NPL
National Physical Laboratory

Report

NPL REPORT
DEM-ES 012

Software Support for Metrology – Good Practice Guide No. 19

Internet-enabled Metrology Systems

R M Barker and G Parkin

Not restricted

June 2006

dti
FUNDED BY THE DTI

National Physical Laboratory | Hampton Road | Teddington | Middlesex | United Kingdom | TW11 0LW

Switchboard 020 8977 3222 | **NPL Helpline** 020 8943 6880 | **Fax** 020 8943 6458 | **www.npl.co.uk**

Software Support for Metrology
Good Practice Guide No 19

Internet-enabled Metrology Systems

R M Barker and G Parkin
Mathematics and Scientific Computing Group

June 2006

ABSTRACT

This guide describes best practice in the use of the internet for metrology services, including calibration. It is based on the experience of NPL in developing and running a number of calibration services over the internet and on reports of other organisations that have had projects involving metrology and the internet. The guide also builds on guidance from projects in the previous SS*f*M programme dealing with security and accreditation in the use of internet by metrology services.

ISSN 1744–0475

National Physical Laboratory
Hampton Road, Teddington, Middlesex, United Kingdom. TW11 0LW

We gratefully acknowledge the financial support of the UK Department
of Trade and Industry (National Measurement System Directorate)

Approved on behalf of the Managing Director, NPL
by Jonathan Williams, Knowledge Leader of the Electrical and Software team

Contents

1. Introduction

1.1 Scope

This guide describes best practice in the development and use of internet-enabled metrology systems: systems that use the internet to deliver services relating to metrology, the science of measurement. One important metrology service that can be delivered over the internet is the calibration of instruments, but there are other services provided by internet-enabled metrology systems. The guide is based on the experience of NPL in developing and running a number of calibration services over the internet and on reports of other organisations that have had projects involving metrology and the internet [15]. The guide also builds on experience from projects in the previous SS*f*M programme dealing with security [2] and accreditation [3] in the use of internet by metrology services.

NPL has developed a number of internet-enabled metrology services for the remote calibration of instruments and artefacts: iPIMMS [5], iVR [1], iColour and iOTDR [7]. As part of the current SS*f*M programme, we have developed an approach to accessing instruments over the internet using software rather than hardware interfaces [16, 17]. There are also internet-enabled metrology services to access materials databases and other resources [9, 10]. These services demonstrate different models (or "types") of internet-enabled metrology and use different techniques for their implementation.

This guide describes the possible operational models for internet-enabled metrology systems, and the issues for implementation of a service: hardware, software, security and accreditation. The guide is primarily concerned with internet-enabled metrology *systems* and not the commercial *services* provided by the system; there is not enough experience of issues relating to business models and pricing to give any generic advice. Strictly, the accreditation issues relate to services rather than systems.

1.2 Benefits of Internet-enabled metrology

The benefits of internet-enabled metrology can be specific to the type of measurement service to which it is applied, but there are many benefits that are common to almost all such services. These include:

Traceability and accessibility

- Internet-enabled metrology has the potential to provide direct traceability to national standards – cutting down the calibration chain to one link.
- Metrology services can be used at a time of the user's choosing, day or night.
- Metrology activities (e.g. calibration) are performed in the user's environment, ensuring that measurement results accurately reflect the conditions relevant to that user's situation.
- User equipment stays in the user laboratory, so there is no transport time, and hence there is a much reduced down time for user equipment.
- Appropriately high levels of accuracy can be transferred to the user's laboratory and this can be the very highest levels of accuracy
- A much better cost to accuracy ratio than for traditional metrology services.

Knowledge transfer and measurement good practice

- Measurement skills are transferred to the user's laboratory – indeed the user's calibration staff may need some special training, which is likely to be of real benefit to their normal work.
- On-line measurement good practice guides can aid the transfer of good measurement practice into the workplace, increasing the confidence in the measurements being made.
- Ease of use. The remote operator will be guided step by step through the calibration process by the service's on-line procedures.

Data-warehousing and other benefits

- Measurement results can be stored by the service provider's database for possible recall by users during subsequent activities such as calibrations and audits. Data warehousing can also provide long-term access to calibration history and provide robust, paperless audit trails.
- This process can lead to data being shared in a common file format throughout an organisation.
- On-line visual monitoring of the measurement processes can be used for troubleshooting purposes. Manufacturers of instruments connected to the system could be given limited access to the measurement history; allowing them to interpret data to see what parts and servicing are likely to be required during service visits and to improve preventative maintenance.

1.3 Acknowledgements

This guide was produced under the Software Support for Metrology programme and we gratefully acknowledge the financial support of the UK Department of Trade and Industry (National Measurement System Policy Unit).

The Software Support for Metrology programme is managed by the National Physical Laboratory. For more information on the programme visit the SS*f*M website at www.npl.co.uk/ssfm, or contact the programme manager on +44 20 8943 7100 (email: ssfm@npl.co.uk) or by post to National Physical Laboratory, Teddington, Middlesex, UK TW11 0LW.

The material in this guide was developed in a number of earlier projects in the SSfM programme and other programmes. The authors would like to acknowledge the contributions of Mike Nash (Gamma Secure Systems), Ian White (Baltimore Technologies), Bernard Chorley, Stuart Prince, Nick McCormick, and Keith Lawrence.

2. Glossary/Acronyms

It is necessary to define some terms that will be used throughout the guide.

3DES	*Triple* DES – strong form of DES: *Data Encryption Standard*
ActiveX	Microsoft technologies for web objects
API	*Application Programming Interface* – a software interface that is provided by a system in order to support requests to be made of it, by other software
CESG	*Communications-Electronics Security Group*
CGI	*Common Gateway Interface*
CSP	internet-enabled *Calibration Service Provider*
DC	*Direct Current*
DMZ	*Demilitarised Zone*
FTP	*File Transfer Protocol*
GPIB	*General Purpose Interface Bus* – defined in IEEE488 [6]
HMAC	Keyed-*Hashing for Message Authentication*
HMG	*Her Majesty's Government* – the government of the United Kingdom
HTTP	*Hypertext Transfer Protocol* or *Hypertext Transmission Protocol*
HTTPS	*Hypertext Transmission Protocol, Secure* – HTTP running over SSL
iCal	*internet Calibration* – software supporting iVR and iOTDR
iColour	*internet Colour* – colour measurement system
ID	digital *identity*
iOTDR	*internet Optical Time Domain Reflectometer* – calibration system
iPIMMS	*internet Primary Impedance Measurement Software* – calibration service
ISP	*Internet Service Provider*
iVR	*internet Voltage and Resistance* – calibration system
MAC	*Message Authentication Code*
MD5	*Message Digest 5*
MySQL	free database software – implementing SQL: *Structured Query Language*
NPL	*National Physical Laboratory*
PC	*Personal Computer*
PDF	Adobe *Portable Document Format*
Perl	a general-purpose programming language
PHP	a general-purpose scripting language – originally *"Personal Home Page"*
Python	a dynamic object-oriented programming language
RS232	*Recommended Standard 232* – a standard for serial binary data interconnection
SHA-1	*Secure Hash Algorithm 1*
SSL	*Secure Sockets Layer*

