NPL Report CMSC 28/03

Report to the National Measurement System Directorate, Department of Trade and Industry

Use of the Internet for Calibration Services – Protecting the Data – Final Report

Robin Barker
Graeme Parkin

July 2003

Use of the Internet for Calibration Services – Protecting the Data – Final Report

Robin Barker and Graeme Parkin
Centre for Mathematics and Scientific Computing

July 2003

ABSTRACT

This report describes the final output from the Software Support for Metrology project "Use of the Internet for Calibration Services – Protecting the Data".

This project comprised of four separate studies, the major two of which were on data security and data warehousing. There were separate reports from the subcontractors for those studies (included as attachments). This report includes summaries of the recommendations of the major studies and the results of the other studies on electronic calibration certificates and firewalls.

ISSN 1471-0005

National Physical Laboratory
Queens Road, Teddington, Middlesex, TW11 0LW

Approved on behalf of the Managing Director, NPL
by Dave Rayner, Head of the Centre for Mathematics and Scientific Computing

Contents

1 Introduction

This is the final report of the Software Support for Metrology (SS*f*M)[1] project 5.1.1 "Use of the Internet by Calibration Services – Protecting the Data". The project provides guidance for the developers of internet-enabled calibration systems on protecting the measurement data that is transmitted over the internet and stored in calibration databases. This guidance is contained in the two subcontractors' reports, attached to this report. The project looked at issues of data integrity, data confidentiality and data warehousing as they apply to measurement data in transmission or in databases. The project investigated particular security issues that apply to the operation of internet-enabled calibration services through firewalls and to the transmission of electronic calibration certificates over the internet: these issues are addressed in later chapters of this report.

The project took a practical approach to these problems by examining developing practice in internet-enabled calibration. To examine the use of data protection mechanisms, the project performed two assessments of aspects of the internet-enabled calibration service for DC Electrical quantities; these assessments will cover both the security aspects of measurement data being transmitted over the internet and the data warehousing issues of measurement data and calibration history. This approach, based on real examples, should give confidence that the outputs address real issues in protecting the data for internet-enabled calibration.

1.1 Background

In February 2001, NPL together with BAE Systems launched the first-ever remote calibration service operated over the internet (now known as an internet-enabled calibration service). This was in the Radio Frequency and Microwave area, a service for calibrating impedance measurement capabilities of automatic network analysers. NPL has already begun work on the development of internet-enabled calibration services in two other fields: resistance and voltage measurements and spectrophotometry. Work has also begun on innovative use of the internet to support remote calibration in the ionising radiation dosimetry field. In parallel with this project were two other SS*f*M projects for the "Use of the Internet by Calibration Services", one to develop a demonstration of the technology for a service in the photonics area (SS*f*M project 5.1.2) and the other covering the areas of promotion of internet-enabled metrology (a wider concept including internet-enabled calibration and other innovative uses of the internet to support measurement services) and liaison on issues such as accreditation as applied to internet-enabled metrology services (SS*f*M project 5.1.3). The report [1] from project 5.1.3 is a survey of the worldwide activity in internet-enabled metrology.

The use of the internet to deliver calibration services offers great potential for the National Measurement System, allowing calibration to be done quicker (less "down time" for the instrument to be calibrated), less disruptively (the instrument does not have to be moved), and leading to increased accuracy of the instrument. The integrity and traceability of the calibration process is crucially dependent on being able to rely on the calibration data. This data is vulnerable when it is transmitted across the internet and when it is stored as part of the calibration history.

[1] See Appendix A for all acronyms

This project addressed these vulnerabilities by providing guidance on security and data warehousing to those intending to establish an internet-enabled calibration service.

1.2 Work programme

The two larger studies on transmission and warehousing of measurement data were progressed by engaging subcontractors with the appropriate security expertises. These were Gamma Secure Systems for the data transmission security study (attachment 1), and Baltimore Professional Services for the data warehousing study (attachment 2). Both studies used as their example system the iVR internet-enabled calibration system for Voltage and Resistance measurement, developed by the DC and Low Frequency part of the Electrical programme. The studies investigated the iCal software on which the iVR system is based; iCal was developed as part of the iVR project and it offers a generic approach to developing internet-enabled calibration systems.

The two studies were progressed similarly, starting with the consultants coming to NPL to discuss the requirements of the security review (or audit). They then conducted review of the security of the internet-enabled calibration system by talking to the iVR project team members, reviewing the software and the documentation, and further consultation with the NPL members of this project team. The output from the consultants was reviewed by the iVR project team and this project, and final reports were produced.

The other studies were progressed by discussions within NPL and research into the appropriate security techniques. The requirements for electronic calibration certificates were difficult to identify but ultimately a number of different sets of requirements were identified by discussing the issue in the NPL Measurement Services Forum. These requirement sets were electronic production of certificates, electronic versions of paper certificates, and on-line access to certificate data. There are separate solutions for these sets of requirements, although the first is not really within the scope of the project.

We discussed issues of firewalls with the NPL internet-enabled calibration projects and discovered a commonality of approach more-or-less dictated by the NPL security policies. We examined other sources of information on firewalls and concluded that the approach adopted by NPL would be appropriate for other providers of internet-enabled calibration services. We present the general issues of how firewalls operate and the NPL approach to allowing the operation of remote services through firewalls. The iVR service has a solution to avoid security issues at the customer site in an internet-enabled calibration service that is also generally applicable.

1.3 Generic mechanisms and products

Most of the recommendations in the report (and the attachments) are based on standard security mechanisms and technologies. But sometimes it has been necessary to name specific products, to give examples and to be definite about how a particular solution could work. Naming of these products is not an endorsement of these products and in most cases there will be a number of products offering similar functionality that could be used to provide a suitable solution.

2 Data security in transmission of measurement data

2.1 Security policy

As part of the first study, Gamma produced a generic security policy (pages 5 and 6) that was discussed and amended by the project. The security policy lays down requirements to be met by both the Calibration Service Provider (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. The review of the security mechanisms used by iVR took the security policy as its starting point.

From the review, there was produced a discrepancy report showing where the current iVR system did not meet the security policy. The recommendations from the report detail how the system could resolve the discrepancies.

The review revealed that some mechanisms, provided by the Secure Sockets Layer (SSL), were not being used consistently with industry best practice. Recommendations on the use of the security mechanisms, and the correct way to use them, formed the final SS*f*M report. The final report of the iVR project described how the recommendations had since been adopted in the iVR system.

2.2 Recommendations

The main recommendations

- The client PC provided to the customer should be based on a version of Windows with greater security features. This would have the following benefits:
  - a) a logon password could be used to authenticate the user of the client PC, rather than relying on weak authentication to the CSP server;
  - b) by restricting the access granted to the customer calibration software and data could be protected from misuse by the customer or third parties;
  - c) an independent audit record of calibration actions and measurements could be kept on the client PC.
- Use of SSL should be reconfigured to require security certificates for both client and server. If not, rules should be set to force use of strong passwords when establishing a calibration session.
- The use of SSL should be explicitly configured to reject null or weak algorithms, although recognising that weak algorithms may provide adequate protection for calibration purposes in many cases.
- A policy is needed on the verification of calibration certificates. This policy should define how a third party would verify that a calibration certificate was valid, and for what period of time verification would be possible. In consequence, it would be necessary to:
  - a) archive calibration data used to issue a calibration certificate outside of the calibration system;
  - b) retain that data for the declared period of time;

c) provide a way that a third party can confirm the validity of a calibration certificate;

d) provide a way (such as digital signature) that the customer can confirm that the results of calibration have not been changed after the calibration certificate was issued.

2.3 Conclusions

The security policy and recommendations from the security audit are a firm basis for the use of the internet for calibration services. There are two points that should be stressed.

- More secure versions of the Windows operating system (e.g. NT, 2000, XP) do offer the benefits over other versions (e.g. Windows 98) described in the first recommendations. But it is dangerous to assume the more secure operating systems would provide complete security over the client's calibration data. It is relatively easy to gain administrative access to a Windows NT/2000/XP system assuming you have local access and can boot it up from a floppy or CDROM.

  So it is possible for someone at the customer site is to meddle with the system configuration or measurement data. This can only be protected by strict (human) procedures for the conduct of the remote calibration.

- Paragraph 14 of the security policy “non-repudiation”, makes serious requirements on traceable reputable time and date stamps. There are commercial products (e.g. “Trusted Time” from Symmetricon) that provide digitally signed time stamps that are traceable to UTC through a network of time servers at metrology institutes, including NPL (see [1] section 2.4)

The recommendations from the final report are being adopted by the iCal software and/or the iVR system as follows:

Recommendation	**Adoption**
The client PC (provided to the customer) should be based on a version of Windows with greater security features.	Done.
Use of SSL should be reconfigured to require both client and server (security) certificates	Will be considered for the final deployment of iCal/iVR
The use of SSL should be explicitly configured to reject null or weak algorithms.	Will be consider for the final deployment of iCal/iVR
A policy is needed on the verification of (calibration) certificates:	The conclusion of the relevant part of this report will be considered for the final deployment of iCal/iVR.

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.

3 Data security in storage of calibration data

3.1 Assessment

The data warehousing study was able to use the generic security policy for internet-enabled calibrations above to define what was required of the security internet-enabled metrology databases. The assessment of the system was summarised against the security requirements taken from the design of the iVR system and the generic security policy. These assessments are given in the annex to the data warehousing report.

The review of the iVR system showed that the security of the system was mainly dependent on the security of the internet access to the server system, which was the subject of the first study. But there were aspects of the data warehousing that could be improved to ensure the integrity of data in the calibration database.

3.2 Threats

The threats to the data in the calibration history database are related to 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 PHP scripting.
3. Internet-based customers are required to enter a valid userid / password combination, that is checked against values stored within the data warehouse. The CSP is responsible for maintaining customer userids and passwords.

The main threat to the confidentiality of the system would be from the unauthorised disclosure of a valid userid / password combination. These values would enable an attacker to gain direct access to customer information through the normal online viewing interface. Access to this 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. Although the userid and password values are protected during transmission, they are not protected at the end-points.

3.3 Recommendations

3.3.1 Password/userid protection

It is recommended that the password values are not stored as clear values upon the database but should be held as message digests. Ideally the user-entered password value would be converted to a message digest value using a suitable one-way-function (e.g. SHA-1 or MD5) as soon as possible. The calculated digest may then be compared to the stored digest value for that userid through the PHP scripts.

3.3.2 Encryption of customer measurement data

Under normal circumstances we do not believe that the encryption of the customer measurement data, or for that matter other application information held with the data warehouse, is necessary. One possible exception to this rule would be where the measurements from the customer standard are given an HMG protective marking greater than RESTRICTED. Under these circumstances it will be necessary to use CESG approved products for implementing hardware-based disk encryption.

3.3.3 Integrity of certificate measurement data

The database should provide integrity protection for the set of measurement data that is used during the certification process. This will also enable the Calibration Service Provider at a later date to provide evidentiary proof in support of their certification of the customer standard. It is recommended that the data used during the certification process should be cryptographically protected to detect unauthorised or inadvertent modification. The simplest form of integrity protection is to generate a message digest; or possibly a message authentication code (MAC) value, for the data, using one of a number of commonly available algorithms. The recommended algorithm is a keyed MAC, based upon the HMAC process [2]. This process creates a 160-bit message digest value from the data (using SHA-1) and then encrypts this value with a secret 3DES key.

