IMTC/06

Proceedings of the 23rd IEEE Instrumentation and Measurement Technology Conference

Sorrento - Italy
24-27 April 2006

IEEE Catalog Number:
06CH37714C
ISBN : 0-7803-9360-0

IMTC 2006 – Instrumentation and Measurement
Technology Conference
Sorrento, Italy 24-27 April 2006

Internet-enabled calibration services: aspects of laboratory information system security

Marko Jurčević, Roman Malarić, Mladen Boršić
Faculty of Electrical Engineering and Computing, University of Zagreb
Unska 3, 10000 Zagreb, Croatia
Phone: +385-1-6129-749, Fax: +385-1-6129-616, Email: marko.jurcevic@fer.hr

Abstract *– A growing number of measurements in commercial and industrial sector needs to refer to the traceability to the national (and also international) standards. Since the internet-enabled metrology is rapidly developing in the recent years, it offers new possibilities for calibration services. In the same time these services must provide the overall security of the calibration data from the point of acquisition to the storage and analysis process. Information security has become a critical part of information and communication systems that are used in ordinary metrology laboratories, especially in those who also perform remote (internet-enabled) calibrations. This paper identifies and explores the different security issues of the internet-enabled metrology and requests for public key infrastructure implementation in a laboratory information system.*

Keywords *– internet-enabled calibration, information security, public key infrastructure (PKI), X.509 standard.*

I. INTRODUCTION

Internet-enabled metrology is a term that covers the use of the internet/intranet (and other telecommunication systems) to provide quicker access to a range of measurement and calibration services [1]. These services usually include:

- remote control and monitoring of instruments,
- traceable measurements that are conducted at a customer location but controlled remotely by the calibration facility (this covers the term i*nternet-enabled calibration*),
- access to measurement and calibration history and other related data,
- access to libraries of testing and metrology software or algorithms.

All of these tasks have become a topic of increasing interest in recent years. Especially the realization of remote calibration systems using some kind of telecommunication services as a mean of transmission is emerging as a solution to the transportation and cost issues compared with the traditional calibration methods. Remote systems like these offer also new possibilities for the National Measurement System, because calibration procedures can be done more quickly and more safely for the instrument or standard that has to be calibrated, everything leading to increased accuracy of the calibrated device.

This approach implies that the traceability and integrity of the calibration process (that is in this case done over some communication network) directly depends on the collected measurement data. This information is constantly vulnerable, but mostly when it is transmitted over the communication network and when it is processed and stored in the laboratory information management system (LIMS) database as a part of calibration data.

Detailed analysis of security requirements for internet-enabled calibration system is a crucial aspect before such service might enter into a commercial appliance.

II. THE PROPOSED INTERNET-ENABLED CALIBRATION SERVICES SYSTEM

Because of the rapid development of PC-based communication and interface standards, every system that remotely controls measurement instruments and processes should include enough software and hardware features, possibly anticipating future technology development. The proposed internet-enabled calibration system [2] has the main goal to enable the control and supervision of the remote standard(s) and instrument(s) that are used in a calibration process. It also needs to control the communication between the remote location (customer side) and Calibration Service Provider (CSP) side.

The architecture of the internet-enabled calibration system is shown on Fig. 1. It consists of a PC-based manageable travelling calibration device (TCD) and a CSP server-side application system that controls and monitors the whole process of calibration.

Travelling calibration device and device (instrument or standard) that is under test and/or calibration (DUTC) must have a communication interface in order to connect them to the client-side PC that controls the calibration event. Application on the CSP side performs calibration procedure without any human assistance on the client side. Operator on the client-side only has to make correct connections between the TCD and the DUTC. Also, client-side equipment (TCD) has to self-recognize

0-7803-9360-0/06/$20.00 ©2006 IEEE

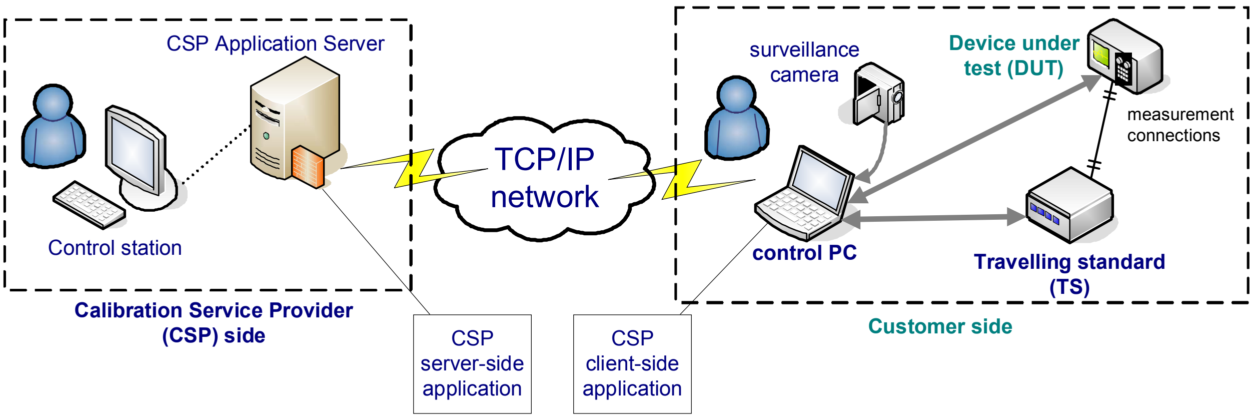

Fig. 1. Proposed architecture of the internet-enabled calibration system.

and make automatic configuration of available interfaces, connected instruments and standards. This means that there is no need for a specialized engineer or technician in the client side laboratory.

The client-side calibration system (which now consists of both TCD and DUTC) receives all the commands and instructions from the CSP server. It makes continuous scanning of the instrument readings and sends those results to the serve on the CSP side. All the relevant operations required to create calibration certificate (data storage, processing and calculation) are executed on the CSP side. After the calibration procedure is successfully completed, a calibration report is returned to the client. It should contain usual relevant information about the calibration event (date and time of a calibration event, some details of the equipment being used during the session, measurement uncertainty, measurement results, traceability chain and calibration session timing).

The software that runs CSP and client-side calibration and certification procedures is being constantly developed combining several available technologies, but mainly *NI LabWindows*^{TM} platform [3], *PHP* scripting language [4] and *PostgreSQL* database server [5]. Applications that run under the *Microsoft Internet Explorer* ^{TM} window has been configured to have access to all the client computer functionality, especially to the IEEE 488 (GPIB for controlling instruments) and USB interface (surveillance camera video streaming). The complete calibration system is under process of constant development in the Croatian Primary Electromagnetic Laboratory (PEL) on the Faculty of Electrical Engineering and Computing, University of Zagreb.

The use of a client-server application is needed in order to monitor the calibration procedure and to perform real-time test of calibration results. In this way the operator on the CSP side is able to warn for every error that could happen while the calibration is in progress. On the other hand, such operation requires protection of sensitive information that is sent over the Internet or other communication media. Also, this process is not in total control of the CSP staff, so the client side PC and calibration management software can be illegally altered before the calibration procedure starts. These security issues will be discussed lately in this paper.

The calibration system as shown above assures the following:

- automatic management of the physical resources is available on the server according to the type of calibration
- integrity and access control between client and server side
- optional upgrades with the newly added hardware components.

More detailed description of the travelling calibration device and information transport between CSP and client side is available in [2].

In the following section, a brief security analysis of the proposed system is discussed.

III. CALIBRATION SERVICES SYSTEM SECURITY

As mentioned earlier, an internet-enabled calibration session takes place between two parties – the CSP, the laboratory with the reference standards, and the customer laboratory with the equipment (standards and instruments) that needs to be calibrated. In this case the measurement data is constantly vulnerable, especially when it is transmitted over the communication media during the calibration process and when it is stored in a database as a part of calibration data. There are two main risks:

- the interception of sensitive information that travels between the TCD and client-side PC and over the communication media (Internet)
- the access to the customer-side PC or TCD of malicious intruders that can affect the calibration procedure

Security policy for internet-enabled calibration provider should identify at least seven major security services as

