ance Review:

Employee Name:	Rahul Bhogal		**Empl Id:**	348080	
Designation:	Project Engineer (PE)		**Educational Qualification:**	M.Tech in Computer Engineering form NIT Kurukshetra	
Group / Team / Project/ Area:	CMVP		**Expected efforts:**	1480.5 hours (9 Months)	1800 hours / year
Review Period	**From:**	**01/08/24**	**To:**	30/04/25	

1. List existing skills used and your Ability to accomplish Assigned Responsibilities: (Provide the detailed description of work done yourself during the period – Contribution towards technical output)

Existing Skills Utilized: C Programming Language**,** Bash Scripting**,** JavaScript**,** Python

1. **Development of Secure Post Quantum Public Key Infrastructure: -**
    - Implementation and IUT validation of Key Generation, Signature Generation, and Signature Verification with intermediate values for ML-DSA based on FIPS204 standard, as per NIST.
    - Parsing NIST Json files, for generating test vector for Algorithm validation.
    - Analyzed and resolved compilation issues and platform dependency for DSA, RSA, and AES on Linux platform.
    - Validated Cryptographic algorithms AES, AES-XTS and SHA-HMAC using NIST and custom test vectors.
2. **Automation and Setting Up of a Reference Lab for Validating Cryptographic Algorithms/Modules as per ISO/IEC Standards**
    - Prepared derived test requirements document based on ISO/IEC 24759 standard for Cryptographic Module validation included all vendor and tester assertions for Module validation at Level 4.
    - Created structured JSON configuration files support automated validation for CMVT web portal.
3. **Design Linked Incentive (DLI)**
    - Developed a Bash script that automates DLI log report generation. Supported three periodic formats: daily, weekly, and monthly.

a. Goal Achievements:

1. Developed Python ML-DSA code per FIPS 204, validated with NIST test vectors for validation.
2. Resolved compilation issues in DSA, RSA, and AES across.
3. Validated AES, AES-XTS and SHA-HMAC using NIST and custom vectors.
4. Enhanced skills in writing Bash scripts to automate DLI log reports.

2. Suggested Area of Improvement:

1. Strengthened knowledge of Post-Quantum Cryptography by implementing additional PQC schemes with thorough documentation.
2. Improved time management skills to consistently meet project deadlines.
3. Enhanced debugging abilities across platforms and learn new tools to support diverse cryptography tasks.

3. Demonstration of Core Values :

1. Actively collaborated with team members to ensure smooth task execution.
2. Participated in regular meetings to share updates and align with project goals.
3. Presented cryptographic algorithms to enhance team understanding.
4. Continuously upskilled in relevant technologies to contribute effectively.

4. Future Plans: Any Interesting observations

1. Continue cryptographic algorithms and module Validation in alignment with ISO/IEC 19790 standards.
2. Design and implement custom test vectors for thorough validation of cryptographic algorithms.
3. Integrate existing cryptographic implementations from CMVTlab into the Crypto Web Application to automate validation workflow.

5. Additional Comments:

None

Rahul		
Rahul Bhogal	Dr. Abey Jacob	Dr. Abey Jacob
Name and Signature: **Employee**	**FLA**	**SLA**

Date: