Global Information Assurance Certification Paper

Ted Demopoulos
GSEC Practical version 1.4b, Option 2

The Logbook of The World

Abstract:
Since the beginning of amateur radio, amateur radio operators have exchanged written confirmations of contacts. These written confirmations, called “QSLs”, are typically on a postcard-sized piece of paper and transferred via the postal service. QSLs are often attractive and many hams enjoy displaying them on their walls. A number of prestigious awards are available to amateur radio operators based on confirmed contacts. Since amateur radio is a technical hobby, and most amateur radio hobbyists (typically called “hams”) are technical, the manual process of filling out paper QSL cards and mailing them was a prime activity to automate. An obvious choice was using digital signature technology and the Internet, especially since most hams already log their radio contacts on computers and have Internet connectivity. However amateur radio is a hobby filled with tradition, and any proposed electronic solution would be contentious. It had to be technically sound, as well as simple to implement on nearly obsolete hardware – many hams reside in third world countries. It also had to complement the current system of exchanging paper cards rather than replacing it.

The Amateur Radio Relay League[i] (ARRL), a large US based non-profit organization with a membership of approximately 160,000, started a project to investigate the concept of electronic QSLs (eQSLs) known as “Logbook of The World” (LoTW) in 2000. Two external consultants with substantial industry security and PKI experience, Ted Demopoulos and Dick Green, were hired as architects for the project. Both the author and Dick Green felt that electronic QSLs were going to eventually become pervasive in amateur radio, and felt passionately that they must be implemented securely and intelligently. The first target for the LoTW project was to provide electronic confirmations and interface with the DXCC[ii] award program. The DXCC award is the premier award program in amateur radio, and the basic award is for confirming contact with 100 entities[iii], which are roughly equivalent to countries. The DXCC award is sponsored by the ARRL and is highly coveted because of its integrity; hence security was a prime concern. Future goals were to provide confirmations for additional award programs sponsored by both the ARRL and other organizations. An excellent introduction to QSLing issues and electronic QSLs is “A Perspective on Electronic QSLing”, http://zs6ez.za.org/articles/e-qsl.htm, by Chris Burger. He reaches the same conclusions as the authors: digital signature technology is required, and that eQSLs must be in some standard format that is easily machine readable.

Before:
Many hams spend a lot of resources collecting QSL cards. QSL cards not only are used to apply for awards, but often have pictures and are attractive as decorations. It is the custom that when requesting another station's QSL the requestor sends his QSL card filled out with the contact information, as well as a self addressed envelope and sufficient return postage. This is often in the form of US dollar bills. As in many countries international postage costs are the equivalent of over US$1, it is usually required to include two US dollar bills.

QSLing becomes somewhat expensive quickly, and is slow and time intensive. There is an alternate method of sending and receiving QSLs in bulk known as "The Bureau"[iv], which relies on national amateur radio societies. Cards can usually be sent for a few dollars per pound, however not all hams belong to their national organization, and this method is painfully slow – it is not uncommon for QSL cards to arrive two or more years after a contact! The author has received cards that were over a decade old via the bureau.

It has been estimated that the total worldwide cost to ham radio operators worldwide for exchanging QSL cards directly and via the "bureau" runs into millions of dollars per year.

Many stations are not interested in obtaining other's QSLs, but QSL mainly as a courtesy. Many of these stations are involved in "contesting". Contests are typically 48-hour competitive events where amateur radio operators contact as many others as possible. A contest station may contact over five thousand other stations in a weekend, and will often make many tens of thousands of contacts in a year. Contest stations often receive many thousands of unwanted QSL cards a year, and answering them is extremely time intensive as well as expensive. The author estimates he has received approximately six thousand QSL cards during the last calendar year and has spent over 100 hours partially answering them.

Qualifying for the basic DXCC award involves submitting 100 cards from different entities to the ARRL. Submitted QSL cards are rigorously screened and if there is any suspicion of fraud, an investigation ensues. The ARRL has a number of employees who are dedicated full time to the secure administration of the DXCC award program.

Clearly it is possible to produce fake paper cards fairly easily, either using a printer or perhaps a print shop. And if someone submits a fake QSL card from a country where amateur radio is widespread, for example Germany or Japan, the chances of the forgery being detected is very slim. However for countries with less common or rare amateur radio activity, for example The Congo or Vietnam, fake QSL cards have a higher chance of being detected. Numerous techniques are used to detect forgeries, including checking with the individual who allegedly is the source of the QSL card.

