ORC und Entrust sichern Cloud-Dienste für die US-Bundesregierung

PIVotal ID™ von ORC, eine von der US-Regierung verwendete Federated-Identity-Lösung, zeigt, wie Cloud-basierte Identity as a Service (IDaaS), die durch robuste Kryptographie geschützt ist, hohe Sicherheit und umfassende Interoperabilität bietet.

Viele Unternehmen spielen mit dem Gedanken, sensible Daten in die Cloud zu verlagern, haben aber große Bedenken hinsichtlich deren Sicherheit. Operational Research Consultants Inc. (ORC) hat als einziges Unternehmen bewiesen, dass die Cloud selbst für Organisationen wie die Regierung der Vereinigten Staaten sicherer als eine On-Premises-Bereitstellung sein kann.

ORC – EIN VORREITER AUF DEM GEBIET DES FEDERATED-IDENTITY-MANAGEMENTS

ORC ist seit Mitte der 1990er Jahre ein zuverlässiger Partner der US-Regierung. Damals führte das Unternehmen die Navy Acquisition Public Key Infrastructure zur Sicherung der Interaktion mit Auftragnehmern und Lieferanten ein. Im Laufe der folgenden zwei Dekaden wurde Informationssicherung zu einem bedeutenden Thema für die US-Regierung. ORC wurde zum bewährten Ansprechpartner für Sicherheitslösungen und erhielt als erstes Unternehmen die Genehmigung, regierungskonforme Identitätsmanagementlösungen bereitzustellen.

Heute verwaltet ORC mehr als drei Millionen Identitäten und hat entsprechend der Vorgaben der US-Regierung mehr als 10 Millionen digitale Zertifikate für zahlreiche Mitarbeiter, Auftragnehmer, Verbündete, Veteranen und Bürger ausgestellt, die in Regierungsgeschäfte involviert sind.

ORC

BEDARF AN SICHERER UND VOLLSTÄNDIG KOMPATIBLER IDENTIFIZIERUNG UND AUTHENTIFIZIERUNG

Im August 2004 erließ die Bush-Regierung eine Homeland Security Presidential Directive (HSPD-12), die vorsah, Bundeseinrichtungen und -ressourcen durch die Einführung regierungsweiter Normen für sichere und zuverlässige Identifizierungsformen zu sichern. Diese Initiative ging weit über die reine Ausgabe von einfachen Ausweiskarten an Regierungsmitarbeiter hinaus. Sie konzentrierte sich vielmehr auf die für die Ausstellung sicherer persönlicher Berechtigungsnachweise erforderlichen Prozesse, die Methoden zur Überprüfung dieser Ausstellungsprozesse und Berechtigungsnachweise sowie auf das Risiko- und Qualitätsmanagement über deren gesamte Lebensdauer.

Das Personal Identity Verification-Programm (PIV) implementiert diese Verfahren, und Federal Information Processing Standard (FIPS) 201 legt die Schnittstellen- und Datenelemente der PIV-Smartcard fest. Zu den Datenelementen auf einer PIV-Smartcard gehören auch ein oder mehrere asymmetrische private kryptographische Schlüssel. Regierungsabteilungen und -behörden müssen eine konforme Public Key Infrastructure (PKI) nutzen, wenn sie digitale Zertifikate für Benutzer ausstellen. Im Rahmen der PIV-Initiative wurden außerdem weitere hochsichere Berechtigungsnachweise eingeführt, die bestimmte Transaktionen zwischen Unternehmen und Regierungen, Bürgern und Regierungen sowie Bürgern und Unternehmen unterstützen und für die Kompatibilität dieser föderierten Identitäten sorgt. Dazu gehören verschiedene PIV-Interoperable- (PIV-I) und PIV-Varianten wie Transportation Worker Identification Credential (TWIC®), First Responder Authentication Credentials (FRAC), Commercial Identity Verification (CIV) und External Certificate Authority (ECA) PIV-I, die unterschiedliche regulatorische Anforderungen erfüllen und sich weltweit skalieren lassen. Die Prozesse und Richtlinien für die Ausstellung von Zertifikaten und die Schutzmaßnahmen für die Schlüssel der wichtigen ausgebenden Root-Zertifizierungsstellen in dieser PKI sind entscheidende Faktoren für die allgemeine Sicherheit des Systems.

DIE HERAUSFORDERUNGEN: ZERTIFIZIERUNG, KOMPATIBILITÄT UND VERTRAUEN

Traditionelle lokale Identitätsmanagement-systeme lassen sich nicht so einfach auf die Cloud erweitern. ORC hat erkannt, dass Sicherheit ein wichtiges Alleinstellungsmerkmal ist, um das Vertrauen der US-Regierung in Cloud-basierte Identitätsmanagementlösungen zu wecken. Daher war ihnen bewusst, dass nur hochsichere Kryptographie geeignet war, um die Sicherheitsvorgaben des NIST zu erfüllen. Für PKI bedeutete das, dass die Schlüssel der ausstellenden Root-Zertifizierungsstelle mit hochsicherer, FIPS-zertifizierter Hardware erstellt und geschützt werden mussten. Dafür gab es neben der offensichtlich benötigten robusten Sicherheit noch weitere Gründe: Die Gefährdung eines dieser Schlüssel hätte die Auswirkung, dass alle unter der PKI ausgestellten Zertifikate annulliert und alle Berechtigungsnachweise erneut ausgestellt werden müssten.

