoT devices through strong root keys & certificates. KeyScaler provides policy-driven end-to-end data encryption for secure delivery and storage of data. KeyScaler ensures IoT device certificates and keys are securely generated, provisioned, managed and signed through policy-driven automation. It also includes an optional feature “Secure Soft Storage” to store certificates and the associated keys encrypted in the device for additional security against theft and unauthorized use.

KeyScaler platform includes Automated Password Management (APM) solution that enables organizations to set and manage local account password on IoT devices at scale. APM significantly helps to reduce the attack surface by enforcing password rotation policies on the devices. KeyScaler provides tokenized security for policy-driven IoT security operations through Delegated Security Management (DSM). DSM provides device makers and IoT applications with a turnkey, plug-and-play IoT security suite that is easy to deploy & manage and provides policy-driven automation for scalability. The comprehensive out-of-the-box security suites for Microsoft Azure and PTC ThingWorx allow customers to quickly implement, accelerate deployment and leverage their existing investments in Microsoft and PTC infrastructure. KeyScaler platform helps in preventing unauthorized software and firmware updates on IoT devices. The platform provides Secure Update and Data Signing solution to ensure software updates are encrypted and restricted to only authorized devices.

Backed by the company's flexible device interface protocol, KeyScaler offers two alternatives for device authentication: agentless PKI Signature+ and agent-based patented Dynamic Device Key Generation (DDKG). KeyScaler’s

Enhanced Platform Integration Connector (EPIC) allows for easy integration with any external platforms and services. KeyScaler also provides configurable service connectors for AWS IoT services and interoperability with public certificate authorities (CA), such as IdenTrust (part of HID Global) or DigiCert. KeyScaler platform includes a Hardware Security Modules (HSM) Access Controller for secure and easy integration of applications, services and devices with off-the-shelf HSMs, via a standard set of RESTful APIs.

KeyScaler platform includes Network Access Control (NAC) functionalities suitable for IoT environment. KeyScaler platform leverages PKI certificates to authorize specific devices to register into the network. The platform can automate the process of managing device identity, device registration & onboarding, PKI lifecycle management for devices, and also provides integration with Microsoft Active Directory for validation during the network authentication process.

Device Authority has partnered with leading IoT platforms including PTC ThingWorx, AWS IoT, and Azure IoT; HSM products including nCipher and Thales (Gemalto); certificate authority including IdenTrust (part of HID Global) and DigiCert. Built on a service-oriented architecture, KeyScaler offers multiple deployment options like on-premise, SaaS, or as a multi-tenant service platform for cloud and service providers.

Analyst Perspectives and Differentiators

Following is the analysis of the Device Authority capabilities in the IoT IAM market:

- Device Authority KeyScaler platform offers robust IoT security solution through a unified trust model by combining device and data trust. KeyScaler IoT IAM platform provides sophisticated functionalities to deploy and manage PKI for IoT devices at scale through automated device onboarding, zero-touch provisioning, authentication, credential management, and end-to-end policy data encryption.

- KeyScaler is device and platform independent, with features like "secure by design", patented DDKG for robust authentication, device bound identity and data security, security suites for IoT platforms for easy integration, EPIC, HSM Access Controller and robust partner ecosystem. The device-bound identity and data security model is unique for this platform and helps to meet the unified security and lifecycle requirements for critical IoT use cases.

- KeyScaler comprehensive architecture enables itself to perform in high security and compliance-driven use cases. Some of the top use cases for KeyScaler deployment include meeting GDPR & HIPAA compliance, PKI certificate & token management, automated identity & data security management and such others.

- From verticals perspective, Device Authority's prime focus is healthcare and medical devices followed by the manufacturing and automotive sectors. Geographically, Device Authority caters to the European Union and America market, with plans to further expand the customer base in the USA.

- As part of the technology roadmap, Device Authority continues to invest in improving its platform by enhancing AI/ML-based authorization, Blockchain identity and access management, user-managed access and 5G.