SS*f*M	*Software Support for Metrology*
TCP	*Transfer* (or *Transmission* or *Transport*) *Control Protocol*
UKAS	*United Kingdom Accreditation Service*
UTC	*Coordinated Universal Time*
VBScript	*Visual Basic Script Edition* – a scripting language based on Visual Basic
XML	*eXtensible Mark-up Language*

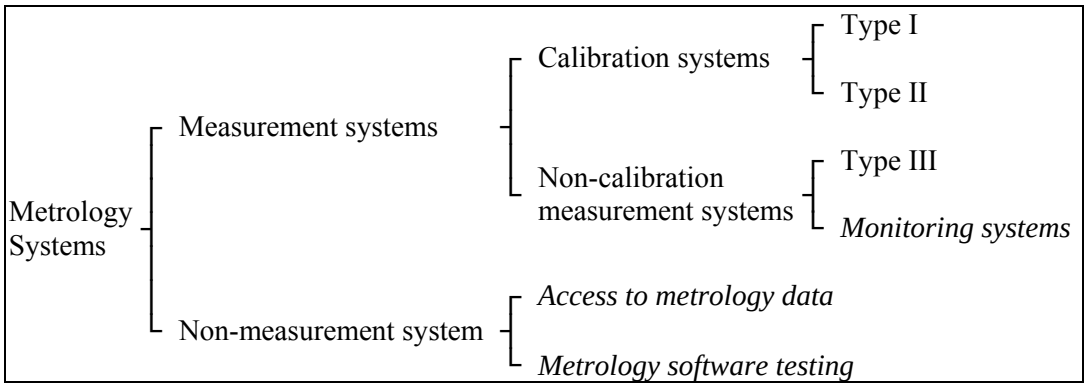
3. Internet-enabled metrology systems

3.1 Types of internet-enabled metrology system

In the main, this guide is concerned with measurement systems where the remote system is engaged in measurement and passes some measurement data to the host system. There are other (non-measurement) internet-enabled metrology systems that do not deal in actual (live) measurement data.

Measurement systems include internet-enabled calibration systems where the host calibration laboratory performs a remote calibration of equipment at the remote site, by transferring an item (an artefact or instrument) that embodies the measurement standard. Other (non-calibration) measurement systems, receive measurement data from the remote site and perform calculation on the data, returning the results to the remote site, or simply monitor the data for abnormalities or inconsistencies that may require other remote intervention. The two types of calibration systems are termed Type I and Type II (depending on the nature of the transfer standard) and the accreditation work identified a further type of non-calibration measurement service (Type III), which can nevertheless be involved in calibration services offered by the remote site.

A possible taxonomy of internet-enabled metrology systems is in figure 3.1.



3.1 Taxonomy of internet-enabled metrology systems

3.1.1 Possible models for internet-enabled calibration systems (Type I and Type II)

Not all calibration processes can be adapted for use remotely via the internet. Some basic requirements are necessary before a system can be considered suitable. Any instrument that is to be considered for calibration via the internet needs the ability to be controlled by a computer, or to be controlled directly over the internet.

The measurement process has to rely on either stable artefacts (reference standards) or a rugged instrument that can be transferred between the primary laboratory and the remote (user's) location for internet-enabled calibration to be feasible.

Two different types of internet-enabled calibration methods have been identified:

- Type I: Transfer of a stable artefact or set of artefacts;Type II: Transfer of rugged high-accuracy calibration device –
  like an extension of the NMI facilities to the remote site.

A typical Type I case run by a National Measurement Institute (NMI) involves the following:

- The NMI effectively transfers the primary standard, knowledge and expertise to a remote user laboratory – like having a piece of the NMI on the remote site
- The user's organisation has its own primary standard (artefact or set of artefacts) characterised by the NMI – in some cases they have this on loan from the NMI, in other cases they have to purchase it for themselves and then send it to the NMI for characterisation
- On-line NMI procedures control the calibration process, usually through web-pages accessed from the remote site
- Calibration data is stored in the NMI's database, and may be downloaded to produce certificate
- Uncertainties of measurements are calculated by the NMI's software (possibly in real-time)
- System performance (repeatability, stability, etc) is evaluated in-situ by NMI software
- There is the ability to check measurements and repeat/disregard bad measurements
- There is the ability to suspend measurement cycle and resume at another time
- A web-cam may be used to allow critical connections and other aspects of the process to be viewed by staff at the NMI and a video record may be created for inclusion in the audit trail

A typical Type II case run by an NMI is very similar but differs in the following respects:

- A rugged high-accuracy calibration device (transfer standard) is transported to the remote laboratory – rather than the user's artefact standard(s)
- The calibration device will probably be owned by the NMI, because the NMI will invest a lot of effort in detailed characterisation of the device before it is transported to the remote site
- The calibration device may well be transported together with a laptop PC from the NMI, containing the relevant software for controlling the calibration device as well as communicating with the NMI – this avoids having to install the software on a user's PC with all the security risks that that would entail
- When the remotely controlled calibrations have been completed, the measurement data is likely to be sent over the internet to the NMI for analysis, and then provisional results returned in real-time to be issued to the user
- The calibration device should then be sent back to the NMI in order to check that it has not sustained any damage and to check whether its measurements have drifted – only then can the uncertainty evaluations be completed and the final calibration certificate issued

3.1.2 Models for internet-enabled measurement systems

There are many possible applications of internet-enabled metrology that do not control a calibration process but do involve processing of measurement data. Usually the measurement data will be processed and stored at the host.

Sometimes the processing of the measurement data will be done to apply corrections to data, using software or further information only available to the host, and the resulting measurement data is returned to the remote site. The iPIMMS system is used to support local

(non-internet) calibrations performed by the iPIMMS client – the processing uses earlier calibration data stored on the iPIMMS server.

When a system is providing measurement processing services on measurement data obtained from a calibration, but where the service host is not performing the calibration, this is termed a Type III service (e.g., for the purposes of accreditation).

