1. Request for Proposals for FACE™ Verification Authority Services

The Open Group, on behalf of the Future Airborne Capability Environment (FACE™) Consortium, is requesting proposals from organizations capable of conducting verification of software conformance to the Technical Standard for Future Airborne Capability Environment (FACE Technical Standard). The FACE Consortium will recognize each organization that meets the qualification criteria as a FACE Verification Authority (VA). This request for proposals (RFP) will remain open indefinitely as no limitations exist for how many VAs may qualify. The FACE Consortium will respond to proposals once a quarter or at periodically scheduled dates depending upon the number of proposals received over a given period.

The intention of the FACE Technical Standard is to reduce costs and speed delivery of military avionics systems. The FACE Consortium, an Open Group Managed Consortium, has concentrated its efforts toward addressing avionics software development and deployment. By codifying a modular architecture, standard interfaces, data models, and conformance criteria into a common operating environment and reusable software components, a means to share capabilities will exist across platforms, military services and avionics vendors.

The FACE conformance certification process provides a formal evaluation assuring that the software component adheres to the FACE Technical Standard. If a software component passes the complete set of conformance tests and other defined required criteria, then it is considered FACE Conformant and is marketable as such with an official certification logo. The FACE Conformance Policy and the FACE Conformance Authorities Plan describes this process in greater detail. These documents are freely available from The Open Group bookstore website. The FACE Conformance Policy is available at https://www2.opengroup.org/ogsys/catalog/X1303 while the FACE Conformance Authorities Plan is located by going to https://www2.opengroup.org/ogsys/catalog/X1302.

FACE Verification activities per se are not funded by the FACE Consortium or the United States Government, and no contractual relationship will exist between them and the VA. The FACE Consortium will register an organization that is qualified and approved as a VA to formalize the governance of the verification process. Approval gives the applicant the authority to function as a VA but does not obligate them to accept any or all VA work. The text below describes the statement of work and the terms and conditions for this relationship, the instructions for candidates to follow in applying as a VA, and the evaluation criteria that the FACE Consortium will follow in accepting the applicant.
2. Verification Authority (VA)

The VA is responsible for conducting the For-the-Record conformance verification test using approved test tools and also for assessing the Verification Evidence provided by the Software (SW) Supplier. The VA will employ a uniform and repeatable verification approach for each segment of the FACE Technical Standard and will issue a pass or fail Verification Statement.

The VA has a responsibility to uphold the FACE brand. This responsibility includes keeping up-to-date with the FACE standards as well as the FACE goals and ideals. The VA should regularly communicate with other VAs and the Certification Authority (CA) to ensure a consistent verification approach throughout the VA community.

2.1 VA Requirements/Tasks/Statement of Work

The VA must:

- Demonstrate and maintain internal or external organizational independence from the development and integration efforts of FACE programs.
  - The VA duties are appointed to a legal business entity that can be an organization, an entire company, or a named organization within a company. Individuals working within that entity cannot be assigned duties developing requirements, designs, or software of FACE products while employed within that organization.

- Remain independent of the software development effort as follows:
  - The VA can specify what failures occur in testing or evidence, but cannot give advice on how to fix issues.
  - The VA may assist in the development and execution of tests, but cannot assist or participate in the development of requirements, design, or software.

- Possess and maintain knowledge of:
  - The FACE Technical Standard.
  - The FACE Conformance verification techniques.
  - All approved FACE Conformance Test Suite(s).
  - Each approved FACE Conformance Verification Matrix version.

- Demonstrate the following experience:
  - Operation within well-defined processes and/or hold process-oriented credentials (such as CMMI, ISO9000, or AS9100).
  - Management of a laboratory equipment configuration control (such as ISO/IEC 17025, ANSI/EIA-649, IEEE/EIA-12207.0, or MIL-HDBK-61A).
Perform the tasks per the FACE Conformance Policy including but not limited to the following:

- Establish a Verification Agreement with each SW Supplier applicant.
- Assess submitted verification evidence for correctness and completeness, including verification of the digital signature generated by the SW Supplier.
- Conduct or witness the For-The-Record verification testing using an approved version of the FACE Conformance Test Suite.
- Review the verification evidence for each requirement in the FACE Technical Standard to confirm that the Software Supplier has correctly identified the set of applicable conformance requirements based on the supplier’s claim of conformance as defined in the Conformance Statement.
- Confirm that the Software Supplier has included all applicable conditional requirements in their Conformance Statement.
- Verify 100% of applicable requirements using the verification method for each that is defined in the applicable Conformance Verification Matrix.
- Enforce policies and procedures that ensure protection of SW Suppliers’ Intellectual Property (IP) including limiting access to any SW Supplier’s IP to only VA personnel who need access to the SW Supplier’s product.
- Provide full confidentiality of all information on verification applications and applicants.
- Produce a Verification Statement for each Unit of Conformance (UoC) that successfully achieves conformance verification per the FACE Conformance Policy, and provide such statement to the SW Supplier per the Verification Agreement.
- Produce a Verification Results Package, comprising the Verification Statement and Conformance Statement, and provide such package along with the Digital Signature to the CA within ten (10) business days of request.
- Establish and maintain a Verification Retention Repository in accordance with FACE Library Requirements and the FACE Conformance Policy.
  - Maintain a separate workspace for each SW Supplier, including handling of IP, etc., during verification process.
  - Maintain this Verification Retention Repository for a minimum of six (6) years from the date of last For-the-Record testing.
• Document and store in the Verification Retention Repository any clarification of evidence that is developed in discussions with a SW Supplier.
• Capture in the Verification Retention Repository associated Verification Statements, Conformance Statements, Digital Signatures, and sufficient records to support an audit.

2.2 Terms and Conditions

If approved, the incumbent VA agrees to perform in accordance with the VA Requirements/Tasks/Statement of Work found above and agrees to adhere to the FACE Conformance Policy, the FACE Conformance Authorities Plan, and associated documents as published by The Open Group on behalf of the FACE Consortium.

The incumbent VA is responsible to maintain current knowledge of the FACE Technical Standard and the approved verification practices, which may change from time to time. To foster consistency of work, the VA will regularly communicate with the FACE Consortium and other approved VA organizations through facilitated round-table discussions.

The FACE Consortium and its Certification Authority reserve the right to disapprove and not accept the deliverable of any VA if it is deemed that the VA Requirements/Tasks/Statement of Work was not met during the course of work. The VA may resubmit affected deliverables after correcting any deficiencies.

The incumbent VA is responsible for all costs incurred as the result of establishing and maintaining this verification capability. No funds will be forthcoming from the FACE Consortium in that regard.

3. Instructions to Offerors

Candidates are instructed to respond to each of the requests located in the following list:

1. Briefly describe how your organization accesses the FACE Reference Repository.
2. Describe how your VA will ensure independence from the software development and software integration activities from your overall organization. (Submission of an organization chart is helpful where appropriate.)
3. Describe how personnel within your VA have demonstrable knowledge of the FACE Technical Standard and its normative references.
4. Describe your VA plan to maintain knowledge of FACE Technical Standard.
5. Describe how personnel within your VA have demonstrable knowledge of the FACE verification techniques.
6. Describe how personnel within your VA have knowledge of the FACE Conformance Test Suite(s).
7. Describe your VA plan to maintain knowledge of FACE Conformance Test Suite(s).
8. Describe your VA organization’s process credentials or its methods for developing and adhering to well-defined processes (software related processes is preferred) and historical evidence for following those processes.
9. Describe your VA organization’s processes for configuration control.
10. Describe your VA plan to conduct or witness For-the-Record Verification testing.
11. Describe your VA knowledge, skills and abilities to objectively assess submitted Verification Evidence and to detect and communicate deficiencies or omissions.
12. Describe your VA plan to enforce policies and procedures that ensure protection of Software Suppliers’ Intellectual Property (IP).
13. Describe your VA plan to protect confidentiality of all information on applications and applicants.
14. Provide a description of the policies and procedures your VA organization intends to utilize for establishing and maintaining a verification retention repository in accordance with applicable FACE documents and requirements.

Responses shall contain non-proprietary information only. The Open Group and the FACE Consortium shall be entitled to use and disclose for any purposes connected with assessing whether or not the organization meets the VA qualification requirements. The submitted information will be destroyed at the end of the assessment.

This RFP is considered open ended. There are no deadlines associated with responding to this RFP as the FACE Consortium will review incoming responses as they are received on an ongoing basis. The FACE Consortium will issue approval announcements on a regular cycle and will endeavor to evaluate all responses received within that cycle.

Interested applicants shall reply by email with their responses to the following address:

ogface-admin@opengroup.org
### 4. Evaluation Methodology

The table below identifies the criteria necessary to reach approval to serve as a VA. The FACE consortium will review all responses received to determine whether they meet the acceptance parameters as shown below.

<table>
<thead>
<tr>
<th>VA Approval Criteria</th>
<th>Acceptance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to the FACE Reference Repository</td>
<td>Ability to access the bookstore/opengroup.org</td>
</tr>
<tr>
<td>Internal or external organizational independence from the development and integration efforts of FACE programs</td>
<td>Either a) enterprise does not perform software development/integration; or b) VA personnel report to a management structure that does not direct the development of software products or integration of those products</td>
</tr>
<tr>
<td>Prove and maintain knowledge of the FACE Technical Standard</td>
<td>Either a) team members have been involved in the development and/or review of the technical standard; or b) documented completion of organic or third-party training curriculum on the FACE Technical Standards, it's normative references, and its ecosystems by VA personnel c) documented experience with the FACE Technical Standard, it's normative references, and its ecosystems</td>
</tr>
<tr>
<td>Prove and maintain knowledge of the FACE conformance verification techniques</td>
<td>Both: a) a training plan for new employees; and b) a plan for learning new FACE standards as they are published</td>
</tr>
<tr>
<td>Prove and maintain knowledge of all approved FACE Conformance Test Suite(s)</td>
<td>Documented past experience showing development or technical review of software test procedures</td>
</tr>
<tr>
<td>Both: a) a training plan for new employees; and b) a plan for learning new FACE conformance test suites as they are published</td>
<td></td>
</tr>
<tr>
<td>VA Approval Criteria</td>
<td>Acceptance</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Demonstrate experience in operating within well-defined processes and/or hold</td>
<td>Either: a) credential for AS9100, ISO9000, CMMI, etc., or b) a organizational policy and historical evidence of adherence to well-defined processes that exists under configuration management and quality control</td>
</tr>
<tr>
<td>process-oriented credentials (such as CMMI, ISO 9000, or AS9100)</td>
<td></td>
</tr>
<tr>
<td>Demonstrate experience in management of a laboratory equipment configuration</td>
<td>The lab must have configuration control policies that cover records for equipment serial numbers, software versions, dates of changes, and a method for capturing the current configuration over time. Experience should reflect at least one of: a) managing such a lab, b) collecting configuration control records of such a lab, or c) auditing the configuration control records of such a lab.</td>
</tr>
<tr>
<td>control (such as ISO/IEC 17025, ANSI/EIA-649, IEEE/EIA-12207.0, or MIL-HDBK-61A)</td>
<td></td>
</tr>
<tr>
<td>The VA must provide the capabilities to conduct or witness For-the-Record Verification testing</td>
<td>The plan must include configuration of the test environment (including test suite version, test suite configuration, compiler, linker, and supplier software), methodology of capturing and storing results, and recording the test personnel involved</td>
</tr>
<tr>
<td>The VA must provide the capabilities to assess submitted Verification Evidence for</td>
<td>Past history of reviewing Design, Requirements, Test Procedures, and Test Reports. Methods for detecting incomplete or inaccurate traces. A plan for communicating deficiencies.</td>
</tr>
<tr>
<td>correctness and completeness</td>
<td></td>
</tr>
<tr>
<td>The VA must provide the capabilities to enforce policies and procedures that ensure</td>
<td>Existence of policies and procedures to generate and honor non-disclosure agreements (as required) and hold submitted materials in confidence. This may include items such as secure storage and networks, a security plan, controlled access to archives, and so forth.</td>
</tr>
<tr>
<td>protection of Software Suppliers’ Intellectual Property (IP)</td>
<td></td>
</tr>
<tr>
<td>The VA must provide full confidentiality of all information on applications and</td>
<td>Plan must treat all communications with suppliers as sensitive information as required by suppliers; including the names of the projects and project schedules.</td>
</tr>
<tr>
<td>applicants</td>
<td></td>
</tr>
<tr>
<td>VA Approval Criteria</td>
<td>Acceptance</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The VA must establish and maintain a Verification Retention Repository in accordance with FACE Library requirements</td>
<td>Plan must include storage of Verification Statements, Conformance Statements, Digital Signatures, and sufficient records to support an audit. Plan must include restricted access to VA personnel only (no supplier access, no access outside of VA group in enterprise)</td>
</tr>
</tbody>
</table>