THALES

www.thales-esecurity.com

FEDERAL GRADE SECURED CLOUD SERVICES WITH ORC AND THALES

ORC's PIVotal ID™, a federated identity solution used by the U.S. government, shows how cloud-based Identity-as-a-Service (IDaaS) backed by hardened cryptography delivers strong security and wide interoperability.

For many companies thinking about moving sensitive data to the cloud, security issues remain a significant concern. But one company, Operational Research Consultants Inc. (ORC), is proving that the cloud really can be made as safe or even safer than on-premise deployments even for organizations as security-focused as the U.S. Federal Government.

ORC – a pioneer in federal identity management

ORC has been a trusted partner of the U.S. government since the mid-'90s, when the company launched the Navy Acquisition Public Key Infrastructure to support secure interactions with contractors and suppliers. As the government's emphasis on information assurance expanded over the next two decades, ORC became a go-to partner for security solutions and one of the first companies authorized to provide government-compliant identity management solutions.

Today ORC manages more than three million identities and has issued more than 10 million federal-compliant digital certificates to a variety of employees, contractors, allies, veterans and citizens conducting business with the government.

The need for secure and interoperable identification and authentication

In August 2004, the Bush administration issued a Homeland Security Presidential Directive (HSPD-12) to secure federal facilities and resources by establishing a government-wide standard for secure and reliable forms of identification. Going far beyond simply issuing ID badges to government employees, this initiative would focus on the processes needed to issue secure personal credentials, on methods to validate those issuance processes and credentials and on managing risk and quality throughout the lifecycle of the credentials.The Personal Identity Verification (PIV) program implements these processes, and FIPS (Federal Information Processing Standard) 201 specifies interface and data elements of the PIV smart card. Among the data elements on a PIV card are one or more asymmetric private cryptographic keys. Departments and agencies must use a compliant public key infrastructure (PKI) to issue digital certificates to users. The PIV initiative has also spawned other high assurance credentials that support specific Business-to-Government, Citizen-to-Government and Citizen-to-Business transactions while supporting federated interoperability between the issued credentials. These include various PIV-Interoperable (PIV-I) and PIV variants, such as: Transportation Worker Identification Credential (TWIC®), First Responder Authentication Credentials (FRAC), Commercial Identity Verification (CIV), and External Certificate Authority (ECA) PIV-I that address various regulatory requirements and are built to scale globally. The processes and policies for certificate issuance and the protections afforded to the critical root and issuing certificate authority keys in that PKI are critical factors in the overall assurance level of the system.

Thales Hardware Security Modules (HSMs) enable companies to:

- Achieve unmatched operational flexibility, high availability and scalability in virtualized and cloud environments.
- Reduce the cost of regulatory compliance and day-to-day key management tasks such as backup and remote management.
- Achieve high assurance business continuity with simplified HSM enrollment, efficient key provisioning and fully resilient hardware features.
- Enhance security for critical applications by protecting cryptographic keys and operations within tamper-resistant hardware.
- Establish strong separation of duties and dual controls through robust administration policies including role-based multi-factor authentication and flexible quorum-based authorization.

ORC
a widepoint company

The Challenges: Certification, Interoperability and Trust

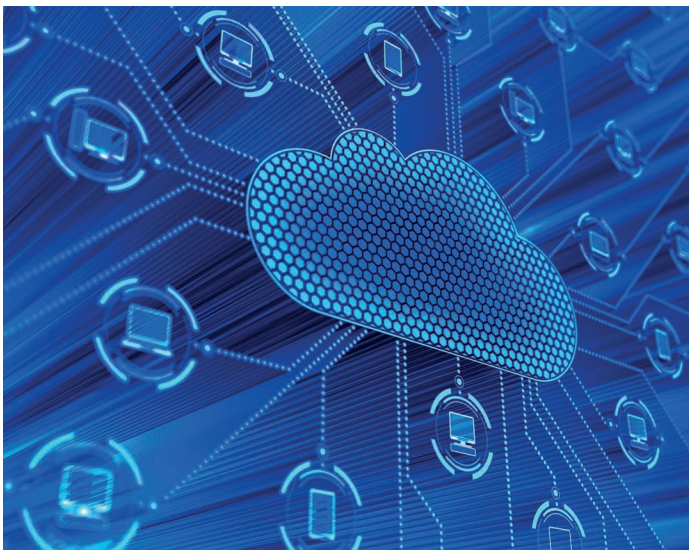
Traditional on-premise identity management systems don't easily extend to the cloud. Recognizing that security was an important differentiator in order for cloud-based identity management to be trusted across the federal government, ORC knew that high assurance cryptography was the only way to meet NIST's security requirements. In the context of PKI, this meant that root and issuing certificate authority keys needed to be generated and protected in high assurance, FIPS-certified hardware. The reasons extended beyond simply strong security: the operational impact of compromise of one of these keys would be that all certificates issued under the PKI would need to be revoked and all credentials re-issued.

ORC also faced multiple certification and accreditation requirements including Federal Bridge, PIV/PIV-I, DoD, and FISMA and the need to support cross-certification at multiple levels, requiring a solution that could support a flexible range of assurance levels and policies. The solution also needed to be proven, and based on open systems standards to assure wide interoperability. Finally, ORC recognized the importance of providing high availability and reliability for cryptographic services in a cloud environment.

The solution: ORC PIVotal ID™ and Thales nShield HSMs

In order to provide high levels of assurance for federal cloud services, ORC offers a suite of solutions called PIVotal ID™. PIVotal ID™ includes certified and accredited managed services for issuing strong identity credentials that are trusted across the federal government and able to federate globally, including the issuance of digital certificates from PKIs underpinned by high assurance Thales Hardware Security Modules (HSMs). ORC has issued and manages millions of compliant credentials enabling secure transactions for U.S. Federal Agencies (Civilian and Defense), their employees, the global contracting community, trading partners, Veterans and citizens who need to conduct business with any facet of the U.S. Government and regulated industries. PIVotal ID™ includes:

- 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 recognized that the Thales nShield family of HSMs offered superior protection and cryptographic acceleration capabilities, as well as the flexibility and scalability to protect and manage root keys and all subordinate keys within its secure cloud service infrastructure.

Cost-effective solutions for robust cryptography

Thales nShield HSMs are built on a hardened, tamper-resistant platform that safeguards and manages sensitive keys used for encryption and digital signing to support virtually any application from identity management, web services and database encryption to tokenization, PKI services and strong authentication. Thales nShield HSMs offer the most cost-effective way to establish the appropriate levels of physical and logical controls for systems where the security offered by software-based cryptography is considered to be inadequate.

About ORC

ORC, a WidePoint company and trusted partner to the U.S. Federal Government, delivers information security solutions to government and enterprise customers, thereby ensuring the fully compliant and trusted exchange and assurance of information. As an elite provider of information assurance and authentication services for business to government, government to government, and citizen to government, ORC's solutions are interoperable with legacy systems and integrate seamlessly with all leading software applications on the market. ORC leverages Thales nShield HSMs to provide federal grade secured cloud identity management services.

Follow us on:

©Thales e-Security • February 2014 • LH3112

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com