ARRL

LOGBOOK OF THE WORLD

Design Specification

Dick Green WC1M
Ted Demopoulos KR1G

Revision 4.1B
May 29, 2001

Acknowledgements

As the availability of computers and electronic communications facilities has grown throughout the world, many amateur radio operators have realized that the cumbersome task of confirming radio contacts, traditionally carried out with paper cards through the mail, could be transformed into a fast and simple process by using “electronic QSL cards” or a central “electronic logbook of the world.”

In recent years, amateurs familiar with advanced data security technology have suggested that digital signatures could be used to ensure the integrity of the QSLing process. Therefore, the fundamental idea of secure electronic confirmations presented in this document is not new, and belongs to the entire amateur community.

Nevertheless, many details had to be worked out to arrive at a truly secure solution that could provide the required functionality in an easy-to-use fashion. In 2000, the ARRL formed a team to create a design for its “Logbook of the World” system. The design team members are:

Dave Patton, NT1N
Wayne Mills, N7NG
Jon Bloom, KE3Z
Ted Demopoulos, KR1G
Dick Green, WC1M

The design team also received valuable review and suggestions from Dave Sumner, K1ZZ, Bill Moore, NC1L, and Darryl Wagoner, WA1GON

Table of Contents

Section 1 — System Overview

1.1 Introduction

Throughout the history of amateur radio, operators have confirmed contacts with each other by exchanging *QSL cards*. The cards are made of paper or cardboard and are almost always exchanged via postal mail. Many amateur radio operators enjoy collecting the cards and displaying them on the wall of their radio shack.

1.1.1 DXing and DXCC Awards

The growth of amateur radio brought with it a growth in *DXing,* the practice of completing radio contacts with other amateurs in as many different countries as possible.

The DX Century Club, or *DXCC,* was established by the ARRL to grant award certificates to amateurs submitting QSL cards confirming radio contacts with at least 100 different countries, which are called DXCC *entities*. Endorsement stickers can be earned by confirming contacts with up to the maximum number of entities defined by DXCC, presently 334. A coveted plaque is awarded for achieving *Honor Roll* status by confirming contacts with 325 entities, and there is a Number One Honor Roll plaque for confirming contacts with all the entities on the list. Endorsable award certificates are also available for confirming contacts with 100 or more entities on each of various frequency bands, and the *5 Band DXCC* plaque can be earned by confirming contacts with at least 100 countries on each of five frequency bands.

Obviously, an amateur must obtain many QSL cards to qualify for these awards. It is not uncommon for an amateur to collect hundreds or even thousands of cards on the road to the top awards. As a result, this most popular of all ARRL programs generates an enormous amount of QSL card traffic: literally millions of cards are exchanged each year.

1.1.2 Your Money or Your Time: QSLing Direct or "Via the Buro"

As mentioned earlier, QSL cards are often exchanged by mail. This is called *direct* QSLing. In the case of a domestic QSL, an inexpensive postcard will sometimes suffice, although many amateurs prefer to use first-class envelopes so there is less chance of the card being damaged. Further, when requesting a QSL card, it is customary to include return postage and a self-addressed envelope. These items cost money and require a stamped outer envelope as well. The cost of postage, envelopes and cards to obtain a single domestic QSL card in the U.S. is at least 75 cents and the cost of obtaining a single DX QSL card can range from about two dollars to nearly five dollars.

Thus, the cost of direct QSLing can make awards chasing a very expensive proposition: some amateurs will spend well over one thousand dollars to collect enough QSL cards to qualify for Honor Roll or 5BDXCC.

Besides the considerable expense, there are other problems with direct QSLing. First, even though it is the fastest way to get a card back, sometimes there are delays of weeks or even months because the time-consuming and inconvenient task of replying may not be the first priority of the other operator. Second, it is risky business sending an envelope with return postage to certain countries. It is not at all unusual for such mail to be pilfered and lost forever. It can take several attempts to get a card from such countries, adding to the cost and turnaround time.

For a long time, the only alternative to the cost, delays and uncertainty of direct QSLing has been the ARRL Outgoing and Incoming QSL Bureaus, known as "the *Buro"*. The buro system allows amateurs to batch large numbers of cards together and mail them to a central domestic collection point where they are sorted by destination and distributed in bulk to corresponding buros in other countries. From there, the cards are sorted by call and held until enough cards are accumulated for a given recipient to make a batch mailing cost effective.

The buro system significantly reduces the cost of QSLing and the probability of theft. However, it has several major drawbacks. First, the turnaround time to receive a card is normally from several months up to several years. This is due to operators at both ends accumulating many cards before shipping any of them, slow bulk shipping at several points in the process, reliance on multiple groups of volunteers, and low priority accorded to buro cards by QSL managers (direct QSLs usually get top priority.) Second, the buro system relies on large numbers of volunteers. As traffic grows, the task of recruiting such volunteers becomes more difficult and has significant hidden costs for the ARRL. Third, bulk postage costs are rising, making the buro route less financially attractive as time goes on.

1.1.3 Contesting Compounds the Problem

Another operating activity that has grown dramatically is contesting. Since contests provide an opportunity to contact hundreds or thousands of stations in a single weekend, many DXCC awards-chasers participate in contests. Their requests for QSL cards often represents a bookkeeping burden for contest operators, many of whom have responded by dumping unsolicited cards for an entire contest log into the buro system. This practice has dramatically increased the amount of buro traffic, resulting in even greater cost and labor requirements.

1.1.4 How much does it cost?

It is estimated that the total worldwide cost to amateurs worldwide for exchanging QSL cards direct and via the buro runs into millions of dollars per year.

1.2 Electronic QSLs

With the proliferation of modern computers and the Internet throughout the world, many amateurs have realized that electronic QSLs can solve virtually all of the problems associated with exchanging paper QSL cards, especially the two most formidable: cost and turnaround time.

1.2.1 Benefits and Challenges of Electronic QSLs

Electronic QSLs offer many potential benefits:

- Fast, automated creation from computerized logs
- Greater accuracy (no errors transposing data from log)
- Virtually instantaneous transmission to target station
- Fast, automated reply processing from computerized logs
- Virtually instantaneous transmission of reply
- Fast, automated record keeping of confirmations
- Fast, automated preparation of submissions for awards credit
- Virtually instantaneous transmission of QSLs for awards credit
- No data entry cost at the ARRL DXCC desk
- Dramatically reduced data entry time at the ARRL DXCC desk
- No data entry errors at the ARRL DXCC desk
- No postage, printing and envelope costs
- No buro volunteers required
- Thousands of hours of labor saved by participants, ARRL and volunteers

Electronic QSLs also present a number of challenges:

- Authentication of identity for online applications is difficult
- State-of-the-art network security measures are required to prevent cheating
- Log programs authors must implement new features
- ARRL must develop a major new software application
- Some designs may result in huge increases in email traffic
- Many amateurs enjoy the images on printed cards
- Many amateurs enjoy collecting and displaying cards
- Some DXpeditions are partly financed by contributions sent with QSLs

1.2.2 Authentication is Critical

While all of the problems enumerated above are important, the most formidable barrier to implementation is authentication. In order for participants to have confidence in an electronic QSL system, they must be assured that each confirmation submitted to the system is authentic – that it comes from the true owner of the associated call.

Until recently, such assurance would have been impossible. However, with the advent of digital signature technology, it is now possible for an amateur radio operator to indelibly mark QSL data with a signature connected to his/her call. The signature cannot be forged and the signed data cannot be changed without detection. The technology used for digital signatures is called *Public Key Infrastructure* or *PKI*. It relies on a pair of mathematically related numbers. One of the numbers is called the *public key,* which can be published, and the other is called the *private key,* which is kept secret. PKI is explained in detail in Appendix A, "Public Key Infrastructure."

However, in order for digital signatures to be trusted, we must be sure of the identity of each person to whom a key pair is assigned. The security of the entire system boils down to the methodology used for proving identity and assigning the keys. This process is called *Authentication*.

Secure authentication for online systems is very difficult. A significant portion of this document is devoted to discussing authentication issues and alternatives.

1.2.3 Emulating the paper QSL system

It is possible to design an electronic QSL system that closely resembles the existing paper QSL system. In such a system, participants would e-mail each other digitally signed QSL data, called *E-QSL*s, much as they mail signed QSL cards to each other today. The recipient would digitally sign the QSL data to confirm the contact and would e-mail the E-QSL back to the recipient or forward it to DXCC. There are a number of problems with an E-QSL system:

- A centralized database and access software are needed for participants to obtain each other's e-mail addresses.
- A centralized database and access software are needed for participants to obtain each other's public key for signature verification.
- Requires at least three steps to send QSL, receive confirmation and submit for awards credit
- Requires at least three e-mails for confirmation, submission to DXCC and status return.
- QSL requests for a major DXPedition or contest operation would result in thousands of incoming and outgoing e-mails.

Fortunately, there is a better way to implement electronic QSLs: The ARRL Logbook of the World.