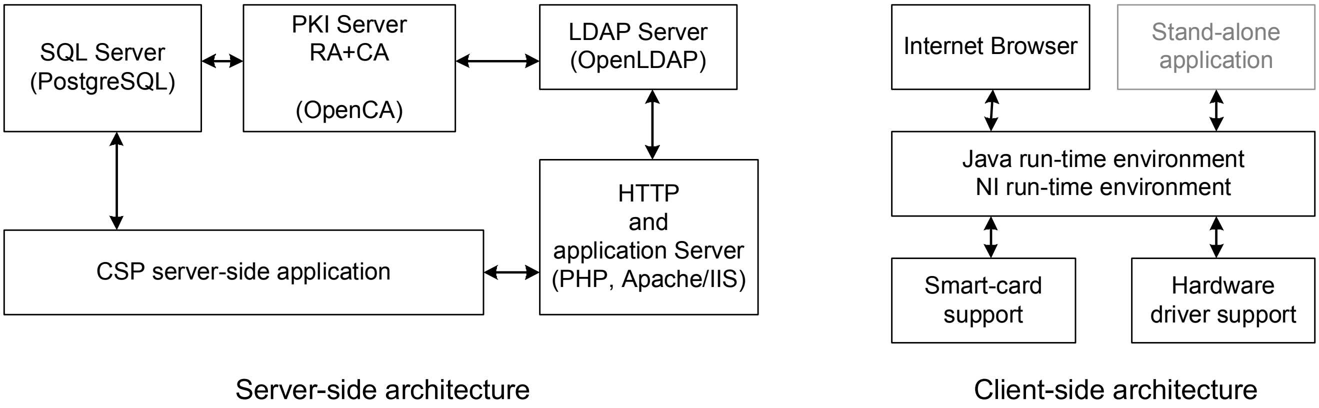

Fig. 2. PEL CSP basic software architecture

important in the process of data acquisition, transmission, storage, process and access: authentication, role-based access control, integrity, confidentiality, non-repudiation, auditing and availability [6, 7].

The first step in the development of CSP security policy creation is to review all the requirements that both the CSP and remote customer need. Security policy provides a set of security objectives and tasks, as for example defined in the mostly used ISO/IEC 17799:2000 computer security standard [8]. Recommendations from this standard should be selected and used in accordance with applicable laws and regulations. This security policy should apply to the:

- human interface, measurement and other connected equipment, at the customer laboratory, form the point of Internet or other media connection to the DUTC (at the client-side),
- communication media used for transmission of measurement data,
- human interface, control and database server and other related equipment at the CSP side.

The main risk points of unauthorized access and alteration of the calibration system are the connection between the client-side PC and TCD and DUTC. Also, the measurement connection between DUTC and TCD can be compromised. To minimize such possibility, the information between TCD and client-side PC should be encrypted. The decryption process would then be performed within the TCD. These risks may also be lowered if the surveillance camera is used (if appropriate). It could provide some kind of visual control for the equipment involved in calibration process.

A. Network security mechanisms

Within seven major security services, authentication can be ranked as most important. Authentication must be performed whenever a connection between the CSP and a client-side is initiated. This mechanism must provide protection against every misleading or incorrect identification of any side. It can be achieved using the Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Access control enables that everyone involved in a calibration process can have access to the resources and data they really need. Auditing subsystem is used to store sufficient data about every relevant action in the calibration system. In this way it can be confirmed that calibration took place and can be determined types of measurement, values ad final result of the calibration process.

Data integrity protection over the communication network can be obtained by using some kind of encryption. In our case it is achieved using integrated IPSec security mechanisms that assure no data has been seen or altered during the transmission over the network [6]. Integrity of the whole calibration system is achieved by combining the use of IPSec, authentication control on the client and CSP side and the storage of all (raw and processed) calibration data on the main CSP server. Confidentiality assumes that the information being transmitted over the communication media is not revealed to anyone other than the receiving party. It is achieved through the same mechanisms as integrity protection (IPSec or plain SSL, authentication control and relevant calibration data storage exclusively on the CSP side).

After the implementation of these security mechanisms in an Internet-enabled calibration system, it is advisable to perform a security audit. It will produce a discrepancy report showing where this system does not meet the security policy standards and how to resolve these problems.

Currently, the PEL CSP information system implements SSL protocol in the *NI LabWindows*^{TM} environment (part that is used for calibration procedure control and network data transfer) as shown on Fig. 2. In the future, it is planned to use Java Secure Socket Extension (JSSE) set of packages. JSSE implements SSL and TLS protocols and includes software parts for server and client authentication, data encryption and integrity. It is also possible to use Java applets to run client-side calibration procedure. In that case security issues related to the connection between server and client can be addressed directly to the secure web server (again using the SSL/TLS methods). These solutions are to be explored in the future.

