CLTA Email Data Protection Guidance

Published: March 2016

Authors

Ryan Murphy, SSCP
IT Division Manager
Placer Title Company

Cyrus E. Childs
EVP – Director of Information Services
Old Republic Title Company

Shabnam Jalakian
Director Information
Security First
American

Overview

The purpose of this document is to provide "data protection" guidance (as it pertains to email) to the California Land Title Association's members for the purposes of complying with the "ALTA Best Practices." Chapter 3 of the "Best Practice" documentation is left very much to the interpretation of the entity seeking compliance with the requirements set forth by the ALTA. This guidance will cover the CLTA's interpretation of Chapter 3 (specifically the "email in motion" portion of assessment procedure 3.09a).

Why protect email data as it traverses the Internet?

As a member of the Title Insurance Industry, your company likely transmits a large amount of personally identifiable information (PII[i]) on a daily basis. Customer PII is entrusted to CLTA members and the security of this data should be of paramount importance.

PII is actively sought by criminals for the purposes of identity theft, social engineering attacks, phishing schemes, and monetary theft. For this reason, emails containing PII should be protected by strong encryption any time it is being transmitted over the Internet to an authorized third party. The biggest problem is that email is text, and if not encrypted while in motion across the Internet, anyone with the determination and means can capture a copy of the data and reconstruct it for nefarious purposes.

Recommended Guidance:

If you only have the resources and means to use a free email service[i], it is advised that you find a service that provides "TLS Encryption" capability and "two-factor authentication[ii]" (2FA). The TLS capability will provide basic encryption for your emails while they are in transit when sent to a recipient that also supports TLS. The 2FA will provide extended security to your email account and make it much harder for criminals to gain access to your email account using stolen credentials.

If you have the resources, it is recommended that a private email service be employed. The private email service should at least support TLS, 2FA, and login-based email encryption. In addition to the security the TLS and 2FA provide, login-based email encryption provides security to your emails even when they are sitting in the mailbox of your recipient. The login-based email encryption will require the recipient to have credentials to login and decrypt the email containing PII before it can be read.

What is encryption?

Encryption is the process of encoding (concealing) data in such a way that an unauthorized person or entity can't read or make sense of it even if they possess the entirety of the transmission. The encoding of the message should be performed in such a way that no reasonable means of "brute force" could decipher or decrypt the data. As access to large-scale computational resources has become affordable for even the smallest of operations, encryption methods and algorithms ***must be regularly improved*** to stay ahead of any actors looking to steal customer PII by means of decryption.

What are the current minimum encryption standards?

Due to the nature of communications in the title insurance industry, the most common encryption method is public-key cryptography (asymmetric)[ii]. The National Institute of Standards and Technology in their January 2015 report state that public-key algorithms (RSA/Diffie-Hellman) should be a minimum of 2048 bits (NIST[iii]). Certificates should be obtained from a global trusted certificate authority and must be regularly renewed prior to their expiration.

In recent months, it was demonstrated that 1024 bit SHA-1 encryption certificates could be cracked using a cloud computing provider and a nominal amount of money (Security Affairs[iv]). ***CLTA members encrypting data should move to a SHA-2 algorithm or better as soon as possible***. Many Certificate Authorities will reissue existing SHA-1 certificates for little to no cost.

How should the email encryption process work in practice?

For an email being sent to an independent third party that contains PII, a CLTA member's email system must encrypt the email *prior* to transmission. The method for invoking the encryption process can be a logical/policy-based[iii] or a manual control[iv]. A logical method for invoking encryption is preferred as it requires less intervention on behalf of the employee sending the email. This is not to say that invoking the encryption process manually is invalid, it only means that there will be more diligence required by employees and more training need delivered by the CLTA member company.

When the encryption process is invoked, the CLTA member's email system should then encrypt the email using a 2048-bit key that attaches the encrypted file as an attachment or as a hyperlink in an email that requires the recipient to login. The recipient must then login to the CLTA members secure email system to decrypt and read the message.

Methods of provisioning accounts for the recipients can be handled several ways (one-time tokens[v], browser cookies[vi], permanent accounts, etc.). For permanent accounts, the process should follow the basic standards of user account controls with regards to password complexity.

For communication between CLTA members or Trusted Third Parties, TLS encryption can be used. [v]

Sources:

[i] NIST: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[ii] There will likely be cases where Title Industry partners may take advantage of symmetric encryption methods. Those cases are going to be much less common and will not be covered by this whitepaper.

[iii] NIST. (n.d.). NIST Special Publication 800-57 Part 3. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf.

[iv] Security Affairs: http://securityaffairs.co/wordpress/40884/hacking/sha-1-collision-attack.html

[v] TLS as explained by IETF: https://tools.ietf.org/html/rfc5246#section-1

Endnotes:

[i] This resource provides an extensive list of services that support two-factor authentication: https://twofactorauth.org/

[ii] Here is a CNET article explaining two-factor authentication: http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

[iii] Logical/Policy-Based email encryption would require a system or service that can scan the content of a given email message and then make a determination as to whether or not the message contains data that needs to be encrypted. Once that decision has been made by the system, the message will be encrypted and sent on to the recipient without requiring any user intervention.

[iv] Manual encryption systems rely completely on the user sending the email to determine if a given email's content contains private information and needs to be encrypted. The system would have a process for the user to explicitly encrypt an email.

[v] https://en.wikipedia.org/wiki/Security_token

[vi] https://tools.ietf.org/html/draft-broyer-http-cookie-auth-00