3.1.3 Non-measurement internet-enabled metrology systems

There are metrology services that are provided over the internet that do not involve (live) measurement data being transmitted to the server and processed for a (real time) measurement process at the remote site. Most obvious are information services, such as web site provided my most NMIs. Many internet-enabled metrology services are not very different from many services offered on the internet; but a notable distinction is that metrology services often involve large data sets both for input and output. This use of large data sets requires different mechanisms for collecting and displaying the results than the usual web forms and web pages. The NPL Materials Centre has a number of services based on materials metrology data (extracted from databases) and the SS*f*M programme has developed a service for testing metrology software.

3.2 How to build an internet-enabled measurement system

This section is based primarily on the lessons learnt in building the iOTDR system. It describes the steps necessary to develop an internet-enabled system that is capable of making traceable measurements at a remote site. It is our experience that missing out steps in this process will lead to many problems at later stages in the development process.

1. Design and develop a prototype measurement system

   This system should be built and tested to ensure the appropriate science has been captured. The operation of the system can involve as much manual intervention and measurement as is necessary.

2. Develop an automated measurement system

   In the first measurement system, replace as much of the measurement by instruments that can be operated and read automatically (i.e., by another machine). Reduce, as much as possible, the manual configuration and intervention that is needed in the measurement system, so the system can perform a series of measurements uninterrupted.

   Consolidate the operation of the system so that it is controlled from one PC that is connected to the instruments. The PC should accept configuration information from the operator, issue instructions to the operator, and then wait for confirmation from the operator before proceeding with further measurements. The PC should check the consistency of the measurement system (and the configuration supplied by the operator) and report anomalies. The PC should perform the required processing on the measurement, present a summary (e.g., a graph) of the measurements and processed data to the operator for validation, and make all the data available to the operator (e.g., by writing a file, or by adding to a database).

3. Design a remote-operated automated measurement system

   Decide what instruments and measurements standards will be assumed to be provided by the remote site and what will have to be transported to the remote site. For an internet-enabled calibration system, it will be necessary to transport at least one instrument or measurement artefact to the remote site: this item will act as the embodiment of the measurement standard against which the calibration will be made.

The remote-operated automated measurement system will consist of identified pieces of equipment provided at the remote site together with equipment provided by the measurement system provider and transported from the server site. Both sets of equipment will be connected at the remote site as for the (locally-operated) automated measurement system and will be controlled by a PC at the remote site.

4. Implement an internet-enabled measurement system

   The functionality of the PC that operates the automated measurement system must be divided between the server and the client PC at the remote site. This split of functionality will depend on the measurement service.

   At a minimum, the server must be capable of recording what took place during a measurement session and storing a copy of the data that was provided to the remote operator. The server should also be able to provide diagnostics to a "local" expert, so the expert can trouble-shoot problems reported by the operator at the remote site.

   Alternatively, most of the functionality can reside within the server: the client software can be largely generic, relaying instructions from the server to the remote operator as web pages/forms, and sending instructions and taking readings from the instruments using standard bus protocols (e.g. GPIB or RS232). Recent work has shown that all interfaces with an API can be controlled remotely, see [16].

3.3 Architecture for internet-enabled measurement systems

This section gives a generic description of an internet-enabled measurement systems – based on the iCal software (used in iVR and iOTDR) – expressed as specification/requirements on the different components.

The aim of the system as a whole is to be able to perform verifiable measurements at the client site which can be recorded and processed at the server site.

This architecture should be sufficient for all internet-enabled measurement systems unless the system is based on transmitting physical quantities between server and client (over the internet). There are systems being developed (in Japan) that attempt to send optical frequency signals, as frequency measurements standards, over optical fibre networks [15]. For internet-enabled calibration (or any measurement system that requires comparison between measurements at the service provider and the remote site) using the architecture described here, there must be a transfer of an instrument or artefact from the service provider to the client.

3.3.1 Server

The server system consists of a server computer, a secure database, connections to an external network for accessing the remote client site, and connections to an internal network.

The server software must be able to:-

- Accept connections from the remote site – usually over the internet, but possibly over a local network (perhaps for testing) or over a private network (for security).
- Send to the client, instructions for the user (web pages) and instructions for the remote equipment (encoded bus messages or code fragments to run on the client).
- Receive from the client, messages from the user (responses from web forms) and information from the remote equipment (encoded from bus responses).
- Accept connections from the local site – usually over a local network, but possibly over the internet or a private network.

- Send to a local administrator/expert: diagnostic information about the state of the system and information from the database.
- Receive from a local administrator/expert: management instructions for the remote measurement system, for the database, or for the server itself.
- Establish connection with a (local) database.
- Create, update, and read entries in the database.

3.3.2 Client

The client system consists of a client PC, connections to a network to access the service provider, measurement instruments, and measurement artefacts. There can also be environmental monitors and audio visual equipment that will be used to record the measurement process and be used as evidence of the proper operation of the system, but may not be involved in the processing of the measurement data.

The client software must be able to:-

- Establish connections with the server – over the appropriate network, see above.
- Receive and display instructions for the user sent from the server.
- Accept input from the user (e.g., configuration information and acknowledgement of completion of instructions) and send this information to the server.
- Receive coded messages for the equipment from the server, decode/interpret the messages, and issue the appropriate instructions as bus protocol or API calls.
- Receive information (measurements and status information) from the equipment via bus protocol or API, encode this information, and send it to the server.

3.3.3 Other components and sub-systems

This is a list of requirements on the components of an internet-enabled metrology system, including human operators and hardware/software sub-systems.

The database must be able to

- Accept connections from server
- Allow creation, update and read instructions from the server

The user (remote operator) must be able to

- Set up the equipment.
- Log in to the client PC and initiate the measurement system, logging in to the server.
- Enter configuration information to the client, describing the measurement to be made.
- Follow instructions displayed on the client: e.g. reconfiguring the equipment (or taking readings from non-automatic instruments).
- Contact the service provider (by other means) to deal with unforeseen circumstances.
- Review summary measurement data displayed on the client, and approve for further processing.
- Request further services based on the processed measurement data, e.g. request calibration certificates.
- Disconnect the measurement system and pack away items for transport back to the service provider, or onwards to other users.

The local administrator or measurement experts must be able to

- Accept out-of band (e.g. by email or telephone) enquiries from (remote) users.
- Log in (over a network) to the server
- Gather information from the server to diagnose the problems
- Issue instructions to the server to resolve problems or otherwise manage the system.

4. Implementation

This section describes the typical hardware and software components of an internet-enabled metrology system and describes two implementations. It is based on the experience of building real systems at NPL.

4.1 Typical hardware components

The hardware requirements necessary to produce an internet-enabled metrology system can be inferred from the section "How to build an internet-enabled measurement system" (section 3.2). It consists of the hardware to operate the metrological aspects of the system and the hardware to connect that hardware to the internet.

In designing and developing a system the metrological hardware should be considered first. Indeed, it is important to develop a version of the metrology system that operates locally before starting to think about a system that operates remotely. The local system should be automated so as to operate as closely as possible to the operation of required internet-enabled metrology service.

The hardware to connect the measurement hardware to the internet will normally consist of a PC connected (via an organisation's internal network). But in the section "Firewalls" (section 5.3.4), it is recommended that the internet-enabled calibration system be capable of operating from a stand-alone PC not dependent on the remote organisation's network, instead the PC is connected to the internet by a modem and an external telephone line to an ISP.

Required hardware:

- Host server machine
- Remote machine –
    - laptop supplied with remote calibration kit or
    - existing client PC
- Remote connection to internet
    - client organisation access, or
    - dial-up from remote laptop (to avoid firewall issues, etc.)
- Instruments that supports some well-known bus, protocol or API; and suitable hardware support in remote/client PC.
- Other peripheral instruments to record measurement process and environment e.g. camera, thermometer, and suitable hardware to take measurement from the peripherals (even if they don't need to be controlled).

4.2 Example implementation – iPIMMS

The iPIMMS system was the first internet-enabled measurement and calibration system developed by NPL. It was developed and operates on Microsoft Windows using proprietary solutions but the implementation solutions could be used in other systems and other operating environments. The systems controls a network analyser at the remote site, which can be calibrated using a transferred artefact and which can then take further measurements, under control of iPIMMS.

The server software is an executable written in Visual Basic, using the Common Gateway Interface (CGI) to interpret requests from the client. It does not use a database, instead data

about different instruments and different operators' sessions are stored in different folders, encoded using the session identifier.

The client is initiated from a web browser (specifically Microsoft Internet Explorer) that logs on to the server from a web page. The client runs VBScript (Visual Basic scripting language) embedded in the web pages and downloads ActiveX components from the server. The operator is prompted to download the ActiveX components when the operator logs in, the components are digitally signed and this is checked (by Internet Explorer) to ensure their authenticity. As a check that the components have been successfully installed, the system attempts to use routines in the components to draw a graph within a web page; if the graph is visible then operator confirms to the system that the installation had completed.

Once the operator is logged on and has installed the new ActiveX components, they use web pages from the server to enter the configuration of the instrument and measurements to be done. VBScript checks and expands the options presented to the operator, depending on earlier selection (and information about what is available at the particular remote site). The operator can also follow links to other web pages to get help on the configuration and measurement. When the initialisation using HTML and VBScript is complete, control is passed to the ActiveX component.

The ActiveX components contain the commands to control the network analyser via GPIB, there are different commands for the different makes of network analysers. During the calibration and measurement, traces/graphs are displayed on the network analyser – this allows the operator to judge if the calibration/measurement is successful. When the process is complete, a VBScript submits the measurement data read from GPIB by the ActiveX.

The operator can then use a separate executable on the server to verify the measurement data, using HTML forms to submit the request and using ActiveX component commands to graph the data.

Observations

- Implementation design depends on measurement system but also on measurement process – need to understand potential internet-enabled measurement processes.
- The server could be implemented in any language, independent of the client. The VBScript in the web pages could be replaced by other scripting languages, and could therefore be (more) client-platform independent. The use of Internet Explorer could be replaced by any browser that supports downloading authenticated software components; and the ActiveX components could be replaced by components could be run in a platform-independent environment.
- So, although the implementation is tightly tied to Microsoft Windows components, the implementation design could (in principle) be achieved in a platform-independent environment; of course in any multi-language, multi-component there is much detail to be resolved, and tying-in to one fixed platform, and compatible languages and components does have advantages.

4.3 Example implementation – iCal for iOTDR

The iCal software system was designed as a generic solution for internet-enabled measurement and calibration systems and first used to implement the iVR system and was then used as the basis of the iOTDR system. In this section we describe iOTDR which is more complex that iVR and subsumes most of the features present in the implementation of the earlier system.

Up to four instruments are required to calibrate the OTDR, with a maximum of four, including the OTDR, being connected to the computer at any one time. Two types of

interface are required: RS 232 (the thermometer and the OTDR) and GPIB (all other instruments). The commands used to control the instruments were complex: it being necessary to check their status before reading data. In particular, it was desirable to write the software in such a way that different OTDRs could be added at a later date, allowing the operator to select the model being used for a particular calibration.

It was required that the client PC be connected to the internet through a mobile phone. In principle should have been easy, but in practice the transfer of data was error-prone and a simple protocol had to be implemented to overcome this by calling for data re-transmission where necessary.

4.3.1 Overall architecture

The software is composed of a client, written in Microsoft Visual Basic [11] that runs on the computer located at the customer's site, and a server program, written in PHP [8], that runs on a server computer at the calibration laboratory. The server controls the calibration process, while the client, using instructions received from the server (in the form of VBScript), controls the equipment and interacts with the operator. Data collected from the instruments is transmitted back to the server for processing, and the results are stored in a database.

Although the server software dictates how the calibration is conducted, the client software is in the driving seat throughout the process, and initiates all the communications. The client sends a message to the server and waits for a reply. On receipt of each message the server acts on the content and then issues a reply.

4.3.2 Implementation details

In the client, a Visual Basic control called INET is used to handle internet communications with the server. A function **execute** is called to send messages. It takes, as parameters, the address of the server, and, in XML format, the message to be sent. (A function for constructing XML was provided as part of the iCal software.)

The iOTDR server is based on the iCal server. It uses a MySQL [14] database for storage, and the XML-RPC [20] protocol to communicate over the internet with the client, and this enables structurally complex and binary data to be exchanged.

The iCal client software was designed to be generically applicable to a variety of calibrations, but it lacked the flexibility required for this more complex calibration, and significant improvements had to be made to it. In particular, it has been extended to enable it to talk to up to four RS232 ports and as many GPIB addresses as the interface card can handle. A Visual Basic control for running VBScript [12] has been added. VBScript is a subset of Visual Basic, and it can be sent down from the server as an ASCII string to be run on the client. The features provided by VBScript that are important for this project are that it can include calls to Visual Basic functions on the client that read data from, or write instructions, to the hardware; and that these function calls can be embedded in loops. Because of using VBScript, fewer interactions with the server are required, and it is possible to make the calibration more efficient in terms of run time and internet traffic.

4.3.3 Software development difficulties

Debugging proved difficult and time-consuming, both for PHP and for VBScript. PHP has no development environment. It is simply written as a text file and left in place for the server to execute the code.

When there are bugs in the PHP, the usual effect is for no response to be returned when the client sends a message. If this happens as soon as the client is started, it generally means there is a syntax error. The procedure here is to look at the PHP using a web browser, and the

syntax error will be reported, with information that is of varying use in locating the fault. It pays to make only small changes to the PHP before checking it with the browser.

