Archived Document

This archived document is no longer being reviewed through the CLSI Consensus Document Development Process. However, this document is technically valid as of January 2017. Because of its value to the laboratory community, it is being retained in CLSI's library.

CLINICAL AND LABORATORY STANDARDS INSTITUTE®

March 2006

AUTO09-A

Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Approved Standard

SAMPLE

This document provides a standard communication protocol for instrument system vendors, device manufacturers, and hospital administrators to allow remote connections to laboratory diagnostic devices. The remote connections can be used to monitor instruments' subsystems; collect diagnostics data for remote system troubleshooting; and collect data for electronic inventory management.

A standard for global application developed through the Clinical and Laboratory Standards Institute consensus process.

Clinical and Laboratory Standards Institute

Setting the standard for quality in medical laboratory testing around the world.

The Clinical and Laboratory Standards Institute (CLSI) is a not-for-profit membership organization that brings together the varied perspectives and expertise of the worldwide laboratory community for the advancement of a common cause: to foster excellence in laboratory medicine by developing and implementing medical laboratory standards and guidelines that help laboratories fulfill their responsibilities with efficiency, effectiveness, and global applicability.

Consensus Process

Consensus—the substantial agreement by materially affected, competent, and interested parties—is core to the development of all CLSI documents. It does not always connote unanimous agreement, but does mean that the participants in the development of a consensus document have considered and resolved all relevant objections and accept the resulting agreement.

Commenting on Documents

CLSI documents undergo periodic evaluation and modification to keep pace with advancements in technologies, procedures, methods, and protocols affecting the laboratory or health care.

CLSI's consensus process depends on experts who volunteer to serve as contributing authors and/or as participants in the reviewing and commenting process. At the end of each comment period, the committee that developed the document is obligated to review all comments, respond in writing to all substantive comments, and revise the draft document as appropriate.

Comments on published CLSI documents are equally essential, and may be submitted by anyone, at any time, on any document. All comments are managed according to the consensus process by a committee of experts.

Appeals Process

When it is believed that an objection has not been adequately considered and responded to, the process for appeals, documented in the CLSI Standards Development Policies and Processes, is followed.

All comments and responses submitted on draft and published documents are retained on file at CLSI and are available upon request.

Get Involved—Volunteer!

Do you use CLSI documents in your workplace? Do you see room for improvement? Would you like to get involved in the revision process? Or maybe you see a need to develop a new document for an emerging technology? CLSI wants to hear from you. We are always looking for volunteers. By donating your time and talents to improve the standards that affect your own work, you will play an active role in improving public health across the globe.

For additional information on committee participation or to submit comments, contact CLSI.

Clinical and Laboratory Standards Institute
950 West Valley Road, Suite 2500
Wayne, PA 19087 USA
P: +1.610.688.0100
F: +1.610.688.0700
www.clsi.org
standard@clsi.org

SAMPLE

AUTO09-A
Vol. 26 No. 11
ISBN 1-56238-599-2
Replaces AUTO9-P
ISSN 0273-3099
Vol. 25 No. 3

Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Approved Standard

Volume 26 Number 11

Randy R. Davis
Bradford T. Hill, DBA, MA, MT(ASCP)
Klaus Kjoller
Andrzej J. Knafel, PhD
Steven S. Pelham
Hiroshi Sekiya
Allan Trochman
J. Mark Tuthill, MD

SAMPLE

Abstract

Clinical and Laboratory Standards Institute document AUTO09-A—*Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Approved Standard* provides a standard communication protocol that will allow remote connections to laboratory devices. It establishes a means to leverage the existing infrastructure provided by the hospital's Local Area Network (LAN) and the Internet to achieve remote connectivity. These remote connections can be used to monitor instruments' subsystems to determine proper operation; collect diagnostic data for remote system troubleshooting; and collect data that would allow for electronic inventory management.

Clinical and Laboratory Standards Institute (CLSI). *Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Approved Standard*. CLSI document AUTO09-A (ISBN 1-56238-599-2). Clinical and Laboratory Standards Institute, 950 West Valley Road, Suite 2500, Wayne, Pennsylvania 19087 USA, 2006.