In the future, the service will use public key cryptography to digitally protect the calibration certificates. It would then be recommended that the use of digital signatures should also be investigated in order to protect the measurement data, as a replacement for the HMAC scheme proposed above.

3.3.4 MySQL vulnerabilities

Finally, the MySQL software includes security and system-related functions for database administration. There have been a number of recently published MySQL security related vulnerabilities that might allow an attacker to gain access to these system functions. It is strongly recommended that these vulnerabilities should be investigated and, where appropriate, fixed through the implementation of the appropriate erratum packages to upgrade the iVR database software to MySQL 3.23.54a.

3.3.5 Backup and secure storage

The other type of unauthorised or inadvertent change to the data warehouse to be considered is where the data warehouse is corrupted or perhaps destroyed and becomes unavailable. The regular taking of backups, and the testing of restore procedures should protect against this possibility. The backup media itself will need to be protected from attack, and we would recommend the use of a fireproof safe for this purpose, ideally located at another site to the data warehouse itself.

3.4 Conclusions

The data warehousing report includes a number of recommendations for techniques and algorithms to be applied to a calibration database used in internet-enabled calibration services. The report was not available while the iVR project was still active but it is likely that, when the iVR service is deployed and the system security reconsidered, the following actions will be taken.

Recommendation	Adoption
SHA-1 or MD5 for userid/password protection	Will be considered for the final deployment of iCal/iVR
Algorithms for encryption of sensitive measurement data	Will be considered if it becomes a requirement of iVR customers
Message authentication code for certificate measurement data (HMAC, SHA-1, 3DES)	Will be consider for the final deployment of iCal/iVR
MySQL vulnerabilities	NPL procedures require that vulnerabilities are investigated and new versions installed
Backups and fire safes	NPL security procedures includes backups and the use of remote fire safes

4 Electronic certificates for calibration services

4.1 Introduction

This study was originally expected to produce "Guidance on transmission of calibration certificates over the internet". The work revealed wider requirements for electronic calibration certificates, addressed in this chapter; the original requirements are specifically addressed in section 4.3.

There have been discussions in NPL on the requirements for electronic calibration certificates. The conclusion from this discussion was that electronic calibration certificates were a solution to three distinct sets of requirements. Some measurement services wanted electronic calibration certificates to be the output of a reliable process for getting calibration data on to a certificate. Some wanted electronic calibration certificates as a way of making calibration data available to the customer over the internet. Finally, there was a requirement to be able to send an electronic calibration certificate to the customer to take the place of a printed paper certificate.

The study examined these different requirements and, after further discussions to clarify what kinds of solution would be acceptable, proposed different solutions to the different problems. The original requirement (as envisaged in the project proposal) 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 not such a perceived 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.

4.2 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 4.3.

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 4.4.

4.3 Transmission of calibration certificates over the internet

4.3.1 Requirements and restrictions

The original requirement for electronic calibration certificates in this project was 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 4.4.

Calibration Service Providers 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). Although the use of digital signatures for data integrity and authentication is well established, the solution described here would have to be approved by UKAS (or its equivalent in other countries) before it could replace paper certificates as part of a UKAS accredited service. In the meantime, it would be possible to send a digitally signed electronic certificate by e-mail and follow up with a traditional paper certificate, but the paper certificate would be the normative version, taking precedence over the electronic certificate in the case of discrepancy or dispute.

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.

4.3.2 Public key infrastructure

To use digital signatures it is necessary to be part of a public key infrastructure by obtaining a private key that is used as part of the signing process. The private key is used to sign electronic documents and then the corresponding public key is used to authenticate the signature. The public key can also be used by others to encrypt message they send to you, only you (the owner of the private key) can read the document: using your private key to decrypt the message. Private keys are issued by suppliers of security products, such as document signing software.

4.3.3 Conversion to read-only format

The calibration certificate to be signed should be converted to a publicly readable read-only format: the most appropriate format is Adobe PDF (Portable Document Format). An intrinsically editable document format, such as Microsoft Word, is not suitable for signing. There are tools (from Adobe) for converting documents from Microsoft Word to PDF; it is also possible to perform this conversion via PostScript (using ghostscript to convert from PostScript to PDF).

4.3.4 Using a document signer

To sign the certificate, you need to purchase and install a document signature product, such as VeriSign Document Signer. The manual for this product also explains how to obtain your own digital ID (e.g. public and private keys), but your organisation may already have keys from VeriSign that are appropriate for the certificate service. The Document Signer is installed as a plug-in to Adobe Acrobat: a signature icon will appear on the toolbar and there will be a sub-window with information about the signatures for the documents.

To sign a calibration certificate, you select the signing tool and drag and drop the signature into the certificate. There may be a series of dialogue boxes to negotiate if you have a choice of digital IDs to use. Once you have confirmed the signing of the certificate, you can view the properties of the digital signature and validate the signature. The digitally-signed calibration certificate can now be sent by e-mail to the customer.

4.3.5 Customer verification of the signature

When the customer receives a calibration certificate electronically, they must verify the signature. Viewing the certificate in Adobe Acrobat Reader with a document signer plug-in, they click on the signature and select “Verify Signature”. If the signature is successfully verified, the verification status is shown in the properties dialogue box. Successful verification of the signature confirms the integrity and authenticity of the certificate: it was signed by the one who it is claimed to be signed by, and the certificate has not been modified since it was signed. The certificate can be used with the same reliance as a traditional paper certificate.

4.4 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.

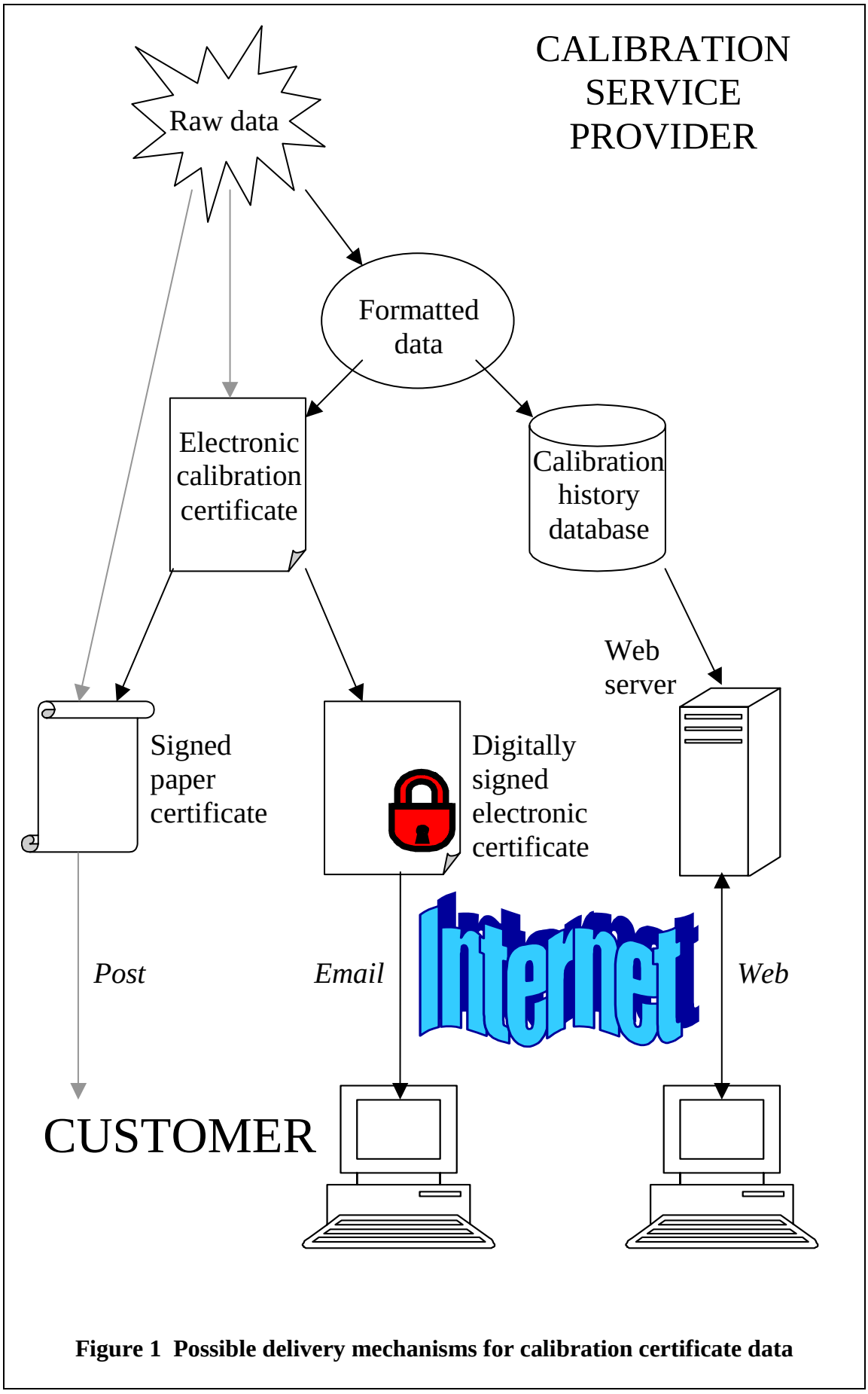


Figure 1 Possible delivery mechanisms for calibration certificate data

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 4.2). 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.

4.5 Conclusions

Electronic calibration certificates are one way of delivering calibration certificate data to the calibration service customer, the alternative delivery mechanisms are shown in Figure 1.

- Electronic calibration certificates will be produced from formatted calibration data in a reliable reproducible process that protects the integrity of the data by avoiding transcriptions errors. These are errors that arise if the certificates (electronic or paper) are produced by hand from the raw calibration data.
- The electronic calibration certificates can be printed and signed and posted to the customer.
- Electronic calibration certificates can be sent to the customer over the internet. The certificate must be converted to PDF and digitally signed using a commercial document-signing product. The Calibration Service Provider and the customer will need to be part of a public key infrastructure to assign and validate the digital signatures.
- The data on the calibration certificates can be made available to the customer over the web, protected by userid/password. The formatted calibration data is stored with previous calibration data in a calibration history database. This database can be accessed over the internet using the same set-up as is used by the iVR system to give internet-enabled calibration customers access to their calibration history data.

