Radiation Physics and Chemistry, 2004, Vol. 71, pp. 369-372.

Next-Generation Services for *e*-Traceability to Ionizing Radiation National Standards

Marc F. Desrosiers,*[†] Mark Klemick,[‡] James M. Puhl,[†] David Uchida,[‡] and Steven Mallis[‡]
[†] Ionizing Radiation Division, Physics Laboratory, National Institute of Standards and Technology, Gaithersburg, Maryland 20899
[‡] Advanced Technology & Research Corporation, 15210 Dino Drive, Burtonsville, MD 20866

An Internet based system for fast, remote certification of high dose radiation sources against the U.S. national standard is being constructed at the National Institute of Standards and Technology (NIST). The new service will establish traceability (through transfer dosimetry) in real time at a lower cost by using automated routines and the Internet. A prototype of this service was successfully demonstrated in 2000 at the American Society for Testing and Materials (ASTM) Dosimetry Workshop in San Diego. Despite this impressive accomplishment, new developments demanded that several aspects of the service be modified. The new service has been completely redesigned to address these new demands and ensure greater accessibility. A description of the hardware and software configurations of this service as well as the communication and information management aspects will be presented. The Internet-based transfer certification program will provide industry with 24-hour, 7-day-per-week, on-demand certifications, immediate turnaround times, and lower cost, ultimately improving the quality of the manufacturing process.

Keywords
Alanine; Certification; Dosimetry; Electron paramagnetic resonance; Encryption; Internet

Contact
Marc F. Desrosiers, Mailstop 8460, Ionizing Radiation Division, National Institute of Standards and Technology, Gaithersburg, Maryland 20899, FAX: 301-869-7682, marc.desrosiers@nist.gov

Introduction

Several years ago, NIST set out to create a system for fast, remote certification of high-dose radiation sources against the U.S. national standard gamma-radiation source using the Internet. The Internet-based system promised to deliver immediate certification results to the industry customer on demand at a lower cost. In earlier work, NIST successfully demonstrated a prototype of this service with modern technologies and commercially available products (Desrosiers et al., 2002). NIST's high-quality electron spin resonance (EPR) alanine system was coupled with the connectivity of the Internet to perform services remotely in real time. However, although the basic functions of this service worked, new developments made it clear that design revisions would be necessary. These changes were primarily driven by new information technology (IT) policies, especially those regarding security. For this reason and others, a drastic overhaul in the Internet-based transfer certification service was undertaken.

Discussion

The original design for the Internet-based transfer certification service required a constant uninterrupted connection between the company's computer and the NIST server throughout the entire measurement session. This requirement came in conflict with new rules against such connections. Moreover, other issues with the service design soon became evident. Connectivity on the industry-end of the service communication link would not be guaranteed to be compatible with the service. The Internet connections for some company sites are limited to dial-up modems. Some company sites do not have the high-speed connection required by the service. It was also apparent that the rigid design of this service would effectively eliminate foreign subscribers. Open high-speed connections would be even more difficult to enable and maintain if the facility was outside the United States. Moreover, the cost of this live connection to a foreign subscriber would likely be prohibitive.

The Internet-based service was born from IT advances that enabled remote control of instrumentation. That freedom opened to question the need to have the controlling computer in the same location as the measurement instrument. In a radical departure from traditional NIST services, the first-generation system was based on the concept of NIST control over customer instrumentation for instantaneous certification. It offered rapid results and reduced cost by eliminating laborious (and expensive) measurements by NIST staff. However, the second-generation service described here evolved from the realization that the system control was software-based and thus not bound to any physical device. Thus, there was no compelling reason to have the controlling software located on a computer physically distant from the spectrometer making the measurements. Thus, it was clear that the controlling software could reside on the computer local to the measuring instrument (as long as this software is tamper proof). Since the system would require approval and verification steps, communication with NIST servers is still required, however, open connections through company and NIST firewalls were no longer a requirement.

The scheme in Figure 1 shows the new design for the Internet-based transfer certification service from a perspective of hardware and the communications flow. There is a dividing line that

denotes the firewall separating the hardware elements outside and inside the NIST firewall. At the top of the scheme are the elements residing outside the firewall, the client's EPR instrument (and controlling computer) and the NIST public server (NPS). Several computers reside internal to the firewall: the Physics Laboratory server (PLS) that is the primary communicant with the public server; Ionizing Radiation Division servers (IRDS) and personal computers; and, the NIST accounting server.