Occasionally individuals are caught trying to submit forgeries and banned from the DXCC program. It is widely accepted that although an individual may be able to cheat, widespread cheating is quickly discovered. Again, the ARRL has a number of employees who are dedicated full time to the secure administration of the DXCC award program.

There was already an existing eQSL system known as eQSL.cc[v] however it essentially offered no security and its "eQSLs" were not accepted by most award sponsors, including the ARRL. Although security features have been added to the system, they have not been deemed as sufficient for the DXCC award programs.

During:
In 2000, the ARRL formed a team to create a design for its "Logbook of the World" system. The team was comprised of three fulltime employees of the ARRL, and consultants Ted Demopoulos and Dick Green. The team's charter was to architect the system – engineering details would be decided by the as yet unselected development team.

The first seemingly obvious approach considered was to use X.509 Certificates[vi] and digital signatures. In practice, it would have worked just as traditional QSLing did: in order to get an eQSL from someone, you would send them a digitally signed email with the appropriate information (i.e., callsigns, frequency, date, time, etc). They would reply would a digitally signed email confirming the information was valid.

Individuals applying for the DXCC award could submit any combination of paper QSL cards and eQSLs to the DXCC Desk.

This approach was desirable for several reasons:

- It was a simple process that mirrored traditional QSLing practice.
- Most email programs supported S/MIME[vii] and hence digital signature.
- Although X.509 certificates would need to be distributed to participants there were several off the shelf commercial solutions available.

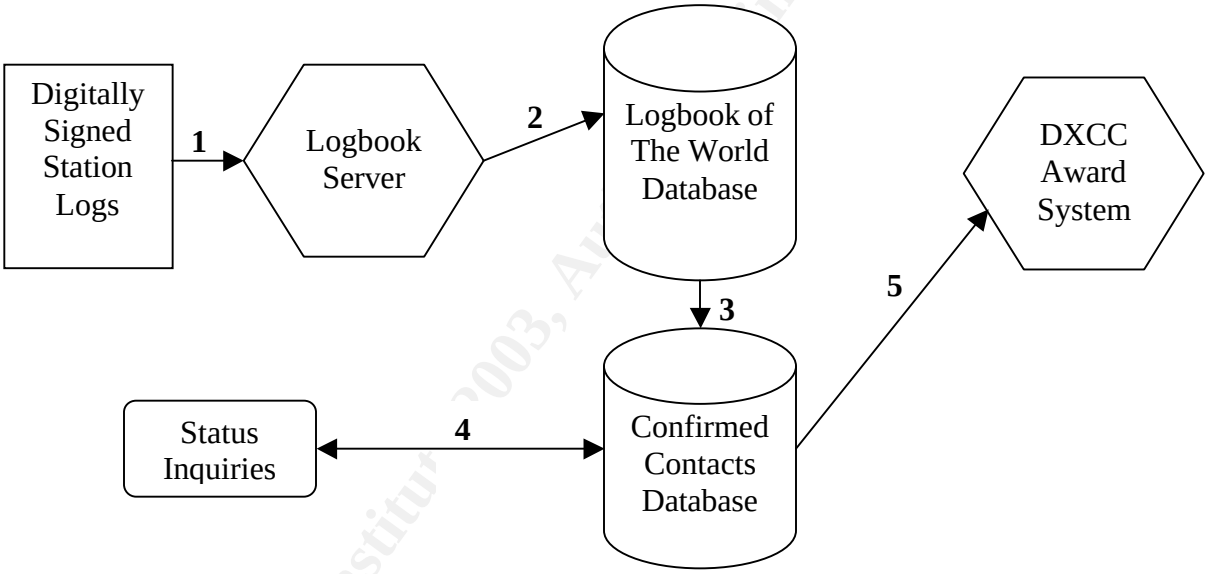
This approach had several difficulties and shortcoming as well:

- In order to send someone an eQSL and receive one in reply you would need to know their email address. Since email addresses can change, and there is no authoritative database of email addresses, this was a major concern.
- In order to confirm the digital signatures on eQSLs, a repository of pubic keys would be required.
- These eQSLs would need to be saved by participants and eventually submitted to the DXCC Desk.
- At least three steps would be required: sending an eQSL, receiving a confirmation eQSL, and submitting it for awards credit.

- At least three e-mails would be required for confirmation, submission to DXCC and status return.
- Someone, probably the ARRL DXCC Desk, had to act as a Certificate Authority. Since the ARRL has a very strong IT department, this was not seen as much of a difficulty.