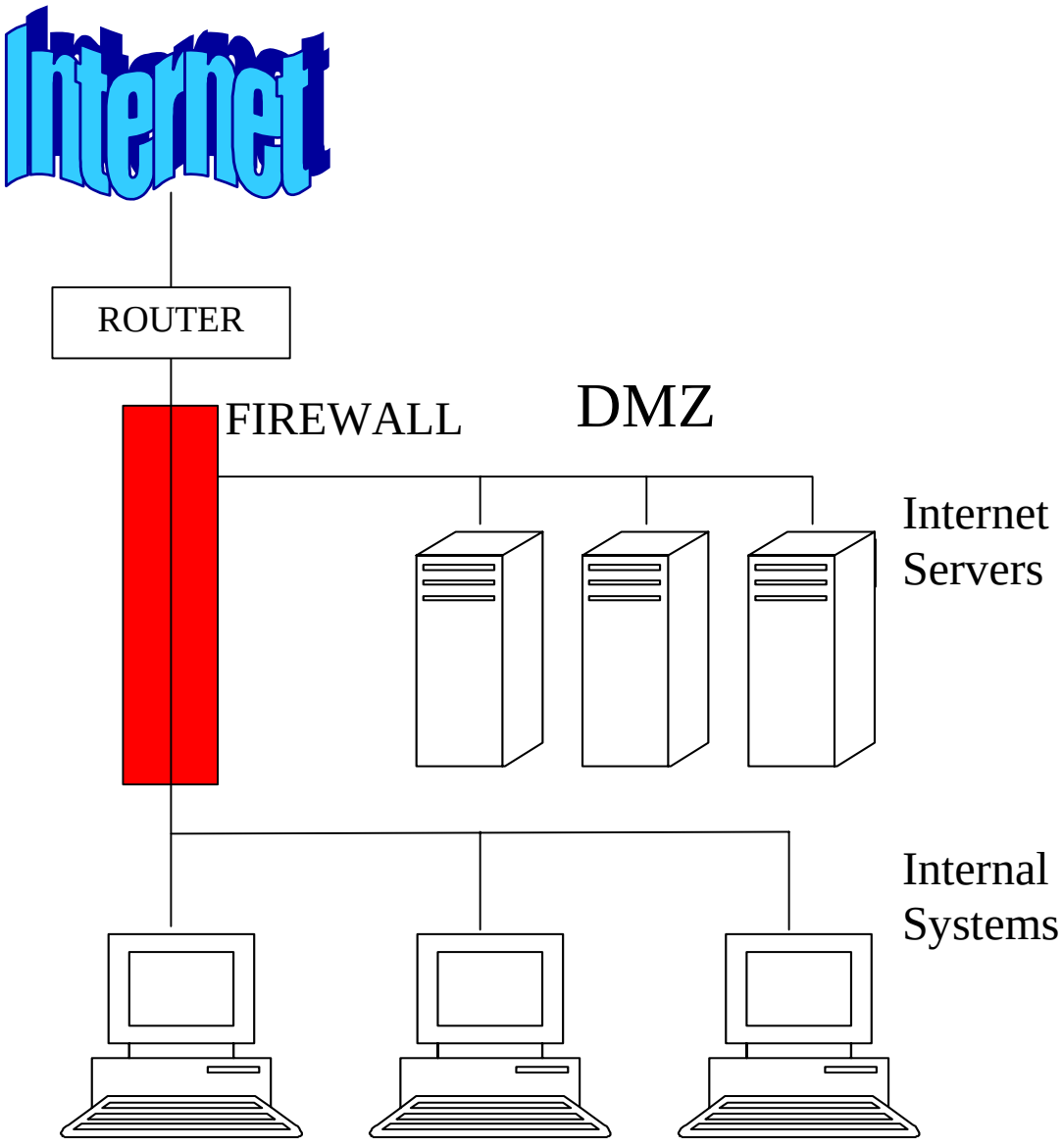
5 Internet-enabled calibration services through firewalls

5.1 Introduction

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 your system from the internet and apply your security measures to the traffic that crosses the boundary.

This boundary and the security measures that it employs constitute a firewall. It allows for a separation of functionality for the systems that use the internet: applications can be built to handle their specific security concerns but handling the generic security can be left to the firewall. Firewall technology is part of the "arms race" of internet security:

Figure 2 Firewall and DMZ



better firewall products are continually being developed to match the increasing ingenuity of the attacks. But deploying newer (better) firewall products is not the complete solution, it is just as important to make sure the firewall you use is properly configured to match your system and your security policy.

5.2 Firewall topology

A firewall is usually arranged with effectively two boundaries, with the internet servers for the system situated between the boundaries, in the Demilitarised Zone (DMZ); see Figure 2 (from [3]). The first line of defence occurs between the internet and the DMZ, allowing only internet messages that the servers in the DMZ are intended to serve. The second line of defence is between the servers in the DMZ and the internal network: only some forms of network traffic are allowed to the DMZ so that if the internet servers become compromised, the more valuable resources available on the internal network cannot be attacked. The firewall can also be used to implement the security policy for traffic from the internal network to the internet (via the DMZ): filtering out inappropriate e-mails or access to inappropriate web sites.

5.3 Protection mechanisms

There are different ways that firewalls can protect the host systems, see [4]. More sophisticated, or bespoke, firewalls solutions can be achieved by building on these technologies.

Packet filters (or Port-based firewalls) are the oldest technology for firewalls and operate at the lowest level of internet communication of any firewall mechanisms. Internet communication is based on packet-switching: each message is broken up into small pieces (called packets), individually addressed and sent off to be routed round the internet, on arrival the individual packets are reassembled to form the message. Packet filtering uses a list of rules to determine whether the packet should be allowed through the firewall. The rules are based on the addressing information and protocol used by the packet. This filtering is fast but, because it operates at a low level, it is the least secure and does not allow protocols with complex exchanges (such as FTP: File Transfer Protocol).

Circuit-level gateways operate at the next higher level of internet communication based on the TCP used to route packets round the internet. They use information about the socket (or Port) used for the TCP connection to determine what connections are allowed. They are more secure than packet filtering but require more work in correctly configuring the firewall to provide the required access for applications (and users), according to the system security policy. This is the mechanism in “SOCKS”-based firewalls.

Application-level gateways operate at a higher level of internet communication based on the specific application that is accessing the internet. They are slower but more secure than the lower level mechanisms and require more configuration for the application, the network and the user. This is the mechanism used by HTTP proxies, where PCs on the internal network cannot access the internet directly, but have to connect via a server in the DMZ that acts as a proxy for the HTTP messages.

Finally, the most secure but most complex technology is termed “stateful, multi-layer inspection firewalls”, e.g. CheckPoint Firewall-1. These firewalls retain information about previous traffic (i.e. “stateful”) and operate across the various levels of internet communication (“multi-layer”) used by the previous mechanisms.

5.4 Current NPL internet-enabled calibration systems

NPL internet-enabled calibration systems follow two models: iPIMMS (used by iPIMMS and iColour), which uses CGI and ActiveX; and iCal (used by iVR and iOTDR), which uses PHP and Visual Basic. Both models use HTTPS to communicate between server and client. This is the standard secure protocol for web pages and the NPL firewall fully expects and allows such traffic between servers and the internet. The CSP should follow current "best practice" in firewall configuration, limiting access to as small a set of services as possible. Applications that make use of non-standard protocols and ports tend to conflict with such a policy and will create problems.

The systems take a different approach to firewalls at the remote site. The client software for iPIMMS runs on the user PC that must be connected to the internet and the service operates on that connection, through the client firewall. Whereas, the iCal client is a PC sent with the calibration transfer device. To avoid problems of connecting an unknown PC to the client's network, the PC is connected to the internet by dial-up to an Internet Service Provider (ISP). Thus, the iCal software does not have to deal with any restrictions from the remote site's firewall or any other aspects of their security policy. The rates of data exchange (the bandwidth) in current internet-enabled calibration systems are moderate and can be operated over ordinary telephone connections, and it is not necessary to have a broadband or ISDN connection.

5.5 Conclusions

The use of servers and firewalls at NPL is now well understood, and the use of standard mechanisms and protocols is now the norm. This allows for greater security in the firewall (because only standard access is required) and ease of development for the implementor.

The recommendation for the use of firewalls for internet-enabled calibration services is to deploy the internet-enabled calibration service over HTTPS and configure the server system firewall to allow HTTPS traffic. This allows the firewall policy to limit access to a small set of standard services.

For the client system, it is necessary to decide what sort of security policies are likely to be operated by potential customers of the internet-enabled calibration service. If the service will use a PC already on the client network and the customer security policy will allow access to the internet, through the customer's firewall, then no further components are needed for the internet-enabled calibration systems.

However, it is recommended that the internet-enabled calibration system be capable of operating from a stand-alone PC connected to the internet by a modem and an external telephone line to an ISP. This will avoid any restrictions from the remote site's firewall or any other aspects of their security policy. If necessary, the internet-enabled calibration Service Provider can provide a PC to run the client system and this PC will not have to be connected to the customer's network nor use their firewall and internet access.

6 Summary

The project has shown that data security methodology is relevant to the use of the internet for enabling remote calibration services. The security requirements have been captured in a Security Policy for internet-enabled calibrations that can be used as a basis of auditing the security of internet-enabled calibration systems. Security mechanisms and technologies can be used in internet-enabled calibration systems to provide the necessary protection to the data handled by the service: whether this data is in transmission over the internet, is being stored in a calibration service database, is an electronic calibration certificate, or is negotiating a firewall.

To protect the data in transmission over the internet, it is recommended to use a commercial 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.

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.

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 Calibration Service Provider.

In order that internet-enabled calibration services can operate through firewalls, it is recommended that the calibration service provider operates a firewall that respects the other security needs of the organisation and that the internet-enabled calibration operates over HTTPS. Because no particular properties of the security policy (including the firewall) at the remote site can be assumed, the client system should be capable of running on stand-alone PC connected to the internet via a modem.

The project interacted with a number of internet-enabled calibration projects and internet-enabled metrology projects at NPL. The solutions recommended in the report have either been adopted by existing internet-enabled calibration systems or will be considered for adoption when these systems are deployed as service and when new systems are developed.

7 Acknowledgements

The work described here was supported by the National Measurement System Policy Unit of the UK Department of Trade and Industry as part of the National Measurement System Software Support for Metrology programme.

The authors would like to acknowledge the contributions of Mike Nash (Gamma Secure Systems), Ian White (Baltimore Technologies), Stuart Prince, Nick McCormick, and Keith Lawrence. The authors are very grateful to the support given to the project by the iVR project team: Adelard, NPL and Fluke.

8 References

1. Rayner, D. *Survey of International Activities in Internet-enabled Metrology*. NPL Report CMSC 21/03, NPL, May 2003. http://www.npl.co.uk/ssfm/download/#cmsc21_03

2. Krawczyk (IBM), H., M. Bellare (UCSD), and R. Canetti (IBM). *HMAC: Keyed-Hashing for Message Authentication*: 1997. http://www.ietf.org/rfc/rfc2104.txt

3. Hills, R. *Securing internet communications*. in *Joint BIPM - NPL Workshop on the impact of information technology in metrology*. 2002. NPL.

4. Rudis, B. and P. Kostenbader. *The Enemy Within: Firewalls and Backdoors*: 2003. http://securityfocus.com/infocus/1701

Appendix A Acronyms

3DES	*Triple* DES – strong form of DES: *Data Encryption Standard*
ActiveX	Microsoft technologies for web objects
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*
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: *Standard Query Language*
NPL	*National Physical Laboratory*
PC	*Personal Computer*
PDF	*Portable Document Format*
PHP	a scripting language – originally *"Personal Home Page"*
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*
XML	*eXtensible Mark-up Language*

Attachment 1

Security Audit – Final Report

(Gamma Secure Systems)

Software Support for Metrology (SS*f*M)

Use of the Internet By Calibration Services

Security Audit

Final Report

Gamma Reference:	4125/5
Date of Issue:	29 November, 2002
Author:	Dr. M J Nash
Reviewed by:	Dr. D F C Brewer

GAMMA SECURE SYSTEMS LIMITED
Diamond House, 149 Frimley Road, Camberley, Surrey GU15 2PS
Tel: 01276 702500 Fax: 01276 692903
Web: http://www.gammassl.co.uk/

Contents

Change Control History

Version	Date	Reason for Issue
0.1	20 Nov 2002	Internal Review
0.2	22 Nov 2002	Draft for Customer Review
1.0	29 Nov 2002	Formal Issue

Management Summary

This is the Final Report on a security audit of the NPL iVR internet-enabled calibrations demonstrator system. The audit was performed by Dr. M J Nash of Gamma Secure Systems Ltd during October and November 2002. It describes how the audit was conducted, what security services are present in the demonstrator and how well those services meet the identified security requirements for internet-enabled calibrations. Finally, it documents the main conclusions and recommendations from the audit.

