Using Digital Certificates for Radiology Result Receipt Confirmation

Gary Wendt, Timothy Kulbago, and Wally Pepler

WHILE THE PROLIFERATION of web-based technologies is making it possible to quickly and effectively distribute radiology results, it is generally left to chance that the intended recipient received the information. We present here the benefits of using digital signature technology to confirm the receipt of clinical results. Whether using web-base viewing or E-mail distribution, there is a need to validate that the intended recipient has viewed the information. This is particularly important in the case of abnormal studies or studies with unexpected results. A solution is presented that uses digital certificate technologies to allow a referring physician to easily indicate receipt of a result, as well as the radiology department to keep accurate records of the receipt.

ENVIRONMENT

The method used is a web-based system for the distribution of clinical results, report text, and images. The server software is running on a Linux Intel-based system and access to the system available from Windows 95, Windows 98, or Windows NT (Microsoft, Redmond, WA) web browser. Referring physicians either receive encrypted E-mail containing radiology results or securely access the results via a web browser. After viewing the results, the user's individual digital certificate is presented for authentication to the server to confirm that the proper person has viewed the results. An audit database containing detailed information regarding access to the system is maintained and available for review by authorized hospital personnel. In addition, it should allow the radiologist to determine which abnormal reports have not been read so a follow-up call can be made, as this is often critical to ensure optimal patient care.

DIGITAL CERTIFICATE OVERVIEW

Digital certificate technology is emerging as a basis for providing encryption and digital signature features to web-based applications. The fundamental theory behind digital certificate technology is that two large, related, numbers called "keys" are generated. To encrypt information you can use either key as the basis for the encryption. The encrypted information can only be decrypted by

the other key. If one of these keys is kept private to a specific user and the other made public, then information can be encrypted and signed as needed.

The need for digital certificates is to ensure the authentic and secure distribution of the public keys. For example, if a user wants to send an encrypted E-mail, the public key of the recipient is used to encrypt the contents of the E-mail. The only person who can decrypt the E-mail is the holder of the private key that corresponds to the public key used to encrypt the message. The sender of the E-mail has to obtain a copy of the recipient's public key. While having a floppy disk with the public key mailed to the sender would be secure, it is time-consuming and impractical. So the public key needs to be available electronically. Sending the public key without a mechanism to verify that it has not been altered would result in the possibility of having the wrong public key. If the public key used to encrypt the E-mail were compromised, that is, exchanged without the knowledge of the sender, then the encrypted E-mail would be accessible by an unintended recipient and not by the intended recipient. Digital certificates provide a mechanism for validating the authenticity of a particular user's public key.

WORKFLOW

The workflow for this study is summarized as follows.

- (1) Radiology examination is performed.
- (2) Report is dictated and transcribed into the radiology information system (RIS).
- (3) Report is sent to web/E-mail server and merged with image data.

From the Department of Radiology, University of Wisconsin-Madison; and Marconi Medical Systems, Cleveland, OH.

Address reprint requests to Gary Wendt, MD, MBA, Department of Radiology, University of Wisconsin-Madison, E3/311 Radiology, 600 Highland Ave, Madison, WI 53792. E-mail: gjwendt@facstaff.wisc.edu.

*Copyright © 2001 by W.B. Saunders Company
0897-1889/01/1402-1038\$35.00/0
doi:10.1053/jdim.2001.23847*

- (4) Images and reports are sent via E-mail to referring doctor.
- (5) Referring doctor receives E-mail and clicks on a URL contained within the E-mail to verify receipt of report and images.
- (6) URL in E-mail requests the referring doctor's digital certificate.
- (7) Audit trails record that a valid certificate is presented for validating that intended recipient received and viewed clinical information.

Steps 1 through 4 are performed as described in a previous presentation and article by Wendt et al.¹ Added to the process is the inclusion of a URL within the E-mail. This URL will retrieve a web page from the server, which will request that the user present their digital certificate. Managed by the web browser, the user can select their digital certificate and have it downloaded to the server. The server can perform a real-time validation of the certificate. If the certificate is proven valid by the certificate authority, then information is stored in the audit database regarding the action that had just been performed.

KEY ISSUES AND BARRIERS

Barriers are networks, computers, E-mail readers, and web browsers of the correct version.

There are a few key issues to address when deploying this workflow scenario. First is the deployment and management of digital certificates. Second is the need for consistent use of the system to provide meaningful audit logs. Last is the user's limitation of certificate management via the web.

Firstly, the deployment and management of digital certificate through a certificate authority and registration authority requires the attention of a qualified administrator. While this process can be highly automated, the availability of a trained sys-

tem administrator and/or security technician is required to maintain a valid set of user certificates. While this was not a specific issue for this trial, it is clear that if there were a large number of users of the system some dedicated time would be required on an ongoing basis.

Second, the auditing reports produced from the system are valuable only within the context of all of the activity within the referring community. If a referring doctor only uses the system for a portion of the cases viewed, then there is no absolute authority for determining if a physician has reviewed a case. A possible to this would be to limit the generated E-mails to only those examinations with abnormal reports; this could be triggered by key word(s) within the dictation. Additionally, a report could be generated periodically by the system for those E-mails that have been sent but not acknowledged by the referring physician. The list could then be used to trigger manual follow-up.

Finally, current certificate technologies within web browsers provide a limited set of mechanisms for accessing certificates from multiple computers. Certificates can be exported to floppy disk or smart cards. Certificates can be part of a centrally stored profile. However, generally, a certificate is most easily accessed when the user is using the same computer and web browser all the time.

CONCLUSIONS

The implementation of this system provides a cost-effective and easy-to-use mechanism for verifying the receipt of radiology results. This provides the radiology department with assurance that their use of internet technologies is secure, effective, and reliable. Likewise, the approach outlined can be integrated into an enterprise-wide solution for the deployment of digital certificate technologies.

REFERENCE

1. Wendt G, Peppler W, Kulbago T: Implementing a Java based image and report distribution system in a non-PACS environment. *J Digit Imaging* 13:142-144, 2000 (suppl 1)