ORC sah sich auch mit zahlreichen Zertifizierungs- und Akkreditierungsvorgaben konfrontiert, darunter Federal Bridge, PIV/PIV-I, DoD und FISMA. Die nötige Unterstützung wechselseitiger Zertifizierung auf mehreren Ebenen erforderte eine Lösung, die eine flexible Zahl an Sicherheitslevels und -richtlinien unterstützt. Diese Lösung musste zudem erprobt sein und auf offenen Systemstandards beruhen, um eine umfassende Interoperabilität zu garantieren. Schließlich erkannte ORC, wie wichtig es ist, dass kryptographische Dienste in einer Cloud-Umgebung hochverfügbar und äußerst verlässlich sind.

ORC

DIE LÖSUNG: ORC PIVOTAL ID™ UND ENTRUST

ORC bietet eine Lösungssuite mit dem Namen PIVotal ID™ an, die einen hohen Grad an Sicherheit für die Cloud-Dienste der US-Regierung bereitstellt. PIVotal ID™ umfasst zertifizierte und akkreditierte Managed Services für die Ausstellung starker Identitätsnachweise, die das Vertrauen der US-Regierung genießen und weltweit als föderierte Identitäten genutzt werden können. Dazu gehört auch die Ausstellung digitaler Zertifikate in PKI, die durch die hochsicheren nShield®-Hardware-Sicherheitsmodule von Entrust gesichert ist. ORC hat Millionen konformer Zertifikate ausgestellt und verwaltet und ermöglicht den zivilen und militärischen US-Bundesbehörden, ihren Mitarbeitern, weltweiten Auftragnehmern, Handelspartnern, Veteranen und Bürgern, die in Geschäfte mit einer beliebigen Stelle der US-Regierung und regulierten Branchen involviert sind, sichere Transaktionen. PIVotal ID™ umfasst:

- Personal Identification Verification (PIV)
- Non-Federal Issuer PIV-Interoperable (NFI PIV-I)
- External Certificate Authority (ECA)
- Access Certificates for Electronic Services (ACES)
- TWIC Certificate Manufacturing Authority
- PIVotal Commercial™ (PIV-CIV)
- PIVotal Validation™

ORC hat erkannt, dass die nShield HSM von Entrust höchsten Schutz und umfassende Möglichkeiten zur Beschleunigung kryptographischer Verfahren sowie innerhalb einer sicheren Cloud-Infrastruktur die erforderliche Flexibilität und Skalierbarkeit für den Schutz und die Verwaltung von Root-Schlüsseln und allen untergeordneten Schlüsseln bieten.

KOSTENGÜNSTIGE LÖSUNGEN FÜR ROBUSTE KRYPTOGRAPHIE

Die nShield HSM von Entrust basieren auf einer gesicherten, manipulationssicheren Plattform, die sensible Schlüssel schützt und verwaltet, die zur Verschlüsselung und zum digitalen Signieren verwendet werden. Daher können sie zum Schutz praktisch aller Anwendungen eingesetzt werden – von Identitätsmanagement, Webdiensten und Datenbankverschlüsselung bis hin zu Tokenisierung, PKI-Diensten und robuster Authentifizierung. nShield HSM sind die kostengünstigste Möglichkeit, geeignete physische und logische Kontrolle von Systemen bereitzustellen, wenn die von Seiten der Software-basierten Kryptographie gebotene Sicherheit als unzureichend gilt.

ORC

MIT nShield HSM VON ENTRUST KÖNNEN UNTERNEHMEN:

- unübertroffene operative Flexibilität sowie hohe Verfügbarkeit und Skalierbarkeit in virtuellen und Cloud-Umgebungen erreichen
- die Kosten für die Einhaltung gesetzlicher Vorschriften und die täglichen wichtigen Verwaltungsaufgaben einschließlich Back-up und Fernverwaltung senken
- hochsichere Unternehmenskontinuität durch unkomplizierte HSM-Bereitstellung, effiziente Schlüsselerstellung und robuste Hardware erzielen
- die Sicherheit kritischer Anwendung durch zertifizierten Schutz für kryptographische Schlüssel und Operationen innerhalb manipulationssicherer Hardware erhöhen
- durch robuste Verwaltungsrichtlinien wie rollenbasierter Multifaktor-Authentifizierung und flexible Quorum-Authentifizierung Aufgaben streng voneinander trennen

ÜBER ORC

ORC, ein Unternehmen von WidePoint und zuverlässiger Partner der US-Regierung, stellt Informationssicherheitslösungen für Regierungen und Unternehmen bereit. Dabei garantieren sie den zuverlässigen Austausch und die Sicherheit von Informationen entsprechend den geltenden Vorgaben. ORC ist führender Anbieter für Informationssicherheit und Authentifizierungsdienste zwischen Regierungsbehörden, Unternehmen und Regierungsbehörden sowie Bürgern und Regierungsbehörden. Die Lösungen von ORC sind mit älteren Systemen kompatibel und lassen sich nahtlos in alle führenden Softwareanwendungen auf dem Markt integrieren. ORC nutzt nShield HSM von Entrust um sichere Identitätsmanagmentdienste in der Cloud anzubieten, die den Vorgaben der US-Regierung entsprechen.

ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com