The audit first produced a generic security policy for internet-enabled calibration services, and then assessed the demonstrator against that policy, identifying the main security mechanisms used within the demonstrator. It concluded that these security mechanisms are not sufficient to meet all of the security requirements identified in the security policy. It recommends that any commercial calibration service should contain a number of additional security measures to those implemented in the current demonstrator. These are identified in the discussion of individual security services within the body of the Report.

1 Overview

1.1 Scope of the Report

This is the Final Report on a security audit of the NPL iVR internet-enabled calibrations demonstrator system. It was performed by Dr. M J Nash of Gamma Secure Systems Ltd during October and November 2002. It describes how the audit was conducted, what security services are present in the demonstrator and how well those services meet the identified security requirements for internet-enabled calibrations. Finally, it documents the main conclusions and recommendations from the audit.

1.2 Acknowledgements and Thanks

Gamma would like to thank Robin Barker and Graeme Parkin of the Software Support for Metrology Programme of the Centre for Mathematics and Scientific Computing, National Physical Laboratory (NPL) for commissioning this audit, providing information, answering questions and reviewing draft deliverables. Their enthusiasm, patience, care and thought are gratefully acknowledged.

Gamma would also like to thank the following additional members of the internet Demonstrator Project Team for their assistance in answering a long and not always very clear security questionnaire:

- Shakil Awan of the Centre for Electromagnetic and Time Metrology, NPL
- Simon Ashford of the IT Service Unit, NPL
- Stephen Bryant of the Centre for Electromagnetic and Time Metrology, NPL
- Mark Finch of Fluke (U.K.) Ltd.
- Luke Emmet of the Adelard Partnership.

2 Conduct of the Audit

2.1 Introduction

This section of the Final Report explains what was done during the Security Audit, and why.

2.2 Preparation of a Generic Security Policy for internet-enabled calibrations

The first step of the audit process was to prepare a security policy for internet-enabled calibration services: security policy in this sense means a high level set of security objectives, as for example defined in the widely used security management standard ISO/IEC 17799 (formerly known as BS 7799).

Gamma suggested an initial set of objectives based on its general knowledge of internet security and some background information on metrology and internet-enabled calibration services obtained from NPL.

This was then refined by face-to-face and internet discussion with representatives from the NPL Centre for Mathematics and Scientific Computing Software Support for Metrology Programme. Finally, a firm policy was produced and agreed. It is reproduced as Annex A to this Report.

During assessment of the demonstrator, it was noted that there may be an additional requirement for "unobservability" (see Annex A paragraph 19). Since this requirement could not be met by the type of internet-enabled calibration system currently envisaged by NPL, the policy has been left unchanged as that used in the assessment.

2.3 Assessment of the Demonstrator

The normal method of performing a security audit of an IT system would be to examine documentation and then perform a gap analysis against the relevant security policy. An audit visit would then be held to investigate the perceived deficiencies and determine if there were actual security weaknesses, and, if so, their potential impact.

As a Gamma research exercise, a slightly different approach was used: a significant number of different organisations and people were involved in developing the iVR demonstrator, and it would have been difficult to hold a single review meeting at which all of the relevant parties could have been present. In particular, different people and organisations had responsibilities for different aspects of the system, and a single meeting might not have reflected all valid views consistently.

Instead, an automated audit tool was used to develop electronic questionnaires on compliance to the security policy for each interested party to complete and return. The tool permitted each respondent to be asked only those questions relevant to their particular areas of authority and expertise. Following receipt of the completed questionnaires, the tool performed the gap analysis automatically.

Respondents found the questionnaire response part of the tool quite difficult to use; their specific difficulties and criticisms have been passed on to the developer of the tool. However, the tool was very effective at identifying areas of non-compliance and misunderstanding, and the overall result was probably more accurate and specific than the normal study and audit visit approach. The actual gap analysis took less than five minutes to execute – manually, it might well have taken at least half a day. On the other hand, preparing the questionnaires took best part of a day, so the overall technique is not particularly viable.

2.4 Analysis of Questionnaire Results

The output from the gap analysis tool was examined, and used to produce a Discrepancy Analysis Report. This was constructed by annotating each policy statement from the internet-enabled calibrations Security Policy with an analysis of how and how well the demonstrator had met that policy objective.

The Discrepancy Report was sent to NPL for comment, and then published with minor modifications as a final document.

2.5 Preparation of the Final Report

Finally, this Report was prepared, analysing the security issues found in the example system, where it was particularly weak or strong, and where additional security mechanisms can or must be recommended for any commercial service based on the demonstrator.

3 Security Issues

3.1 Introduction

The Generic Security Policy for internet-enabled calibrations identified ten security services as relevant to internet-enabled calibrations:

- Authentication
- Access Control
- Confidentiality
- Integrity
- Non-repudiation
- Availability
- Audit
- Privacy
- Certification
- General Protection.

Of these, the NPL Demonstrator Project Team ranked Authentication, Integrity and Audit as the most important, followed closely by Access Control. Confidentiality, Non-repudiation and General Protection were less important and the remaining services (Availability, Privacy and Certification) were considered not to be of significant importance.

Each of these services will now be considered in turn, in order of importance as ranked by the Project Team.

3.2 Authentication

Authentication in the demonstrator is achieved through the Secure Sockets Layer (SSL) secure channel establishment process. SSL is the most common form of security protection found in internet commerce. Originally developed by Netscape, it acts as an intermediate layer between the application and transport protocols used to provide communications between a web browser and a web server. The protocol is supported by all widely available web browsers and servers. The latest version has been adopted as an internet standard (RFC) under the name Transport Layer Security (TLS).

Within the demonstrator, SSL is used by the client to authenticate the server, and the secure channel that is then set up is used to pass a password from the client to the server in order that the server can authenticate the client. For the demonstrator, the relevant packages used were Apache/SSL for the CSP server and Internet Explorer 5 running under Windows 98 for the customer PC client. Default settings were used for both Apache/SSL and Internet Explorer.

SSL is a fully adequate mechanism to meet the demonstrator authentication requirements. However, there were a number of weaknesses in the demonstrator configuration. These weaknesses will now be discussed in turn.

Windows 98 does not guarantee that information held on a computer cannot be extracted, even if explicitly deleted. Thus it might be possible for an impostor with physical access to the customer PC to extract the password and masquerade as the legitimate user. Indeed, it is usually possible to instruct IE5 to cache passwords so that they do not have to be entered each time a connection is established. Since Windows 98 does not authenticate users of the PC, anyone with access to the client can potentially establish a calibration session.

There are two possible counters to this problem. The first is to rebuild the client PC using an operating system from the Windows range that has better security functionality, i.e. NT, 2000 or XP. All of these can be configured to ensure that all access to the PC is blocked until a logon password is entered, thus ensuring that the user is authenticated to the PC. In addition, all these operating systems provide further security measures that would make misuse much more difficult. In particular, access control lists could be used to restrict use of the demonstrator client software to known and approved users, and the object reuse mechanisms would make password scavenging far more difficult.

The second counter is to configure the CSP server to require the client to present an SSL certificate to the server as part of the SSL Handshake Protocol secure session initiation. Essentially, this removes the need for the user to remember and offer a password to the server. However, this only proves that the demonstrator client PC is being used, not that its user is the authorised customer. In conjunction with the logon controls from a more secure version of Windows, this would provide the greatest assurance that the user of the demonstrator service is a legitimate customer.

Using client certificates requires a secure certificate distribution system from the CSP to the customer. So long as all access is made using a PC supplied by the CSP, this process is trivial – the certificate can be preloaded before despatch. If access if permitted from customer provided PCs, certificates must be transmitted by some agreed secure means – for example, as a file on diskette sent by post.

It is possible for a user to configure IE5 such that warnings about invalid server certificates are suppressed. In this case, a rogue server could masquerade as the CSP server and establish an SSL connection, and then for example ask for and obtain the user's demonstrator password. However, the risk associated with this weakness is low as it would be difficult to exploit, and relies on the user first setting IE5 into a less-than-fully secure configuration. It is possible to program or script the client software to override this browser setting.

There is also a potential weakness in the way that the client password is transmitted to the server. It is protected against interception by SSL encryption, and this can be disabled. For further details see the confidentiality service discussion below.

Since the client authenticates to the server, there is a risk that a third party might masquerade as a legitimate demonstrator user and successfully log on after a brute force attack of trying lots of possible passwords. The counter to this is to set rules on the format of permitted legitimate passwords, such as minimum length, or other

constraints such as insisting that there is at least one non-alphabetic character included.

In practice, despite these weaknesses, it is likely that both CSP and customer could verify that the other party was the intended participant with sufficient confidence to support a commercial service, based on the demonstrator system.

3.3 Integrity

Integrity in the demonstrator is achieved by a combination of four mechanisms:

- use of SSL message integrity checks to confirm that data has not been modified during transmission over the internet;
- authentication controls on the CSP server to ensure that only authorised CSP staff can access or modify calibration data stored on the CSP server;
- an internet firewall at the CSP site to prevent unauthorised internet users accessing the calibration service or data;
- not storing persistent calibration data on the client PC between calibration sessions.

There is no protection against authorised CSP users making improper modifications to calibration data, or against unauthorised access to the PC supplied to the customer for use as the demonstrator client by anyone with physical access to it.

Since the client initiates all internet connections, and will expect a valid CSP server certificate in response, it would be exceptionally difficult for any third party to modify software or data on the client by establishing a connection over the internet during a legitimate calibration session. Of course, if customer staff use the client PC for other purposes such as connecting to other internet sites, anything is possible on a Windows 98 machine.

The major weakness is therefore the lack of effective access controls to the client PC. Although no persistent calibration data is stored on the client between calibration sessions, there are no controls to prevent modification of the client software, which would enable a malicious user to subsequently access or modify calibration data. The countermeasure would be to upgrade the client PC to a more secure version of Windows, as described under Authentication, and use access control lists to limit non-execution access to the demonstrator client software to a CSP administrator account only, not accessible by the customer.

There is no way that authorised CSP staff can be prevented from making improper modifications to calibration software or data, whether on the server or the client, as there is no way that the system can easily distinguish between legitimate and unauthorised changes.

There is a potential weakness due to the integrity algorithm options permitted by the SSL protocol. When setting up an SSL session, the client offers choices to the server for both secret-key and one-way hash algorithms. The secret key algorithm is used to provide message confidentiality, the one-way hash to provide message integrity. The

server chooses one of each of the options offered or otherwise rejects the proposed connection.

The three one-way hash algorithm choices that the client can offer the server are:

- Message Digest 5 (MD5), a proprietary algorithm developed by RSA Data Security;
- Secure Hash Algorithm (SHA), a US Federal Standard;
- none, i.e. no checking.