The Clinical and Laboratory Standards Institute consensus process, which is the mechanism for moving a document through two or more levels of review by the health care community, is an ongoing process. Users should expect revised editions of any given document. Because rapid changes in technology may affect the procedures, methods, and protocols in a standard or guideline, users should replace outdated editions with the current editions of CLSI documents. Current editions are listed in the CLSI catalog and posted on our website at www.clsi.org. If your organization is not a member and would like to become one, and to request a copy of the catalog, contact us at: Telephone: 610.688.0100; Fax: 610.688.0700; E-Mail: customerservice@clsi.org; Website: www.clsi.org.

Copyright ©2006 Clinical and Laboratory Standards Institute. Except as stated below, any reproduction of content from a CLSI copyrighted standard, guideline, companion product, or other material requires express written consent from CLSI. All rights reserved. Interested parties may send permission requests to permissions@clsi.org.

CLSI hereby grants permission to each individual member or purchaser to make a single reproduction of this publication for use in its laboratory procedure manual at a single site. To request permission to use this publication in any other manner, e-mail permissions@clsi.org.

Suggested Citation

CLSI. *Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Approved Standard.* CLSI document AUTO09-A. Wayne, PA: Clinical and Laboratory Standards Institute; 2006.

Previous Edition:
January 2005

Reaffirmed:
March 2014

Archived:
January 2017

SAMPLE

ISBN 1-56238-599-2
ISSN 0273-3099

Contents

SAMPLE

Foreword

Remote access to laboratory instrument systems and medical devices has become an essential tool that allows *in vitro* diagnostic suppliers a means to maximize equipment uptime. Maximum equipment uptime is clearly a shared goal between device manufacturers, system vendors, and hospital laboratory managers. Many current devices are connected using modems over telephone lines. Although this approach is viable for a small number of systems and/or infrequent access, it is not practical when monitoring a large number of systems on a continuous basis. It is well-established that the Internet provides an extremely cost-effective way to provide two-way electronic communication, and there is an increasing number of remote access and monitoring systems in use over the Internet. Given that a typical hospital LAN (local area network) will normally support the Internet communication protocols (TCP/IP), and that most hospitals have existing Internet access, the ideal state is to allow instruments to connect to the Internet via the hospital LAN. However, this does introduce certain security concerns for a hospital network administrator. There are a number of emerging secure protocols and techniques, however, that can allow both the cost-effective and efficient communication channels provided by the hospital LAN and Internet, while at the same time providing the needed security.

Note that the trade name Bluetooth® is included in Sections 3.4.4 and 3.4.4.2 of this document. It is Clinical and Laboratory Standards Institute's policy to avoid using a trade name unless the product identified is the only one available, or it serves solely as an illustrative example of the procedure, practice, or material described. In this case, the subcommittee and area committee believe the trade name is an important descriptive adjunct to the document. In such cases, it is acceptable to use the product's trade name, as long as the words, "or the equivalent" are added to the references. It should be understood that information on this product in this standard also applies to any equivalent products. Please include in your comments any information that relates to this aspect of AUTO09-A.

Key Words

Access control, deidentify, encryption, unidentify

SAMPLE

Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Approved Standard

1 Scope

This document will address connections by public networks, but not direct point-to-point connections. It will also address information protection issues, and remote operation of instruments from both intranets and the Internet. Requirements for patient privacy and information security are addressed, for example, HIPAA (the Health Insurance Portability and Accountability Act of 1996) and the European Union Privacy Directive 95/46/EC.

This document has been developed for instrument system vendors, device manufacturers, and healthcare administrators as a standard for communication protocols to allow remote connections to diagnostic devices. This standard is not intended to address remote access to the healthcare organization's information system. It establishes a means to leverage the existing infrastructure provided by the healthcare facility's local area network (LAN) and the Internet to achieve the remote connectivity. This standard discusses which characteristics of communication protocols (Internet and others) are required.

