IDC LINK
Real-time IDC Research® opinion on industry news, trends and events

Entrust Demystifies Cryptographic Security Practices Offering Scanners and Skills for Rent

November 30, 2020

By: Jay Bretzmann

IDC's Quick Take

Entrust née Entrust Datacard is packaging its 25+ years of cryptographic security expertise into five defined services for helping organizations develop, review, and modernize crypto and PKI infrastructures. As encryption usage expands, organizations are losing control of their infrastructures while thousands of incremental IoT devices are beginning to connect to their networks. In a marketplace where overall cybersecurity skills are in short supply, cryptographic skills and expertise are doubly so.

Five years ago, this type of initiative would've likely been a *fries with that* offering. Mobile device access and cloud computing were not viewed as a primary part of a network's infrastructure, less sensitive data existed and lived somewhat safely behind perimeter defenses, fewer and weaker regulations threatened insignificant fines for noncompliance, and people worked in secure office locations. Today IDC believes interest in this sort of offering could be closer to buying a *Happy Meal* via a drive thru.

Product Announcement Highlights

The first thing to understand about this announcement is that Entrust's goal is to help its customers establish their own Cryptographic Center of Excellence (CryptoCoE) rather than it being an initiative to sell subscription SaaS services. Establishing a CryptoCoE means developing a central authority for owning everything using cryptographic software technology including software encryption ciphers, keys, certificates, and secrets applied to network transmissions, remote system access, file system protections, and authentication capabilities for people and things.

The core offering is a set of very structured engagements that leverage Entrust's pool of cryptographic experts across five primary services:

- Cryptographic Health and Governance:
  - Crypto Health Check
  - Crypto Governance Consulting
- PKI Health and Governance:
  - PKI System Health Check
  - PKI Governance Health Check
  - PKI Governance Consulting

Health checks assess where an organization is today, while the governance and consulting services provide advice about how to maintain and improve crypto capabilities going forward. A key area of focus is reviewing an organization's defined roles, processes, and policies and then discovering where all its sensitive data resides — traditional challenges for most enterprise environments.

Like many other security assessments, the process starts with a scan of the environment to find out what's in use where and at what level of currency with available software patches and technology updates. The scanning software — Crypto Analytics — is sourced from an Entrust partner, InfoSec Global. The results are compiled into actionable reports that help security teams discover the extent of their issues and recommend actions to be taken.

The scans are then paired with an Entrust Expert-by-Your-Side to help interpret the results, identify any existing skill gaps, and help execute an agreed-upon remediation plan. These experts will also present best practices recommendations for expanding and managing a customer's cryptographic plans to address emerging needs, helping customers avoid repeating any disconnected development efforts. Customers can purchase a single engagement or an annual subscription that will revisit an organization's crypto health status up to four times a year.

IDC's Point of View

For many organizations, cryptographic practices aimed at establishing trusted digital environments are nothing short of a mess, getting hotter with each passing year. The underlying cause is a lack of centralized planning ownership and expertise. The corporate needs were generally limited to certain applications within certain business units.

Today's digital transformation projects are changing all of that. Crypto is now a necessary part of applications, application development, communications, data privacy, and identity technologies, the status of which are often unknown. A PKI infrastructure developed years ago is probably not aligned with today's management requirements with certificates that may never expire or expire without prior warning.

Key management is another area where organizations struggle to maintain adequate protections and rotation schemes mandated by updated and newly emerging industry and governmental regulations. Organizations might have a hardware HSM, or two or three, but chances are good they're operating as siloed resources. In the event of a detected network breach, many businesses would likely scramble to perform adequate key rotations attempting to contain any possible data exfiltrations.

SSH keys for machine-to-machine or human-to-machine access control is another crypto problem for hundreds of organizations using them to conduct file transfers, perform disaster recovery services, log in with privileged access management, perform software and patch management, or even dynamically provision cloud resources. SSH is an operating system resource for any Unix/Linux platform and a very simple means for providing administrator-level access. Millions of keys have been issued over the years and most still exist and are discoverable.

IDC believes Entrust is in a strong position with these service offerings and that it will challenge systems integrators and other providers of similar services with its framework rather than an ad hoc approach. It has been an authority for cryptographic solutions for more than two decades and serves as a leading certificate authority (CA) and HSM technology provider, offering identity verification services and advanced authentication products including smart cards, e-passports, and student IDs.

Earlier in 2020, the company changed its name from Entrust Datacard to just Entrust, which IDC believes helps the company position itself as a broader provider of digital trust solutions beyond a historical business associated with multifactor authentication technologies of all kinds. The tag line and mission

statement is "Securing a World in Motion," meaning its products help people confidently log on to networks, protect critical data, shop online, cross borders, enter buildings, and make payments.

As with any services-intensive business, the challenge will be providing enough skilled practitioners to meet market demand. Entrust has produced a services road map for its CryptoCoE offerings with initial coverage limited to North America and EMEA through its direct sales force through 2021, adding new services, geographical regions, and partner involvement into 2024.

Subscriptions Covered:
Data Security, Identity and Digital Trust Software