1.3 Logbook of the World

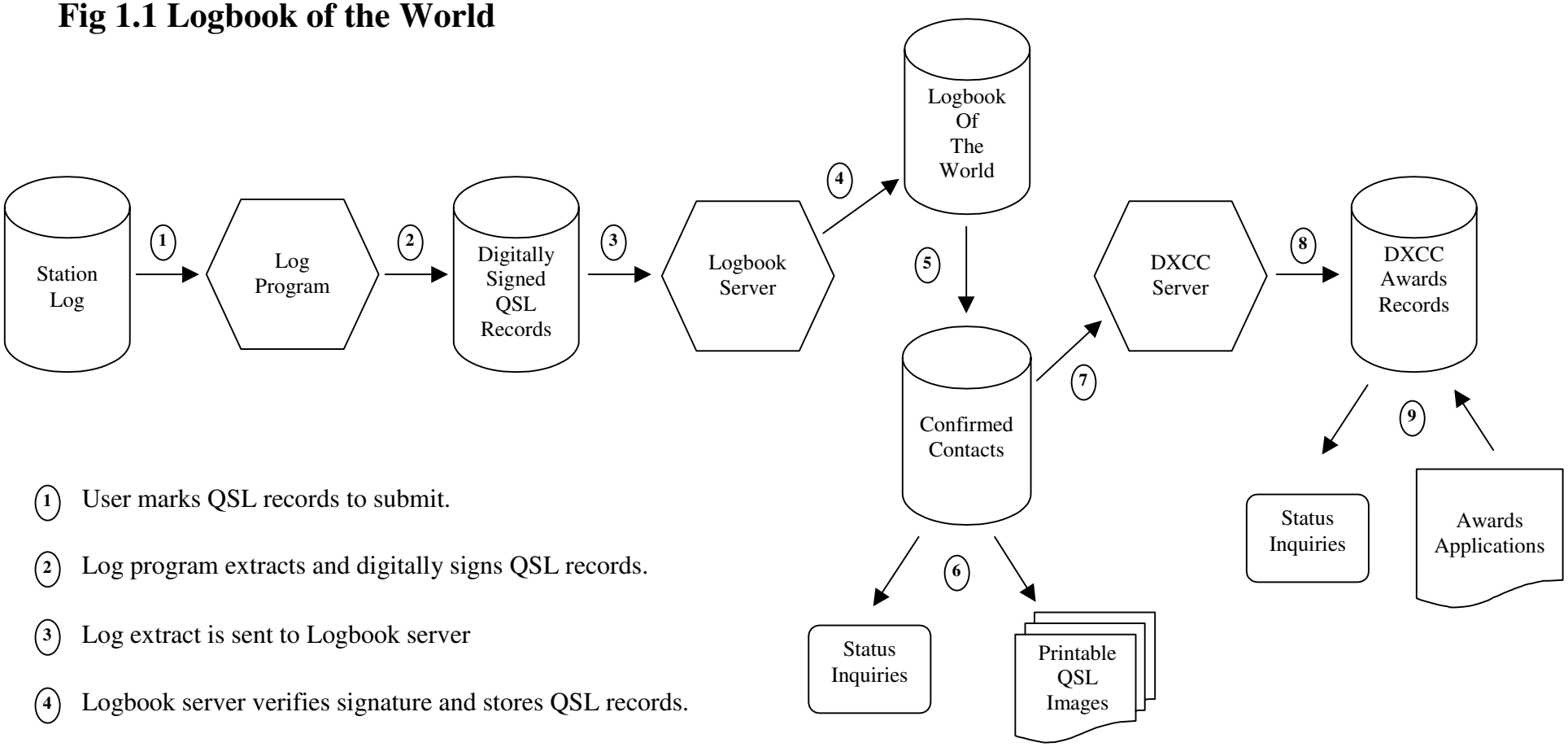
The ARRL Logbook of the World allows participants to submit radio logs containing digitally signed *QSL records*. Logs from all participants are collected in a central database, where they are scanned for matching confirmations. When a pair of matching QSL records is found, confirmation is sent to the ARRL DXCC system, where awards credit for both participants is automatically recorded.

There are many advantages to the Logbook of the World:

- Simple one-step submission process
- Minimizes e-mail traffic
- Can be hybridized with existing paper system
    - Users can send log extract *and* paper cards
    - DXCC can check the cards against the log extract
    - Eliminates QSL data entry step for DXCC
- Can be used for scientific and operating studies
    - Long-term propagation trends
    - Most-wanted surveys
    - Operating patterns
- Attractive system for contesters, QSL managers and DXpeditions
    - Just ship the log
    - No individual card processing
    - No card printing costs

Figure 1.1 illustrates the ARRL Logbook of the World system.

Fig 1.1 Logbook of the World



1. User marks QSL records to submit.
2. Log program extracts and digitally signs QSL records.
3. Log extract is sent to Logbook server
4. Logbook server verifies signature and stores QSL records.
5. When matching QSL records are received, confirmations are generated.
6. User can display confirmation status and download printable QSL images.
7. Confirmation records are sent to DXCC server.
8. DXCC server updates awards records
9. User can display awards status and apply for awards.

1.4 Authentication Overview

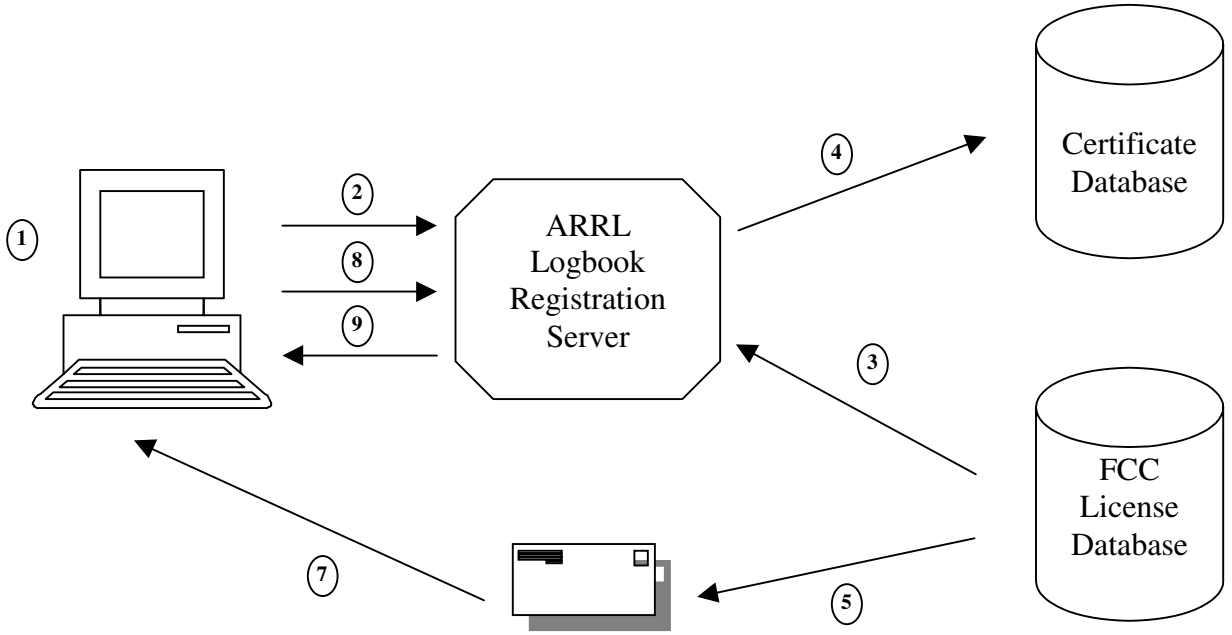
The digital signatures used for the Logbook of the World system ensure that every QSL record can be traced to the participant who submitted it. The signature cannot be forged and the QSL data cannot be altered without detection. But how do we know the identity of the participant who digitally signed the QSL record? This is the job of the Logbook authentication system.