IE5 will by default offer all of these, and Apache/SSL will select MD5 by choice but will by default accept any that is offered – including <none>.

IE5 can be configured to offer a lesser set, and Apache/SSL can be configured to reject some or all of the possible choices. The way that IE5 is configured is extremely complex as the algorithms actually form part of the underlying operating system and at one time some algorithms were not supported in copies sold legally outside the US, or were only supported in a weakened form. Unfortunately, US forms of both operating system and browser upgrades would upgrade the algorithms used regardless of the original export status, and following relaxation of US export controls, application of later patches sourced from anywhere in the world would also upgrade the algorithms. Without looking at registry settings, it is therefore impossible to be absolutely certain what algorithms are currently being offered by the browser.

Misuse of SSL in this way is extremely unlikely, but would not be obvious in ordinary use: the padlock will still indicate a secure connection and the fact that data is not necessarily being checked for integrity would not be visible to the user.

It is therefore recommended that the <none> hash option is disabled. It is only permitted in older versions of the SSL protocol, and is disabled by removing SSL Version 2 from the list of permitted protocol versions.

For IE5 running on modern Windows platforms, this is best done by editing Registry entries. Microsoft Knowledge Base article Q245030 provides details. The way that Apache/SSL is configured to reject <none> for the hash algorithm depends on the version of SSL in use, but usually involves a rebuild with an SSLBANCIPHER NONE command.

Improper modification of calibration data by authorised CSP staff cannot be prevented, and this weakness must therefore be accepted in any commercial service based on the demonstrator. It should be noted that the audit and non-repudiation services that would minimise the impact of this weakness are also not fully satisfactory. The ease with which anyone with physical access to the client PC can modify software or encryption settings is not acceptable in a commercial service. The use of default hash algorithm settings and a browser with indeterminate algorithms is unlikely to present a real security risk in practice, but is likely to give a poor public perception of the service if known about. With these exceptions, the integrity mechanisms in place do provide adequate protection against unauthorised modification.

3.4 Audit

The audit requirement for internet-enabled calibrations is that a third party can subsequently determine that a calibration took place, and determine the measurements, values and outcome of calibration. Sufficient information is held in the calibration database to meet this requirement, but unfortunately there are no controls to prevent the relevant database entries being subsequently modified or deleted by CSP staff – deliberately or by accident. In addition, there is no policy as to how long the information is retained.

It is therefore recommended that an information retention policy is developed, including procedures to make archived copies of the data from completed calibrations. The copies should be stored securely away from the CSP system, for an agreed minimum period of time, so that they can be used to prove to third parties what actually happened at the time of calibration.

These additional services should be provided in any internet-enabled calibrations commercial service.

3.5 Access Control

There is no functionality in the customer PC client software that would enable the CSP to gain access to non-calibration customer resources (and, since the PC is CSP property, it should not have any non-calibration data or software on it, anyway).

The CSP firewall restricts access from the internet to the CSP server to HTTP/HTTPS traffic. The CSP server uses the customer's authentication password to limit access on the server to only that customer's calibration data and other resources. This is implemented using standard operating system and database controls.

There are no obvious access control weaknesses.

3.6 Confidentiality

Confidentiality is achieved by analogous mechanisms to those used to maintain integrity of calibration data that have already been discussed, namely:

- use of SSL secret key encryption to encrypt data during transmission over the internet;
- authentication controls on the CSP server to ensure that only authorised CSP staff can access calibration data stored on the CSP server;
- an internet firewall at the CSP site to prevent unauthorised internet users accessing the calibration service or data;
- not storing persistent calibration data on the client PC between calibrations.

Calibration traffic on the HTTPS socket is encrypted using an SSL session key, which means that third parties intercepting the internet traffic would not be able to decode it. This also applies to the webcam images, which are encoded as base64 and included in

the XMLRPC stream. There is currently no requirement to conceal from other parties that an internet-enabled calibration is taking place, and in fact the identities of both the CSP and the customer can be deduced from their internet addresses. Since there are no other secure services offered by the CSP, an eavesdropper could deduce that a calibration is taking place from the fact that an SSL session is in progress. The eavesdropper could therefore easily identify when a new customer started using the CSP's service and this might not be acceptable to some potential customers.

It might also be possible for the eavesdropper to deduce the nature of the standard being calibrated by traffic flow analysis of the volume of traffic or the number of interchanges of data. Such an analysis would be very difficult in practice, even if the messages could be consistently intercepted, and this weakness is therefore judged to be an acceptable risk.

There is no protection against authorised CSP users accessing calibration data without authorisation, or against customer staff reading data without authorisation by making unauthorised access to the PC supplied for use as the Demonstrator client. These weaknesses have already been assessed above as integrity weaknesses and countermeasures proposed.

There is a final potential weakness due to the encryption algorithm options permitted by the SSL protocol, analogous to the weakness already described in message integrity protection. When setting up an SSL session, the client offers choices to the server for both secret-key and one-way hash algorithms. The secret key algorithm is used to provide message confidentiality, the one-way hash to provide message integrity. The server chooses one of each of the options or otherwise rejects the proposed connection.

The five secret-key algorithm choices that an SSL/TLS client can offer its server are:

- Fortezza, a US Government hardware based encryption algorithm;
- DES, the Data Encryption Standard (including use of Triple DES with longer keys);
- RC2, a proprietary algorithm developed by RSA Data Security;
- RC4, another proprietary algorithm developed by RSA Data Security;
- none, i.e. no encryption.

Some of these can be offered with different key lengths – for some years US products that supported 40 bit keys could be exported more easily than those with longer keys.

IE5 does not support Fortezza but can offer all the others – the key lengths offered depend on how and when IE5 was installed or last upgraded. Apache/SSL supports all five choices with a variety of key lengths, and in addition supports the IDEA algorithm, as used in PGP. The combinations of key length and algorithm supported are extremely complex, but in practice the most likely algorithm to be selected, if offered, is RC4 using 128 bit keys.

Both IE5 and Apache/SSL implement the <none> option, and there is therefore a risk that it will be offered and selected, particularly if one product is an export restricted

version and the other has been configured to reject short keys. Misuse of SSL in this way is extremely unlikely, but would not be obvious in ordinary use: the padlock will still indicate a secure connection and the fact that data is not encrypted would not be visible to the user.

It is therefore recommended that the <none> secret key option is disabled. For IE5 running on modern Windows platforms, it is disabled by default. This can be confirmed by checking the relevant Registry entry. Microsoft Knowledge Base article Q245030 provides details. The way that Apache/SSL is configured to reject <none> for the secret key algorithm depends on the version of SSL in use, but usually involves a rebuild with an SSLBANCIPHER command.

As stated above, SSL permits 40 bit key versions of RC2, RC4 and DES to be used as well as the full strength versions. In practice, the short key length versions would offer perfectly adequate confidentiality protection against anyone without National Security Agency capabilities. However, there is a public perception that 40 bit keys are inadequate for commercial use, and it is therefore recommended that the IE5 browser is checked and if necessary upgraded to use full length keys, and that Apache/SSL is configured not to permit use of 40 bit keys.

It must be stressed that forcing the use of no encryption or of exploiting weak keys over the internet would be difficult to engineer and exploit. However, the public perception is different, and therefore the weakness should be addressed.

There are no significant confidentiality weaknesses that are not also integrity weaknesses.

3.7 Non-repudiation

There is a session log on the CSP server that includes timestamps, which can be used as evidence or calibration activities by the CSP. However, there are no mechanisms that prevent the session log from being modified subsequently, and thus in evidential terms its value is limited.

The customer has no way to prove what he did or when he did it, other than the description on the invoice or bill from the CSP of the service provided. The CSP application displays uploaded GPIB data back to the customer. This could be photographed or recorded by the customer as evidence that the CSP had received the data, but of course the display could easily be faked or refer to data that was subsequently modified.

Once a physical certificate is issued, it is impossible for either party to deny that calibration took place, or to deny the results of calibration as stated on the certificate. This may be sufficient in practice to meet market requirements; if not, the current mechanisms are inadequate. Possible additional mechanisms are discussed below under Certification.

3.8 General Protection

This refers to the use of good security design practice throughout the calibration service.

There are two major areas where best practice is not followed: SSL configuration and client operating system.

As described under integrity and confidentiality above, the SSL Handshake Protocol contains options for the security algorithms to be offered and accepted. Some of the possible choices are not secure or use (theoretically) weaker keys. It is not good design practice to permit default choices to be offered and chosen by the client and server respectively , particularly as the default choices within by the chosen client (Internet Explorer 5) vary depending on when and how it was installed. It is recommended that the algorithms offered and accepted are set explicitly. There is nothing to be gained by permitting more than one algorithm of each type. 128-bit key RC4 as the secret key algorithm and MD5 as the hashing algorithm would be the normally commercial choices, although DES and SHA would be equally suitable. For HMG use, the recommended algorithms are specified in CESG Manual T – and are Triple DES and SHA respectively. It is really a marketing decision whether to go with the CESG recommendations or normal commercial best practice.

The customer is supplied with a dedicated and pre-configured laptop PC for use as the calibration service client. The customer's ability to misuse the demonstrator system is supposed to be limited by the provision of this custom client with very limited customer configurability. Unfortunately, the current client operating system, Windows 98, is not generally regarded as a suitable platform for secure applications as it lacks effective authentication and access control services.

It is recommended that the client is upgraded to a secure Windows platform (Windows NT, 2000 or XP), built in such a way that the user's logon account has only execute access to the demonstrator client, and therefore is unable to read or modify the application code. After configuring suitable access controls, this would also enable calibration information to be retained on the client in a way that could not be modified by the customer, but would provide independent evidence of calibration results if the copy on the CSP server was subsequently corrupted or modified.

3.9 Availability

There are no requirements to provide any guaranteed minimum quality of service, minimum periods of availability or maximum calibration time. The customer can cancel a calibration session before it is finished through a menu option. Otherwise a session can only be terminated by drastic action such as server shutdown or aborting the application. This is not seen as a significant weakness.

3.10 Privacy

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).

It would theoretically be possible for a competitor to determine that a calibration was taking place, or to detect that a new customer was using the calibration service, or even to establish the type of standard being calibrated, but not to determine the results of the calibration.

A customer might not want competitors to know that a new type of standard was being calibrated, but none of these theoretical attacks are seen as a significant weakness.

3.11 Certification

At present, all certificates are physical in form. The issue of electronic certificates was considered to be out of scope of the audit. A certificate, once issued, can be linked to entries in the calibration database, but there is no policy on how long the relevant information would be retained, and no way to prove that the database information had not been modified after the certificate was issued.

This may be sufficient to meet market and accreditation requirements; if not, a policy is needed on the validation lifetime of certificates, and mechanisms needed to prove that retained results have not been modified. This could be achieved by hashing the calibration results and printing the hashed value on the certificate; a suitable algorithm is already present in the server as part of SSL.

4 Further Issues

4.1 Introduction

This section of the Report deals explicitly with a number of specific issues that were identified in the Audit Terms of Reference. In most cases, there is little of note to add to the policy based coverage of the previous section.

4.2 Directory-Based Web Access Control

There is a lot of interest currently in the remote execution of access control restrictions over the internet; this is often referred to as "single sign on", but the underlying technologies such as Microsoft Active Directory and the Lightweight Directory Access Protocol LDAP are of wider application.

