KNOWLEDGE BRIEF

Device Authority is Positioned Amongst 2019 Technology Leaders in the SPARK Matrix Analysis of IoT IAM Market

KNOWLEDGE BRIEF

BY

Quadrant
Knowledge Solutions

Device Authority is Positioned Amongst 2019 Technology Leaders in the SPARK Matrix Analysis of IoT IAM Market

IoT devices are increasingly becoming an integral part of business as well as industrial operations. IoT devices are widely being adopted from a simple functionality of tracking product use and re-order alerts to a complex application of inter-connected products with built-in intelligence to communicate and take actions. Widespread adoption of smart IoT devices in various business and industrial applications have significantly increased attack surface as well as the number of potential threats. Growing security concern has emerged as the biggest barrier in the adoption of IoT devices for industrial applications since a compromise in IoT security can have far more devastating consequences from monetary loss, data loss, to the life-threatening impact.

The scale of internet-connected devices, applications, data and users has grown tremendously in the past few years. With more and more devices connected to the internet, the threat of cybercrime has increased and thereby the need to secure IoT devices has become a prime concern across industry segments. 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.

IoT IAM market includes 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. 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.

Quadrant Knowledge Solutions recent study "Market Outlook: IoT Identity & Access Management (IoT IAM), 2019-2024, Worldwide" analyses 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.

SPARK Matrix Analysis of the Global IoT IAM Market

Device Authority is Positioned amongst the 2019 Technology Leaders in the Global IoT IAM Market

Quadrant Knowledge Solutions conducted an in-depth analysis of the major IoT IAM vendors by evaluating their product portfolio, market presence, and value proposition. The IoT IAM market outlook provides competitive analysis and a ranking of the leading vendors in the form of proprietary SPARK Matrix. SPARK Matrix analysis provides a snapshot of key market participants and a visual representation of market participants and provides 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. 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%

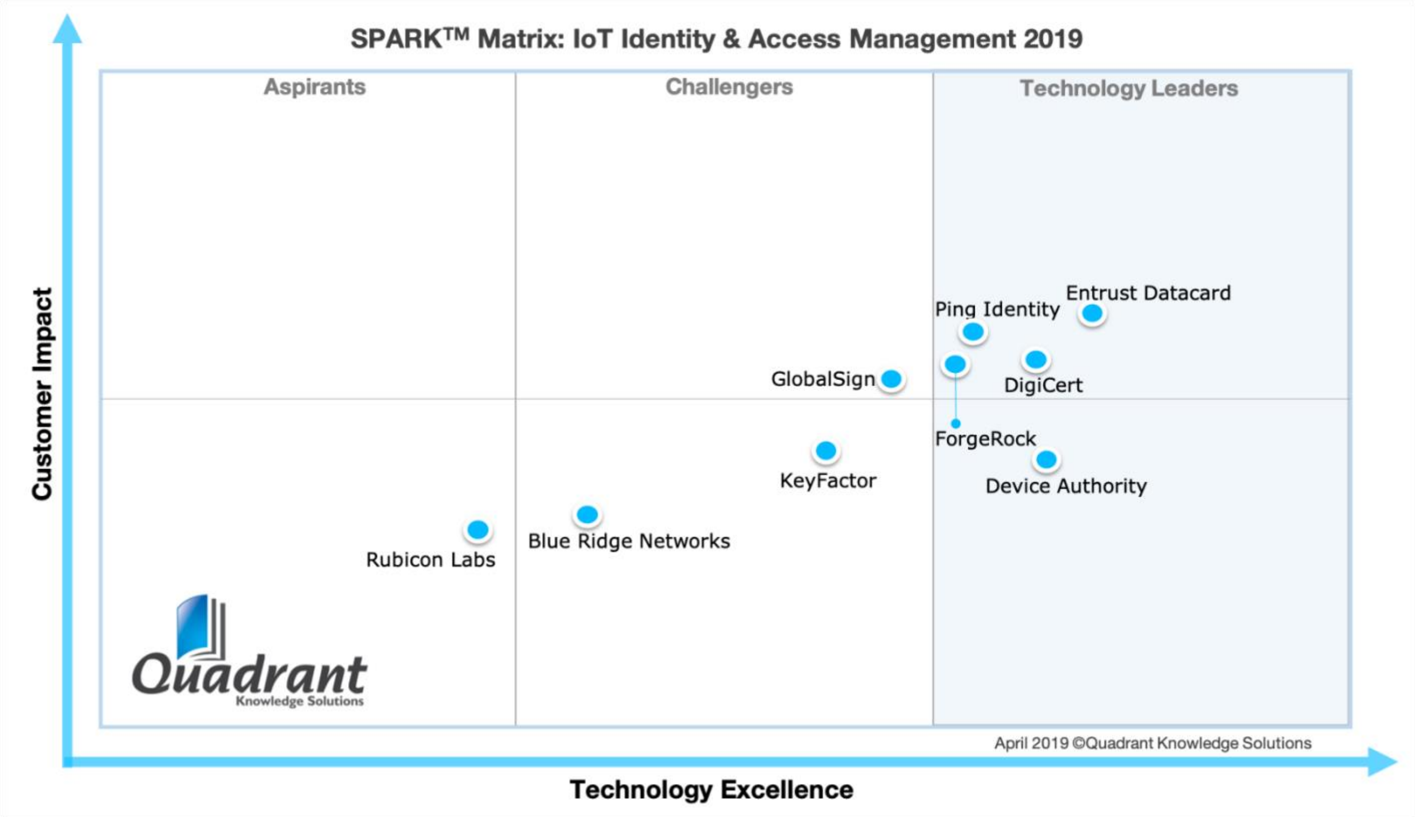
According to the SPARK Matrix analysis of the global IoT IAM market, Device Authority, with the comprehensive IoT Identity & Access Management (IoT IAM) capability, is positioned amongst the 2019 technology leaders in the global market. Device Authority's leadership recognition is driven by its comprehensive technology platform, advanced functional capabilities, and strong overall customer impact.

"Device Authority with its advanced IoT IAM platform and continued focus on building strong partnership initiatives is well positioned to help organizations in delivering automated device provisioning, authentication, and end-to-end policy-based data security solution to accelerate IoT adoption at scale," according to Piyush Dewangan, Industry Research Manager at Quadrant Knowledge Solutions. "The company has demonstrated its technology value proposition with multiple successful

Proof of concept (POC) implementation in the industrial, medical, and healthcare sector. With the right competitive and growth strategy, Device Authority is well positioned to cause major disruption in the global IoT IAM market," adds Dewangan.

Figure: 2019 SPARK Matrix

(Strategic Performance Assessment and Ranking)



Device Authority's Capabilities in the Global IoT Identity & Access Management (IoT IAM) Market

KeyScaler delivers comprehensive IoT security solutions with 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 platform is built on a service-oriented architecture and can be deployed as SaaS, on-premise, or as a multi-tenant service platform for cloud and service providers.

- **Device Registration, Onboarding and Provisioning**: KeyScaler enables policy-driven registration control for secure and automated onboarding and provisioning of IoT devices at scale. It helps in securing the integrity of the IoT applications and the associated data processing. KeyScaler platform supports device authentication through its Dynamic Device Key Generation (DDKG) and PKI Signature+ methods. DDKG provides hardware-level device identification and generates dynamic device keys unique for each authentication session. DDKG is provided as a development library, with documentation and source code samples, which can be added to new or existing applications. PKI Signature+ is designed for lightweight devices and leverages existing public keys to authenticate devices to the KeyScaler platform. PKI Signature+ is based on an agent-less and developer-independent implementation suitable for low-power embedded devices.

- **Data Security and Compliance**: KeyScaler platform helps in ensuring policy-driven end-to-end data encryption leveraging its patented dynamic key generation, device-derived key technology and crypto-policy agents. The crypto-policy agent provides application-level encryption and is configurable for specific data payloads and transmission. The agent processes and encrypts a large amount of data generated at the device and network edge. It helps in meeting the compliance requirements for data security, and privacy, including GDPR, HIPAA, and others.

