

DUTY STATEMENT

Employee Name:	Position Number: 580-152-1415-008
Classification: Information Technology Specialist III	Tenure/Time Base: Permanent/ Full Time
Working Title: Cryptography and Certificate Services Specialist	Work Location: 1616 Capitol Ave., Sacramento, CA 95814
Collective Bargaining Unit: M01	Position Eligible for Telework (Yes/No): Yes
Center/Office/Division: Information Technology Services Division	Branch/Section/Unit: Technology Integrations Services Branch

All employees shall possess the general qualifications, as described in California Code of Regulations Title 2, Section 172, which include, but are not limited to integrity, honesty, dependability, thoroughness, accuracy, good judgment, initiative, resourcefulness, and the ability to work cooperatively with others.

This position requires the incumbent to maintain consistent and regular attendance; communicate effectively (orally and in writing) in dealing with the public and/or other employees; develop and maintain knowledge and skill related to specific tasks, methodologies, materials, tools, and equipment; complete assignments in a timely and efficient manner; and, adhere to departmental policies and procedures.

All California Department of Public Health (CDPH) employees perform work that is of the utmost importance, where each employee is important in supporting and promoting an environment of equity, diversity, and inclusivity, essential to the delivery of the department's mission. All employees are valued and should understand that their contributions and the contributions of their team members derive from different cultures, backgrounds, and life experiences, supporting innovations in public health services and programs for California.

Competencies

The competencies required for this position are found on the classification specification for the classification noted above. Classification specifications are located on the [California Department of Human Resource's Job Descriptions webpage](#).

Job Summary

This position supports the California Department of Public Health's (CDPH) mission and strategic plan by creating customer focused solutions that are responsive and agile; supporting a modern infrastructure, tools, architecture, and standards; to effectively provide efficient services following service level agreements. The Information Technology Services Division (ITSD) leverages data and technology to create sustainability across CDPH by creating efficient solutions that meet customer expectations and reduce waste. As well as, creating innovative solutions, strengthening partnerships and collaborations, and embracing technology.

Under administrative direction of the Information Technology Manager (ITM) II, Chief of the Technology Integration Services Branch (TISB), the Information Technology Specialist (ITS) III

provides critical technical oversight for cryptography and certificate lifecycle services deployed and being deployed at CDPH to strengthen the Department's security posture, ensure crypto-agility, and support emerging program needs, audits, and compliance activities. This includes, but is not limited to, leading enterprise Quantum-Resistant Cryptography readiness and post-quantum migration efforts, developing foundational Public Key Infrastructure and certificate automation architecture frameworks and processes across on-premises and cloud platforms, collaborating with the Security Operations Center and cross-functional teams to ensure appropriate monitoring and controls for certificate and key management systems, and making recommendations to improve performance, reliability, and scalability.

The ITS III performs duties within the System Engineering and Information Security Engineering domains.

Special Requirements

- ☐ Conflict of Interest (COI)
- ☐ Background Check and/or Fingerprinting Clearance
- ☐ Medical Clearance
- ☐ Travel:
- ☐ Bilingual: Pass a State written and/or verbal proficiency exam in
- ☐ License/Certification:
- ☐ Other:

Essential Functions (including percentage of time)

- 25% Plans, develops, and documents policies, procedures, requirements, and methodologies; implement security and privacy controls across multiple information technology disciplines; conduct presentations or briefings to executive management; contribute in the planning of the overall organizational information technology strategy and direction, identify current and emerging trends in technology and recommend appropriate courses of action, and advise management and executive level staff on governance and policy that support forward movement, aligning with technological modernization strategies in support of CDPH programs.
- 25% Serves as CDPH's technical lead for preparing the enterprise's transition to Quantum-Resistant (post-quantum) Cryptography in alignment with the National Institute of Standards and Technology (NIST) finalized standards – Federal Information Processing Standards (FIPS) 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) and applicable federal and state migration timelines. Supports and monitors for compliance with emerging standards and deadlines. Develops and maintains an enterprise cryptographic inventory / Cryptographic Bill of Materials (CBOM). Identifies uses of quantum-vulnerable public-key algorithms (RSA, ECC, and Diffie-Hellman) across applications, certificates, protocols, code repositories, and infrastructure.

Assesses and prioritizes systems by risk and data-confidentiality longevity, mitigating the "harvest-now, decrypt-later" threat, and develops a phased, risk-based QRC migration roadmap. Designs and pilot's hybrid (composite) certificate deployments and quantum-safe algorithms in non-production environments, validating performance, interoperability, and backward compatibility before production rollout. Establishes cryptographic governance,

standards, and a crypto-agile architecture that enables, CDPH to measure and change cryptographic algorithms efficiently as standards evolve. Advises executive leadership on emerging quantum-computing threats and post-quantum cryptography strategy.

- 25% Leads the issuance, automation, renewal, and governance of digital certificates across all CDPH on-premises and cloud platforms, ensuring the Department meets the CA/Browser Forum reduction of SSL/TLS certificate lifetimes. Architects, deploys, and supports automated certificate lifecycle management. Integrates certificate services with cloud platforms (Sectigo Certificate Manager with Microsoft Azure Key Vault and Microsoft Entra ID), managing SCEP/ACME endpoints, RA certificates, managed identities, and automated CSR generation, storage, and rotation. Automates certificate operations via REST API's and PowerShell and manages certificate provisioning for on-premises VMs and Azure Enterprise Applications including installation, export, thumbprint management, and scheduled-task automation.

Monitors certificate health, expiration, and agent activity using Azure Monitor / Microsoft Sentinel, maintaining an accurate enterprise certificate inventory to prevent outages, security incidents, and compliance gaps. Collaborates with the Information Security Office (ISO), NetOps, IAM, and Server Architecture teams to deliver the enterprise automated certificate management effort, and provide guidance, documentation, and proof-of-concept testing to ITSD staff.

- 20% Acts as the Expert Advisor for all other cryptography and certificate-based needs across CDPH, ensuring compliance with NIST 800-53, FIPS 140-2/140-3, Health Insurance Portability and Accountability Act (HIPAA), and State Administrative Manual (SAM)/SIMM requirements. Administers Public Key Infrastructure (PKI) services, obtaining public key certificates from ISO-approved providers and enforces defined key activation/deactivation dates and rotation policies.

Establishes and enforces on key vaults (Azure Key Vault), and relevant cryptographic standards including Role-based Access Control (RBAC)/least-privilege access, managed identities, expiry times, auto-rotation through partnered Certificate Authorities, purge protection, and diagnostic/audit logging. Supports secure key, secret, and certificate management for code signing, S/MIME, device/user certificates, TLS termination, and transmission confidentiality/integrity across on-premises and hybrid-cloud environments. Provides expert consultation to programs, project teams, and executive leadership on cryptographic controls. Develops policies, standards, and procedures. Represents Technology Integration Services in enterprise architecture, security, and change-control forums.

Marginal Functions (including percentage of time)

- 5% Performs other work-related duties as assigned.

☐ I certify this duty statement represents an accurate description of the essential functions of this position. I have discussed the duties and have provided a copy of this duty statement to the employee named above.

☐ I have read and understand the duties and requirements listed above and am able to perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation may be necessary, or if unsure of a need for reasonable accommodation, inform the hiring supervisor.)

Supervisor's Name:	Date	Employee's Name:	Date
Supervisor's Signature	Date	Employee's Signature	Date

HRD Use Only:

Approved By: D.S.

Date: 10/7/26