Logbook of the World uses two methods for authenticating the identity of participants, one for U.S. calls and one for non-U.S. calls.

Authentication for U.S. calls relies on a combination of the *FCC license database* and postal mail addresses. Figure 1.2 illustrates the process. The applicant initiates registration through a computer *log program*. First, the log program creates the keys that will be used for digitally signing QSL records. Then the log program sends a registration request to the *Logbook Registration Server* via the Internet. The server looks up the applicant's name and call in the FCC license database to verify that they are valid. The server then generates an identification record, called a *certificate,* and a unique activation password. The password is written to a postcard, along with the call sign owner's name and address from the FCC license database. The postcard is mailed to applicant. When the applicant receives the postcard, he or she enters the password in the log program, which sends it to the server via the Internet. The server activates the certificate and sends it back to the applicant via the Internet. The address in the FCC database and the security of the postal mail system identify the owner of the call and ensure that the certificate is issued to the right person.

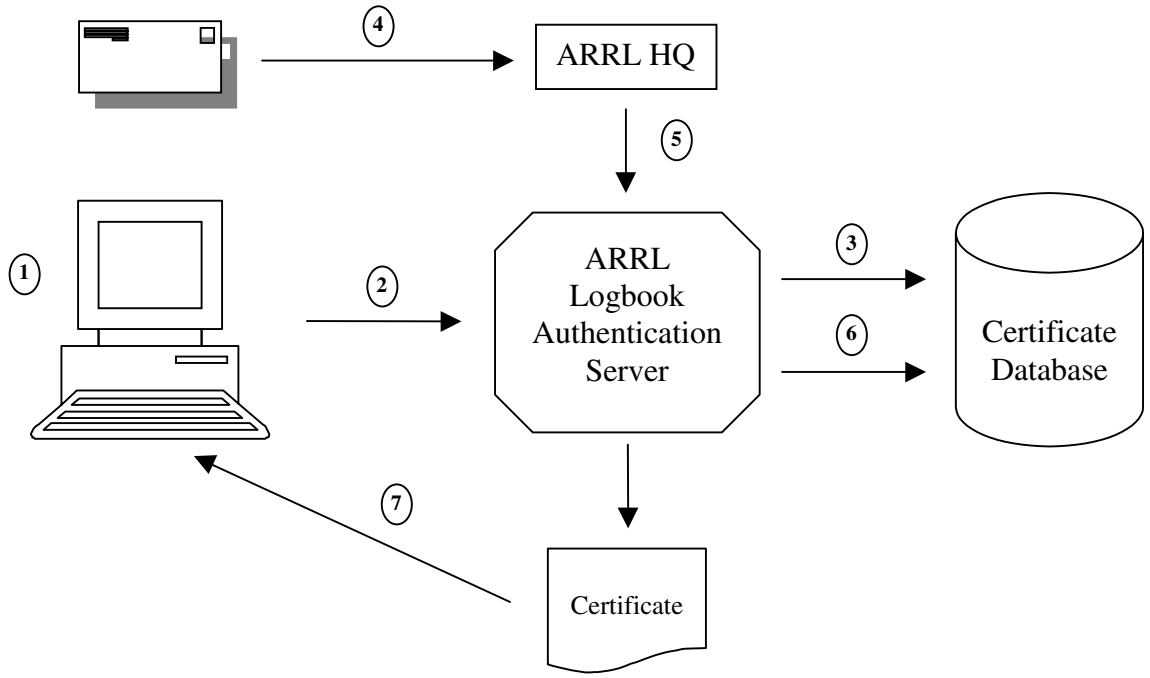
Authentication for non-U.S. calls relies on photocopies of a radio license and an official identification document. Figure 1.3 illustrates the process. The applicant initiates registration through a computer log program, which creates the digital signature keys that will be used for signing QSL records. Next, the log program sends a registration request to the Logbook Registration Server via the Internet, and the server generates a certificate. The applicant then sends a photocopy of his or her radio license, an official identification document, and a printout of certain digital signature key information to ARRL HQ via postal mail. When the documentation is received, an operator at ARRL HQ examines it and activates the certificate. The certificate is then sent to the applicant via the Internet.