We decided that the entire QSLing process needed to be examined and that simply mimicking current physical QSLing processes electronically was not necessarily the best solution.

After much analysis and discussion, a reengineered solution was put forth. Instead of hams emailing each other eQSLs, entire logs would be digitally signed and sent directly to the ARRL. The following diagram outlines the proposed solution, which was adopted with some minor changes.



1. A user submits a digitally signed log to the ARRL's logbook server. A log consists of records of one or more contacts made by radio.
2. The Logbook Server verifies the signature on the log and sends the log information to the Logbook of the World Database.
3. When a contact is confirmed by both parties it is added to the Confirmed Contacts Database. Only confirmed contacts, i.e. a contact for which both parties involved have submitted a log record, are available for award purposes. This adds an additional level of security over the paper QSL mechanism as described below.
   A small percentage of log data has errors. Sometimes the callsign is incorrect, perhaps the frequency, etc. These errors can occur for many reasons including operator error, such as miscopying a callsign, or logging errors, such as typographical mistakes. Unless both parties agree to the contact details, the contact is considered invalid.

With the existing paper QSL system, a QSL can be submitted for award credit, even though it may contain errors and the contact may be invalid. Since many hams receive hundreds or thousands of QSLs a year, the submitter may not even know that the contact is invalid. Slightly over 1% of the paper QSLs received by the author are for contacts that never occurred. Many radio amateurs do not check the validity of each card – it is simply too time consuming and not enjoyable.

4. Users can make status inquiries via a web front end to the Confirmed Contacts Database and see which of their submitted contacts have been confirmed.
5. The Confirmed Contacts Database is accessed by the DXCC Award System (and in the future other award systems) for specific award processing. This would require changes to the DXCC system. Fortunately the DXCC System was in the early stages of a major rewrite by external consultants.

At this stage we had the following open concerns and issues:

- With the current design, the Logbook Server stripped the digital signature off each log before sending it to the LoTW Database. It would be preferable to have each log record, i.e. the data for each contact, individually signed and have these digital signatures stored in the database along with the data. However this could not be done easily with a generic mail client.
- Some entity would need to create certificates for all hams that wanted to participate in the LoTW system, i.e. function as a Certificate Authority. Since it was decided that participation would be free for all radio amateurs, regardless of whether they were members of the ARRL or not, potentially a huge number of Certificates would be needed.
- The software needed for the ARRL to function as a Certificate Authority was very expensive, and outsourcing Certificate Authority functionality would also be very expensive.
- Securely distributing digital certificates to participants was difficult. Except for the United States, there are no definitive databases of ham callsigns and their owners.
- The rewrite of the DXCC software was already in progress. In would be necessary to coordinate with the team doing the rewrite to ensure interoperability. The rewrite had been outsourced to a group of non-amateur radio operators, so communication would need to be very specific and detailed.

I felt that the additional security of having each contact record individually signed outweighed the ease of using a standard email client to sign logs and helped convince the rest of the team. Although the DXCC program has never had an insider attack on its integrity (to the best of the team's knowledge), having

individual contact records signed and having those signatures stored in the LoTW Database along with the data would make an insider attack more difficult. To facilitate this, the following applications and source code would be made available:

1. A stand-alone application that can be used to sign log files produced by ham radio logging programs.
2. Open Source code that ham radio logging programs can incorporate to integrate log file signing functionality.
3. A simple application that can be used to create signed log files from log data, intended for those not using computer logging.

It was decided that the ARRL's IT department would be a Certificate Authority. Unfortunately commercial software was much too expensive, especially since most vendors charged per Certificate, and the ARRL intended to make Certificates available to free of charge.
We decided that the ARRL would develop their own Certificate Authority code. This was initially contentious, as most programmers are not cryptographers and history is full of examples of badly designed and/or implemented cryptography and other security code. In particular, I had severe reservations. Although the ARRL had several superb programmers, there were neither cryptographers nor security experts. The ARRL was extremely lucky to hire a developer with extensive cryptography and Public Key Infrastructure experience, and my objections went away.
Although the initial thought was to use X.509 Certificates due to the support in most email clients and the availability of commercial software, this was no longer an issue. Also, the ARRL would be the only Certificate Authority, and since interoperability with other Public Key Infrastructure systems was neither needed nor desired, following the X.509 standard was no longer mandatory. I felt that there was no strong reason not to follow the standard, but was eventually convinced that following the X.509 standard should not be required. It was left open as a development issue to be addressed by the development team.

