UK Digital Evidence Validation Service (UK/DEVS) : DRAFT Proposal

Introduction

At the Forensic Science Regulator's specialist group meeting on 25th February 2009, the digital evidence group agreed the adoption of 6 principles relating to the provision of digital evidence services. Of these, principle 4 may be the most significant new requirement for DE practitioners since the introduction of the ACPO principles.

The regulator's 4th principle places a requirement on providers to have the ability to demonstrate that "all tools, techniques and methods are fit for purpose".

Conseidration of this principle leads to the conclusion that it is no longer acceptable for providers and practitioners to rely on anecdotal evidence, personal experience or the guarantees offered by vendors & manufacturers. Rather, they must have in place an appropriate system to perform rigorous validation and verification of their systems & methods, including appropriate configuration management, systems development and error recording systems.

This proposal does not address the error recording issue as this can only realistically be carried out during live use of systems and methods, but it does address, at least in part, the other issues identified.

Options

Superficially, at least, it seems that there are three options available to provide verification and validation mechanisms to ensure compliance with the Regulator's standards and principles :

1. In-house
2. Manufacturer & vendor provided
3. Independent third party service

Option 1 (In-house) reflects how many "conventional" laboratories provide validation & verification within their existing QA/QM systems and is a viable option. However, given the nature of digital evidence work it is believed that this is likely to be a time-consuming and costly option for most providers/practitioners. In order to complete this process successfully, even a small provider is likely to have to undergo several cycles of testing each year following any upgrade or configuration change. Additionally, because a range of hardware and software is likely to be in use, a mix of skills and experience is likely to be needed to perform appropriate testing. As a result, the cost of conducting the process in-house is likely to be prohibitive for all but the larger organisations.

Option 2 (Manufacturer/Vendor) is discounted from this discussion as it would probably prove impossible for any manufacturer to provide cost-effective and complete testing services for all possible configurations, particularly where competitors' products form part of the standard configuration for a customer. Issues of commercial confidentiality and profit-margins would inevitably compromise their ability to provide a 100% guarantee that all configurations could be validated and verified. It is also difficult to envisage how open-source and in-house tools can be

dealt with through this system without resorting to some form of Option 1 running in parallel. Costs associated with Option 2 would, inevitably, be passed on to customers and there may be some unwillingness to place full trust in certification provided by the very body which provides the tools as certification may be seen as a commercial advantage and hence less trustworthy.

Option 3 (Independent third party) seems to offer more scope for both rigour and cost-effectiveness. By creating a completely independent non-profit body for the industry as a whole, proper consideration can be given to all software and hardware configurations without issues of commercial confidentiality and independence/reliability arising. Because many of the validation and verification tasks will be common across providers/practitioners, there is real potential for costs to be shared and thus reduced for all parties.

Proposal

The proposal, therefore, is to establish a UK-wide non-profit organisation to manage the service on behalf of the industry. This organisation would employ staff to devise and carry out validation and verification processes on tools and methods and make the results available to the industry as a whole. Therefore, the organisation would be given responsibility for :

- Establishing minimum and desirable definitions and tests for fitness for purpose*
- Identifying tools (software. hardware, algorithms etc.) in common use across the industry*
- Developing and performing independent testing of identified tools on behalf of end-user organisations
- Producing correct documentary evidence of test results, including configuration data
- Act as a repository for knowledge about error conditions and error rates
- Provide independent advice and assistance to end-user organisations
- Assess and disseminate new techniques and methods in the context of established standards
- Review standards
- Provide tools to allow end-user organisations to conduct internal re-validation/re-verification
- Provide representative data & materials for competency testing
- Subject to agreement, performing testing on behalf of vendors

It is further proposed that this organisation should be based across two UK Universities to provide access to an appropriate infra-structure for the rigorous scientific and engineering processes required. By distributing effort across two teams which can operate independently, the teams can monitor each other to ensure internal compliance with standards and procedures appropriate to the service's function. The use of Universities in this way should give access to truly independent and highly competent staff who are at the forefront of development of the tools, techniques and methods which will be deployed in the future. Furthermore, the University teams should be free of many of the operational and commercial pressures found in other organisations, thus guaranteeing their ability to deliver the required service to the highest level possible.

As part of its activity, UK/DEVS would develop a set of tools which can be used to carry out on-site validation and verification as part of the configuration management process (e.g. resulting from the installation of service packs or minor version number upgrades) as well as gathering information about configurations in use across the industry, to be held in strict confidence and used to inform

* These are major tasks for the early stages of the project.

* These are major tasks for the early stages of the project.

further work on the development of validation & verification processes. Because UK/DEVS would receive data from all member organisations, it would be in a unique position to create a comprehensive repository of knowledge and data about common issues encountered during forensic examination of digital devices which could be used to assist in the improvement of tools, methods and techniques. Information thus garnered could be made available to allow organisations to make more informed & justifiable choices during purchasing/upgrading processes.

UK/DEVS could also assist with the conduct of blind competency testing as used in other forensic sciences (e.g. biology) to check laboratory procedures and results.

Funding

Funding for the organisation would be through two main revenue streams :

1. Subscriptions from member bodies. These bodies would have full access to all data and tools produced by UK/DEVS in return for an annual fee. They would also be provided with a dedicated "helpline" in order that queries relating to new products, apparent inconsistencies or new configurations can be dealt with promptly.

   Initial estimates suggest that an figure of around £5k per member body per annum should provide adequate funding for the service to operate (This should be contrasted with the costs likely to be incurred for in-house validation & verification). This results in an estimated operating budget of £250k to £300k per annum, assuming full participation from police and larger commercial providers.

2. Sale of validation data & tools to non-member organisations. Smaller providers/practitioners may not have the same levels of complexity in their configurations and may prefer to purchase only those elements of the UK/DEVS "product" which satisfy their immediate requirements.

Any surplus funds would be used to support appropriate research into new methods, tools & techniques appropriate to the industry.

Management, operation and oversight.

Day to day management of UK/DEVS would be delegated to a pair of Directors appointed by the managing Universities. The Directors would recruit and manage teams of appropriately qualified Research Assistants to develop and carry out the tasks identified above. Staff from the member bodies may be seconded to the teams subject to agreement by their employers and the management committee (see below). Some of UK/DEVS work may be sub-contracted to appropriate specialist providers where necessary.

The subscribers would appoint/elect a management committee with responsibility for agreeing the aims, objectives and targets of UK/DEVS to ensure that it continues to meet the needs of the industry and the Regulator. The UK/DEVS directors would be ex-officio members of this committee. The management committee would also consider & approve applications for funding for research projects in the event that surplus funds were available. This committee should meet 4 times per year.

In the event of UK/DEVS being wound up, funds remaining would be returned to subscribers in proportion to their subscription for the financial year(s) in question.