Fig. 1.2 Logbook Authentication for U.S. Call Signs



1. Digital signature keys are created by log program.
2. Registration request is sent to ARRL Logbook Registration server
3. Call and name are checked against FCC License Database.
4. Pending certificate is created and written to certificate database.
5. Licensee name and address are written to a postcard.
6. Activation password is written to the postcard.
7. Postcard is mailed to the applicant.
8. Applicant sends password to server.
9. Certificate is activated and sent to applicant.

Fig. 1.3 Logbook Authentication for Non-U.S. Call Signs



1. Digital signature keys are created by log program.
2. Registration request is sent to ARRL Logbook Registration server.
3. Pending certificate is created and written to certificate database.
4. Applicant mails copies of license, ID, and key info to ARRL.
5. ARRL checks documentation and authorizes applicant.
6. Certificate is activated.
7. Certificate is sent to applicant.

Section 2 — Functional Specifications

2.1 Authentication Process

2.1.1 Introduction

Authentication of identity and call sign ownership is required before the system can issue the certificate and private key that allow a participant to submit log extracts.

This section details the functional specifications for authenticating a Logbook participant. A general outline of the authentication process may be found in section 1.4, "Authentication Overview". A discussion of authentication security issues may be found in section 3.1, "General Security Issues. A detailed analysis of alternative approaches to authentication may be found in section 3.2, "Authentication Analysis".

2.1.2 Logbook Registration Rules

Registration rules for Logbook of the World will be as follows:

1. **U.S. Call Signs --** Online registration for any currently-held U.S. call. The applicant must reside at the address listed in the FCC license database. An activation password will be returned by postal mail to that address.

2. **Non-U.S. Call Signs** – Online registration for any currently-held call. Requires mailing a photocopy of the license, photocopy of one official identification document and certificate printout to HQ. Registration notice is returned via e-mail or website.

3. *Note: It is possible to use authentication rule #2 for* all *participants, regardless of where the call was issued. The primary advantage of this approach is that it shifts the postage cost from ARRL to the participants. It is quite possible that labor costs for processing under rule #2 will be similar to or lower than the cost of postage, postcards and handling required for processing under rule #1.*

4. Foreign portable calls where no license is issued (e.g., NT1N/F) require reasonable proof that the applicant was in the country in question (photocopy of visa, passport stamp, plane/train ticket, hotel receipt, etc.)

5. Domestic portable calls (e.g., NT1N/7) and domestic location information (e.g., county or grid square) are not authenticated. This information optionally may be supplied in submitted signed QSL records.

6. Persons registering a call for an entity that is defined as "rare" by DXCC will be required to mail DXCC a certificate printout for that call, along with the usual documents required by DXCC.

7. Each call must be separately registered. One key pair and certificate will be issued for each registered call.

8. A call may not be registered more than once, except for renewals (i.e, there can be only one active certificate per call.)

9. A certificate will be issued only to the holder of a currently valid license. Calls issued under expired licenses cannot be registered for Logbook.

10. An existing certificate for a given call will be revoked if someone with a current valid license for that call subsequently registers (the assumption is that the call was reissued to someone else.)

11. The date on each submitted QSL record cannot be earlier than the date the certificate was issued nor later than the date the certificate expired or was revoked. This rule does not apply to certificate renewals.

12. A previous holder of a call must submit all QSLs for that call before some else registers the reissued call.

13. Expired and revoked certificates will be permanently retained so that signatures can be verified indefinitely. However, signatures made after the certificate has expired or is revoked will be invalid. The standard software supplied for the system will prohibit signing a QSL after the certificate has expired.

14. Certificate will expire one year from date of issue, or when ARRL membership expires, depending on pricing model. Certificate may be renewed without authentication. [Alternative: Certificate expires when license expires. U.S. calls renewed online without authentication. Non-U.S. calls require authentication. Capturing expiration date from license may be difficult.]

2.1.3 Authentication Protocols

The following subsections detail the Logbook authentication protocols. Figure 2.1 illustrates the general processing flow.