If the browser shows no fault, but, at some point during the calibration, there is no response from the server, then some other problem has occurred. Typical examples would be attempting to write to a MySQL table without first opening the database, or attempting to write to a file that is not open.

Sometimes strange effects were observed. Inadvertently putting a comment in the PHP text file, but outside the PHP begin and end brackets, had the effect of increasing the server response time roughly tenfold. The cause of this problem was uncovered when the XML returned to the client was examined.

By default PHP scripts have a 30 second timeout. This needed to be switched off because iOTDR scripts can run for considerably longer.

Errors in VBScript are not trappable. Syntax errors are detected as soon as an attempt is made to run the script, usually with an unhelpful message, such as "statement expected", or "faulty script", being reported. Run time errors have the effect of terminating the script immediately. It is not possible to detect if a script has been interrupted in this way or if it has terminated normally. It is recommended to build in a mechanism for determining that a script has run to its proper conclusion.

4.3.4 Operation

An operator of a service for iOTDR calibration starts by establishing a link from a portable PC to the internet, using a mobile phone if required. Next the iOTDR client software must be started. The client automatically dials up the server over the internet, and establishes a dialogue. The operator is required to log in, and a session identifier is allocated which will allow the operator to return to the session later.

The server presents the operator with a list of available services, and once a service has been selected, the server guides the operator through it by sending instructions to the client software, which passes them on to the operator, displaying them on the PC screen. Typical instructions would explain how to connect the instruments and cables. Once the equipment is ready and the server has been informed of this by the operator, the server sends down commands (in the form of VBScript) to the client to control the measurements.

Before any part of the calibration can be performed, the operator must identify the equipment in use. The specific items known by the server are present in drop-down lists for the operator to make a choice. The operator also specifies the RS232 and GPIB port numbers for the equipment. These numbers are stored on the database and are used by default for future calibrations.

Much of the calibration is temperature-critical, the allowed temperature range being stored by the server on the database. Before a calibration commences, a command is sent to the client to read the temperature from the thermometer. The reading is returned to the server, where it is compared with the stored maximum and minimum values. In the case where the reading lies outside the valid range, a message is sent to the client and the operator is informed that the calibration cannot proceed.

All data collected is returned to the server and stored in the database. All analysis of the data is done on the server.

Faulty connections to equipment are detected. Error codes are sent from the client to the server, and meaningful error messages are displayed to the operator on the screen. Care has been taken to deal with transmission faults, which are prone to arise when using the mobile phone link. Often a recovery can be effected without having to abort the calibration.

4.4 Other implementations

The Norwegian Metrology Service (Justervesenet) has developed an implementation of internet-enabled measurement which is similar to iCal but uses .NET technology and .NET "remoting" for internet communication. A major difference between this and iCal is that the Justervesenet solution allows a remote operator to control a measurement. For a much more detailed comparison see .

Recently NPL and Justervesenet collaborated to produce an even more generic solution which gives:

- A completely generic client in that any instrument can be controlled remotely provided it has an API so this includes GPIB, RS232 and many more interfaces.
- Allows the scripting language to be replaced with a programming language in this case C# (a .NET language).
- Allows a remote operator to control a measurement.
- Can be implemented in various ways but in this case uses NET (C#) and XMLBlaster [21].

A more detailed description is contained in .

4.5 Software for internet-enabled measurement systems

4.5.1 Software design

The key issue in designing and implementing the software for an internet-enabled measurement system is deciding which component will contain the instructions for the measurement instruments. There are various possible solutions:

- The instructions are installed in the client system.
- The instructions are downloaded from the server when the system starts.
- Each group of instructions is encoded and sent by the server as needed, and must be decoded by client before instructions are issued to the instruments.

The iPIMMS system effectively uses a combination of the first two mechanisms: instructions are hard coded in the client but the system can download new versions of the client software (which could include new instruction sets) as needed. The iCal software aimed to produce a generic solution, with the client software being independent of the particular internet-enabled metrology service, so it adopts the third mechanism.

The first mechanism is the easiest to code, the second is more flexible, and the third is the most flexible but hardest to code. In the second mechanism, the software must handle loading new code in place of old code in the client. In the third mechanism, the software must be able to encode and decode groups of instructions that are sent over the internet: there is some subtlety in designing and implementing a sufficiently general encoding for the instructions.

The generic software architecture in iCal has been used in two implementations: it tries to reduce the amount of application-specific information on the client, so the client software can be used for different systems with minimal change.

The software should be produced using a development method that allows for prototyping. It is important that assumptions about how the different software and hardware components work together are tested as soon as possible and as frequently as possible during the development process.

Languages for server and client can be different, and the system should use open protocols (and data formats) over the internet – so different ends of the systems can be implemented

(and re-implemented) independently. The current systems use different message protocols / formats: SOAP [18] (iPIMMS) and XMLRPC [20] (iCal).

4.5.2 Issues for server software

The server should follow industry good practice in internet server applications: for robustness, scalability, maintainability – we recommend LAMP: Linux, Apache, MySQL and PHP/Perl/Python. Current examples use CGI scripts (iPIMMS) and PHP (iCal) on server.

As measurement and uncertainty calculations will be done on the server, the software needs access to industry-standard floating point calculations and perhaps industry-leading numerical library software. Our testing suggests PHP/Perl/Python are suitable for floating pointing calculations (despite not being primarily aimed at numerical applications), but an application developer should test their fitness for purpose for the particular application; Java is another possibility. NAG is a suitable numerical software library, which can be accessed from Perl by calling the C NAG library, and no doubt can be accessed from other scripting languages.

SS*f*M BPG12 *Test and Measurement Software* [4] gives guidance on the development of software for measurement systems and is applicable to internet server software. SS*f*M BPG1 *Validation of Software in Measurement Systems* [19] gives techniques for assessing fitness for purpose of measurement software.

4.5.3 Issues for client software

The client software should follow good practice for measurement acquision software [4]: including the ability to control hardware "drivers", and also ability to decode (and encode) control and data messages sent from/to the server using the protocol/format. Current example systems use Visual Basic for the client software.

5. Security issues for internet-enabled metrology

5.1 Introduction

Internet-enabled metrology services operate between different organisations, over public networks, and security will be an issue. They are usually developed from locally-operated metrology systems, and the developers will not have had to consider security issues. Although the security issues are new to measurement science, from the perspective of internet-based applications in general, the requirements for internet-enabled metrology are not new and the security solutions can be provided by standard commercial products.

Why security is needed

> Security is needed to protect the organisations that operate and/or use the internet-enabled metrology services, to protect the hardware and software that provide the service, and to protect the data being stored and transmitted as part of the service.

Costs of inadequate security

> Poor security can lead to direct costs in time and money to repair damaged systems; and direct loss of money through fraud. There are also costs to the service in term of loss of quality of the service, leading to loss of business and loss of reputation for the service provider.

Costs of security provision

> But there are also cost in providing security: costs of time in development, and costs from deployment of specific professional products (in purchasing, understanding, installing, and configuring the products). There are also direct costs to the operation of the service itself: the security provisions will increase the size of data to be stored and transmitted, and will decrease the speed of processing of the data.

Requirements for security

> Typical applications require integrity and authentication, but may also need confidentiality and anonymity. The requirements and the level of protection needed will be determined by undertaking a risk analysis of the system. The risk analysis will result in a security policy for the system, saying what is to be protected, who to protect it from and what the threats are.

An earlier report (the "Gamma" report, see [2]) included a generic security policy that goes some way to resolving these issues for a general internet-enabled *calibration* services. It may be more generally applicable to other internet-enabled metrology services – but the more the metrology service is different in nature from a calibration service, the less the generic security policy is relevant. Starting from the generic security policy, the earlier report details products and algorithms that implement the appropriate security techniques. It also includes information on practicalities such as configuration of commercial products.

Physical security issues are also relevant – security is also an issue for management, human resources and human-computer interaction.

5.2 Threats

The threats to the calibration data are mitigated by the following system features.

1. Use of the Secure Sockets Layer (SSL) network protocol to encrypt the customer data as it traverses the internet. This will protect any transmitted data, including the customer userid and password values.
2. Combination of the physical security controls surrounding the server and the use of a server application interfacing between the client from the database.
3. Internet-based customers are required to enter a valid userid / password combination that are checked against values stored within the data warehouse.

The main threat to the confidentiality of the system would be from the unauthorised disclosure of a valid userid / password combination. This would enable an attacker to gain direct access to customer information through the normal online viewing interface. Access to such information may provide a commercial advantage to an attacker, and if discovered would lead to a possible loss of reputation for the Calibration Service Provider (CSP) . Although the userid and password values are protected during transmission, they are not protected at the end-points.

5.3 Recommendations

The general advice on security for internet-enabled metrology systems is to use up to date commercial solutions for the provision of security mechanisms to protect business critical information.

5.3.1 Measurement data in transmission over the internet

To protect the data in transmission over the internet, it is recommended to use a standard security protocol such as the Secure Sockets Layer (SSL) and it is important that the use of SSL is configured not to use the default settings but settings that provide protection appropriate to the security policy. It is also recommended to use modern PC operating systems for the server and client system that, for instance, provide real user authentication.

The detailed recommendations are related to the Generic Security Policy for Internet Calibration Services from the "Gamma" report. The security policy (reproduced in Appendix A) lays down requirements to be met by both the CSP and the remote customer. When these requirements are met by both sides, they can both see what security features can be expected of the internet-enabled calibration system.

5.3.2 Online calibration databases

To protect the data in a database that supports an internet-enabled calibration system it is recommended that SHA-1 or MD5 is used to protect the userid/password data and that a message authentication code is used to protect the certificate measurement data. It is necessary to keep up to date with versions of software packages that offer protection from security vulnerabilities and the physical security of database should be protected with back-ups and the use of fire safes.

5.3.3 Electronic calibration certificates

Electronic calibration certificates are one way of delivering calibration certificate data to the calibration service customer. To protect the integrity of certificates delivered electronically to customers it is recommended that the electronic certificate be prepared in mechanical and repeatable way from the calibration data. The certificate should be converted to PDF and

digitally signed using a commercial document-signing product, using public key infrastructure. For some calibration services, it may be more appropriate to offer on-line access to the calibration data through a server maintained by the CSP.

There is more detail on the requirements and implementation of electronic calibration certificates in Appendix B.

5.3.4 Firewalls

Firewalls have become an essential component for systems that use the internet. The internet is a chaotic system with little regulation or policing. This means that accidental or malicious activity can affect your systems through the internet and only you are in a position to stop them. The only practical method of preventing intrusion into your system is to separate it from the internet and apply your security measures to the traffic that crosses the boundary.

It is recommended that the internet-enabled calibration system be capable of operating from a stand-alone client PC connected to the internet by a modem and an external telephone line to an ISP. The CSP should follow current "best practice" in server firewall configuration, limiting access to as small a set of services as possible, this set of services should include HTTPS.

6. Accreditation requirements on internet-enabled metrology systems

The guide [3] was developed by NPL as part of DTI's Software Support for Metrology Programme. It provides guidance to assessors and laboratories on how to apply ISO/IEC 17025 *General requirements for the competence of testing and calibration laboratories* in the area of internet-enabled metrology. The guidance is based on the experience of UKAS assessors and NPL staff and will be reviewed following its use in UKAS' assessment of an internet-enabled calibration service. It is anticipated that this practical application, along with a UKAS review aimed at ensuring alignment with the latest accreditation policy, will result in a version being issued as part of the UKAS LAB series.

ISO/IEC 17025 contains the requirements that testing and calibration laboratories (TC laboratories) have to meet if they wish to demonstrate that they operate to a quality system, are technically competent and are able to generate technically valid results.

Traditionally, TC laboratories either test or calibrate items that have been transported to them from the client, or personnel from the TC laboratories visit the client's premises to perform the test or calibration. Internet-enabled metrology, introduces an alternative method of working, where the client's items are tested or calibrated remotely, with control of the process applied over the internet. In some internet-enabled metrology services a calibrated artefact is sent by the TC laboratory to the client's site to be used to calibrate the client's instrument (Type I, see section 3.1). In other services a measurement instrument, which has been calibrated at the TC laboratory, is sent to the client for use in the test or calibration (Type II, see section 3.1). In either case a server at the TC laboratory controls the measurement process and the data from the remote measurements are processed by software.

In a third class of service the TC laboratory makes use of a web based service provided by another organisation (Type III, see section 3.1).

In all cases a significant part of the test or calibration takes place out of the direct control of the TC laboratory, and staff working for the client may play a key role. This leads to a variety of concerns in the application of ISO/IEC 17025 such as:

- maintaining traceability;
- demonstrating operator competence;
- monitoring environmental control;
- application of quality procedures;
- implementation of security.

The requirements of ISO/IEC 17025 are best met if the client's laboratory is

1. independently accredited against ISO/IEC 17025, or
2. is a sub-contractor (ISO/IEC 17025 clause 4.5), or possibly
3. is viewed as providing an external service.

The guidelines given are intended both to set down accreditation policy with regard to internet-enabled metrology and to provide a consistent approach to the assessment of such activity.

7. References

1. Awan, S.A., J.M. Williams, S. Bryant, and P.C.A. Roberts. *Progress towards Internet-based calibration of electrical quantities.* in *BEMC 2001- 10th British Electromagnetic Measurement Conference*. 2001. Harrogate, UK.
2. Barker, R.M. and G.I. Parkin. *Use of the Internet for Calibration Services – Protecting the Data – Final Report.* NPL Report CMSC 28/03, NPL, July 2003. http://www.npl.co.uk/ssfm/download/documents/cmsc28_03.pdf
3. Chorley, B.J. *Application of ISO/IEC 17025 to Internet-Enabled Metrology.*, NPL, 2004. http://www.npl.co.uk/ssfm/download/documents/17025guide.pdf
4. Clements, T., L. Emmet, P. Froome, and S. Guerra. *Test and Measurement Software.* Software Support for Metrology Best Practice Guide No. 12, NPL, October 2002. http://www.npl.co.uk/ssfm/download/bpg.html#ssfmbpg12
5. Dudley, R.A. and N.M. Ridler. *Internet calibration direct to national measurement standards for automatic network analysers*. in *IMTC 2001 - 18th IEEE Instrumentation and Measurement Technology Conference*. 2001. Budapest, Hungary.
6. IEEE 488.1-2003, *IEEE Standard for Higher Performance Protocol for the Standard Digital Interface for Programmable Instrumentation*. 2003, Institute of Electrical and Electronics Engineers.
7. Ives, D.J., G.I. Parkin, J. Smith, M. Stevens, J.A.F. Taylor, and M.C. Wicks. *Use of Internet by calibration services: demonstration of technology.* NPL Report CMSC 49/04, March 2004. http://www.npl.co.uk/ssfm/download/documents/cmsc49_04.pdf
8. Lerdoff, R. *PHP: Hypertext Preprocessor,*. http://www.php.net/
9. McCormick, N.J., M.R.L. Gower, and L.N. McCartney. *An Internet accessible system for simulating damage in composite laminates during bending deformation.* NPL Report MATC(A)96, April 2002. http://publications.npl.co.uk/npl_web/pdf/matc96.pdf
10. McCormick, N.J. and K. Lawrence. *The impact of new Internet technologies on SmartManuals and other MATC Internet projects.* NPL Report MATC(A)97, May 2002. http://publications.npl.co.uk/npl_web/pdf/matc97.pdf
11. Microsoft. *Visual Basic*. http://msdn.microsoft.com/vbasic/
12. Microsoft. *VBScript*. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/vtoriVBScript.asp
13. Microsoft. *.NET*. http://www.microsoft.com/net
14. MySQL-AB. *MySQL*. http://www.mysql.com/
15. Rayner, D. *Survey of International Activities in Internet-enabled Metrology.* NPL Report CMSC 21/03, NPL, May 2003. www.npl.co.uk/ssfm/download/#cmsc21_03
16. Sand, Å., G. Parkin, and M. Stevens. *A Dynamic Instrumentation Framework for Remote Operation of PC-Connected Devices*. in *IEEE International Conference on Virtual Environments, Human-Computer Interfaces, and Measurement Systems*. 2006.
17. Sand, Å., M. Stevens, and G. Parkin, *Internet-Enabled Calibration: An analysis of different topologies and a comparison of two different approaches.* IEEE Transactions on Instrumentation and Measurement, 2007.

18. W3C. *SOAP Version 1.2 Part 1: Messaging Framework*: 2003. http://www.w3.org/TR/2003/REC-soap12-part1-20030624/

19. Wichmann, B.A., R.M. Barker, and G.I. Parkin. *Validation of Software in Measurement Systems.* Software Support for Metrology Best Practice Guide No. 1, NPL, March 2004. http://www.npl.co.uk/ssfm/download/documents/ssfmbpg1.pdf

20. Winer, D. *XML-RPC Specification*: 1999. http://www.xmlrpc.com/spec

21. xmlBlaster.org. *XMLBlaster*. http://www.xmlblaster.org/

Appendix A Generic Security Policy for internet-enabled calibrations

Concept Definition

1. An internet-enabled calibration takes place between two parties – the **Calibration Service Provider** (**CSP**), the laboratory possessing the reference standards, and the **customer**, the laboratory possessing the equipment and standards to be calibrated.

2. This policy applies to:

- the interface, measurement and connected equipment at the customer site, as far as the point of connection to the artefact being measured,
- the internet or other transmission networks,
- the interface, measurement, control and recording equipment at the CSP, together with any other CSP systems able to access that equipment.

Authentication

3. Both parties in an internet-enabled calibration session shall be able to verify that the other party is the intended participant. Verification shall be performed whenever an internet connection is established and shall be repeated whenever the connection between the two parties is disrupted or broken and subsequently re-established.

4. The verification mechanism shall provide protection against subsequent impersonation through communications eavesdropping or interception of a successful authentication exchange.

5. The verification mechanism shall provide protection against subsequent impersonation by replay of successful participation in an authentication exchange.

6. The verification mechanism shall provide protection against impersonation through brute force repetition of authentication requests.

Access Control

7. Parties in an internet-enabled calibration session shall only be permitted access to resources belonging to the other party that have been authorised by the owning party. This authorisation may be implicit through the establishment of a calibration session, or may be statically or dynamically controlled by the owning party or an authorised automated process acting on their behalf.

Confidentiality

8. Information transmitted during an internet-enabled calibration session shall not be revealed to or be deducible by anyone other than the receiving party.

9. There is no requirement to conceal from other parties that an internet-enabled calibration session is taking place, or to conceal the identities of the participating parties, although the nature of the standard being calibrated shall not be deducible.

10. Protection against disclosure through authorised access to the CSP equipment is outside the scope of this policy.

Integrity

11. It shall not be possible for information transmitted during an internet-enabled calibration session to be modified, deleted or substituted in transmission over the internet without detection.

12. Protection against modification, deletion or substitution through authorised access to the CSP equipment is outside the scope of this policy.

13. When an internet-enabled calibration session is terminated before successful completion, this shall be evident to both parties.

Non-repudiation

14. Neither party in an internet-enabled calibration session shall be able to subsequently deny the origination of information successfully transmitted during the session, or the time and date of that transmission.

15. Neither party shall be able to subsequently deny the receipt of information successfully received by them during an internet-enabled calibration session, or the time and date of the delivery of that information.

Availability

16. Either party in an internet-enabled calibration session shall be able to terminate a calibration session, whether completed or not, without the active consent or participation of the other party or any provider of internet connectivity.

17. There are no requirements to provide any guaranteed minimum quality of service, minimum periods of availability or maximum calibration time.

