thalestct.com

THALES

Fortify your Public Key Infrastructure

Information Security CORPORATION

The Challenge

CertAgent® by Information Security Corporation (ISC) is a customer-hosted (on-premise or cloud), self-contained, and easy-to-use Certificate Authority serving as the cornerstone of a Public Key Instrastrucure (PKI). Certificates and Certificate Revocation Lists issued by CertAgent comply with all relevant federal and industry standards, and it can be used with hundreds of existing applications for the protection of email, authentication of users and web servers, etc. Designed to scale from small to large organizations, CertAgent provides all the functionality needed to PKI-enable an enterprise.

CertAgent 7.0 has been awarded NIAP certification for compliance with the Common Criteria Protection Profile for Certification Authorities (v2.1) and also appears on the National Security Agency's Commercial Solutions for Classified (CSfC) list. When used with ISC's software cryptographic module, CertAgent complies with NIST FIPS 140-2 Level 1 requirements. However, many federal organizations require a higher level of FIPS 140-2 assurance and the use of a hardware security module (HSM) to protect the most critical keys in the PKI. In addition, for CSfC registration, a CertAgent-based solution must be paired with an HSM approved by the NSA for use in the National Security Systems Public Key Infrastructure (NSS PKI).

The Solution

Thales Trusted Cyber Technologies (TCT)Luna HSMs are FIPS 140-2 Level 2 or 3 validated* (depending on configuration) and are approved by use in the NSS PKI by the National Security Agency. By using a TCT HSM, organizations can be assured the most critical keys in their PKI are generated and stored in a validated and trusted HSM designed and built in the United States for specifically for that purpose. Private keys generated in the HSM never leave the hardened appliance and are utilized by CertAgent via cryptographically secured communication links. At no

time are these critical keys exposed to threats that exist in the external operating environment.

By utilizing an integrated ISC CertAgent and TCT Luna HSM solution, federal organizations can build a Public Key Infrastructure meeting the most stringent of security standards and also work with two companies founded for the purpose of providing security solutions to the U.S. Federal Government.

ISC CertAgent Key Benefits

- NIAP evaluated and NSA approved as a CSfC component
- Supported on both Windows and Linux platforms
- Appropriate for organizations of any size, scaling up to millions of certificates
- Uses NIST CMVP-validated FIPS 140-2 cryptography and proven security standards, including ANSI X.509 and IETF PKIX, OCSP, TLS, and S/MIME

TCT HSM Key Benefits

- Provides centralized lifecycle management of cryptographic keys in a purpose-built, FIPS 140-2 Level 2 or 3 validated appliance approved by NSA for the NSS PKI
- Offloads and accelerates cryptographic operations to a dedicated cryptographic processor
- Available in multiple form-factors, including a USB-attached model ideal for offline root CAs
- Can be grouped together to provide high availability for critical PKI applications
- Developed, manufactured, and supported solely within the boundaries of the U.S., thus providing a completely trusted U.S.-based source

About Information Security Corporation

Information Security Corporation (ISC) is headquartered in Oak Park, IL with additional sales offices in Rochester, NY and Arlington, VA. Our development offices are located in Oak Park, IL and Santa Cruz, CA. The company was founded in 1989 by Thomas Venn and Michael Markowitz to develop and market data security products based on public key cryptography. For its first two decades, ISC focused on the Federal Government market, but in the last decade has become increasingly involved in the private sector. ISC has provided cutting-edge PKI-based security solutions to the world's most security conscious organizations for more than thirty years. From data protection and digital signatures, to complete PKI management, ISC's product suite makes it easy.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled.

Contact Us: For more information, visit www.thalestct.com

*FIPS Validation Pending

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com