DigiCert Non-Federal Shared Service Provider Public Key Infrastructure (SSP PKI) Platform

DigiCert Non-Federal Shared Service Provider Public Key Infrastructure (SSP PKI) Platform is designed for non-federal organizations, such as state and local governments, government contractors, universities and health care providers that require an enterprise PKI solution and secure interoperability with the U.S. Federal Government. Non-Federal SSP PKI Service provides interoperability with the Federal PKI (FPKI) through cross-certification with the Federal Bridge Certification Authority (FBCA) and enables non-federal entities to rapidly deploy a robust PKI service to meet mission-critical security needs. Non-Federal SSP PKI Service is fully hosted and managed by DigiCert. It leverages the same technology, standards, and infrastructure that DigiCert delivers with its SSP PKI Service to provide managed PKI services to U.S. Federal agencies seeking to comply with Homeland Security Presidential Directive 12 (HSPD-12).

Mission-critical reliability

Non-Federal SSP PKI Service is hosted in high security data centers managed by DigiCert. All transactions are mirrored over a dedicated secure link from the primary data center to the backup disaster recovery data center. Non- Federal SSP PKI Service is operated 24 hours a day, seven days a week, 365 days a year with availability in excess of 99.9 percent.

Standards compliance

Non-Federal SSP PKI Service is tightly integrated with MyID® Personal Identity Verification (PIV) for DigiCert, a Federal Information Processing Standard 201 (FIPS 201)-compliant Card Management System (CMS). This provides non- federal entities the option to issue a variety of smart card types with embedded PKI-based digital certificates, including PIVinteroperable smart cards for applications requiring access and secure communication with federal agencies.

Non-Federal SSP PKI Service also enables state and local governments to issue digital certificates on a First Responder Authentication Credential (FRAC). This supports compliance with standards being developed by the U.S. Department of Homeland Security to establish interoperability between federal, state, and local first responder credentials. Several state governments have already successfully issued FRAC cards using Non-Federal SSP PKI Service.

Support for multiple assurance levels

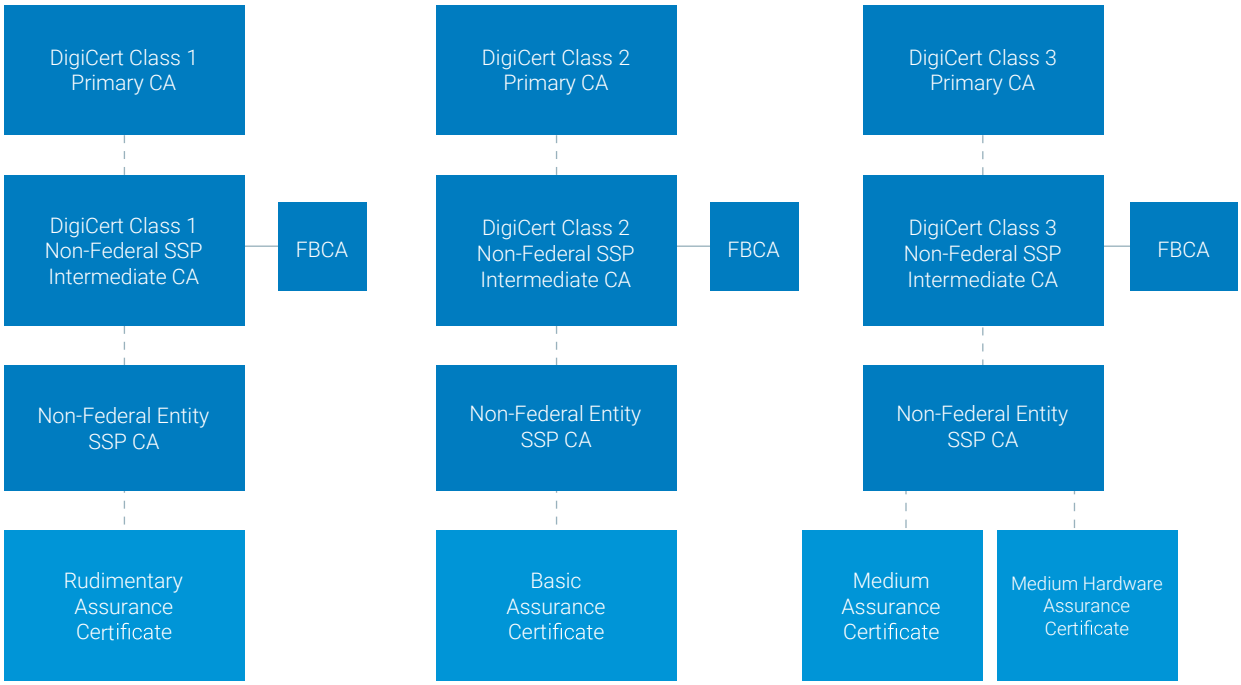

Figure 1: Non-Federal SSP PKI Hierarchy

Non-Federal SSP PKI Service provides the capability to issue and manage digital certificates at multiple assurance levels required to meet the broad PKI needs of non-federal organizations. In addition to the medium hardware level required by federal agencies, Non-Federal SSP PKI Service can provision digital certificates at the rudimentary, basic and medium assurance levels. The service enables non-federal entities to leverage digital certificates for applications requiring security services including authentication, encryption, digital signature, non-repudiation, and physical/logical access control.

The Non-Federal SSP PKI hierarchy, with Certification Authorities (CAs) at multiple assurance levels, is depicted in Figure 1.

Features & benefits

Feature	Benefit
Hosted certification authority (CA)	DigiCert hosts and operates at least one dedicated CA for each customer, which includes the following: • FIPS 140 Level 3 hardware security modules for CA key generation and storage. • Support for multiple client and device certificate types for both internal and external users. • Certificate revocation list (CRL) issuance as often as once per hour.
Registration authority (RA)	Provides administratores secure, remote control to: • Authenticate, approve/reject, and revoke certificate requests from subscribers. • Generate reports on certificate activity.
Key management Services (KMS)	Includes an integrated key management service with these capabilities: • Generation and distribution of user-private encryption keys and certificates. • Local Triple-DES encrypted sotrage of user-private encryption keys. • Two-man control for secure recovery for user-private encryption keys and certificates. • Support for leading secure messaging solutions.
Mission-critical reliability	Delivers reliability and availability levels that help meet mission-critical needs; including 24x7x365 monitoring, management, archiving, and full disaster recovery.
Card management system support	Integration with MyID PIV for DigiCert enables issuance of multiple smart card types, including PIV-interoperable smart cards, and delivers: • An easy-to-use, Web-based interface that allows secure management of the entire lifecycle of smart cards and digital certificates. • Support for various deployment modules, including local printing and remote bureau printing for large volume deployments. • Access to the system controlled through definable roles and smart card-based authentication.
Archive and reporting	An Oracle® database records signed audit information for all transactions. An integrated reporting tool is also included.

Feature	Benefit
Online certificate status protocol (OCSP) service	Includes a distributed OCSP validation service to enable timely retrieval of certificate status.
Interoperability with the Federal PKI (FPKI)	Cross-certification with the Federal Bridge Certification Authority (FBCA) at multiple assurance levels enables secure interoperability with federal agencies, states, and other non-federal entitites that are cross-certified with the Federal PKI.
Multiple assurance levels	Enables state and local governments to issue digital certificates at the assurance levels defined by the federal e-Authentication program (i.e., rudimentary, basic, medium/medium hardware, and high). This range of assurance levels meets security requirements for state and local government applications.
Compliant with federal standards	• Complies with the Federal Bridge Certificate policy. • Enable issuance of digital certificates for use with smart cards including PIV-interoperable cards like FRAC and a variety of others FIPS 140-certified hardware tokens.
Implementation and support services	DigiCert Professional Services alleviate the burden of planning, implementing, and maintaining an in-house PKI support infrastructure. • Includes 24x7x365 Level 2 help desk support and all required training for federal agency operations personnel.
Physical and logical access security	Multiple certificate types enable security for physical and logical access to applications in intranet, extranet, and Internet scenarios.

Find out more

DigiCert provides enterprise-class SSL, PKI and IoT security solutions for some of the world's biggest organizations–providing peace of mind and keeping them and their data secure at all times.

For more information, call 1.801.770.1736 or email pki_info@digicert.com.