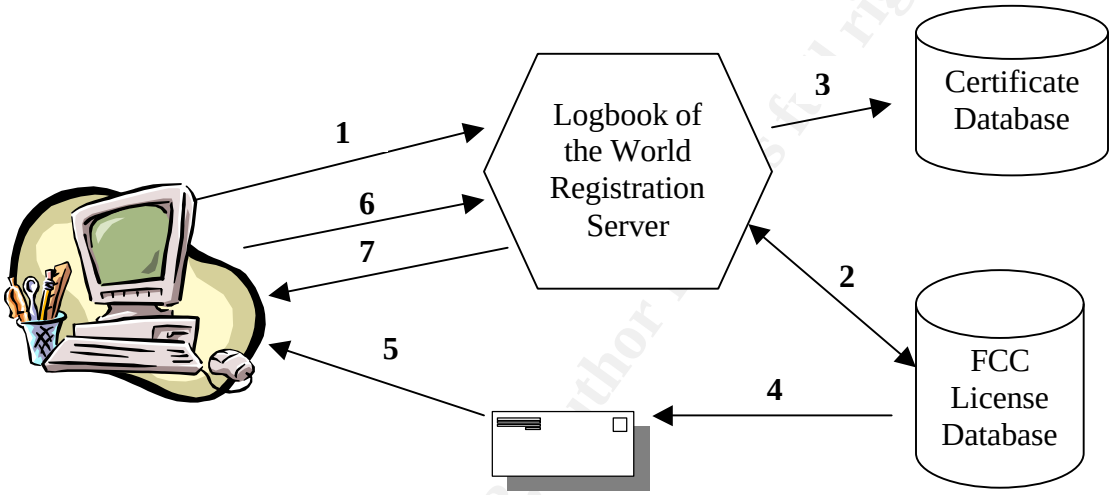
Deliberations discussing user's initial registration into LoTW were lively. As expected, they focused on getting the correct balance between security and ease of use for the end user. One line of thought was that for members of the ARRL who already had a login to the member's only area of the ARRL Web site, registration would be almost automatic. They would just click on a button and have a Certificate issued. However, users regularly forget their passwords and are reissued new passwords over the phone. This was sufficient for protecting access to the read only access to the members only area of the website, but not necessarily for controlling registration to the LoTW.

In the end, Dick Green and I convinced the ARRL management that security should initially be tight – it could easily be loosened in the future, but the converse was not true. A document was written discussing possible mechanisms for user's initial registration, as well as the security concerns, ease of use, and

potential attacks for each mechanism. The mechanisms chosen are described below.

Two different mechanisms were chosen to initially distribute Certificates; one for USA licensed radio amateurs and one for all others. The reason for two mechanisms was simple: The Federal Communication Commission (FCC) makes available the definitive database of licensed radio amateurs in the USA, and there is no such definitive database for any other country available.

Initial Registration and Certificate Request, USA licensed Radio Amateurs



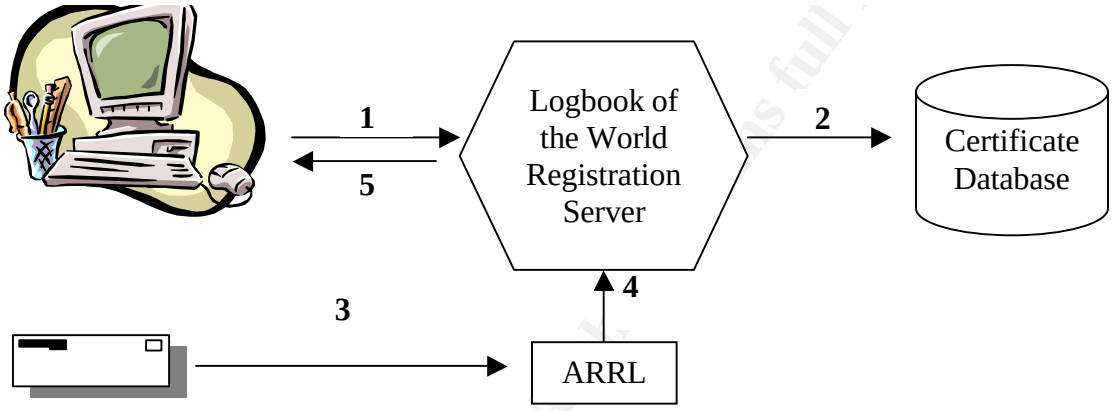
For USA licensed amateur radio operators, the initial registration process is illustrated in the above diagram and described below:

1) The applicant makes a request to enroll in the LoTW program. The request includes the public key of a key pair created by the applicant's registration software.
2) The applicant's license details are checked in the Federal Communication Commission's database for validity.
3) A non-signed Certificate is created and written to the Certificate Database.
4) The applicant's postal address is extracted from the FCC database and written to a postcard.
5) An activation password is written to the postcard and the postcard is sent to the applicant.
6) The applicant submits the activation password to the Logbook of The World registration server.
7) The Certificate is signed by the ARRL's CA private key, sent to the applicant and written to the Certificate Database.

There were two concerns with this approach: the costs of postcards/postage, and errors in addresses in Federal Communication Commission's database.

The ARRL concluded that the costs of postcards and postage was minimal, and long term would easily be compensated within the DXCC program by the need for less resources to manually check paper QSL cards.
Many hams do have incorrect addresses in the Federal Communication Commission's database, often as a result of moving. Hams are supposed to inform the Federal Communication Commission when they move, but in practice rarely do until it is time to renew their license (every ten years). Since hams can easily update/correct their address electronically or via postal mail, this concern was satisfied.

Initial Registration and Certificate Request, non USA licensed Radio Amateurs



For non USA licensed amateur radio operators, the initial registration process is illustrated in the above diagram and described below:

1) The applicant makes a request to enroll in the LoTW program. The request includes the public key of a key pair created by the applicant's registration software.
2) A non-signed Certificate is created and written to the Certificate Database.
3) The applicant's sends the ARRL a copy of their amateur radio license, a copy of nationally issued identity document such as a passport or national ID card, and a certificate printout produced from the registration software in step 1.
4) The ARRL checks the documentation sent in step 3 and either accepts or rejects it.
5) If the documentation was accepted, the Certificate is signed by the ARRL's CA private key, sent to the applicant and written to the Certificate Database.

Initially we had concerns that the DXCC desk would receive lots of documentation in a myriad of foreign languages, especially since there are hams in almost every country. However the DXCC Desk already receives much documentation in foreign languages and has procedures in place to handle it.

It was decided by the ARRL that development of the LoTW system would be done internally by the IT group at the ARRL. Previous results with having software built externally had met with mixed results. Also, since the IT group was in regular contact with the external consultants rewriting the DXCC system, communications would be facilitated.

After:
The schedule for Logbook of the World has been severely impacted by the delivery of the new DXCC software, which is very late.

The LoTW server side software has been written although it cannot be fully tested as the new DXCC software is not yet finished. The Digital Signature Standard (DSS)[viii] is used for digital signature, and the X.509 specification has NOT been followed, as there was no benefit and there would have been additional implementation overhead. In addition, initial client side code for integration with amateur radio logging programs is available, and the following Windows based client side applications have been written:

tQSLCert – This is the application for registration. It creates key pairs, and sends requests to the LoTW Registration Server for certificates. It implements a "Registration Wizard" and has proven to be easy to use.

TQSL – This is the application for signing the records in a log file. It can sign the records in a log file in the Cabrillo[ix] or ADIF[x] formats. All modern amateur radio logging programs support at least one of these formats. It can also create the log file, allowing the user to type in details for each radio contact in the log, The signed logfile is then emailed to a robot at the ARRL.

Initial external testing of LoTW began in early January 2003 and lasted for several weeks[xi]. Dozens of amateur radio operators took part including the architects of the system and developers of amateur radio logging programs. The results were fantastic and only minor bugs were reported. General beta tested is expected soon.

"LoTW beta testing for the general Amateur Radio public is expected to begin soon. The ARRL has not announced a specific inauguration date for Logbook of the World. " (ARRL, "Limited "Logbook of The World" Testing is a Hit" 23 January 2003).

Other major amateur radio award sponsors have expressed interest in LoTW. Several models are being explored, including the ARRL licensing the Confirmed Contacts Database to award sponsors and the ARRL running entire award programs for sponsors for a fee. The details of these discussions have not been made public yet.

Summary:
The author has participated in architecting several Public Key Infrastructure projects. Most have failed due to non-technical reasons, most commonly lack of funding or lack of clear goals. Failure of Public Key Infrastructure projects has been commonplace.