Although the CSP holds calibration data relating to more than one customer, the customer is not able to access that data other than through the calibration application. Similarly, no calibration data is kept on the client PC between calibration sessions. Thus the question of web based access control does not currently arise. Without a major change to the calibration service model, whereby customers would be permitted to access raw data held on the CSP server, these technologies are irrelevant.

4.3 Integration of Remote Calibration Operations with Firewalls

Currently the demonstrator uses a single host server at the CSP, and uses only two TCP/IP services, HTTP and HTTPS, to establish its SSL encrypted communication. Only a limited number of TCP/IP ports need to be enabled. This is about as simple a form of internet communication as you can get, and any commercially available firewall will be able to be configured to pass this traffic and block all other traffic to and from the CSP server. This is commercial best practice and cannot be easily improved.

4.4 Transmission of Formal Calibration Certificates Over the Internet

NPL currently has no plans to offer electronic certificates, thus this topic was not addressed during the audit.

4.5 Use of a Customer PC for the Calibrations Client

Providing a pre-configured PC for use as the calibration service client not only reduces interfacing and support problems, but also provides a potentially much more secure platform for the customer to use. Unfortunately, this is currently spoilt by the choice of Operating System for the client, which provides no protection against customer corruption or misuse.

It would be possible to provide a pre-packaged application for the customer to install on his own PC. It would also be possible to add a facility whereby the server could confirm by checksumming that the application has been correctly installed and has not

been modified or had persistent data altered. The necessary algorithms are already present as part of the support for SSL.

5 Conclusions and Recommendations

5.1 Conclusions

It has been possible to develop a Security Policy for internet-enabled calibrations; the agreed version of that policy is attached to this Report as Annex A.

A security audit of the NPL iVR Metrology Demonstrator has been successfully conducted against that policy and identified that the main security mechanisms used within the demonstrator were:

- use of the Secure Sockets Layer (SSL) protocol to protect data in transmission over the internet;
- authentication and access controls on the CSP server to ensure only authorised CSP staff can access or modify calibration data stored on the CSP server;
- an internet firewall at the CSP to prevent unauthorised internet users accessing the calibration service or data;
- provision of a dedicated and pre-configured laptop PC to the customer for use as the calibration service client, with no calibration data stored on the PC between calibration sessions.

These security mechanisms are not sufficient to meet all of the security requirements identified in the security policy. The main security weaknesses identified in the demonstrator were:

- There is only weak authentication of the customer – physical access to the client PC for a short period of time could enable a third party to masquerade as the customer.
- The client PC software is not protected against modification or copying by anyone with physical access to the PC.
- There are no mechanisms to prevent or deter authorised CSP users making improper access or modifications to stored calibration data.
- Through the use of default settings, there are theoretical weaknesses in the use of SSL.
- The customer has no independent way to prove what he did or did not do during a calibration session, other than the information on his invoice.
- The only evidence of completed calibrations is stored in the calibrations database. There is no policy on the retention of calibration data, and data can be modified after a certificate has been issued without detection.
- The information on a calibration certificate cannot be independently verified by a third party.

Some of these weaknesses impact on areas of security policy (authentication, integrity) that were judged important by the Demonstrator Project Team. Some additional security measures are therefore likely to be required.

5.2 Recommendations

There are a number of areas where it has been recommended that any commercial internet-enabled calibration service should contain additional security measures to those implemented in the demonstrator. These are identified in the discussion of individual security services. However, in summary, the key issues are:

- The client PC provided to the customer should be based on a version of Windows with greater security features. This would have the following benefits:
  a) a logon password could be used to authenticate the user of the client PC, rather than relying on weak authentication to the CSP server;
  b) by restricting the access granted to the customer, calibration software and data could be protected from misuse by the customer or third parties;
  c) an independent audit record of calibration actions and measurements could be kept on the client PC.
- Use of SSL should be reconfigured to require both client and server certificates. If not, rules should be set to force use of strong passwords when establishing a calibration session.
- The use of SSL should be explicitly configured to reject null or weak algorithms, although recognising that weak algorithms would provide adequate protection for calibration purposes in practice.
- A policy is needed on the verification of certificates. This policy should define how a third party would verify that a certificate was valid, and for what period of time verification would be possible. In consequence, it would be necessary to:
  a) archive calibration data used to issue a certificate outside of the calibration system;
  b) retain that data for the declared period of time;
  c) provide a way that a third party can confirm the validity of a certificate;
  d) provide a way (such as digital signature) that the customer can confirm that the results of calibration have not been changed after the certificate was issued.

Appendix 1 – Generic Security Policy for internet-enabled calibrations

Concept Definition

1. An internet-enabled calibration takes place between two parties – the **Calibration Service Supplier** (**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. [Electronic certificates and certification are a distinct issue, to be addressed separately.]

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 (CESG).

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.

Attachment 2

Report on Data Warehousing and Storage

(Baltimore Technologies)

REPORT ON
DATA WAREHOUSING AND STORAGE
FOR THE
NATIONAL PHYSICAL LABORATORY

BY

BALTIMORE TECHNOLOGIES (UK) LIMITED

EME-00293-01-03-01

Written by: Ian White

Version: 1.1

Date: 26th March 2003

Approved by:

Baltimore Technologies (UK) Limited, Innovation House, Mark Road, Hemel Hempstead, HP2 7DN
Tel: +44 (0) 1442 342600 Fax: +44 (0) 1442 266438
Website: www.baltimore.com

DOCUMENT HISTORY

Version	**Date**	**Description**
0.5	27 January 2003	Final Draft version of report
1.0	3 March 2003	First version
1.1	26 March 2003	Minor change to remove "client confidentiality" classification

Written by:	Ian White
Date:	26 March 2003
Signature:	
Quality Reviewed & Approved by:	
Date:	
Signature:	

CONTENTS

1 MANAGEMENT SUMMARY

Baltimore Technologies have been requested by the NPL to conduct a paper based security review of the data warehouse associated with the internet Voltage and Resistance (iVR) system. This system is the first internet-enabled calibration to use the generic iCal software, which is being further developed under the DTI Software Support for Metrology (SS*f*M) programme.

The data warehouse is a central repository of information about the NPL Customers, environmental factors associated with a particular set of measurements and the measurement data itself from the Customer Standard. The stored measurement data may be nominated by the Customer to be used for certification purposes. Access by a Customer to their data is managed through an internet-based administrative interface by NPL.

The main conclusion from the review of the security of the data warehouse is that the main security requirement is to protect the integrity of the measurement data and associated environmental information. This is particularly true when a set of captured measurements form the basis for NPL to certify a Customer Standard. Unauthorised modification of the measurement data either before or after the certification process might lead to the NPL suffering a loss of reputation and possible litigation in the event of a third party relying upon the result of the certification. To mitigate the risk of inadvertent or deliberate modification of the measurement data we recommend that the captured information should be associated with a cryptographic HMAC value. This encrypted message digest value will enable the NPL to detect any changes in the measurement data and assist in the fulfilment of any request to provide historical measurement data for evidentiary purposes. If and when there is a future requirement for a third party to be able to verify across the internet that an NPL Certificate and the associated measurement data is genuine, then we recommend that the use of digital signatures based upon public key cryptography should be investigated as a possible alternative technique.

The confidentiality of the Customer details and associated measurement data is important, but we believe that the existing network and application security controls, in conjunction with the physical protection of the server at the NPL, provide an appropriate level of protection for the majority of the stored data. One exception is where the customer user password value is stored within the database in a ‘clear’ format. In line with security best practice, we recommend that these password values are stored as message digests. Note that there is an underlying assumption that the information held in the Data Warehouse is commercially confidential but not formally protectively marked, for example under CESG InfoSec Guidelines. Should information that has been protectively marked be stored in the Data Warehouse then the use of data encryption, possibly using an approved hardware-based product, would need to be reviewed.

There does not appear to be a high requirement for availability of the Data Warehouse and we recommend that the development and testing of operational processes for data backup should be adequate.

The choice of hardware and software platforms appear to be adequate from a security point of view, providing recent security vulnerabilities in the MySQL product are fixed through the implementation of the appropriate patches.

Finally, whilst this report focuses specifically upon the iVR system it is anticipated that the conclusions and recommendations will also apply to other applications using the same approach to Internet-enabled calibration.

2 INTRODUCTION

Established over 100 years ago, the National Physical Laboratory (NPL) is the UK's national standards laboratory and provides accredited measurement, calibration and testing services to a wide range of customers.

Under the DTI Software Support for Metrology "SS*f*M" programme the NPL has been investigating the use of Internet based calibration "iCal" systems. Under this programme, measuring instruments may be installed at a customer location and the measurement data associated with the customer standard may be collected and analysed at a central location.

The iCal system is designed to be flexible, supporting a number of different calibration services by the NPL. In each case the appropriate measurement equipment will be deployed at the customer site and connected through the internet to a server located at the NPL. The measurement readings, as well as other appropriate environmental information, will be stored within an NPL Calibration Data Warehouse. Customers may subsequently access their own measurement results held within this Data Warehouse, through an internet-based interface. The Customer can elect to use their measurement data in conjunction with the NPL certification process.

The internet-based DC Electrical Voltage and Resistance "iVR" project is one of the first of the proposed iCal systems to be developed. In conjunction with two external organisations, Adelard and Fluke, the NPL have deployed an initial system that supports the remote calibration of a Customer Standard using the Fluke 4950.

As an accredited organisation, the NPL is itself subject to inspection and assessment through UKAS in order to ensure that the certification process is performed in accordance with agreed procedures.

2.1 Objectives

The objective of this work is to assess the security requirements for the Data Warehouse containing Customer measurement data, located at the NPL.

2.2 Scope

The scope of this study is identifying the security requirements for information held locally in the Data Warehouse at the NPL.

The scope includes providing recommendations on the secure medium-term storage of the information.

The scope does not include the security of the application, or the network connection between the Client and Server.

The scope does not include the security of the Customer location, or that of the NPL itself.

The scope does not include an assessment of the security of the client or server platforms and their associated security related system software configuration settings and parameters.

2.3 Assumptions

The main assumption is that the iVR application, equipment and associated infrastructure are protected from both internal and external attack to a level commensurate with the value of the information processed within them. For example, through NPL implementing suitable network controls (e.g. SSL) and appropriate physical security measures.

The assumption is also made that the information held within the data warehouse is derived from systems that have not been protectively marked in line with HMG guidelines. The maximum required level of confidentiality for the measurements and customer related information is assumed to be ‘Customer Confidential’.

3 SYSTEM DESCRIPTION

3.1 The Internet DC Voltage and Resistance (iVR) System

This slide (Figure 1), taken from a joint presentation on the system by the iCal consortium partners, Fluke, Adelard and NPL, shows the main system components for the iVR and their relationship to each other.

