Choosing a Third Party Test Laboratory

Deciding to work toward validation of the conformance of your product to standards such as Common Criteria, FIPS 140-2, cryptographic algorithm validation, Personal Identity Verification (PIV), SCAP and GSA FIPS 201, represents a substantial commitment to a sponsor. An important part of such a project is choosing the right test lab to test or evaluate your product for validation and certification.

Price is certainly an important factor, but it is also important to make some appropriate checks and consider other relevant criteria before you invest. The following are some questions to ask to ensure that you choose the best partner to help you achieve your goals.

☑ Is the laboratory properly accredited?

Always check that any claimed accreditations are valid and in good standing. Most programs offer a reference list where you can check. To delve a bit deeper, does the laboratory offer any additional certifications not demanded as part of the accredited program? For example, ISO/IEC 27001 is not usually a requirement but may give extra confidence to sponsors that basic information security controls are in place and properly managed.

☑ Is the test laboratory able to pursue a range of certifications through multiple programs and schemes?

Many sponsors need several different certifications. This can include cryptographic module testing, cryptographic algorithm testing, PIV, inclusion on the GSA FIPS 201 Approved Product List, Common Criteria in many nations, or a variety of other validations. Depending on your needs, a breadth of services may help in establishing a long-term trusted relationship.

☑ Does the test laboratory have a proven record of successful, on-time work?

This question speaks for itself. If the laboratory were consistently late or typically needs a lot of rework, then that pattern might continue.

☑ Is the test laboratory financially independent?

Obviously, the laboratory needs to be independent of the developer, but sometimes debt, financing commitments or dependence on external partners for financial support can be an issue.

☑ Is the laboratory independent?

Does the laboratory develop or resell any hardware or software from any vendor?

Is the laboratory, its management or investors involved at all in the design, manufacture, supply, installation, purchase, ownership, use or maintenance of the items to be tested?

Are there any contractual commitments from a larger organization, even if it has sub-divisions that may influence the results?

☑ Is the test laboratory an industry leader, helping to promote and shape the standards?

Leadership in the security testing industry may be demonstrated by commitment to helping shape the standards and the programs themselves whenever possible, contributing to technical communities, or participating in industry events. Such involvement helps demonstrate that the lab understands any issues with the standards and that they are up to date with forthcoming changes.

☑ Does the test laboratory go beyond simple testing; does it also add value by helping improve the customer's product and processes?

The quality of reports can include revealing a thoughtful analysis of the content of document evidence presented (not just a cursory look at the titles of documentation evidence). The reports provide real value to sponsors, going well beyond simply filling out a checklist of requirements to achieve certification. The independent examination can also result in an opportunity for better products and improved processes for your organization.

☑ Does the test laboratory let you reuse your test reports?

This can be an important contractual issue. If in the future you decide to change labs, the ability to reuse past reports can affect the amount of work that the new lab has to do in order to get up to speed with the prior work.

☑ Is the test laboratory able to offer expertise and evaluation experience in your technologies?

The experience of the laboratory staff or the focus of the laboratory itself can affect the choice. It's important that the staff understand the technology presented to them, that the laboratory has maturity and the right tools to support the assessment of that technology. Competence and experience in a technology contribute to the ability to catch vulnerabilities and issues that other testers might miss.

☑ Is the test laboratory able to offer service around the world?

For some companies this is a very important issue. Certification and validation programs can differ around the world; for others the ability to talk to technical developers in their native languages or to be able to travel relatively cheaply to foreign development sites can be useful.

☑ Who are the test laboratory's other customers?

It's worth investing some research on this question. Look at other public evaluations performed by the lab. Were they complex projects? Is the right technology type included? Are the other customers happy with the work being done?

☑ What are you getting for the price?

Apart from the quoted assessment, are charges made for "extras?" A common complaint is that "a laboratory nickel and dimed us." It's important that you know what is included. Such extras may include documentation, support, project management, quality assurance, travel, telephone calls, fees to the certification program, certificate maintenance, liaison, and rework.