HPE PUBLIC KEY INFRASTRUCTURE SERVICES

Advisory and Professional Services from HPE Pointnext Services

SERVICE OVERVIEW

HPE Public Key Infrastructure (PKI) Services are designed to assist Customer in design and implementation of a new PKI solution and/or to extend the capability of the existing PKI infrastructure for new business needs.

X.509 public key certificates standard is one of the most cost-effective solution in use today that facilitate the secure electronic transfer of information when advanced digital authentication, data integrity, and confidentiality are needed. Therefore, introducing, updating and/or extending PKI in the environment not only can reduce operational cybersecurity risk, but it can also enable new business operation models such as IoT device authentication to fulfil new business requirements.

HPE PKI Services are constructed under a flexible modular structure where Customers can choose one or more service module(s) in an engagement that matches their business needs. Table 1 lists the available modules.

TABLE 1. Available modules

Module name	Module description
Core modules	
PKI security assessment	For Customer who needs to verify and identify the current security PKI status (including certificates, hardware security module [HSM]), and identifies a road map to improve it
PKI process and procedure	For Customer who needs to have a **Digital certificate lifecycle process** and creation of Certificate Procedure (CP) and Certificate Practice Statement (CPS)
PKI design and implementation	For Customer who needs to implement new PKI or needs major update/upgrade of existing PKI
PKI OCSP	For Customer that would like to extend the revocation procedure with Online Certificate Status Protocol (OCSP)
Use case modules	
PKI for LTE/5G	Enable existing PKI to support Long-Term Evolution (LTE)/5G-specific usage and protocols needs
PKI for end entity (EE)	Enable existing PKI for users and server use cases (such as auto enrolment, authentication, digital signature, and others), and signing option like Signing Code with a Code Signing Certificate
PKI for IoT	Enable existing PKI for IoT devices using a protocol gateway and customized procedures
PKI for MDM and AD	Integrated external secure PKI system in Microsoft Active Directory (AD) to allow and authenticate the user and mobile devices
PKI for V2X/M2M	Enable existing PKI for Vehicle-to-X (V2X) and machine-to-machine (M2M) communications
Value added modules	
PKI value added	Design and enable value-added solutions including: • PKI reporting system • Security Credential Management System (SCMS) (Smartcard/OTP) • PKI active monitor • PKI RA automation

Duration of the project depends on the number of modules involved and the size of the in-scope environment.

Table 2 provides additional information on the features available under this service.

SERVICE BENEFITS

- **Reduce operation security risk—**Enhance data security and privacy by enhancing integrity and confidentiality in user-to-user, user-to-device, or device-to-device communication
- **Simplify operation**—Leverage public key certificates to simplify identify enrolment, management, and revoke
- **Accelerated transformation**—Adaption of PKI enable business to securely scale users, devices, and machines quickly to meet changing business goals
- **Simplify resource and budget planning**—Modular engagement model that can be tailored to meet Customer resource, timeline, and budget needs

SERVICE FEATURE HIGHLIGHTS

TABLE 2. Service features

Feature	Delivery specification
PKI security assessment	• Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules • Design and implementation – Assessment based on encipher model, encryption model certificate quality and procedure, compliance with CPS/CP – Road map to improve **Service deliverables** • Security assessment document (in Word/Excel format) • Road map document
PKI process and procedure	**Service activities** • Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules • Design and implementation – Design and set up certificates workflow over PKI system – Based on assessment, create the CPS and CP – Configuration based on workflow design **Service deliverables** • Service certificate workflow design document (in Word format) • CP/CPS

TABLE 2. Service features (continued)

Feature	Delivery specification
PKI design and implementation	**Service activities** • Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules • PKI—CP and CPS (if applicable) – Create the customized CP and CPS based on RFC 3647 (in Word format) • PKI design and implementation – Create high-level and low-level design (in Word format) – PKI software implementation and baseline setup – Integration with identities database (where needed) • Optional: HSM integration – Set up HSM for private keys (PKCS#11) storage (Hardware license need to be purchased and provide by Customer.) • Optional: PKI OCSP setup – Configure and customize OCSP • Root CA key ceremony • Knowledge transfer and operation handover – Create PKI administration documentation – Create PKI operations documentation – Knowledge transfer session for administration – Knowledge transfer session for operations – Operation handover **Service deliverables** • CP and CPS documents • High-level design document • Low-level design document • Administration and operations document
PKI OCSP	**Service activities** • Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules • PKI—CP and CPS – Customize the existing CP and CPS based on RFC 3647 • PKI OCSP design and implementation – Create high-level and low-level design (in Word format) – PKI software implementation and baseline setup – Integration with PKI system • Knowledge transfer and operation handover – Create PKI OCSP administration documentation – Knowledge transfer session – Operation handover **Service deliverables** • CP and CPS documents • High-level design document • Low-level design document • Administration and operations document

TABLE 2. Service features (continued)

Feature	Delivery specification
PKI for LTE/5G	**Service activities** • Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules • Design and implementation (Delivery task may include but not limited to the following—based on requirements.) – Review PKI design for LTE support – Creation/review of CPS – Creation of certificate template according to CP/CPS – Configuration of use cases in the PKI □ Set up CA to LTE service □ Set up certificate enrolment to authenticate eNodeB/Service Gateway (SG) □ Set up Simple Certificate Enrolment Protocol (SCEP)/Certificate Management Protocols (CMP)/Certificate Management Cent (CMC)/Enrolment over Secure Transport (EST) (or specific protocol) for auto-enrolment □ Validate timeline of certificates □ Certificate renewal before expiration – Pilot LTE use case with a subset of end entities • Knowledge transfer and operation handover – Review PKI administration documentation – Review PKI operations documentation – Knowledge transfer session for administration – Knowledge transfer session for operations – Operation handover **Service deliverables** – Service design document (in Word format) – CP/CPS review – Configuration of PKI to support use case – Pilot with limited number of EE – Administration and operations document (review)
PKI for EE	**Service activities** • Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules • Design and implementation (Delivery task may include but not limited to the following—based on requirements.) – Identification of use cases – Creation/review of CPS – Creation of certificate template according to CP/CPS – Configuration of use cases in the PKI – Pilot each use case with a subset of end entities • Knowledge transfer and operation handover – Review PKI administration documentation – Review PKI operations documentation – Knowledge transfer session for administration – Knowledge transfer session for operations – Operation handover • Service deliverables – Service design document (in Word format) – CP/CPS review – Integration in the software development lifecycle (SDLC) framework – Test plan – Configuration of PKI to support use case – Pilot with limited number of EE – Administration and operations document (review)

TABLE 2. Service features (continued)

Feature	Delivery specification
PKI for IoT	**Service activities** • Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules • Design and implementation (Delivery task may include but not limited to the following—based on requirements.) – Identification of use cases – Creation/review of CPS – Creation of certificate template according to CP/CPS – Configuration of use cases in the PKI – Pilot each use case with a subset of end entities • Knowledge transfer and operation handover – Review PKI administration documentation – Review PKI operations documentation – Knowledge transfer session for administration – Knowledge transfer session for operations – Operation handover **Service deliverables** • Service design document (in Word format) • CP/CPS review • Test plan • Configuration of PKI to support use case • Pilot with limited number of EE • Administration and operations document (review)
PKI for MDM and AD	**Service activities** • Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules • Design and implementation (Delivery task may include but not limited to the following—based on requirements.) – Identification of use cases – Creation/review of CPS – Creation of certificate template according to CP/CPS – Configuration of use cases in the PKI – Pilot each use case with a subset of end entities – Integration with MDM – Integration with AD • Knowledge transfer and operation handover – Review PKI administration documentation – Review PKI operations documentation – Knowledge transfer session for administration – Knowledge transfer session for operations – Operation handover **Service deliverables** • Service design document (in Word format) • CP/CPS review • Integration in the SDLC framework • Test plan • Configuration of PKI to support use case • Pilot with limited number of EE • Administration and operations document (review)

TABLE 2. Service features (continued)