The session begins with the client certification program (CCP) logging in to the NPS (Step 1 in Figure 1) to request a validation ticket that will enable the CCP to perform a dose certification session. The request includes client accounting information, instrument data files, dosimeter data files, and software/firmware versions. The data submitted is checked and logged. Assuming positive acknowledgment of the request, a validation ticket is issued (Step 2) by the NPS to the CCP along with key material that is used to generate an encryption key to be used by the CCP and NPS for encrypting and decrypting messages. The receipt of the validation ticket is an indication to the CCP to proceed with the dose certification session. The CCP proceeds with the certification session without any open connection to the NPS. With regard to the instrument technician at the company site, the CCP interacts with them by requesting information or issuing commands. It protects the integrity of the measurements by preventing the technician from adjusting any spectrometer settings (through a software control lock).

During the certification session, the CCP oversees the incremental collection of data, as well as the processing and logging of data into the certification report. To prevent unauthorized viewing of the certification report, each data entry is encrypted, then locally written into the report. All data is encrypted at all times; the technician does not have access to the key required to decrypt the data. All events are logged and date/timestamped during the course of the certification process. This includes the logging of activities performed on the instrument (i.e., operator logins, prompts, dosimeter measurements, errors, etc.).

The certification report, once complete, is subject to a "hash" by the CCP. The hash process involves processing the file through a function that produces an abbreviated unique identifier or fingerprint of the file. This hash is signed with a private key and sent along with the encrypted certification report to the NPS (Step 3). Upon receipt of the encrypted report and hash they are decrypted by the NPS. The report is subjected to a second hash by the NPS. Certification integrity is validated by comparing these two hashes. Report verification generates release of the provisional certificate report to the technician (Step 4). The provisional certificate contains all the information (i.e., dosimeter doses, measurement uncertainties, etc.) that would be contained in the final certificate. It lacks only signatures of NIST staff that validate it.

This hash and report is again encrypted and sent to the PLS (Step 5) and archived (Step 6). A readable certificate report data file is sent to the IRDS for review by NIST calibration service staff (Step 7). After a comprehensive review of the certification event is performed, the final certification report is signed (Step 8), a bill for service is generated (Step 9), and the report is sent to the company's designated recipient (Step 10).

The software architecture (Figure 2) is based on the Real-time Control System[1] (RCS) methodology for control of intelligent systems originally developed at NIST (Albus, 1992; Quintero and Barbera, 1992). The RCS methodology uses a unique task-based approach to organize information during the design phase of an automated system. High-level tasks are broken down into smaller subtasks. The software modules built around these tasks have very limited specific functions and are coordinated and managed by upper level "manager" modules (Figure 2). The modules are organized into a hierarchy that is unrelated to the computer or physical location in which the module may be resident. The highest level managers in the scheme may do nothing more than coordinate other modules and ensure that these lower level modules complete their tasks appropriately. Some descriptions of modules and their duties are detailed below:

- The Electronic Certification Session Manager oversees certification activities and required resources. Responsibilities include: maintaining resources required for certification, maintaining interface to the ISSC[2] and accounting activities, and, authorizing certification services.
- The Certification Manager coordinates activities required to issue certified dosimetry measurements. Responsibilities include: receiving requests for validation tickets, creating job order in database, initiating certification session, requests review/approval process, issuing final certificates, and, archiving reports and certificates.
- The Certification Session Manager coordinates activities between report sessions and service activities. Responsibilities include: processing requests to process session, issuing validation tickets, and, managing report processing.
- The Instrument Certification Manager manages instrument activities required to create a certificate report. Responsibilities include: initiating request for validation ticket, receiving validation ticket, interfacing with technician/operator, coordinating activities required to create a certification report.
- The Measurement Manager coordinates sequences and prompts between the technician and instrument for dosimeter measurements. Responsibilities include: processing request to perform dosimeter measurements, coordinating instrument control with technician and prompts for dosimeter manipulations, reports status of measurements.

Conclusion

This next-generation Internet-based dose certification service is a vast improvement over the rudimentary system demonstrated three years ago. Its revamped security features are compatible with current computer security policies. The new communication mechanisms (encryption

[1] The mention of commercial products throughout this paper does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that products identified are necessarily the best available for this purpose.

[2] All NIST calibration services report to the NIST Information System to Support Calibrations (ISSC) database.

versus open connections) are based on standard practices that should enable it to be adaptable to future changes in security policies. The next-generation service is also more compatible with industry systems capabilities and offers full accessibility to foreign subscribers. Most comforting to those concerned about attacks on IT systems are the multiple levels of state-of-the-art encryption technology that will ensure the protection of private information as well as the highest degree data integrity.

ACKNOWLEDGMENTS
The authors thank the Bruker EPR Division staff for their cooperation.