B. Data security mechanisms

Another aspect of security in an internet-enabled calibration system is data security in CSP application system. The main threat to the confidentiality of this system can be from unauthorized access to valid user identification (for example: username and password, token, user private security certificate). This information would enable an attacker to have access to customer information through the normal CSP application interface. Access to this information could lead to a possible loss of reputation for the CSP. It is advisable to encrypt and protect the customer data as it travels through the communication media. This will protect any transmitted data between CSP and the customer, including user identification information. Also, it is necessary to establish a physical security control surrounding the CSP server.

Customer and measurement data that is stored in a database can be encrypted if needed, but this is not necessary. Data back-up security is an important consideration. It will be preferable to have a system which will work with a database located on a network server which makes daily back-ups without the intervention of the calibration management system supervisor. The database should provide integrity protection for the set of measurement data that is used during the certification process. This will also enable the CSP at a later date to provide adequate proof in support of their certification of the customer standard. This data should be cryptographically protected to detect unauthorized or modification. The simplest way to perform this is to generate a message digest (for example: *MD5* or *Whirlpool*) value, for the data using one of commonly available algorithms. Digital signatures maintained under a Public Key Infrastructure (PKI) system [9] are a much better solution for this, but also are more sophisticated.

The PEL CSP database is run under *PostgreSQL* database server [5]. It is an object-relational database management system (ORDBMS) based on POSTGRES, Version 4.2, developed at the University of California at Berkeley Computer Science Department. POSTGRES pioneered many concepts that only became available in some commercial database systems much later. And because of the liberal license, *PostgreSQL* can be used, modified, and distributed by everyone free of charge for any purpose, be it private, commercial, or academic.

C. Digital signatures for data protection

Public Key Cryptography (PKC), invented almost 30 years ago [9-12], provided the ability to digitally sign documents but also eased the main problem with conventional symmetric key system - the initial distribution of secret keys between the two communicating parts. However, mainly due to the nature of applications that required PKC, wide-scale exploitation of this technology is only in a last couple of years taking place. In the metrology laboratory, for example, a calibration certificate could be sent over the email to the customer. Even a calibration of an instrument could be done using the Internet-enabled calibration services. All of these not only require digital signatures, but also need scaleable and secure key management schemes to support encryption and authentication as well.

Public Key Infrastructure achieves privacy and data protection through an architecture that operates using public/private key pairs. In that way, PKI can provide higher levels of confidence for exchanging information over some communication network. It offers certainty of the quality, source and destination of information sent and received electronically. It also assures the time that information was sent and received (if known) and ensures the privacy of information sent.

A PKI consists of the following elements: *certificates* (constitutes the digital identification of a user or device and has the user's public cryptographic key, one or more user attributes and one or more issuers binding these elements to the certificate), Certificate Authority-CA (manages certificate applications and issues, signs and stores them in public directories [12] where they can be retrieved or revoked as needed), Registration Authority-RA (optional component that acts as a intermediate between CA and end users), Certificate Directory (place for certificate storage, usually based on X.500 standard).

It is vital in a PKC system to ensure that the private key remains secret and is usable only by the same person or device that is identified in the corresponding public key certificate. Private keys of end users, RAs and CAs must be protected from unauthorized access. The private keys of end users can be stored in tamper-resistant hardware tokens (usually smartcards) or stored in an encrypted form on the user's hard disk or some other storage media. It is important that, in either case, access to the keys is protected by one or more identification and authentication mechanisms (e.g. password, biometric systems etc.).

Requirements for electronic calibration certificates that are equivalent to a paper calibration certificate are protected integrity, authenticity and non-repudiation of certificate. The process of creating an digitally signed calibration certificate is as follows: (1) generate relevant certificate data from the raw measurement data, (2) generate calibration certificate document (and make it read-only, if necessary), (3) sign the calibration certificate using a calibration laboratory private key, (4) send the digitally signed document to the customer, who can verify it's authenticity using calibration laboratory's public key.

To use digital signatures it is necessary for a calibration laboratory to be part of a PKI by obtaining its own private and public key. Digitally signed electronic calibration certificates provide equivalent version of a paper certificate in terms of integrity and authenticity. Unfortunately, they are not the most practical way of giving the customer access to the data in the certificate. More convenient way of doing this is through a web application that gives the user ability to see all the data and calibration history of their instruments. This solution might work equally for traditional and internet enabled calibration services.