Audit

18. The CSP shall store and retain sufficient information to ensure that a third party, acting with the CSP's consent, can, for a declared period of time, confirm that calibration took place, and can determine the measurements, values and outcome of calibration.

Privacy

19. There are no requirements for customer anonymity (i.e. for the customer to participate in a calibration session without revealing their true identity to the CSP) or for unobservability (i.e. for the customer to participate in a calibration session without their participation being evident to any third party, such as Internet Service Providers).

Certification

20. When an internet-enabled calibration is certified, the certificate shall be linked to the measurements, tests and results of the calibration, in such a way that a third party, acting with the CSP's consent, can, for a declared period of time following the certification, confirm the validity of the certificate. This applies whether the certificate is electronic or physical in form.

21. The issue of electronic certificates for successful internet-enabled calibration sessions is outside the scope of this policy

General Protection

22. Participation in an internet-enabled calibration session shall not require either party to relax or remove standard internet security measures as found in a secure browser/server environment. Standard in this sense means security measures supported and recommended by

the manufacturers of the browser and server, or recommended in standard policy guidance issued by the UK Government's National Technical Authority for Information Assurance.

23. Where the customer is required to use particular makes or versions of browser, this shall be verified by the CSP during initiation of the calibration session.

24. Where the IT system hosting the client software used by the customer is supplied by the CSP, the customer shall not be able to extract calibration information from the client system without the consent of the CSP. The customer shall not be able to reconfigure the client software without the consent of the CSP. Any export or amendment of calibration data, or reconfiguration of client software, shall be recorded in an audit log which cannot be amended or erased by the customer, but which can be accessed by the CSP.

Appendix B Electronic calibration certificates

B.1 Introduction

"Electronic calibration certificates" are a solution to three distinct sets of requirements. Some measurement services want electronic calibration certificates to be the output of a reliable process for getting calibration data on to a certificate. Some want electronic calibration certificates as a way of making calibration data available to the customer over the internet. Finally, there is a requirement to be able to send an electronic calibration certificate to the customer to take the place of a printed paper certificate.

The (original) requirement for transmitting an electronic form of a paper certificate can be done securely by creating the document as PDF and using the encryption and digital signature mechanisms provided by products that support PDF. There is no need to create an electronic version of the data from a certificate where that data may cover many pages of a certificate. In this case different mechanisms should be use to give the calibration service user electronic access to the measurement data and calibration coefficients.

B.2 Electronically produced calibration certificates

The first requirement for electronic calibration certificate is to protect the integrity of the data in the process of producing calibration certificates. Where calibration certificates are produced by hand, the data on the certificate can fail to match the original data because of transcription errors. This occurs either when the data is written on the certificate or when the data is typed into a certificate on-line; in either case there is a possibility of the person copying the data to misread and/or then miswrite or mistype the numbers in the certificate. This threat to data integrity is present whether the certificate is being prepared to be printed and sent to the customer in the traditional manner, or the electronic certificate is to be sent to the customer as described in section B.3.

This aspect of electronic calibration certificates was not originally envisaged as part of the study but NPL has experience of producing certificates automatically (i.e. as part of an automated, repeatable process) and we believe the process can improved by using generic formats for the calibration data. The solution we propose is that all data that is output from the calibration be stored in a structured format that reflects the nature of the measurement data and the requirements of the calibration certificate. The aim would be that the format of the calibration data would be sufficiently general that the conversion to an electronic version of the calibration certificate could be done by one program, using the calibration data and a template describing the certificate for a particular service as input. The measurement system producing the formatted data and the program to produce the electronic calibration certificate would have to be tested and validated to ensure the integrity of the measurement/calibration data was preserved. The advantage of using a common format for the data is that only one program is need to produce the certificate, and the testing and validation of that program only has to be done once, regardless of how many calibration services it is used for.

We propose that XML (eXtensible Mark-up Language) be used for the formatted calibration data; this is a non-proprietary format that is human-readable and widely used for web applications. Having measurement/calibration data in a common format would have a number of further benefits beyond a unified approach to the electronic processing of calibration certificates. The XML format would serve to document the data that would allow other scientists working on the same project a better chance to understand the meaning of the data. (This will also be true for the original scientist coming back to the project.)

The XML format is an open format that can be easily understood (read, processed, and written) by any programming language, so other scientists (from other projects, other

programmes, or even other institutes) could use the XML data in combination with their own data, without having to understand the measurement system that produced the original data. XML is extensible so more information can be included in the data at a later date, while still remaining compatible with the old data. Finally, XML formatted calibration data can be read into a database of calibration history data, see section B.4.

B.3 Transmission of calibration certificates over the internet

The original requirement for electronic calibration certificates is to be able to send an electronic equivalent of a paper calibration certificate to the calibration customer, protecting the integrity and authenticity of certificate. If providing the customer with access to the data is the real requirement, rather than providing an equivalent of the paper certificates, then see section B.4.

CSPs have strict procedures to ensure the integrity and authenticity of paper certificates produced by their services and these procedures have to conform to UKAS requirements if they are part of a UKAS accredited service (or conform to the relevant accreditation requirements, in countries outside the United Kingdom).

The process of signing a document is as follows:

- Obtain and install a document signing software product.
- Obtain a public and private key for your organisation.
- Convert the electronic calibration certificate to a read-only format.
- Sign the calibration certificate using the document signer.
- Send the signed document to the customer, who can authenticate it.

B.4 Electronic access to calibration certificate data

Digitally signed electronic calibration certificates provide the closest electronic analogue of paper calibration certificates in terms of integrity and authenticity, but they may not be the most convenient way of giving the customer access to the data in the certificate. This access is thought to be best provided by an internet-enabled metrology database, where the user can access not just the data relating to the current calibration but the whole calibration history of each of their instruments.

The solution would work equally for traditional calibration services and (internet-enabled) remote calibration services.

- For remote calibration services, the measurement data will be stored in a database and a history of calibrations of a particular instrument will be built up. In the iVR internet-enabled calibration system for voltage and resistance measurement, the customer can logon and access the information in the database relating to his calibrations, even when not engaged in a calibration. This allows the customer to download and analyse this information to look for trends in the historical data, or retrieve the current calibration correction coefficients for a given instrument.
- This solution can be adapted for any calibration service. The calibration history database can be built up from calibration/measurement data, preferably presented in a common format (see section B.2). Internet access to the database can be built using the generic iCal software that was used for iVR, following the recommendations above on data security and data warehousing.

This solution to providing electronic access to calibration certificate data is more flexible than digitally signed electronic calibration certificates but does not offer tangible evidence of the calibration at the customer site. Much more information can be put in the calibration history

database and the web access to the database can be integrated with other metrology application to give richer internet-enabled metrology services.