REFERENCES
Albus, J.S. "RCS: A Reference Model Architecture for Intelligent Control." IEEE Computer. May 1992: 56-59

e-Calibrations: Using the Internet to Deliver Calibration Services in Real Time at Lower Cost, M. Desrosiers, V. Nagy, J. Puhl, R. Glenn, R. Densock, D. Stieren, B. Lang, A. Kamlowski, D. Maier, A. Heiss, Radiat. Phys. Chem. (2002) 759-763.

Quintero, R,, and Barbera, A.J., "A Real-Time Control System Methodology for Developing Intelligent Control Systems". NISTIR 4936. National Institute of Standards and Technology. Gaithersburg MD (1992)

Radiation Physics and Chemistry, 2004, Vol. 71, pp. 369-372.

Figure 1. Hardware configuration and communication scheme for Internet-based certification service.

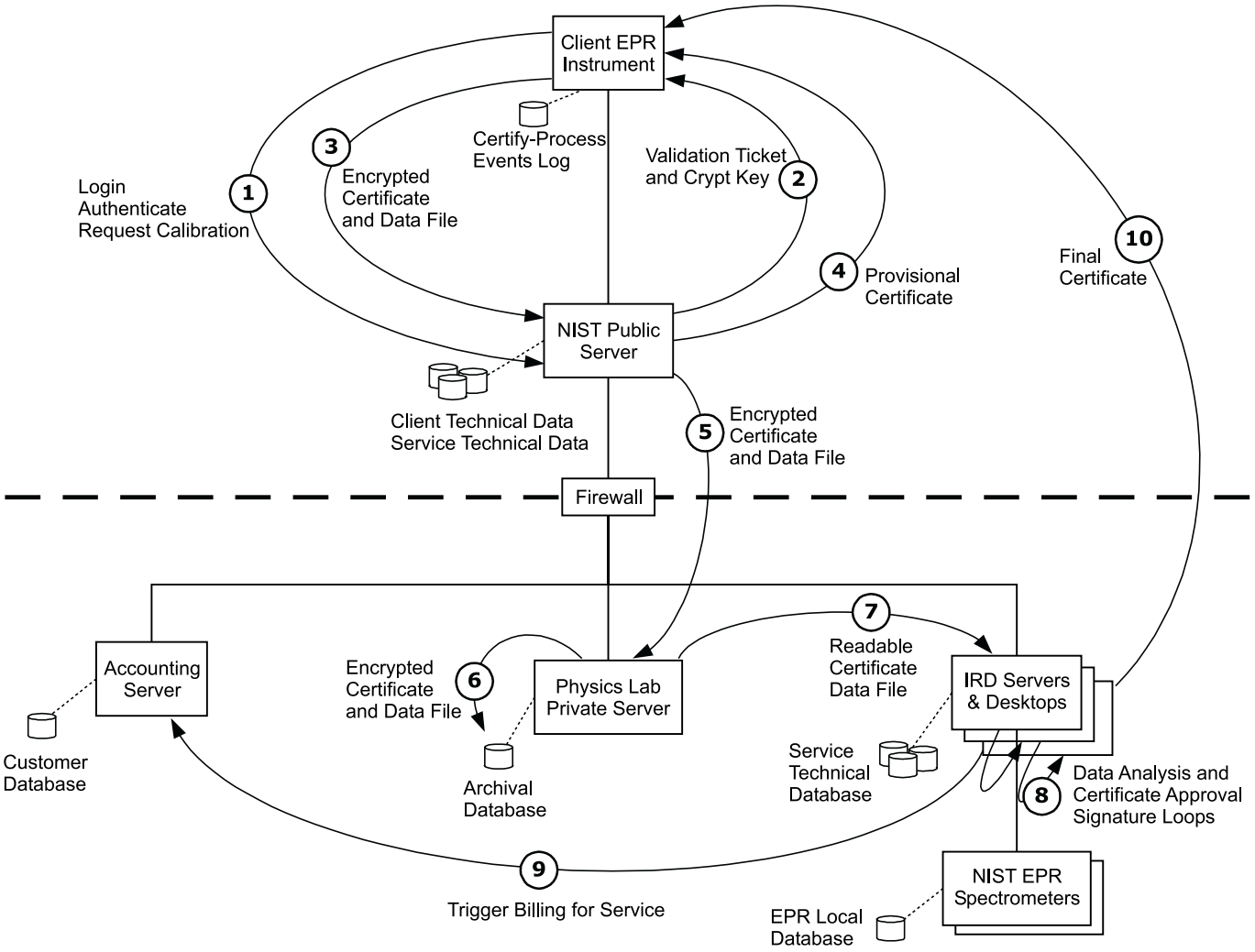

Figure 2. Software module hierarchy for Internet-based certification service.