ABI RESEARCH COMPETITIVE RANKING

ENTERPRISE PUBLIC KEY INFRASTRUCTURE VENDORS

ENTRUST

OVERALL: 92.4 | INNOVATION: 89.1 | IMPLEMENTATION: 95.7 | RANK: 2

ENTRUST

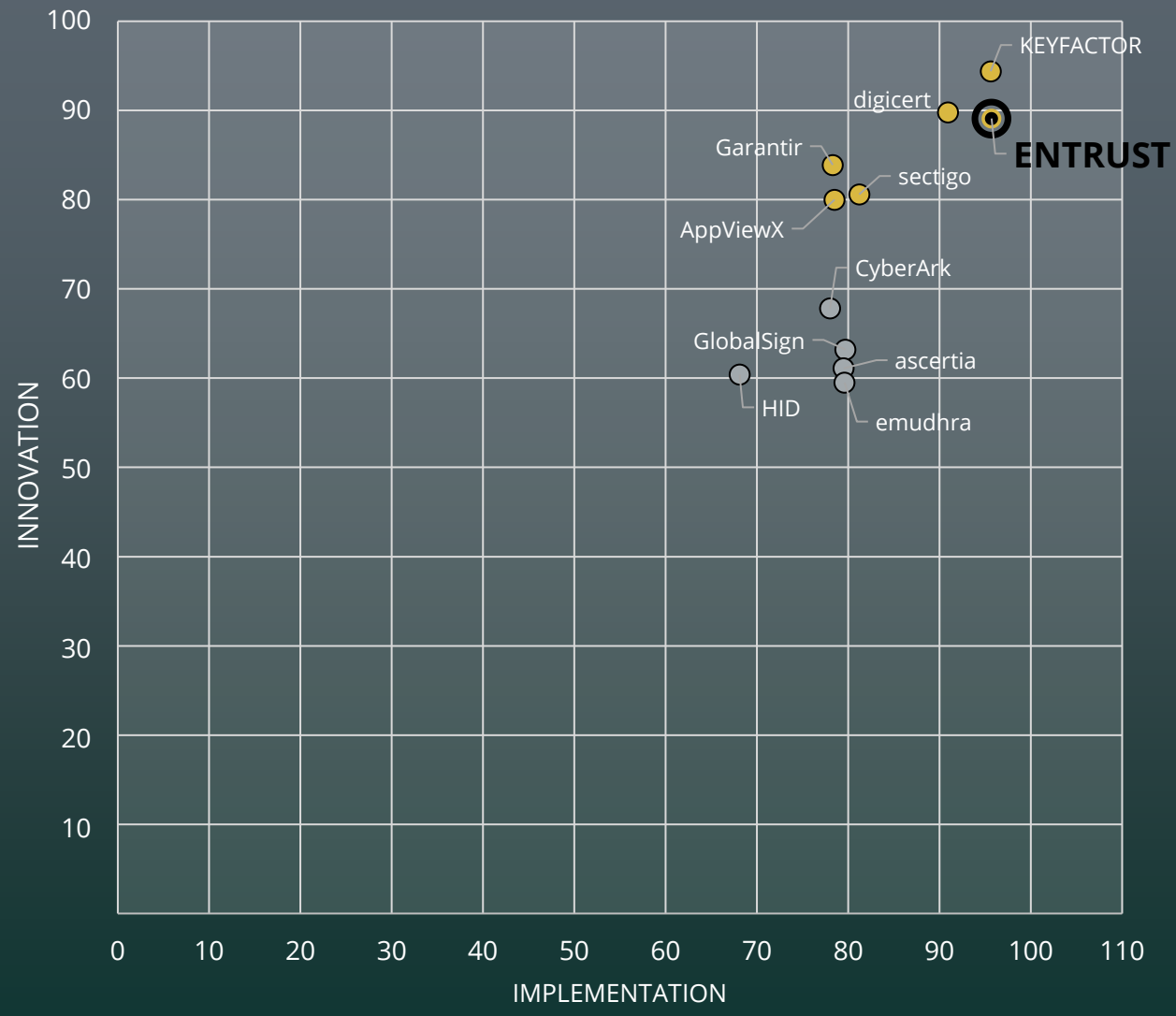
LEADER
ABIresearch.

TOP INNOVATOR
ABIresearch.

TOP IMPLEMENTER
ABIresearch.

OVERALL: 92.4 | INNOVATION: 89.1 | IMPLEMENTATION: 95.7 | RANK: 2

INNOVATION *VERSUS* IMPLEMENTATION MATRIX



INNOVATION

ENTRUST

INNOVATION SCORE: 89.1

Entrust provides PKI support across any and all CA architectures, including hierarchical, federated, decentralized, and cross-certified setups. As enterprise environments become increasingly complex, hybridized, and interconnected with third-party systems, Entrust's support for an expansive spectrum of CA architectures elevates its market potential within the PKI space.

Security is top of mind for vendors contending among the best PKI providers and this is another category in which Entrust excels. Key recovery services are hosted by Entrust mPKI, while retention of certificate records for 7+ years—in line with compliance requirements—is supported by its SaaS offering. Meanwhile, Entrust remain one of the only vendors to possess national security level and staff clearances in its delivery of PKI solutions and services, making it well-positioned for success not only in government PKI schemes or projects partnered with Tier One banks, but also for providing commercial or enterprise PKI to central government departments. Stringent adherence to PKI policy and processes is increasingly emphasized as regulatory requirements become more stringent and enterprise ecosystems more complex. Thus, Entrust's appreciation for the significance of policies and process within PKI, alongside the technology itself, render it a top-performing player in the overall PKI market.

As one of the first-movers to embrace platformization as a PKI delivery strategy, Entrust has a decided competitive advantage in this subsegment. Entrust's Cryptographic Security Platform (CSP) is its crown jewel product in this regard, offering a comprehensive management system for cryptographic asset security that encompasses PKI and CLM, but also Key Management Services (KMS), HSMs, as well as compliance validation and risk assessment services. Through the subsummation of PKI services into a broader digital trust platform, Entrust's approach is set to capture a larger market share over time. Thus, while Entrust's CLM capabilities may still be catching up to those of Keyfactor, Sectigo, or CyberArk, by offering an integrated platform, it is able to offer a comprehensive answer to enterprises' security concerns, helping to close any gaps between its competition on specific PKI or CLM functionalities. CSP also integrates risk radius assessments, granting users with an overview into the "blast radius" or system-wide impact if certain compliance requirements are not met or given certificates are not in line with compliance standards. This places Entrust out ahead of much of its competition with regard to enhancing regulatory adherence and enhancing users' compliance with PKI standards and best practices.

INNOVATION

ENTRUST

INNOVATION SCORE: 89.1

Beyond its own CSP, Entrust boasts one of the most extensive integration portfolios across the PKI vendor landscape, integrating with MDM systems (jamf, MaaS360, SOTI, Workspace ONE, ivanto), IT Service Management (ITSM) providers (Ansible, servicenow, Jenkins), IoT vendors (Bosch, Device Authority, Chargepoint, Fresenius), card management systems (Versasec, Intercede, HID), and telco network infrastructure (Cisco, Nokia, VMware, Palo Alto Networks, Citrix NetScaler). By integrating highly targeted partnerships with entities in the IoT and telco spaces, Entrust is well-positioned to take advantage of emerging and quickly growing PKI subsegments, including PKI-IoT, ensuring that Entrust retains its position as a key PKI provider as the overall market continues to evolve and expand.

Finally, Entrust's Cryptographic Center of Excellence is a stellar example of pioneering support, education, and advisory services, tailored to quantum security and resilience. Through this service-based offering, Entrust provides Post Quantum (PQ) maturity assessments—including tailored remediation and roadmap advice—crypto and PKI governance consulting and health checks, and PKI discovery services, digging into rogue, isolated, and siloed PKIs and providing a migration plan that considers the functional and non-functional needs of given PKIs within an enterprise system. Unlike some of its competitors, Entrust's Cryptographic Center of Excellence is a consultancy-based service, orientated around neutrality, and can be purchased by non-Entrust customers or as part of an enterprise PKI solution. Through this expansive and neutral advisory hub, Entrust has positioned itself as a leading reference to both its customers and others in the march toward quantum-resilient PKI, boding well for its future in the PKI market as quantum security moves up enterprises' list of priorities.

IMPLEMENTATION

ENTRUST

IMPLEMENTATION SCORE: 95.7

When it comes to breadth of offering, Entrust is unparalleled in the PKI market. This includes the number of PKI applications covered by Entrust's PKI offerings, the extensive range of PKI solutions offered, and the wider CSP provided by the digital trust behemoth; enabling it to cater to customers' security needs across each layer of their enterprise environments.

As a holistic cryptographic security platform, CSP offers both PKI and CLM within one platform, available on-premises with a built-in HSM, as a software appliance on-premises, as a self-managed software appliance in the cloud, and as a hybrid offering: via a combination of CSP-as-a-Service (CSPaaS) and CSP on-premises. Beyond CSP, Entrust also offers Entrust mPKI and Entrust PKIaaS, providing both a managed PKI solution and self-service offering to complete its comprehensive PKI portfolio.

As a well-established player in the PKI market, Entrust is an all-rounder when it comes to PKI applications, leading the pack in terms of the range of PKI use cases that its solutions serve, granting it a significant competitive advantage when it comes to PKI implementation. From securing cloud application access and service mesh to code, software, and firmware signing, Entrust is well-versed in the traditional enterprise PKI applications. Yet, beyond this, Entrust is a giant in the national and payments credentials spaces; offering PKI within ePassports, national IDs, and driver's licenses. Through long-running partnerships with industry leaders in the manufacturing and automotive spaces, Entrust has been quick to address the growing market in PKI for connected driving and the smart home. It provides PKI verification and authentication beyond certificate injection at the manufacturing phase, assisting with integrating IoT devices during operational and connected service setup, and securing communications between industrial gateways within connected systems. Given the holistic approach of its new CSP, Entrust provides PKI and broader cryptographic asset management at each layer of multivariate PKI use cases, including emerging applications of PKI in connected mobility and smart city scenarios.

Moreover, Entrust brings powerful cryptographic expertise to the PKI market. Its solutions incorporate support for diverse cryptographic primitives, including extending support to legacy primitives to support customers' needs with regard to backward compatibility and outdated systems. This includes support for a plethora of symmetric encryption algorithms on its HSMs (3DES, AES, CAST, CAST3, CAST5, DES, RC2, RC4), digital signature algorithms (RSA, DSA, ECDSA, ML-DSA), and hash functions (SHA-1, SHA-224, SHA-256, SHAKE, MD2, MD5, IDEA, NTRU, RIPEMD-160). For customers seeking to integrate PKI and ensure interoperability with legacy assets, Entrust's PKI offerings boast a comprehensive suite of cryptographic algorithms, aiding it in securing long-term customer relationships and cultivating brand loyalty.

CRITERIA AND METHODOLOGY

VENDOR MATRIX

Methodology: After individual scores are established for innovation and implementation, an overall company score is established using the Root Mean Square (RMS) method:

$$Score = \sqrt{\frac{innovation^2 + implementation^2}{2}}$$

The resulting overall scores are then ranked and used for percentile comparisons.

The RMS method, in comparison with a straight summation or average of individual innovation and implementation values, rewards companies for standout performances.

For example, using this method, a company with an innovation score of nine and an implementation score of one would score considerably higher than a company with a score of five in both areas, despite the mean score being the same. ABI Research believes that this is appropriate as the goal of these matrices is to highlight those companies that stand out from the others.

RANKING CRITERIA

Leader: A company that receives a score of **75 or above** for its overall ranking.

Mainstream: A company that receives scores **between 60 and 75** for its overall ranking.

Follower: A company that receives a score of **60 or below** for its overall ranking.

Innovation Leader: A company that receives a score of **75 or above** for its innovation ranking.

Implementation Leader: A company that receives a score of **75 or above** for its implementation ranking.

INNOVATION CRITERIA

The innovation criteria take into account novel capabilities in technology development and deployment, as well as in commercialization.

- **Configuration & Capabilities:** Assesses capacity and performance, software and firmware, CAs, availability, security, and support provided. This includes looking at certificate issuance and revocation rates, key ceremony processes, access control, CA architectures supported, and support provided for system setup and deployment.
- **PKI Service Options:** Assesses the different deployment models and features supported, including managed and self-service PKI as well as Generative Artificial Intelligence (Gen AI) or Agentic AI functionalities, monitoring capabilities, and Bring Your Own Root of Trust (BYOROT) support.
- **CLM Service Options and PKI Management Platform:** Examines the CLM services supported, including CLM, discovery and onboarding of certificates, and automated renewal and revocation. Examines the management platforms used for PKI and CLM, key management, cryptographic inventory, remote management & configuration capabilities, backup systems, and trust list management.
- **Partner Ecosystem & Integration Capabilities:** Assesses the partner ecosystem supporting the PKI service(s) or product(s) including CLM, key management, Hardware Security Modules (HSMs), third-party PKI or CAs, DevOps, asset management systems, Identity Access Management (IAM), PAM, servers, load balancers, incident and workflow tools, Unified Endpoint Management (UEM), Mobile Device Management (MDM), FIDO card management systems, and Operational Technology (OT) systems. This criterion looks at the degree of integration; from an orchestrated integration with a given application to integration via cryptographic Application Programming Interfaces (APIs).
- **Quantum-Safe Capabilities:** Assesses the integration of PQC algorithms into key encryption and digital signatures, as well as hybrid bridge capabilities. This criterion also looks at general PQC support such as CA switching capabilities, Post-Quantum (PQ) Root of Trust (RoT), and custom assessments and encryption advisory services provided.

IMPLEMENTATION CRITERIA

These criteria relate to the breadth of solutions, features, and capabilities of enterprise PKI offerings in order to assess their completeness and fitness for purpose.

- **PKI Solutions:** Assesses the range of offerings including hardware, software, and service offerings.
- **Applications:** Examines the PKI applications supported by the service(s) and/or product(s), including application security, cloud application access, device authentication, code signing, IoT device provisioning, and credentials issuance.
- **Cryptographic Algorithms, Protocols, & Certificates:** Assesses the cryptographic algorithms, PKI-related protocols (e.g., Transport Layer Security (TLS), Online Certificate Status Protocol (OSCP), Enrollment over Secure Transport (EST), and Automated Certificate Management Environment (ACME)), certificate types, and certificate extensions
- **Standards & Regulation:** Examines the degree of compliance with relevant PKI, connected services (e.g., HSM), and other industry or region-specific standards and regulatory frameworks.
- **Go-to-Market (GTM):** Assesses the business and pricing models used by each vendor, investigating direct sales, channel partners, and availability for online evaluation and integration testing.

October 27, 2025

New York, NY 11771 USA
Tel: +1 516-624-2500
www.abiresearch.com

ABI Research is uniquely positioned at the intersection of end-market companies and technology solution providers, serving as the bridge that seamlessly connects these two segments by driving successful technology implementations and delivering strategies that are proven to attract and retain customers. For further information about subscribing to ABI's Research Services as well as Industrial and Custom Solutions, contact us at +1.516.624.2500 in the Americas, +44.203.326.0140 in Europe, +65.6592.0290 in Asia-Pacific or visit www.abiresearch.com.