Domain: Google Key Management Service

Objective	As a Cloud Security Architect, I need to certify Google Cloud HSM as a Citi approved HSM solution and managed by Citi Key Management Center (KMC).
Acceptance Criteria	• Secured architecture for Cloud KMS using CloudHSM. • Certified to an AL5 with classification of "Restricted" • Support requirements from different teams including Google Foundations, VDI, EAP and XCS Projects • Create /update existing TFE Module to provision approved architecture. • Protect existing projects with HSM backed KMS keys to remove existing RE.
Stakeholders	• CISO Cloud Security Architect Team • CISO Cloud Encryption team • CISO Threat Modelling Team: • VDI Project team • XCS Project team • EAP Project team • CTI Public Cloud Team • ISRP .
Resourcing	CISO Cloud Security Architect-1E
Milestones	Recertify Google Cloud KMS service with approved HSM solution- RFI/RFP TFE module Threat model ISRP Approval for AL5 with classification of "restricted"
Submitter	Oliver Klein

Please reach out to Haripriya Jagannathan/Siddhi Revandkar/Dolapo Kukoyi once the document is ready for review and post it in **GCP Public Cloud Enablement-CTI-NAM** >> **Foundations** channel >> **User Stories** File by Oct 3rd

For Reviewers Use Only

Feedback	Feedback will be provided by reviewers here. Reviewers should record feedback as follow. Date – Reviewer Name – Feedback e.g. 2 Oct, 2024 – Mo Alslaoom – consider deletion of requested accounts to be added to success criteria.
Status	Review | Approved

Domain: Bare Metal (Rack) HSM

Objective	I need to certify the Bare Metal HSM to provide classic HSM functionalities for applications hosted on GCP, that requires PKCS11/JCE/KSP interfaces for securing application related secrets and provides cryptographic functionalities. HSMs and surrounding services are managed by KMC / HSM operations.
Acceptance Criteria	- Approved and secured architecture - Certified to AL5 with classification of "Restricted - Successfully deployed HSM HW on Google DCs - Create TFE provisioning for addition elements (Compute Engine / GKE)

	- Key backup/restore/inventory solution is designed and implemented
Stakeholders	- CISO DSS – HSM engineering - CTI Public Cloud Team - CISO Threat Modeling Team - ISRP - CIVA?
Resourcing	
Milestones	Approved architecture Physical HSMs are procured and delivered Network is up and running devices are accessible TFE module Thread model ISRP approval RFP
Submitter	Gal, Csaba

For Reviewers Use Only

Feedback	
Status	