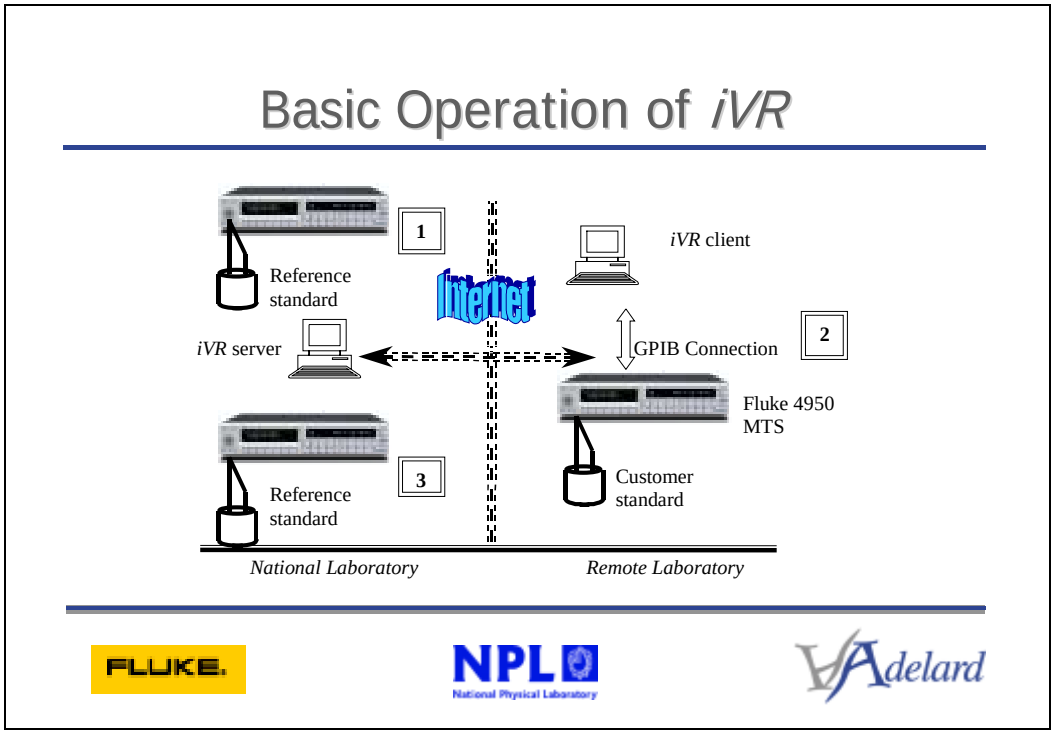


Figure 1 - iVR Basic design

The Fluke 4950 is tested at the NPL and then calibrated against the National Reference Standard (step 1). The performance of the Fluke 4950 is then characterised across a range of environmental conditions (e.g. temperature, humidity and changing main supply). This data is stored for subsequent calibration calculations.

The same Fluke 4950 is shipped to the NPL Customer, along with the iVR Client and associated equipment, for example a temperature sensor and the Webcam.

At the Customer site, the equipment is unpacked and set-up by the Customer. As part of this process the Customer will log into the iVR server, using the iVR client, and enter details about the measurements to be conducted. For example the type of measurement, range of measurement, number of measurements and other related information. The Webcam will also be connected and positioned so that the Fluke 4950 and the Customer Standard are fully visible to the NPL.

One or more sets of measurements will be generated using the Customer Standard and transmitted to the server where they will be placed in the iVR Data Warehouse. Information about the environment, for example the internal Fluke 4950 temperature, and a snapshot from the Webcam of the customer equipment and its connections will also be stored in the Data Warehouse as part of each set of measurements (step 2).

When the session is completed the Customer will log out of the server. The Customer may subsequently log onto the iVR server to conduct further measurement sessions. At the conclusion of all of the measurement sessions the Fluke 4950 and associated equipment will be either returned to the NPL or possibly transported to another NPL Customer.

When the Fluke 4950 is finally returned to the NPL it will again be tested against the National Reference Standard. This testing checks that its characteristics have not significantly altered during the Customer measurement process (step 3).

The main equipment located at the Customer site, including the Fluke 4950, Customer standard and Client laptop with Webcam attached, are shown in Figure 2.

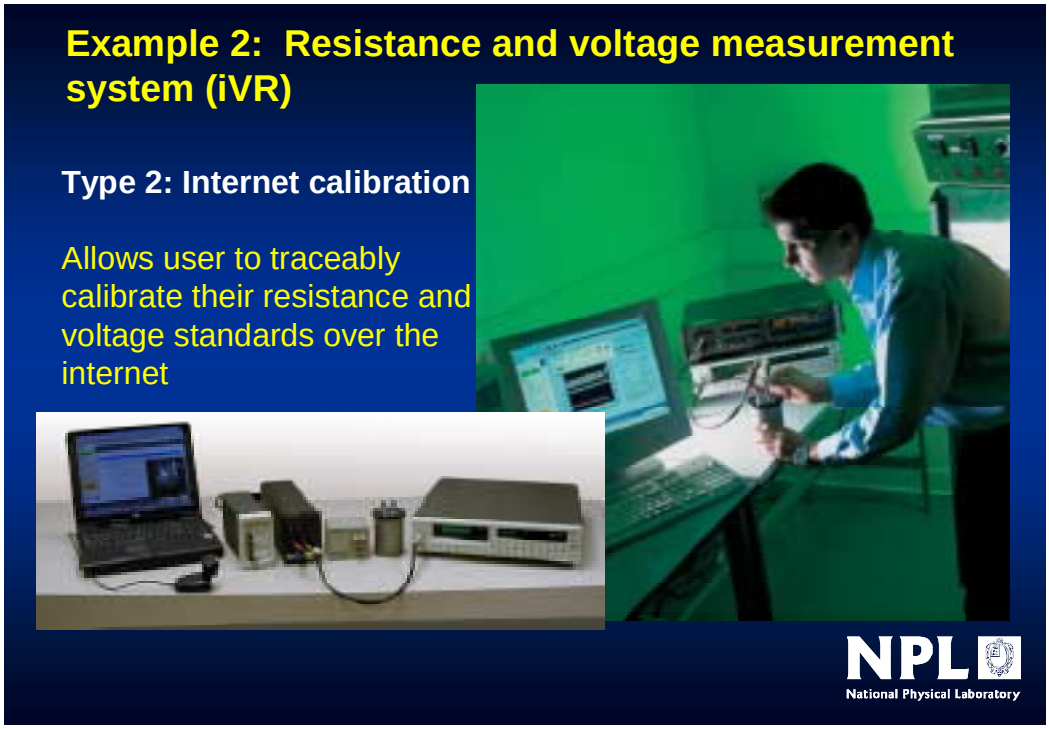


Figure 2 - iVR Equipment

The Customer is able to review their stored measurements either as part of a measurement session or subsequently when they log onto the iVR server through the internet.

The Customer can also decide which of their measurements, if any, are to be submitted to the NPL certification process. The certification process will review the measurement data, in conjunction with any 'correction data' relating to the specific environmental conditions associated with the measurements. These environmental corrections are also stored in the Data Warehouse and form part of the data used in conjunction with the certification.

Finally, the Customer interface provides a number of administrative functions that enable NPL to manage the users on the system. For example, creating a new Customer userid that can access the data for that Customer.

3.2 The Data Warehouse

The data warehouse comprises a relational database, defined using the MySQL open source software. Online access to the database will be through PHP scripts running on the iVR server. The same database is currently used for all customers of the iVR service. For the purpose of this report the term data warehouse will be considered to include the Customer and system data, metadata held in the database, and backup other media containing copies of the data.

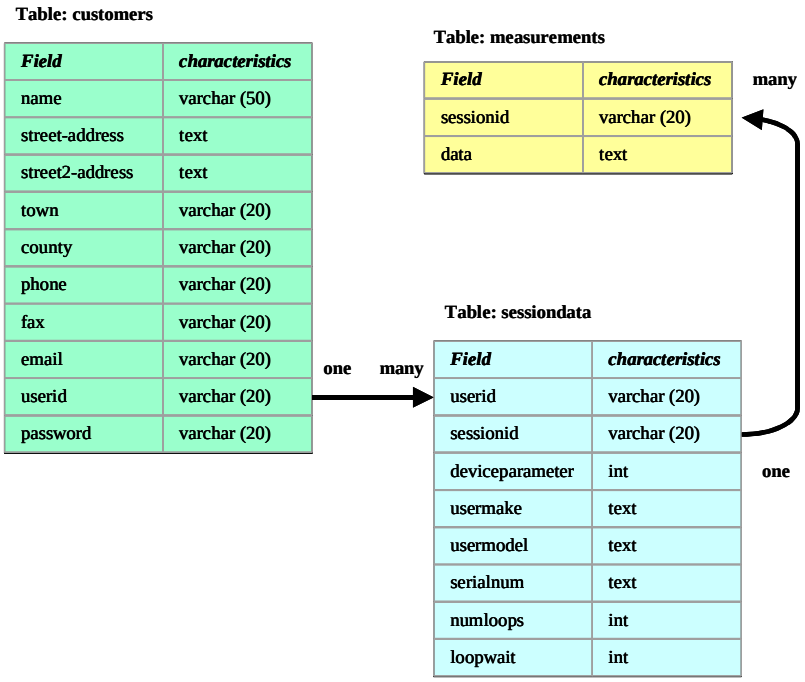


Figure 3 - Data Warehouse schema (main tables)

The main parts of data warehouse database schema are shown in Figure 3. This shows that the database is logically split into the three main tables 'customers', 'sessiondata'

and ‘measurements’. In addition, there are also Customer related images captured from the Webcam and details of any environmental corrections that need to be applied to the measurement data.

When a user starts a new session, or attempts to gain access to data from a previous session, their entered userid and password details will be checked against the values held in the ‘customers’ database table. The PHP scripts ensure that only the data linked to that user can be accessed. The built-in security access controls within MySQL are not used to directly control this access.

For a particular Customer there are likely to be a number of sessions, each of which will have been allocated a unique identifier or sessionid. Each of these sessions will in turn be linked to one or more sets of measurements stored in the database.

The measurement data will include a status flag that indicates whether or not this set of measurement data is being submitted to the NPL certification process.

When a Customer Standard is certified by the NPL, the measurement data and any associated environmental corrections form an integral part of that certification.

4 DATA WAREHOUSE SECURITY

4.1 Security Requirements

This section briefly discusses the main security requirements and associated required controls for the information assets held within the data warehouse. Recommendations for enhancements to the existing controls are provided, where a possible control weakness has been identified.

When considering the security requirements associated with the iVR Data Warehouse it is useful to separate the requirements into those that relate to the confidentiality of the data, those that relate to the integrity of the data and those that relate to the availability of the data. A fourth category for non-repudiation is also considered, where the data or meta-data held within the data warehouse might be required for evidentiary purposes. For example, where the measurements held in the data warehouse provide the basis for the NPL certifying a Customer Standard and there is a subsequent dispute concerning that Customer Standard.

Further details on the security requirements associated with the iVR Data Warehouse information assets are provided in Appendix A of this report.

4.2 Protection of the Data Assets

The design of the iVR system includes the 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, from unauthorised disclosure and/or modification during transmission. The protection of the data held in the data warehouse is through a combination of the physical security controls surrounding the server and the use of PHP scripting. Internet based Customers are required to enter a valid userid / password combination, that is checked against values stored within the data warehouse. Providing they enter a valid userid / password combination, they will be granted the appropriate level of access to the sets of measurement data and static information (e.g. address details) relating to their company.

NPL will be responsible for maintaining Customer userids and passwords, with values being stored in clear[1] format in the database. The measurement data is also stored in clear format within the data warehouse.