2 Definitions

The following text applies to the RFC 2828 definitions listed below:

"Copyright and Reprint Permissions: The Internet Society owns the copyrights for these publications. You may freely reproduce all or part of any paper for noncommercial purposes if you credit the author(s) (Robert Shirey), provide notice to the Internet Society, and cite the Internet Society as the copyright owner."

access control – protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy.[1] (RFC 2828)

Advanced Encryption Standard (AES) – a future Federal Information Processing Standards (FIPS) publication being developed by NIST to succeed the Data Encryption Standard (DES). It is intended to specify an unclassified, publicly disclosed, symmetric encryption algorithm, available royalty-free worldwide.[1] (RFC 2828)

block cipher – an encryption algorithm that breaks plaintext into fixed-size segments and uses the same key to transform each plaintext segment into a fixed-size segment of ciphertext. (See: stream cipher.)[1] (RFC 2828)

certificate (digital certificate) – a certificate document in the form of a digital data object (a data object used by a computer) to which is appended a computed digital signature value that depends on the data object.[1] (RFC 2828)

certificate revocation list (CRL) – a data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire.[1] (RFC 2828)

certification authority (CA) – an entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.[1] (RFC 2828)

ciphertext – data that has been transformed by encryption so that its semantic information content (i.e., its meaning) is no longer intelligible or directly available. (See: plaintext.)[1] (RFC 2828)

SAMPLE

©*Clinical and Laboratory Standards Institute. All rights reserved.*

cryptology – the science that includes both cryptography and cryptanalysis, and sometimes is said to include steganography.[1] (RFC 2828)

customer – all components of a healthcare organization where the IVD device is installed.

data confidentiality – the property that information is not made available or disclosed to unauthorized individuals, entities, or processes (i.e., to any unauthorized system entity).[1-4] (RFC 2828; ISO/IEC 7498-1, 7498-2, 7498-4)

Data Encryption Standard (DES) – a U.S. government standard[5] that specifies the Data Encryption Algorithm and states policy for using the algorithm to protect unclassified, sensitive data. (See: AES.)[1] (RFC 2828)

data integrity – the property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.[1] (RFC 2828)

deidentify – use of a system that would create a new index that would relate to the patient; **NOTE:** This value would be sent in the data to the vendor. If information about a patient sample was required, the issuing institution would look up the information using this value. With this system, all the patient information would reside solely in the healthcare facility.

denial of service (DoS) – the prevention of authorized access to a system resource or the delaying of system operations and functions.[1] (RFC 2828)

digital signature – a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.[1] (RFC 2828)

Digital Signature Algorithm (DSA) – an asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified. (See: Digital Signature Standard.)[1] (RFC 2828)

Digital Signature Standard (DSS) – the U.S. government standard[6] that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.[1] (RFC 2828)

Encapsulating Security Payload (ESP) – An Internet IPsec protocol[7] designed to provide a mix of security services—especially data confidentiality service—in the Internet Protocol.[1] (RFC 2828)

encryption – cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.[1] (RFC 2828)

firewall – an internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall).[1] (RFC 2828)

Global System for Mobile Communications (GSM) – standard for digital mobile communications, with a capability for international roaming; **NOTE:** GSM is operated in the 900-MHz and 1800-MHz frequency bands in Europe and Asia, and in the 800-MHz and 1900-MHz frequency bands in the U.S.

SAMPLE

 ©*Clinical and Laboratory Standards Institute. All rights reserved.*

The Quality System Approach

Clinical and Laboratory Standards Institute (CLSI) subscribes to a quality system approach in the development of standards and guidelines, which facilitates project management; defines a document structure via a template; and provides a process to identify needed documents. The approach is based on the model presented in the most current edition of CLSI/NCCLS document HS1—*A Quality Management System Model for Health Care*. The quality system approach applies a core set of "quality system essentials" (QSEs), basic to any organization, to all operations in any healthcare service's path of workflow (i.e., operational aspects that define how a particular product or service is provided). The QSEs provide the framework for delivery of any type of product or service, serving as a manager's guide. The quality system essentials (QSEs) are:

Documents & Records	Equipment	Information Management	Process Improvement
Organization	Purchasing & Inventory	Occurrence Management	Service & Satisfaction
Personnel	Process Control	Assessment	Facilities & Safety

AUTO09-A addresses the quality system essentials (QSEs) indicated by an "X." For a description of the other documents listed in the grid, please refer to the Related CLSI/NCCLS Publications section on the following page.

