Carillon
INFORMATION SECURITY

CertiPath Certified
Managed PKI

Cross-Certified PKI Operations… *Simplified*

AEROSPACE
DEFENSE
GOVERNMENT
CNI

Is your organization considering digital certificates for secure inter-company information sharing, access management and/or for use with your business partners within a safer common network?

How critical is the integrity of those certificates, and the costs associated to acquiring and managing them?

Carillon can provide cross-certified Managed PKI solutions, a private branded CA Service for organizations that need to integrate a higher level of secure information sharing, without the complexity and high-cost of an in-house PKI system.

The Key Advantages of the Carillon Managed PKI Service

Rapid Deployment – issue credentials in weeks, rather than the typical 18 months it takes an organization to attain CertiPath cross-certification.

Professional Management – our team of PKI experts can be trusted to maintain your PKI according to the strict requirements of the CertiPath policies.

Economical Solutions – our Managed PKI service is as much as 80% less expensive than in-house PKI solutions.

Compatibility & Interoperability – CertiPath cross-certified certificates provide aerospace, defense and government potential compatibility and certificates that comply to necessary FIPS-201 standards. Allows for integration with e-commerce portals and company intranets.

The challenges of buying digital certificates

Public Key Infrastructure (PKI) based digital certificates are the foundation to secure document exchange, collaborative engineering, secure e-mail, digital signatures and transaction security between systems. Purchasing digital certificates and smartcard credentials for identity management of employees, customers, suppliers or devices can be a fairly easy task considering the large number of certificate providers today. However, when these credentials need to be tightly and securely associated with individual identities, this task becomes a much more complicated one, if used for sharing valuable intellectual property within companies and with business partners.

Many types of low assurance level ID certificates are now available on the market from a growing number of sources, but very few can provide the required advantages to securely share sensitive or often critical information within a controlled and reliable network. These common low assurance level certificates are generated with very little care in verifying the true identity of the requestor, therefore certificates of this type can potentially be created using some else's identity, without thorough ID verification or face-to-face meeting for further confirmation. Even fewer are certificate issuers that can generate certificates which would be compatible or truly interoperable with the CertiPath PKI Bridge, the central hub that provides a secure and reliable way of communication between some of the main U.S. Aviation companies, International Governments and U.S. Federal Government Departments.

The challenges of standing up an In-House PKI system

Cost, complexity, and compatibility, can be some of the greatest challenges for a company exploring the possibilities of standing up their own in-house PKI system. Establishing a proper PKI from the ground up, involves a designated secure hosting facility for the Certificate Authority (CA), the associated hardware, software, disaster recovery procedures, along with other strict policies and procedures needed to create and manage cryptography-protected certificates following industry standards. It also requires trained and qualified staff to oversee the many steps of capturing and verifying the required identity details, conducting a face-to-face meeting and processing that information in order to generate and manage certificates correctly, to reduce the risks that can compromise the integrity of the whole PKI effort, and possibly expose information to unwanted parties.

The Solution

Carillon Information Security is one of few companies that offers a CertiPath cross-certified managed PKI solution that can generate certificates suitable for aerospace, government, defense and other applications requiring high-reliability and integrity for secure information sharing, to true PIV-I compliance and FIPS-201 standards. With the increasing need for trusted digital identities expanding throughout many industries, Carillon's services will help provide customers with a simpler, more cost-effective way of generating higher level assurance digital certificates and credentials, and to also ensure a higher level of security for future challenges.

By taking advantage of the cross-certified Managed PKI solution, Carillon's customers can have their own private label Certificate Authority. This enables their organization to have the most control over the management of their PIV-I credentials, without engaging in the costly start-up, maintenance and responsibilities of their own full PKI system. Furthermore, this solution allows companies, associations, state and local governments to issue other credential types.

Carillon's managed PKI service includes a private label root Certificate Authority (CA), which issues its own self-signed certificates, that can be used as a trust anchor for relying parties. Our managed PKI also includes a customizable card management service (CMS) and other related support staff procedures needed to securely, issue, recover, revoke, store and verify the status of certificates and certification paths. Our service is as much as 80% less expensive than creating an in-house solutions and can help generate secure credentials within weeks, rather than the typical 18 months it takes an organization to attain cross-certification with the CertiPath PKI Bridge. Carillon's highly experienced and proficient team of PKI experts can be trusted to maintain your PKI according to the strict requirements of the CertiPath policies.

The following components are included in the Managed PKI Service:

Service	Description
Root CA	A Certificate Authority which issues its own self-signed certificate and which may be used as a Trust Anchor for Relying Parties
Signing CA	A Certificate Authority which issues Certificates to End Entities and/or another Certificate Authority when acting as a Principal CA for cross-certification
CSA (Certificate Status Authority)	A central Online Certificate Status Protocol (OCSP) Responder which provides the status of Certificates and/or certification paths
CMS (Card Management Service)	A central content-signing system which communicates with various enrollment stations during the issuance of credentials to manage smart card token content
KRS (Key recovery System)	The system hardware, software, staff and procedures needed to securely store and recover Subscriber Encryption Certificate keys

Roles and Responsibilities

Role	Carillon Provided	Customer Provided
Creation of Dedicated CP, CPS, and KRPS Documents	✓	
Enrollment Process & Procedures	✓	*
Secure Hosting and Operation of Components	✓	
Operational Authority Personnel	✓	
Registration Authority & Trusted Agent Personnel		✓
Trusted Agent Enrollment Stations	✓	*
Operational Key Recovery Agent Personnel		✓
Key Ceremony Witness Personnel		✓
Ongoing Policy Management	✓	
Archive & Disaster Recovery	✓	
Test Bed & Pre-Production Facility	✓	
Commissioning of Third-Party Audits	✓	*
Maintaining CertiPath Cross-Certification Contract	✓	*

*These features may optionally be provided by the customer, depending on the type and level of service requested.

---

about **Carillon** INFORMATION SECURITY

Carillon Information Security Inc. is a full service Public Key Infrastructure (PKI) and Federated Identity service firm. From consulting, to Managed Service, to tools to make PKI easier to use, we offer a dedicated and knowledgeable team. Our main customers are major entities in the aerospace and civil air transport industries, service providers to large government agencies, and public utilities.

As the only company in the CertiPath cross-certification family whose main activity is managing PKI solutions, consulting on PKI implementations, Carillon is the leader in the field of cross-certified PKI implementation. With solutions ranging from PIV-I to ATA Spec42 compliant PKI, to simple and quick-to-deploy PIV-C / CIV, Carillon's highly experienced and proficient PKI team can help customers explore the benefits of PKI in its many flavors, and guide them through a completely successful and rapid PKI project deployment.

Contact Us Today for more details!

356 Joseph Carrier
Vaudreuil-Dorion, QC
Canada J7V 5V5

Carillon INFORMATION SECURITY
www.carillon.ca

Phone: +1 514 485 0789
Fax: +1 450 424 9559
Email: info@carillon.ca