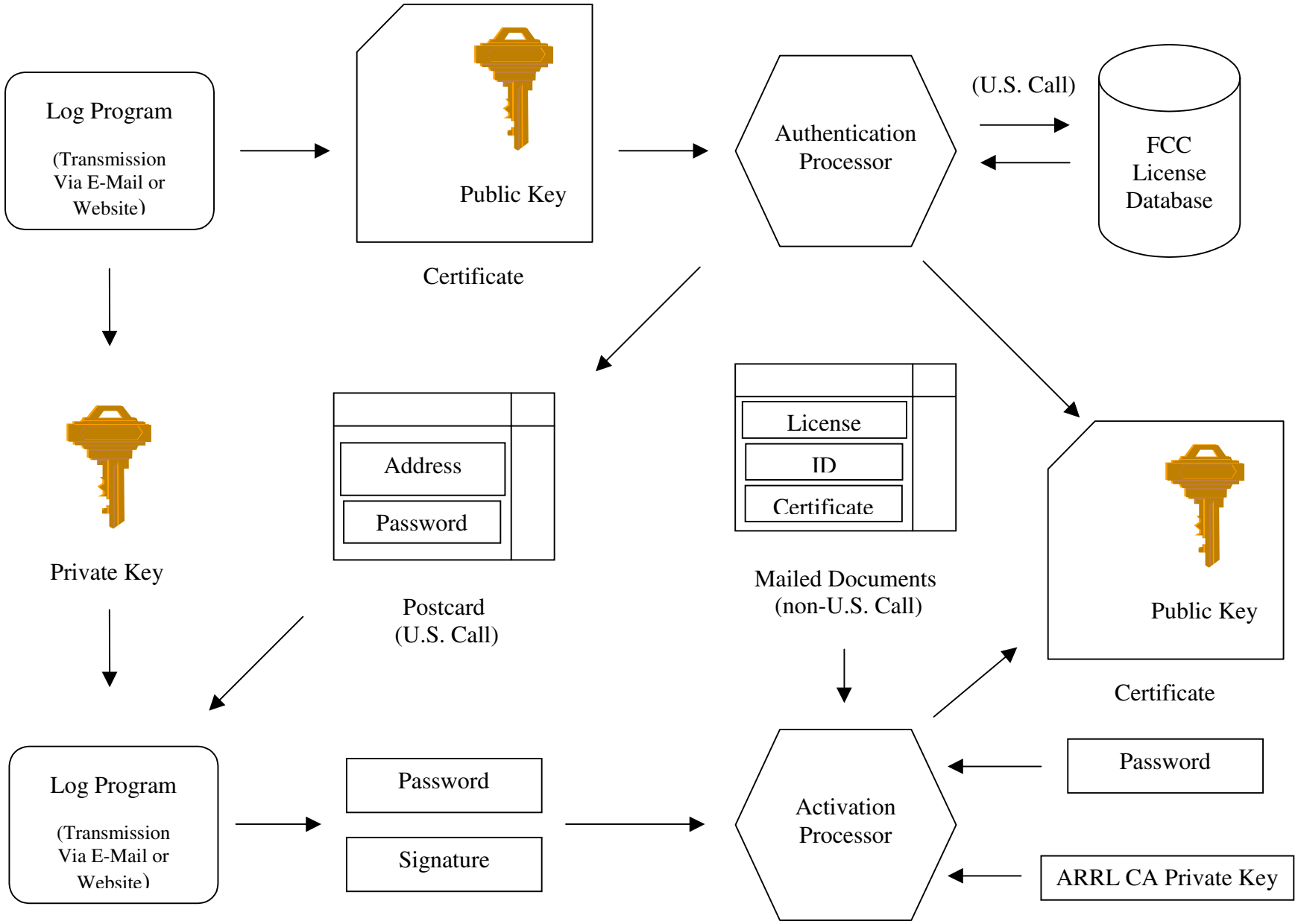
2.1.3.1 U.S. Call Sign

1. Key pair is created by log program on applicant's computer.
2. Certificate request containing call, name, public key and other information is sent to the ARRL server via e-mail or browser.
3. Server checks name and call in FCC license database.
4. Server generates certificate.
5. Applicant's name and address are printed on a postcard.
6. Server generates random password and prints it on postcard.
7. Postcard is mailed to applicant. Applicant enters in log program.
8. Log program sends signed password to the ARRL server via e-mail or browser.
9. Server signs certificate with ARRL CA private key.
10. Certificate and notification are sent to applicant via e-mail or website.

2.1.3.2 Non-U.S. Call Sign

1. Key pair is created by log program on applicant's computer.
2. Certificate request containing call, name, public key and other information is sent to server via e-mail or browser.
3. Server generates certificate.
4. Applicant mails photocopy of license, identification document and certificate printout to ARRL HQ.
5. HQ worker checks documentation.
6. HQ worker authorizes or rejects application at server workstation.
7. If authorized:
    - Server signs certificate with ARRL CA private key.
    - Server returns certificate and notification via reply address from e-mail received in step 3, or via website.
8. If rejected, server returns notification via reply address from e-mail received in step 3, or via website.

Fig. 2.1 - Authentication Protocol



2.1.4 Additional Authentication Specifications

2.1.4.1 Information Required for Registration

The log program registration function must have entry fields for all non-generated information required for the server to build the certificate. See section 2.2, “Certificate Authority” and section 2.3, “Log Program Specifications”. The required information will be included in the certificate request sent to the server during registration.

2.1.4.2 Key Generation

The key pair will be generated by the log program on the applicant’s computer (see section 2.3, “Log Program Specifications”.) The private key will be stored using standard PKI procedures in the key store on the applicant’s computer. The private key will *never* be sent to the ARRL server.

2.1.4.3 Certificate Creation

The server will create certificates in the format defined in section 2.2.3, “Certificate Specifications”. The public key and information from the registration form will be stored in the certificate. It is permissible to use the extended information portion of the certificate where necessary to store Logbook-specific parameters.

2.1.4.4 Password Generation and Mailing

The server will generate a random password at least eight characters in length. The password will be signed by the ARRL CA and will be stored pending entry by the applicant. The password will be printed on a postcard along with the address. Postcards will be mailed on a daily basis.

2.1.4.5 Password Entry / Certificate Activation

When the applicant receives the password, he/she will enter the password in the log program. The log program will send the password to the server via e-mail or a browser. The server will use the password to lookup its stored copy of the password and certificate.

If there is a match, the certificate will be signed with the ARRL CA private key. The password will be deleted. If there is no match, certificate activation will be denied.