Feature	Delivery specification
PKI for V2X/M2M	**Service activities** • Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules Design and implementation (Delivery task may include but not limited to the following—based on requirements.) – Review PKI design for LTE support – Creation/review of CPS – Creation of certificate template according to CP/CPS – Configuration of use cases in the PKI □ Set up CA to LTE service □ Set up certificate enrolment to authenticate OnBoard Unit/intelligent transport station □ Set up dedicated protocol management for auto-enrolment □ Validate timeline of certificates □ Certificate renewal before expiration – Pilot LTE use case with a subset of end entities • Knowledge transfer and operation handover – Review PKI administration documentation – Review PKI operations documentation – Knowledge transfer session for administration – Knowledge transfer session for operations – Operation handover **Service deliverables** – Service design document (in Word format) – CP/CPS review – Test plan – Configuration of PKI to support use case – Pilot with limited number of EE – Administration and operations document (review)
PKI value added	**Service activities** • Project kick off – Scope review/confirmation – Identify related stakeholders – Identify prerequisites and constraints – Gather information on the in-scope environment – Create project schedules • Design and implementation (Delivery task may include but not limited to the following—based on requirements.) – Design and set up PKI reporting system – Design and set up SCMS – Design and set up PKI active monitor – Design and set up PKI RA automation – Design and set up backup • Knowledge transfer and operation handover – Review PKI administration documentation – Review PKI operations documentation – Knowledge transfer session (up to two hours) – Operation handover **Service deliverables** • Service design document (in Word format) • Test plan • Set up of new service • Administration document (review)

PREREQUISITES

- These services may involve procurement software and/or license from Microsoft, Nexus, GlobalSign, Venafi, or from Customer's existing PKI vendor. Software and license may be required to be purchased and installed prior the engagement.
- Before the start of service delivery, Hewlett Packard Enterprise and the Customer will agree upon all the software and tools used for this service and the tasks and scope of this service.

COVERAGE

- Services will be provided during local HPE standard business days and hours excluding HPE holidays.

CUSTOMER RESPONSIBILITIES

- Provide a contact to organize project logistics and act as the escalation point
- Respond to all requests for information and artefacts as requested by HPE
- Provide subject matter experts (SMEs) as required to clear up any areas of confusion or uncertainty
- Purchase or provide all hardware, software, licenses, staff, current maintenance contracts, and environments necessary for HPE to provide this service
- Install and manage all tools and software necessary for HPE to provide this service
- Provide a resource to configure all infrastructures, machinery, and end-user components (network, cloud compute and storage assets, hypervisors, endpoints, machine, and others) necessary for HPE to provide this service
- Report and notify HPE consultants on any service disruption during the process
- Review and approve deliverables
- Provide a suitable work area commensurate with the number of on-site HPE consultants, including desks, chairs, and telephones and at least one analogue line suitable for modern digital data transmission for communicating with HPE network remotely
- Allow HPE consultants access to locations where the service is to be delivered

SERVICE LIMITATIONS

- Limitation of each service feature is outlined in Table 2. Additional charges incur for any additional services required.
- The entire deliverable documentation created for this engagement will be available in Microsoft Word or PDF electronic format.
- Services are deemed accepted upon performance.

GENERAL PROVISIONS/OTHER EXCLUSIONS

- Our ability to deliver this service is dependent upon the Customer's full and timely cooperation with HPE, as well as the accuracy and completeness of any information and data the Customer provides HPE.
- HPE reserves the right to reprice this service if the Customer does not schedule and provide for subsequent delivery within 90 days of purchase.
- To the extent HPE processes personal data on the Customer's behalf in the course of providing services, the HPE Data Privacy and Security Agreement Schedule—HPE Support and Professional Services found at hpe.com/info/customer-privacy.html shall apply.

ORDERING INFORMATION

Availability of service features and service levels may vary according to local resources and may be restricted to eligible products and geographic locations. To obtain further information or to order this service, contact a local HPE sales representative and reference the following service name:

- HPE Public Key Infrastructure Services

LEARN MORE AT

hpe.com/us/en/services/consulting/security.html

Check if the document is available in the language of your choice.

Make the right purchase decision.
Contact our presales specialists.

Chat Email Call

Share now

Get updates

Hewlett Packard
Enterprise

This data sheet is governed by the Hewlett Packard Enterprise current standard sales terms, which include the supplemental data sheet, or, if applicable, the Customer's purchase agreement with Hewlett Packard Enterprise.

a50000205ENW, November 2019