FAQ for QVI Application Questionnaire

What Origin QVI Kit Provides

GLEIF's QVI Application Questionnaire is challenging. It asks for a lot of details. QVI candidates who are responding to GLEIF, and who plan to use Origin QVI Kit (OQK), may wonder how many of GLEIF's requirements are addressed in full or in part by the Origin platform, and what they still have to implement themselves. Below are many questions from GLEIF, with comments from Provenant to help inform your answers.

In the comments, inline notes in the form (DF-???) reference platform tasks that Provenant is tracking internally, related to the topic. In many cases a simple form of the feature already exists; what we are tracking may be an enhancement, a need for documentation, or some test scenarios. Release notes will reference and explain these tasks as they become relevant.

Section F, Q1.0

If you will charge for vLEI Issuance and/or revocation will/do you have a standard process for receiving payments from a Legal Entity?

> Provenant intends to add a billing and payment collection module to OQK (DF-860), but this is not yet available. For now, QVIs should address this requirement on their own.

Section F, Q2.0

How will/do you ensure processing applications for issuance and revocation of vLEIs without delay?

> OQK models the vLEI issuance process from beginning to end, and automates many aspects. The most time-consuming parts of the process are: searching public records to identify the DAR, doing identity assurance on LARs, and conducting the issuance ceremony. If QVIs that use OQK are already LOUs, or if they can partner with LOUs so the public record search is collapsed into the same task that happens during LEI issuance, the first of these tasks becomes trivial (DF-861). Identity assurance is fully automated and can be completed in minutes. The issuance ceremony itself is scheduled and then orchestrated carefully by Origin, so the QVI staff has little to learn, and few details to track manually.

All individuals or organizations that use Origin's web wallets, including all QVIs, can enumerate credentials to which they are associated (e.g., as issuer, issuee, or part of the vLEI trust chain). A simple right-click on a vLEI credential exposes a "request revocation" action. This action triggers an automated workflow that sends automated notifications to all stakeholders, allowing them to approve or deny the request if they have appropriate permissions, and automatically scheduling a meeting for members of a multisig if needed. The workflow guarantees correct analysis and conformance to GLEIF governance rules. The revocation workflows are shown in the My Work view for all stakeholders, allowing them to monitor progress and escalate if some other party is slow to react.

In addition, each QVI that uses Origin QVI Kit can connect its own reporting mechanisms to these automated workflows by API call. For example, Provenant accepts input about vLEIs via its public mailbox, vlei-support@provenant.net, and can use such emails to trigger automated revocation workflows. [DF-1374]

Section F, Q3.0

Will/do you have a process in place to verify that the Legal Entity Identifier (LEI) of the Legal Entity has an entity status of Active and an LEI registration status other than Lapsed, Retired, Duplicate or Annulled in the Global LEI system?

OQK automatically monitors the LEI status of all organizations that receive a vLEI (DF-862). Within a few minutes of an LEI status changing, Origin will learn about the update and issue notifications to a QVI if any action is required on their part (DF-291). Origin also issues automatic renewal reminder emails as the expiration of an LEI approaches. Typically these automated reminders occur at 30 days, 10 days, and 3 days before expiration, but the intervals can be customized (DF-863).

Origin also calls the GLEIF APIs automatically, just before issuing a vLEI, as a final guarantee that LEI status complies with governance framework rules (DF-862).

Section F, Q4.0

How will/do you inform the Legal Entity of needed amendments to their instructions or refusal to issue vLEIs?

OQK has a notification system that automatically generates emails (DF-866) or SMS (DF-864) to employees of a vLEI client organization. Any time a vLEI-related workflow (e.g., issuance, revocation) requires an approval or an action on the employee's part, notifications are emitted, and the system tracks the fact that work is paused, waiting for the employee to respond. Provenant will eventually add automatic escalation logic (DF-865, DF-867).

Parties that receive notifications all have the opportunity to configure these notifications — for example, preferring SMS or email, or updating the phone numbers or emails where the notifications are sent. We know that the initial contact information for these parties is correct, because we verify control of email address when they join Origin, and we verify control of phone number during identity verification. Origin will reverify if the contact info changes. [DF-1375]

Section F, Q5.0

In the case of vLEI Credential Issuance, will/have you implemented the necessary Identity Verification requirements?

Yes. OQK uses a validation agent, IDVerse, that is specialized in identity verification and that complies with NIST IAL2 requirements as specified by the vLEI governance framework. When a person needs identity verification, OQK explains to the person that they will need a passport or other suitable government-issued photo ID (e.g., a driver's license, a US green card, etc.). It then gives IDVerse the person's phone number.

IDVerse immediately contacts that person by SMS. Without installing an app, the person visits a link on their phone. They upload a photo of their physical credentials. The photo undergoes a sophisticated analysis for telltale signs of counterfeiting. IDVerse also performs OCR to extract machine-readable information. It then calls government APIs to prove that the extracted information corresponds to an actual legitimate and unexpired credential. The person undergoes a liveness test, and the face captured during liveness is compared to the photo on the government ID using facial recognition. All of this takes about 1-2 minutes.

IDVerse generates a careful audit trail that can later justify the identity verification decision it makes. It also allows Origin to fetch the photo as captured during the liveness test. During vLEI issuance, Origin requires the QVI staff to compare this photo to the faces it sees in the webmeet (DF-868). This guarantees that the person who's undergone identity verification is the same person that Origin is now connecting to cryptographic keys. This whole process has been demoed to and verbally approved by GLEIF as a satisfactory implementation of their requirements.

After the link between legal identity and cryptography has been proved, Origin throws away the photo of the individual, minimizing the PII retained by the QVI and the platform. (Origin retains the person's legal name and their email address.)

QVIs that have their own identity assurance solution can plug it in to OQK as an alternative to IDVerse, as long as that solution meets GLEIF's requirements. The interface is quite simple; OPK just needs an API to start identity verification, an API to fetch status on a pending job, the ability to receive a callback at a webhook when the process completes, and an API to fetch photos (DF-880).

Section F, Q6.0

Will/do you validate the name of the person and the Official Organizational Role of the Legal Entity Official Organizational Role vLEI Credential using one or more official public sources?

Yes, a certification by the QAR that this requirement has been met is built into the workflow that OQK provides for credential issuance (DF-869).

Section F, Q7.0

Will/do you access, using the GLEIF API, the lists of Official Organizational Roles maintained by GLEIF to choose the correct OOR code to be embedded in OOR vLEI Credentials?

Yes. Although GLEIF has released the official list of OOR codes, GLEIF's API hasn't been released, and the current OOR credential schema still calls for free-form text in this field. When the schema is updated, and the API exists, OQK will begin issuing with the codes (DF-870).

Section F, Q8.0

Will/do you have processes and procedures to manage, research and validate incoming challenges regarding the name of a person and/or their Official Organizational Role in a Legal Entity OOR vLEI Credentials?

> Yes. The landing page for Origin includes the support email for the QVI, so any member of the public can contact QVI support to report such issues (DF-871).

Section F, Q9.0

Will/have you complied with the requirements defined for all vLEI services included in the Appendix 5 to the vLEI Issuer Qualification Agreement – Service Level Agreement (SLA)?

> Yes, OQK meets these requirements.

Section F, Q10.0

Will/do you call the vLEI Reporting API with each issuance of a Legal Entity vLEI Credential and for each Legal Entity Official Organizational Role vLEI for which the Legal Entity has confirmed the consent of the OOR Person?

> Yes. OQK does this automatically (DF-872).

Qm1.0

Will you have a process to monitor compliance with the Service Levels as defined in the vLEI Service Level Agreement (Appendix 5)?

> Yes, OQK will generate an SLA compliance report (DF-874).

Qr1.0

Will/do you have followed the policies for revocation of vLEI Credentials specified in vLEI Ecosystem Governance Framework?

> Yes, OQK complies. Revocation of an LEI causes an automatic, cascading revocation of the LE vLEI, for example (DR-875).

Qr2.0

Will/do you have a process to check the status of the LEIs for which vLEIs have been issued for those LEIs with renewal dates of 30 days or less?

Yes, OQK checks automatically, and it issues reminder notices to staff of the legal entity by email and/or SMS (depending on their communication preferences). These checks get more frequent the closer the renewal date is.

Qr3.0

How will/do you inform the Legal Entity of potential revocation of their vLEIs if their LEI lapses?

This is part of the text of the reminder emails that OQK automatically sends out as the renewal date of the LEI approaches.

Qr4.0

Will/do you have a process to trigger the revocation of a Legal Entity vLEI?

Yes, OQK does this automatically if an LEI is revoked.

Qr5.0

Will/do you check your public Verifiable Data Registry for vLEI credential issuance and revocation registry for erroneous or malicious issuances and revocations (primary issuances) in order to inform your management process that a key rotation/recovery may be required?

Yes, OQK uses a super watcher service that detects malicious use of AIDs and reacts accordingly (DF-877).

Qr6.0

Will you notify GLEIF to revoke your Qualified vLEI Issuer vLEI Credential if you choose to no longer operate as a Qualified vLEI Issuer?

If an OPK customer announces that they intend to discontinue their OPK subscription, Provenant will make reasonable efforts to remind them of this duty.

Section I part A Q2.0

Will/do you have a document which describes the software development tools and environment in place for vLEI operations?

OPK has such a document. It is available upon request from vlei-support@provenant.net (DF-878). QVI customers should supplement it with any tools and infrastructure that they layer on top.

Section I part B Q1

Will/have your developers follow the security recommendations in the vLEI Ecosystem Governance Framework when designing software or services for use with vLEI credentials and the vLEI Ecosystem?

Yes. OPK has been designed after months of careful study of the governance framework. It is also the result of years of architectural experience with SSI and cryptographic systems by Daniel Hardman, Provenant's CTO, and it has been discussed at length in community meetings and in private conversations with Sam Smith, Phil Faeirheller, and others.

Section I part B Q2

Will/do you have a process in place to manage the security of your cryptographic keys?

OQK uses GLEIF's Signify/Keria technology for management of keys. This includes keys of a QVI's customers, but also keys of the QVI staff itself. OQK requires users (including QVI staff) to store their wallet passcode in a password manager of their choice.

Keys are generated in a secure wallet on the client side, and are never visible in unencrypted form on servers. The agent must call the client anytime keys are used, and the client gets the user's permission to take cryptographic actions with those keys.

OQK can work with keria hosted off the Origin platform, if people want to host their own. This allows customers of the QVI to get wallet hosting anywhere. It also allows people to change their mind about wallet hosting at any time.

Section I part B Q3

Will/are specific holders of cryptographic keys kept confidential and are to be determined by your Qualified vLEI Issuer internal policy?

> OQK does not reveal the names of the individuals who hold QVI multisig keys, nor the names of the individuals who hold LE multisig keys. There is no way to discover this information easily.

Section I part B Q4

Will/have signing keys to be rotated whenever there is a likelihood of key compromise?

> OQK will provide key rotation features that make this easy.

Section I part B Q5

Will/are the time and place of key rotation kept confidential among the key holders until after the rotation has been completed?

> Yes, OQK accomplishes this with private notifications to the affected parties.

Section I part B Q6

In the case of the key compromise, will/have key compromise recovery operations be reported to GLEIF within 24 hours of gaining knowledge of the key compromise?

> Yes, OQK will ask users if they are rotating keys because of a suspected key compromise — and if yes, will report this to GLEIF and to the QVI automatically [DF-1048].

Section I part B Q7

Will/have all key compromises been investigated as expeditiously as possible at your own expense to determine the source of the key compromise and a full report of the investigation will/has been made to GLEIF?

Origin has not experienced any key compromises.

Section I part B Q8

Will/do you use best practices for code delivery and observe library usage for signature verifiable infrastructure?

Origin source code is stored in carefully secured private or public GitHub repositories. Both repository types are modified through pull requests, and are configured to allow merge only after receiving approval from a second set of eyes. Builds are reproducible and associated with tagged commits. Commits are signed. We run static source code analysis tools that check for vulnerabilities in the direct code, and that also study the code dependencies. These tools automatically recommend updated dependencies if upstream libraries have known vulnerabilities, and they distinguish between minor vulnerabilities and serious concerns with proof of concept exploit code. We have an engineer who is specifically tasked with being our champion/advocate for secure coding practices, and for monitoring our responsiveness to the static code analyzers. He meets with a supervisory committee monthly.

Section I part B Q9

For your QVI Delegated AID, will/do you use at least a 2 or 3 thresholded multi-sig scheme for added security and for each key-pair in a thresholded multi-sig, will/do you use a non-co-located key store for adding security?

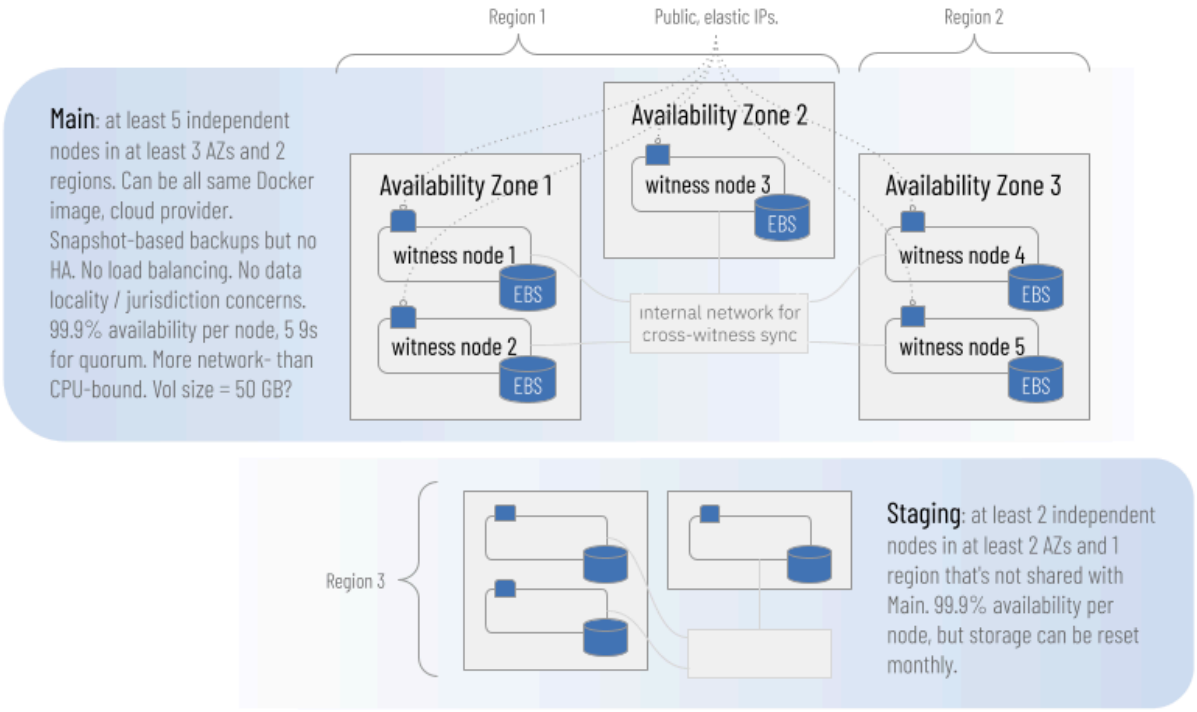
Yes. OQK enforces the 2 of 3 policy for QVI multisig, so any QVI that uses OQK is guaranteed to be using such a policy [DF-1049]. The keystore for each participant in the multisig is managed by Signify+Keria, which guarantees that the keystores are only decrypted in client-side code in the browser of each user; keystores cannot be accessed by malicious sysadmins or hackers who gain access to the hosting platform.

Section I part B Q10

Will/does your Endorser use either a Witness Pool or a Ledger Registrar for Endorsement?

OQK will add to its production witness pool 5 new witnesses in 3 AWS availability zones in 2 geographical regions, each time a new QVI begins using the OQK product. These witnesses will be dedicated to service the activities of just the new QVI, and will be appropriately backed up, load balanced, and hardened. Thus, the ecosystem's witness pool will grow in capacity and robustness as the EGF requires.

> Individual QVIs that use OQK, such as Origin, can override or supplement their witness pool if they wish. In addition, companies and individuals who receive vLEIs can specify which witnesses they prefer to use.



Section I part B Q11

Will/does your KERI Witness Pool have a minimum pool of five (5) Witnesses?

Yes, five unique witnesses per QVI. See above.

Section I part B Q12

Will/do you publish your Witnesses to at least one ecosystem discovery mechanism: KERI Distributed Hash Table (DHT), DID method resolvers or Ledgers?

The witnesses used by OQK are discoverable via KERI. The AID of each QVI appears in GLEIF's KEL in conjunction with its QVI vLEI issuance event. This connects the QVI's witnesses to GLEIF's internal records, so anybody traversing the GLEIF ecosystem will discover all of the QVI's witnesses. In addition, the QVI'switnesses will be discoverable through any did:webs DID document that is based on an AID referencing the witnesses, making them discoverable to the larger DID community as well.

Section I part B Q13

For your Witness Pool, will/does the encryption key store reside on a different device or host from that of the Witness service?

Yes, OQK enforces this.

Section I part B Q14

For your Ledger Registrar, if the Registrar Signing Key Pair Key store resides on the Registrar Service host, will/are dedicated user only permissions used on the key store directory and its contents?

OQK uses a witness pool instead of a Ledger Registrar.

Section I part B Q15

For your Ledger Registrar, will/does the encryption key store reside on a different device or host from that of the Registrar service?

OQK uses a witness pool instead of a Ledger Registrar.

Section I part B Q16

For your Watchers, if the Watcher Signing Key Pair key store resides on the Watcher Service host, will/are dedicated user only permissions used on the key store directory and its contents?

Yes, OQK will enforce this.

Section I part B Q17

Also, when used, will/does the encryption key store reside on a different device or host from that of the Witness service?

Yes, OQK will enforce this.

Section I part B Q18

Will you successfully install, test and implement the vLEI Issuer software within the stated timeframes and will you use the vLEI software package for hosting Witnesses, Watchers, Discovery and Oracles for Key Management?

OQK offers a no-install model where LOUs can simply subscribe to the service. This allows them to be up and running in minutes.

OQK uses all relevant GLEIF software packages. For example, it uses the API that GLEIF provides for notifying GLEIF of DARs and of issuances of vLEIs. OPK also calls a GLEIF API to check the LEI status of orgs prior to issuance. When GLEIF exposes an API to find OOR codes, OPK will call that API as well

Section J Q1.0

Please describe the current service/hosting environment. It is hosted, in-house, via a third-party, etc.? Describe the use of any cloud-based resources such as Amazon Web Services or Microsoft Azure. Relevant process documents

OQK is hosted on AWS. The unit of deployment of OQK is called a "cell". This is a kubernetes cluster that bundles many interelated services. A given cell is deployed in a

single AWS region. Two cells are offered: North America (AWS US East region) and Europe (AWS Frankfurt). Additional cells can be added.

Section J Q2.0

Will/do you perform any monitoring over the vLEI Issuer-related IT infrastructure? Relevant process documents

Yes, k8s health monitoring plus AWS health monitoring plus probes of various kinds.

Section J Q3.0

Will/are there any redundancies built into the hosting platform and hardware? Copies of the related agreements

Yes, redundant DB, redundant FS (6 9s), redundant web services inside k8s cluster that is automatically load balanced and automatically restarts downed services.

Section J Q4.0

Has there been any unscheduled downtime of your own network or system in the past twelve (12) months? Relevant process documents

No. See this doc.

Section J Q5.0

Will/do you have a current disaster recovery and/or business continuity plan in place? How often will/is it tested? Has the continuity plan needed to be invoked during the past 3 operating years? Relevant process documents

Provenant has plans to ensure business continuity. However, each QVI that uses OQK should make their own plans on the assumption that the platform could be a point of degraded service or failure.

Some relevant documents that OQK customers can use when building their own plans include: 1, 2

Section J Q6.0

Will/do you have structured backup policies and practices? Relevant process documents and technical diagrams

Backups of OQK occur hourly for most data, and daily for more stable data, via AWS snapshots.

Backup policy

Resource Type	Stored data	Backup Frequency	Backup Retention	Note
EFS 1 (Wallet data)	Wallet	Daily	35 Days	
EFS 2 (Application data & logs)	Application data & Logs	Daily	35 Days	
Root DB	Standard Data	Hourly	30 Days	Continuous Backup
Witness (EBS)	Witness Wallet	Daily	30 Days	

Section J Q7.0

Will/are third party services (e.g., augmented staff, cloud services, data centers) utilized in order to provide Qualified vLEI Issuer services? Relevant process documents and technical diagrams

Yes. OQK uses AWS for many IaaS needs. It also uses N8N for distributed workflow, Jitsi (8x8's JaaS services) for web meetings, and IDVerse for identity verification.

Section J Q8.0

Will/do you have a formal vetting process for evaluating the reliability of third-party service providers? Relevant process documents and technical diagrams

Section J Q9.0

Will/does this process evaluate: Financial stability, Market reputation, Ability to meet vLEI Ecosystem Governance Framework requirements, Evaluating the potential risks of utilizing the services provided? Relevant process documents and technical diagrams