In contrast, The ARRL's LoTW gives every indication of succeeding – it already functions extremely well, and has only been held up by the lateness of the new DXCC software with which it must closely interface. The external testing has been an absolute success. In comparing the success of this project with the failures of others the author has been involved with, there are some clear cut differences:

1) There was a clear mandate from management, the ARRL Board of Directors, in favor of this project. They not only understood the project well, but its implications for the ham radio community.
2) Expenses were understood and budgeted for. They were kept reasonable and also minimized due to "rolling" our own Public Key Infrastructure software.
3) There was a clear-cut separation between architecture and development. Only after the architecture had been completed and agreed upon had the development begun.
4) The deliverables were clearly defined and understood. Other PKI projects I have been involved with were implementing PKI frameworks for no specific reasons, for example designing a general purpose certificate for electronic banking purposes, or implementing a corporate PKI framework for "future" uses. All the PKI projects I have worked on that had loose or ill-defined goals have had minimal success.

Although my involvement as a paid consultant ending in late 2001 when the "ARRL Logbook of The World Design Specifications" were accepted by the ARRL's Board of Directors, I have remained on the project as an unpaid advisor. I'm looking forward to the wide scale public testing of the LoTW which should begin very soon.

Glossary:

ARRL – The Amateur Radio Relay League is the national membership association for Amateur Radio operators. It has approximately 160,000 members and is a not-for-profit organization.

DX – A Radio term for long distance. In practice DX refers to distant contacts or contacts with uncommon areas. For example, North Korea, which has traditionally banned all amateur radio would be considered DX, even in South Korea.

DXCC – An award program by the ARRL. The basic award is for submitting QSLs from 100 entities, roughly equivalent to countries.

DXCC Desk – The group within the ARRL which runs the DXCC program.

Entity – The DXCC is program is based on entities, which include sovereign nations, and other landmasses such as territories, some uninhabited atolls, and disputed areas.

eQSL – an electronic confirmation of a radio communication. See QSL.

eQSLing - the process of sending and receiving QSLs electronically.

QSL – a written confirmation of a radio communication. Amateur radio QSLs are typically post card sized pieces of paper or cardboard that contain contact information, which as a minimum will include date, time, call signs of the stations, frequency, and mode (e.g. morse code or FM).

QSLing – the process of sending and receiving QSLs.

References:
Demopoulos, Ted and Green, Dick. “ARRL Logbook of The World Design Specifications.” Version 4.1, 29 May 2001.
http://trustedqsl.sourceforge.net/lotwspec.pdf (3 April 2001).

Burger, Chris. “A Perspective on Electronic QSLing.” 31 March 2002.
http://zs6ez.za.org/articles/e-qsl.htm (7 April 2003).

Morris, Dave. “Step-by-Step Overview of How eQSL.cc Works.”
http://www.eqsl.cc/qslcard/Presentation.cfm (5 April 2003)

Footnotes:

[i] “About the ARRL.” 5 September 2001.
http://www.arrl.org/aarrl.html (21 April 2003).

[ii] “The ARRL DX Century Club Program.” 17 March 2003.
http://www.arrl.org/awards/dxcc/ (21 April 2003).

[iii] Moore, Bill. “ ARRL DXCC List.” April 2003.
http://arrl.org/awards/dxcc/dxcclist.txt (3 April 2003).

[iv] Cook, M. “ARRL QSL Bureaus.” 16 October 2002.
http://www.arrl.org/qsl/ (3 April 2003).

[v] “eQSL.cc The Electronic Card Centre.”
http://www.eqsl.cc (3 April 2003).

[vi] Housley, R. et. al. “Internet X.509 Public Key Infrastructure Certificate and CRL Profile.” January 1999.
http://www.faqs.org/rfcs/rfc2459.html (15 March 2003).

[vii] Ramsdell, B. “S/MIME Version 3 Message Specification.” June 1999.
http://www.faqs.org/rfcs/rfc2633.html (15 March 2003).

[viii] “Digital Signature Standard (DSS).” 19 May 1994.
http://www.itl.nist.gov/fipspubs/fip186.htm (18 April 2003)

[ix] “Cabrillo Standard Summary Sheet Proposal V2.0.”
http://www.kkn.net/~trey/cabrillo (15 March 2003).

[x] “Amateur Data Interchange Format.” 10 April 2003.
http://www.hosenose.com/adif (15 March 2003).

[xi] "Limited 'Logbook of The World' Testing is a Hit." 23 January 2003. http://www.arrl.org/news/stories/2003/01/23/100/ (21 April 2003).
.

Last Updated: September 22nd, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive