X9extra

Volume 2, Number 4
August 2011

Dear X9 Members:

In this issue of X9 EXTRA, Ed Scheidt, Chair X9F on security has developed an easy to understand overview of the basic security approaches using various encryption tools. What Ed has developed is an "Encryption Primer" members can use when asked 'what's encryption'.

Elsewhere in this issue is an article on the industry acceptance of a new ISO standard prepared through X9s international group, TC68. The standard should prevent some of the confusion that was associated with the financial collapse of 2008.

Also, X9 is putting the final details for the upcoming All Committees Meeting (ACM) set for the week of October 24th in San Antonio, Texas. Here X9 will announce the winners of the service awards for outstanding work provided by individuals on behalf of X9 standards. If you have not registered for the ACM, please do so now.

Best Regards,

Cindy Fuller
X9 Executive Director

Cryptography 101 Demystifying the Concept

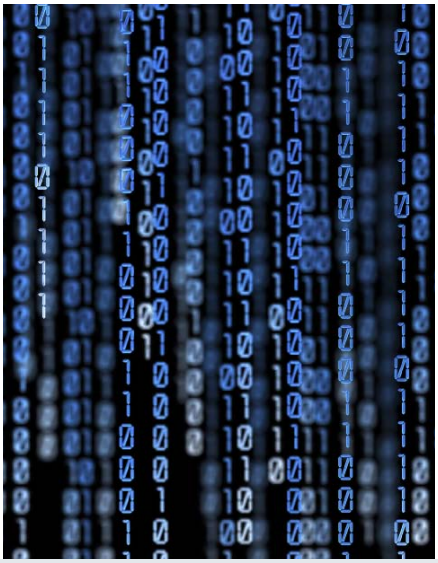
By Ed Scheidt, Chair, X9F, Data and Information Security

Cryptography has a long history. The difference between contemporary usage and the usage of old can be attributed to the introduction of mathematics to the process. The Greeks defined cryptography as hiding something through writing. Today this has been replaced by creating a 'secret' that is bound to the information through a mathematical process. How today's secret is established includes three basic elements: the information itself or the data, a transposition algorithm, and the locking and unlocking keys.

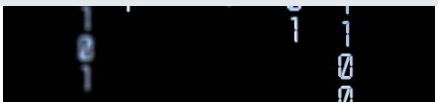
a) *Information* and the secrecy of the information come with many definitions, but most simply, the secretive information is something that one may want to hide from someone.
b) The *algorithm* is a mathematical representation of a coding schema that acts on the information. Today the algorithm comes in many variations. In our digital encryption world, this can simply be 'asymmetric' encryption or 'symmetric' encryption, or some combination of the applicable mathematics. However done, essentially the algorithm is used to transform the data that is to be kept secret.
c) The *keys* are the fundamental secret portion associated with encryption. The algorithm is applied to the data using the keys, both for transformation and reversal. Thus, if the keys are compromised, the information by definition is compromised, because the algorithms are often publicly known.

Delivery Channels, Data Residency and Data Usage

For financial services companies implementing cryptography or encryption, X9 has developed a variety of standards on encryption algorithms, cryptographic frameworks, and cryptographic and algorithmic implementation guidelines. The challenge for financial services companies may be taking what is most suitable from the available inventory of stan-



ACCREDITED STANDARDS COMMITTEE X9, INC.
1212 WEST STREET, SUITE 200, ANNAPOLIS, MD 21401
410.267.7707 WWW.X9.ORG



dards and mapping an encryption process to a business need, while maintaining the secret associated with the encryption. The business cases wherein encryption can be considered a major security tool include a gamut of solutions. These solutions can be described as end-to-end, end-to-many, or many-to-end. But any chosen solution model must leverage the banking infrastructure. If successfully applied, the possibility of having an encryption solution as part of a Return-on-Investment (ROI) undertaking is within reach.

Computing has changed. We have evolved from mainframes, to mini computers, to Personal Computers, to mobile devices, and now to Cloud-based services. All these media have and can use encryption, but performance, recoverability, and scalability place limitations on where a certain encryption paradigm is used.

Experience has shown that secure channels can be effective for end-to-end protection, but they become harder to manage when applied to more distributed information management and delivery architecture. The advent of the 'secure channel' was intended to protect information that is exchanged between two business entities, with the use of encryption. One entity is generally central and fixed (the 'provider'), and the other entity can be one of many (the 'subscribers'). This security paradigm can be referred to as the *Data-in-Transit* model.

Now there is another security paradigm referred to as the 'Data-at-Rest-Over- Time' model. It essentially extends the protection of information to storage of the data. Secure Cloud computing is an example of this model. What is now emerging as a fundamental requirement is to leverage encryption as an enforcement tool to protect content (the data at rest), while simultaneously including security tools to protect the network (the data in transit).

As technology continues to advance, creating new business opportunities for value added service delivery, the landscape for the application of cryptographic protection expands. As one example, it is interesting to note that secure mobile banking and secure mobile payments offer a convergence of multiple different avenues for the implementation for encryption, some more recent and some more traditional. Some examples follow.

a) *Identity assurance* for the approved customer can include encryption in the form of signing or a biometrics tied to encryption.
b) *Differential access* to content can be enforced by encryption for distributing banking data for government purposes versus commercial purposes, addressing both the privacy and liability regulations of each type of access.
c) The use of traditional encryption can protect messaging within the banking digital infrastructure.