Documents & Records	Organization	Personnel	Equipment	Purchasing & Inventory	Process Control	Information Management	Occurrence Management	Assessment	Process Improvement	Service & Satisfaction	Facilities & Safety
GP19	GP19	GP19	GP19	GP19	X AUTO3 GP19 LIS1 LIS2 LIS5 LIS9	AUTO3 GP19 LIS1 LIS2 LIS5	GP19		GP19	GP19	GP19

Adapted from CLSI/NCCLS document HS1—*A Quality Management System Model for Health Care*.

SAMPLE

 ©*Clinical and Laboratory Standards Institute. All rights reserved.*

Related CLSI/NCCLS Publications*

AUTO3-A **Laboratory Automation: Communications with Automated Clinical Laboratory Systems, Instruments, Devices, and Information Systems; Approved Standard (2000).** This document provides standards to facilitate accurate and timely electronic exchange of data and information between the automated laboratory elements.

GP19-A2 **Laboratory Instruments and Data Management Systems: Design of Software User Interfaces and End-User Software Systems Validation, Operation, and Monitoring; Approved Guideline—Second Edition (2003).** This document identifies important factors that designers and laboratory managers should consider when developing new software-driven systems and selecting software user interfaces. Also included are simple rules to help prepare validation protocols for assessing the functionality and dependability of software.

LIS1-A **Standard Specification for Low-Level Protocol to Transfer Messages Between Clinical Laboratory Instruments and Computer Systems (2003).** This specification describes the electronic transmission of digital information between the clinical laboratory instruments (those that measure one or more parameters from one or multiple samples) and computer systems (those that are configured to accept instrument results for further processing, storage, reporting, or manipulation).

LIS2-A2 **Specification for Transferring Information Between Clinical Laboratory Instruments and Information Systems; Approved Standard—Second Edition (2004).** This specification covers the two-way digital transmission of remote requests and results between clinical instruments and computer systems. It enables any two such systems to establish a logical link for communicating text to send result, request, or demographic information in a standard and interpretable form.

LIS5-A **Standard Specification for Transferring Clinical Observations Between Independent Computer Systems (2003).** This specification details how clinical observations can be transferred between independent computer systems.

LIS9-A **Standard Guide for Coordination of Clinical Laboratory Services Within the Electronic Health Record Environment and Networked Architectures (2003).** This guide covers the process of defining and documenting the capabilities, sources, and pathways of data exchange within a given network architecture of a Health Information Network (HIN) serving a set of constituents.

SAMPLE

* Proposed-level documents are being advanced through the Clinical and Laboratory Standards Institute consensus process; therefore, readers should refer to the most current editions.

©*Clinical and Laboratory Standards Institute. All rights reserved.*

CLINICAL AND LABORATORY STANDARDS INSTITUTE®

Explore the Latest Offerings From CLSI!

As we continue to set the global standard for quality in laboratory testing, we are adding products and programs to bring even more value to our members and customers.

By becoming a CLSI member, your laboratory will join 1,600+ other influential organizations all working together to further CLSI's efforts to improve health care outcomes. You can play an active role in raising global laboratory testing standards—in your laboratory, and around the world.

Find out which membership option is best for you at **www.clsi.org/membership.**

Find what your laboratory needs to succeed! CLSI U provides convenient, cost-effective continuing education and training resources to help you advance your professional development. We have a variety of easy-to-use, online educational resources that make *e*Learning stress-free and convenient for you and your staff.

See our current educational offerings at **www.clsi.org/education.**

When laboratory testing quality is critical, standards are needed and there is no time to waste. eCLIPSE™ Ultimate Access, our cloud-based online portal of the complete library of CLSI standards, makes it easy to quickly find the CLSI resources you need.

Learn more and purchase eCLIPSE at **clsi.org/eCLIPSE.**

For more information, visit www.clsi.org today.

SAMPLE

SAMPLE

CLINICAL AND
LABORATORY
STANDARDS
INSTITUTE®

950 West Valley Road, Suite 2500, Wayne, PA 19087 USA

P: +1.610.688.0100 **Toll Free (US):** 877.447.1888 **F:** +1.610.688.0700

E: customerservice@clsi.org **www.clsi.org**

ISBN 1-56238-599-2