The PEL was always looking for better ways of secure data flow, and improving secure authentication and authorization procedures, so the PKI infrastructure implemented in PEL network is a step of following that goal.

The PKI solution in PEL was based on open source PKI solution named *OpenCA* [13]. *OpenCA* is a free non-government project, based on RFC 2459 and RFC 3280 also known as X.509 format [11]. The *OpenCA* PKI Development Project is a collaborative effort to develop a robust, full-featured and Open Source out-of-the-box Certification Authority implementing the most used protocols with full-strength cryptography world-wide. *OpenCA* is based on many Open-Source Projects. Among the supported software is *OpenLDAP*, *OpenSSL*, *Apache Project*, *Apache mod_ssl*. The topology of *OpenCA* in PEL network is implemented on two servers: one offline root CA, for issuing and revoking certificate request, and self signed certificate authority, and one online server, on witch RA was installed, that checks persons who are applying for digital certificate, and after approving request, sending it to the CA for finale conformation. On the online side was also implemented the public web portal, on which the user can make request for his digital ID, and it is also used as a publishing point of valid, revoked and suspended certificates. On the user side, the use of PEL PKI open source solution can be seen in digital certificate of every PEL employees, who can use his digital certificate, safely store on smart card (along with his private key), used it as authentication tools for next implemented services:

- as digital ID for signing e-documents,
- under Windows OS, as a tool for logging on Windows network domain,
- use for https web login,
- use for VPN authentication connection, etc.

The PEL CSP public-key infrastructure part is being tested using this solution. Although the PKI infrastructure in PEL network was made using open-source tools, which can not be by default administered as an admissible in a Court of Law (because of open-source), *OpenCA* solution is a good example of practical use in metrology laboratory environments because it fulfils all requirements: it is free, it can be upgraded and customized for every need of academic society.

In the future it is planned to build-up standalone in-house PKI solution that will be integral part of CSP application devoted specially to remote measurements and calibration purposes.

IV. CONCLUSION

This paper has shown a client-server architecture devoted to the Internet-enabled instrument calibration and management system to be implemented in Croatian Primary Electromagnetic Laboratory.

The key feature of the proposed distributed calibration system is its usability and extensibility. A client-server application manages the calibration process and implements security solutions that minimize the possibility of fraud. It is important to consider that the data security methodology is relevant to the user of Internet-enabled calibration services. All security requirements that are implemented in a security policy for Internet-enabled calibration can be used as a basis for auditing and modification of security in these systems.

The system proposed could become the kernel of a future accredited certification service based on remote on-site calibrations.

REFERENCES

[1] R. A. Dudley, N. M. Ridler, "Traceability via the Internet for Microwave Measurements Using Vector Network Analyzers", *IEEE Trans. Instrum. Meas.*, vol. 52, no. 1, pp. 130-134, February 2003

[2] M. Jurčević, M. Boršić, D. Cmuk, "Design of an internet-enabled calibration system", *Proc. 19th Metrology Symposium*, September 2005, pp 118-121.

[3] National Instruments LabWindows/CVI development platform, http://www.ni.com/labwindows

[4] PHP scripting language, http://www.php.net/

[5] PostgreSQL Open Source Database Server, http://www.postgresql.org/

[6] Stallings, W., "Cryptography and Network Security", Prentice Hall, 2002

[7] M. Jurčević, R. Malarić, M. Boršić, "Security issues of internet-enabled calibration services", *Proc. 6th Semetro - International Seminar on Electrical Metrology*, September 2005.

[8] "ISO/IEC 17799:2000 Information technology - Code of practice for information security management", http://www.iso.org

[9] W. Diffie, M. Hellman, "New directions in Cryptography", *IEEE Transactions on Information Theory*, vol. 22, pp. 644-654, 1976.

[10] C. Breed, "PKI: The Myth, the Magic and the Reality", *Information Security*, vol. 2, no. 6, pp. 20-27, 1999.

[11] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 public key infrastructure certificate and CRL profile", *RFC 2459*, January 1999.

[12] ITU-T Recommendation X509, "Information Technology – Open Systems Interconnections – The Directory: Authentication Framework", 1997.

[13] OpenCA open-source PKI project, http://www.openca.org