2.1.4.6 Certificate Download

The certificate will be downloaded by the server to the client via e-mail or a browser. A secure connection is not required.

2.1.4.7 Certificate Renewal

When the certificate expires, the participant may renew it through the log program interface. The following steps will be taken:

1. Participant's computer generates a certificate renewal request.
2. Certificate renewal request is signed with the old private key.
3. Certificate renewal request is sent to the server via e-mail or a browser.
4. Server verifies the signature on the certificate request.
5. Server generates a new certificate and signs it with the ARRL CA private key.
6. New certificate is stored in the certificate database.
7. Old certificate is revoked.
8. New certificate is returned to participant via e-mail or a browser.
9. New certificate is stored on participant's computer.

Note that authentication is not required. Neither documentation nor a one-time password need be sent via postal mail.

[Optionally], the Logbook system will check the FCC database for a valid license record when a certificate containing a U.S. call is renewed.

Under the alternative presented in Rule 14 in section 2.1.1, "Logbook Registration Rules", certificates expire when the license expires. If this alternative is selected, then a step is added to the above sequence between steps 4 and 5:

> For a U.S. call the server obtains the new license expiration date from the FCC license database. For a non-U.S. call, the server puts the renewal on hold until a copy of the new license and a printout of the old certificate are received at HQ. The expiration date from the new license is entered by an operator and the sequence resumes with step 5.

2.2 Certificate Authority

2.2.1 Introduction

A *Certificate Authority,* or *CA,* is an entity responsible for issuing and managing PKI certificates (see Appendix A, "Public Key Infrastructure"). The ARRL will act as the Certificate Authority for the Logbook of the World.

2.2.2 Issuing Certificates

The process for issuing certificates is detailed in section 2.1, "Authentication Process".

2.2.3 Certificate Specifications

1. If possible, certificates should be X.509v3 compliant. However, the engineering team may select another format depending on implementation considerations.

2. If X.509v3 certificates are used, extensions will be allowed , as defined in the X.509v3 specification.

3. There will be one certificate per call sign.

4. Each certificate will contain a unique identifier. This is expected to be an integer.

5. Each certificate will contain at least the following fields:

    - *Certificate number (integer)*
    - *Issue date*
    - *Expiration date*
    - *Public key*
    - *Call Sign*
    - *Name*

6. There will be a database, separate from the main certificate store, containing any volatile data associated with certificates. At least the following fields will be included for each certificate:

    - *Certificate number*
    - *ARRL member number (if any)*
    - *Postal address*
    - *E-Mail address*

7. Certificates expiration and renewal: see Rule 14 in section 2.1.1, "Logbook Registration Rules", and section 2.1.4.7, "Certificate Renewal".

8. The digital signature algorithm will use either the RSA or DSA standard. The choice of digital signature standard will be made by ARRL after investigating possible export/import restrictions. If there are no applicable restrictions against either standard, or if the same restrictions apply to both standards, then the engineering team will select the standard. In either case, SHA will be used for the hash algorithm and the minimum public key size will be 1024 bits. If DSA is used, the values chosen for p, q and g will be fixed in order to eliminate covert channels.

9. The database in which certificates are stored initially will be accessible only by the ARRL. Should this database or a replica be accessible from outside the ARRL in the future, it shall be accessible via the industry standard Lightweight Directory Access Protocol (LDAP). In this case, a standard mechanism for revoking certificates shall be implemented, either Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP).

10. The certificate database format will be determined by the engineering team responsible for implementation.

2.2.4 Certificate Authority Implementation Options

The ARRL must either build or acquire CA software, or must outsource the CA functionality. These alternatives are discussed below.

2.2.4.1 Building CA Software

Since The ARRL PKI requirements are straightforward and simple, it is reasonable to develop the CA software instead of purchasing it.

It is estimated that the task of building CA software will not be extensive because few PKI features are needed: either X.509v3 certificate format without extensions or a custom certificate format probably can be used, direct access to the certificate database can be restricted to the ARRL

internal network, complex certificate revocation mechanisms are not required, and the client side functionality will be provided by ARRL in a programming library.

However, finding developers with a strong security background and expertise with X.509v3 is difficult and expensive. There are far fewer organizations capable of this type of development than are available to develop typical web and database applications.

Building the ARRL software in house or outsourcing it is a valid approach for the ARRL, assuming the necessary expertise can be obtained.

2.2.4.2 Buying CA Software

With the exception of Microsoft, discussed below, CA software is expensive. Although there are open source initiatives to build CA software, they are not yet ready for primetime.

Some notable vendors of CA software include XCert, RSA Security, Entrust, and Baltimore Technologies. None of them make their pricing models publicly available. However, their bids on various PKI implementations have usually been quite similar in the past. The following numbers must be considered only as a very rough price estimate, but will provide an idea of per-certificate pricing.

1500 Certificates	approximately $25-$35 per Certificate
10,000 Certificates	approximately $20 per Certificate
50,000 Certificates	approximately $15 per Certificate

In addition, there are always support changes for software updates, etc. These tend to run approximately 20-30% per year.

It must be noted that vendor offerings typically bundle more functionality than the ARRL requires, such as Certificate Revocation Mechanisms and LDAP compliant Certificate Directories.

Purchasing commercial CA software is a valid, although extremely expensive, approach.