We believe that the main threat to the confidentiality of the system would be from the unauthorised disclosure of a valid userid / password combination. These values would enable an attacker to gain direct access to customer information through the normal online viewing interface. We believe that access to this information may provide a

[1] The term ‘clear format’ indicates that the values are stored unchanged in the database and would be intelligible to someone who had access to the record.

commercial advantage to an attacker, and if discovered would lead to a possible loss of reputation to the NPL. Although an attacker with a valid userid / password combination might also be able to create new measurement data, we believe that this is unlikely as they would also need access to the appropriate NPL supplied equipment.

Although the userid and password values are protected during transmission, they are not protected at the end-points. That is within the client, server or for that matter on any backup media for these systems. We recommend that the password values are not stored as clear values upon the database but should be held as message digests. Ideally the user entered password value would be converted to a message digest value using a suitable one-way-function (e.g. SHA-1 or MD5) as soon as possible. The calculated digest may then be compared to the stored digest value for that userid through the PHP scripts.

Under normal circumstances we do not believe that the encryption of the Customer measurement data, or for that matter other application information held with the data warehouse, is necessary. One possible exception to this rule would be where the measurements from the Customer Standard are considered as being particularly sensitive. For example, where the measurements are given an HMG protective marking greater than RESTRICTED. Under these circumstances it will be necessary to investigate the implementation of appropriate encryption mechanisms to protect the data from unauthorised disclosure. For example, implementing CESG approved products for implementing hardware-based disk encryption.

The data warehouse holds the measurement data, including the set of data that a Customer decides should be used for certifying their Standard. Unauthorised changes to this information may influence the outcome of the certification process, possibly leading to a certificate being erroneously granted or for that matter denied, by the NPL.

Whilst we believe that unauthorised changes to the measurement data is unlikely to happen, we do however believe that the NPL should provide integrity protection for the set of measurement data that is used during the certification process. This will also enable the NPL at a later date to provide evidentiary proof in support of their certification of the Customer Standard. We therefore recommend that the data used during the certification process should be cryptographically protected to detect unauthorised or inadvertent modification.

The simplest form of integrity protection is to generate a message digest or possible a message authentication code (MAC) value for the data, using one of a number of commonly available algorithms. The disadvantage with this approach is that an attacker might alter the measurement data and then re-create the digest or MAC value using the same algorithm. To ensure that this is not possible we recommend the use of a keyed MAC, based upon the HMAC process[2]. This process creates a 160-bit message digest value from the data (using SHA-1) and then encrypts this value with a secret 3DES key, known only to the NPL.

[2] Refer to rfc2104, available from www.ietf.org, for a description of the HMAC process

Looking to the future, the NPL may decide to extend their range of internet-based services to include an internet Customer Standard certification status checking service. If such a future service uses public key cryptography to digitally protect the certificates then we would recommend that the use of digital signatures should also be investigated in order to protect the measurement data from unauthorised modification. This would replace the HMAC scheme proposed for the service.

The other type of unauthorised or inadvertent change to the data warehouse to be considered is where the data warehouse is corrupted or perhaps destroyed and becomes unavailable. The regular taking of backups, and the testing of restore procedures by the NPL should protect against this possibility.

The backup media itself will need to be protected from attack, and we would recommend the use of a fireproof safe for this purpose, ideally located at another site to the data warehouse itself.

Finally, the MySQL software includes security and system related functions for database administration. Access to these high privilege functions provides a user with the ability to view and modify all the information held within the database. There have been a number of recently published MySQL security related vulnerabilities that might allow an attacker to gain access to these system functions. We strongly recommend that these vulnerabilities should be investigated and where appropriate fixed through the implementation of the appropriate erratum packages to upgrade the iVR Data Warehouse software to MySQL 3.23.54a.

APPENDIX A SECURITY REQUIREMENTS

A.1 Confidentiality

This section provides a short analysis of the main security requirements for the **confidentiality** of the data assets. That is, the need to protect the Data Warehouse information assets against unauthorised disclosure. As the measurement data may be used in support of an application for a Customer Standard to be certified by the NPL, the possible implications arising from unauthorised disclosure of data assets on the **non-repudiation** of events and data are also considered in this section.

Asset	Description of Asset	Threat Assessment	Requirement
User password (table: customers)	Password required in order to access the iVR system.	Access to a valid Userid / password combination gives access to the customer details and the calibration data. This may be of value to a competitor.	High
Personal information (table: customers)	Information about the customer.	This asset includes customer contact details and other personally identifiable information. The NPL are required to protect it in line with the requirements of the Data Protection Act.	Medium
Customer equipment information (table: sessiondata)	Details about the equipment undergoing calibration.	This information might be of interest to a competitor, especially if this is a new piece of equipment.	Low
Measurement data (table: measurements)	The measurements from the Customer standard.	The actual measurements may be of interest to a competitor, especially if they contain evidence of a product weakness.	Medium

Asset	Description of Asset	Threat Assessment	Requirement
		Unauthorised disclosure of data by the NPL will potentially damage the reputation of the NPL brand.	High
Measurement data status	The status of the measurement data. For example, whether this data is being used for certification of a Customer standard.	There is little impact arising from the unauthorised disclosure of this information.	Low
Environment and Correction data	The environmental conditions and associated Fluke 4950 correction data linked to measurement data.	There is little impact arising from the unauthorised disclosure of this information.	Low
Webcam data	Photographic evidence that the calibration at the customer site was conducted in a specific way.	There is little impact arising from the unauthorised disclosure of this information.	Low
System data	The database schema and the MySQL configuration information.	There appear to be no particular requirements to protect this information from disclosure.	Low
Database permissions	The MySQL database permissions set within the Data Warehouse.	Access to this information is unlikely to assist an attacker.	Low
Administration password details	The MySQL administrative account details, including password values.	Access to this information can result in an attacker gaining access to all of the other information held within the Data Warehouse.	High
Backup media	Contains a copy of all data stored in database.	Access to the backup will provide access to all the information held on the tape.	High

A.2 Integrity and Non-repudiation

This section provides a short analysis of the main security requirements for **integrity** of the data assets. That is, the need to protect the Data Warehouse information assets against unauthorised modification or destruction. As the measurement data may be used in support of an application for a Customer Standard to be certified by the NPL, the possible implications arising from unauthorised modification or destruction of data assets on the **non-repudiation** of events and data are also considered in this section.

Asset	Description of Asset	Threat Assessment	Requirement
User password (table: customers)	The password required to access the iVR system.	Unauthorised modification or destruction of this information would create problems for users attempting to access the system. In effect it would result in a 'denial of service' attack. This type of problem would however be easy for NPL to fix and would have a limited impact.	Low
Personal information (table: customers)	Information about the customer, including their contact details.	Changes to this information would be unlikely to have a significant impact.	Low
Customer equipment information (table: sessiondata)	Details about the equipment undergoing calibration.	Unauthorised changes to this information might make the analysis of the results harder, but would be unlikely to have a significant impact.	Low

Asset	Description of Asset	Threat Assessment	Requirement
Measurement data (table: measurements)	The measurements from the Customer standard.	Unauthorised changes to the calibration data will directly affect the integrity of the NPL measurement and certification processes. Whilst such unauthorised modifications are likely to be detected by the NPL and/or the Customer, they might cause some damage to the reputation of the calibration service if they become widely known.	High
		Changes to the data would be particularly important where they affect the data used in support of a Customer Standard certification application. Such changes to the data may directly affect the certification decision.	High
		Changes to the measurement data after the certification process has been completed may affect the ability of the NPL to provide evidence in support of the certification of a Customer Standard (non-repudiation). This may result in a loss of reputation to the NPL in the event of a legal dispute.	High

Asset	Description of Asset	Threat Assessment	Requirement
Measurement data status	The status of the measurement data. For example, whether this data is being used for certification of a Customer standard.	Unauthorised modification may lead to some confusion but is unlikely to have a major impact. NPL would be able to deduce what the correct status settings should be and change them back.	Low
Environment and Correction data	The environmental conditions and associated Fluke 4950 correction data linked to measurement data.	Unauthorised modification might affect the outcome of the certification process in a borderline case, but is not considered to be the main target for such changes.	Low
Webcam data	Photographic evidence that the calibration at the customer site was conducted in a specific way.	Unauthorised modification or destruction of the photographic data would not have a direct impact upon the measurement of certification process.	Low
		Loss of this data might weaken the evidence provided by the NPL in support of the certification of a Customer Standard (non-repudiation).	Medium
System data	The database schema and the MySQL configuration information.	Unauthorised modification to the database schema and other parameters might result in either loss of availability of data to customers or even the granting of access to the wrong data.	Medium

Asset	Description of Asset	Threat Assessment	Requirement
Database permissions	The MySQL database permissions set within the Data Warehouse.	Unauthorised changes to this information are unlikely to be useful to an attacker, as they would already have access to the actual Customer data if they could perform this level of change to the database.	Low
Administration password details	The MySQL administrative account details, including password values.	Unauthorised changes to this information may result in the database becoming unusable, with the NPL administrator being unable to gain access.	High
Backup media	Contains a copy of all data held in database.	Unauthorised changes to this asset would possibly render it unusable. This would have little impact under normal circumstances but would have a major impact if the backup media was needed to recover the database.	High

A.3 Availability

This section provides a short analysis of the main requirements for **availability**. That is, the need to make the Data Warehouse information assets available to the NPL and its Customers in a timely fashion.

Asset	Description of Asset	Threat Assessment	Requirement
User password (table: customers)	Password required to access the iCal system.	If the user password information was not available, Customer users would not be able to login to the system. This would stop new measurement data being captured, or existing data being reviewed.	Medium
Personal information (table: customers)	Information about the customer, including their contact details.	The non-availability of this information to the NPL or a Customer would be unlikely to have a significant impact, although it might delay performing the certification process.	Low
Customer equipment information (table: sessiondata)	Details about the equipment undergoing calibration.	The non-availability of this information to the NPL or a Customer would be unlikely to have a significant impact, although it would delay the certification process.	Medium
Measurement data (table: measurements)	The measurements from the Customer standard.	The non-availability of this information to the NPL or a Customer would be unlikely to have a significant impact, although it would delay the certification process.	Medium
Measurement data status	The status of the measurement data. For example, whether this data is being used for certification of a Customer standard.	The non-availability of this information to the NPL or a Customer would be unlikely to have a significant impact, although it might delay performing the certification process.	Low

Asset	Description of Asset	Threat Assessment	Requirement
Environment and Correction data	The environmental conditions and associated Fluke 4950 correction data linked to measurement data.	The non-availability of this information to the NPL or a Customer would be unlikely to have a significant impact, although it would delay performing the certification process.	Medium
Webcam data	Photographic evidence that the calibration at the customer site was conducted in a specific way.	The non-availability of this information to the NPL or a Customer would be unlikely to have a significant impact, although it might delay performing the certification process.	Low
System data	Information about the database schema and MySQL configuration.	The non-availability of this information to the NPL or a Customer would have an impact by preventing access to the database, thereby preventing new measurement data being captured or existing data being analysed.	Medium
Administration password details	The MySQL administrative account details, including password values.	The non-availability of this information to the NPL would be unlikely to have a significant impact in the short term.	Low
Backup media	Contains a copy of all data held in database.	The non-availability of this information to the NPL would be unlikely to have a significant impact, unless the backup was required to re-create the data warehouse.	Medium