Another view to consider related to protecting content is the *usage*. For example, a name, address and phone number can be used in a public domain where encryption would not be needed; whereas the same name, address and phone number may need to be protected in a banking scenario where customer privacy must be considered.

Key Management

Let's shift to another important element of encryption, the key management. So far, we have a secret that we want to keep and the means to render it 'unintelligible' to a viewer. This is easily done if one simply wants to contain the secret only to oneself. However, it becomes more complex if one wants to share that secret with another party. The main point is that a 'specific secret' needs to be established strictly between the two involved parties at each end. For example, my bank wants to protect my information from others having similar access, so my information cannot be read without my permission, while similarly allowing another's private information exchange with the same bank. This is the basic tenant in secure banking. Encryption is a great tool for accomplishing this, but there are keys that must be associated with the encryption process in order to protect the one-on-one privacy between the two entities.

We Want You!

You like to put your thoughts into words, and you like to express your ideas to others. You take pride in your writing talent, and you know how to get your thoughts across to your reading audience. You can project your thoughts in a deep technical and elevated level. Actually, you think of yourself more as an author, not just a technical writer.

If this sounds like you, why not contribute your skills and knowledge to writing an article for the X9 EXTRA. You could be helping your fellow X9ers learn something they perhaps never knew or realized about our community and standards development.

If this peaks your interest, then please contact Ed Stana ed.stana@x9.org of the ASC X9 Marketing and Membership Committee. You don't need to be a professional writer, you just require the knack for written communications and you need to know your subject matter. Above all, you're interested in doing something perhaps different and challenging for X9. Thanks for your help.

—Encryption can be considered a major security tool—

As encryption has evolved over the years, so has key management. Key management may be viewed in a simple sense as a random number that can be associated with a specific encryption algorithm. This key must be kept secret if the information associated with this key is to remain secret and easy to use. However, the process to keep the keys secret and to distribute these keys can become very complex. Much study has been done to create frameworks that result in a complete business life cycle for these keys, from creation to cancellation. Current examples of X9 standards that identify algorithms and key management frameworks for banking business solutions include: Key Agreement and Key Transport using Elliptical Curve Cryptography can be found in X9.63, Certificate Management information that can be found in X9.79-1 PKI policy and Practices Framework, and, dynamic key management of CKM for content that can be found in X9.73 Cryptographic Message Syntax: ASN.1 and XML. Beyond these examples there are other X9 standards that offer different usages of encryption.

Summary

As a security tool, encryption has dependencies. Encryption can be used to protect information, but to be effective the encryption itself must be protected. The extent of the risk and trust associated with the exchange become the measure of the level of protection that is afforded to safeguarding the encryption process. Higher risks can result in a multiple dimension solution; whereas, lesser risks can result in a simple solution, for example, a fixed processing platform and a dedicated pin. Encryption may be embodied in a box with inputs and outputs, or encryption can be deployed as a software application. In the digital world, any encryption must ultimately reside on some computing platform, which can range from a specialized chip or a cell phone to a mainframe computer.

Let's not forget the long history of encryption. As a point of reference, the Knights Templar in the 12th Century were conducting banking and using encryption, although in those days they were with analog encryption, or rather, procedures that were not based on current technology. Today's business usage of encryption is deployed through the *implementation of digital encryption*. Standardizing these encryption implementations, as X9 has done over the years, offers acceptance, interoperability and other core business benefits to the financial services indusry.

X9 is continuing to look to future usages for encryption within the financial services. Many of the popular encryption tools and methodologies have been identified in the X9 standards. But cryptographic services can never be satisfied with the status quo. Encryption and cryptographic processes must be periodically refreshed to keep abreast of new financial services requirements, new security enabling platforms, and most importantly, increasingly sophisticated threats.

Financial Services Standard Wins Support Six Months Before Publication

Six months before the expected publication of the completed document, a draft ISO standard for the financial services industry has earned significant recognition and endorsement as a global solution for the accurate and unambiguous identification of entities engaged in financial transactions.

ISO 17442, *Financial services - Legal Entity Identifier (LEI),* is currently at the Draft International Standard stage and expected to be published as an ISO International Standard by January 2012. However, it was recently recommended by the Global Financial Management Association (GFMA) - a federation of global financial services trade associations - as a basis for a viable, uniform and global LEI solution.

The standard is being developed by ISO technical committee ISO/TC 68, *Financial services,* whose Secretary, Cindy Fuller, said the committee believed that the voluntary standards it develops can fulfill the requirements of both national and global regulators as they develop solutions addressing the data collection and analysis needs resulting from the recent global financial crisis. Ms. Fuller welcomed the GFMA support for ISO 17442 and said that the global marketplace would be developing governance to use the standard.

Karla McKenna, Chair, of ISO/TC 68, commented further: "We are pleased with the recommendation from global industry and await endorsement of the LEI standard for use by global regulators in the collection of information for the analysis of systemic risk."

Key attributes of the standard, addressing the requirements from global industry and regulators are:

- Enables unique identification of global entities requiring an LEI
- Defines robust open governance of the issuance and maintenance of the LEI scheme
- Defines an LEI that contains no embedded intelligence
- Can be applied worldwide to support the financial services industry
- Leverages the expertise of ISO/TC 68 in defining and maintaining identifier standards
- Is persistent
- Defines a scheme that is scalable and free from assignment limitations.