- **Automated Certificate Management**: KeyScaler ensures IoT device certificates and keys are securely generated, provisioned, managed and signed through policy-driven automation. With automation, it provides scalability to deploy a large scale IoT implementation. 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 also provides configurable service connectors for AWS IoT services and interoperability with public certificate authorities (CA), such as IdenTrust (part of HID Global), Sectigo or DigiCert.

- **Automated Password Management**: 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.

- **Token Authentication**: KeyScaler platform includes Delegated Security Management (DSM), a tokenized security model for enforcing policy-driven IoT security operations. DSM helps to integrate secure and dynamic device authentication into IoT platforms using standardized public key signatures. As part of the DSM model, the device first authenticates with KeyScaler and receives a short-lived singed authentication token. The IoT platform uses the KeyScaler public keys to validate the signature and verify the metadata in the authentication token for a secure device connection. IoT platforms can leverage KeyScaler platform to delegate key security operations, including enforcing certificate management policies, device updates, password management, and identity validation checks. These security operations are enforced before issuing an authentication token to the IoT devices to ensure that the device is compliant to security policies before its connection to the IoT platform.

- **Secure Update**: KeyScaler platforms 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. Secure Update solution verifies the update sources and integrity of the updates to facilitates end-to-end protection for device updates. The solution is transport agnostic and supports various transport protocols for both Over-the-Air (OTA) and Over-the-Network updates.

- **Network Access Control (NAC) for IoT**: Traditional NAC solutions are not suitable for IoT application as it requires significant scalability to support huge volume and a wide variety of IoT devices. Additionally, since most of the IoT devices are headless with no GUI and no users to self-remediate, it creates further complexities for implementing access control policies. KeyScaler platform includes network access control 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 (AD) for validation during the network authentication process. Device Authority also provides connectors to enterprise HSMs, such as nCipher Security nShield, Gemalto SafeNet and CAs such as IdenTrust (part of HID Global), Sectigo and DigiCert.

Competitive Differentiation and Strengths

Device Authority's KeyScaler is a purpose-built device-centric IAM platform and delivers device bound data security solution to support IoT-specific use cases. Device Authority's technology differentiation can be attributed to its sophisticated functional capabilities, technology innovations, and the ability to support massive scalability required to protect IoT devices, applications, and data. Device Authority KeyScaler platform with 15 technology patents offers strong authentication and authorization capabilities suitable for IoT-specific security requirements. The company's patented Dynamic Device Key Generation (DDKG) technology provides a robust authentication model that ensures secure device registration, onboarding, and provisioning of devices IoT scale.

Device Authority has partnered with leading IoT platforms including PTC ThingWorx, AWS IoT, and Azure IoT; HSM products including nCipher and Gemalto; certificate authority including IdenTrust (part of HID Global), DigiCert and Sectigo. The company continues to focus on building a robust ecosystem of partners with system integrators, mobile network operators, device OEMs and gateway provides, and such others. Device Authority has significantly grown its revenue and client-base since it has launched KeyScaler platform in 2017. The company, with several successful POC implementations and transitioned to full-scale production, is expected to grow its revenue many-fold in the next two to three years.

The Last Word

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. IAM solution for IoT requires a purpose-built platform that enables organizations to manage device authentication, identity management and governance at IoT scale.

Device Authority’s KeyScaler IoT IAM platform provides comprehensive functionalities to deploy and manage PKI for IoT devices at scale through automated device onboarding, provisioning, authentication, credential management, and end-to-end policy data encryption. Device Authority, with its comprehensive end-to-end IoT IAM capabilities, has received strong ratings for its sophisticated technology platform, competitive differentiation strategy, integration & interoperability, technology vision, and overall customer impact. Driven by strong overall ratings, Device Authority has been positioned amongst the technology leaders in the 2019 SPARK Matrix analysis of the global IoT IAM market.