2.2.4.3 Microsoft

Microsoft bundles CA software called “Microsoft Certificate Services” with all versions of Windows 2000 Server. This software was first introduced in a “Service Pack” for Windows NT 4.0 Server.

Although Microsoft Certificate Services could theoretically be used by the ARRL, and the pricing is currently superb (included with Windows 2000 Server), there are several potential problems. Most importantly, Microsoft Certificate Services must be considered as essentially Beta software. There are no known substantial commercial implementations and its stability and reliability are unknown. Also, it is likely that the extremely attractive pricing model will change with its next release to be more in line with other Microsoft products and other CA software.

The use of Microsoft Certificate Services by the ARRL cannot be recommended at this time.

2.2.4.4 Outsourcing CA Functionality

Certificate Authorities and PKI can be outsourced. There are number of companies who are very capable of managing of a PKI deployment of almost any size. The best known of these companies is VeriSign and their "Onsite" service. There are no public price lists, but prices quoted in the past have been significantly higher than the costs for purchasing CA software alone. Outsourcing CA functionality is an excellent choice for organizations with limited technical expertise that wish to concentrate on their core business.

Outsourcing the ARRL Certificate Authority would be a reasonable approach, except that the pricing probably does not fit in with the ARRL's model. Therefore it is not recommended, unless substantial pricing concessions can be obtained.

2.3 Log Program Specifications

2.3.1 Introduction

The participant's log program will perform the tasks of Logbook registration, renewal, preparation and submission of QSL records, retrieval and display of status information, and preparation and submission of awards applications.

ARRL will supply log program authors with a programming library that simplifies these tasks by providing interfaces to the Logbook server and performing the required PKI functions.

The following specifications for log program features and library functions are preliminary. It is expected that the ARRL programming staff will work with a group of leading log program authors to finalize the design and specifications for this portion of the Logbook system.

2.3.2 Log Program Features

This section contains proposed specifications for log program features related to Logbook of the World. Note that many of these features will be extensively supported by the ARRL-provided programming library. Items marked with an asterisk are optional, but highly recommended.

2.3.2.1 Logbook Registration and Renewal

- Provide user interface for Logbook registration and renewal.
- Initiate registration and renewal sequences.
- Supply the following registration information to server
    - Call
    - Name
    - Address
    - E-mail address
- Provide interface for entering activation password for U.S. calls. (Depends on final authentication rules. See section 2.2.1, "Logbook Registration Rules".)
- Receive and display registration and renewal status messages from server.

2.3.2.2 Log Submission

- Provide user interface for log submission
- Mark one or more selected QSL records for submission.
- Extract all QSL records marked for submission.
- Each QSL record will contain at least the following information:
    - Date of contact
    - Time of contact (UTC)
    - Certificate number of station submitting QSL
    - Call of station submitting QSL
    - Call of station contacted
    - Frequency
    - Mode
    - [optional] QTH (e.g., state, county, grid square, etc.)
    - [optional] RST sent
    - [optional] Ancillary information (e.g., power, EME, etc.)
- Digitally sign each extracted QSL record.
- Transmit one or more signed QSL records via e-mail or browser.
- * Mark each transmitted QSL record with “Transmitted” status.
- Receive confirmation of submission from server. Display result.
- * Mark each confirmed QSL record with “Submitted” status.
- Transmit confirmation status inquiry. Receive and display result.
- * Mark each confirmed QSL record with “Confirmed” status.

Note: no provision is made for editing or deleting QSL records from the Logbook server. If a participant detects an error in a QSL record, a replacement record may be uploaded without negative consequences.

2.3.3 Logbook Programming Library Functions

This section contains proposed specifications for the Logbook Programming Library.

- The library will conform to Open Source standards.
- The library will be made available for Windows 95/98/ ME/NT/2000/ XP and Unix/Linux platforms.
- * The library will be made available for Apple MacIntosh platforms.
- **Key Pair Generation**: The library will provide a function to generate a key pair in accordance with the requirements in section 2.2.3, "Certificate Specifications".
- **Certificate Generation**: The library will provide a function to generate a certificate in accordance with the requirements in section 2.2.3, "Certificate Specifications".
- **Registration:** The library will support transmission of registration information and a certificate to the server via e-mail or a browser.
- **Registration Status and Completion:** The library will support reception of registration status information and certificates from the server via e-mail or a browser.
- **Expiration and Renewal:** The library will support reception of certificate expiration status and transmission of renewal sequence.
- **Digital Signature:** The library will provide a function to digitally sign QSL data in accordance with the requirements in section 2.2.3, "Certificate Specifications".
- ***Signature Verification:** The library will support verification of a digital signature, given input of a document, a digital signature and a certificate. This function is not needed for Logbook of the World, but could be used later for an E-QSL system.
- **QSL Record(s) Submission:** The library will support transmission of signed QSL records to the server via e-mail or a browser.

- **Submission Status:** The library will support reception of submission status information for each submitted QSL record from the server via e-mail or a browser.

- **Confirmation Inquiry:** The library will support transmission of confirmation status inquiries concerning one or more QSL records to the server via e-mail or a browser.

- **Confirmation Status:** The library will support reception of confirmation status information for each confirmed QSL record from the server via e-mail or a browser.

2.3.4 Sample Program for Registration and Submission

Along with the Logbook Programming Library, ARRL will provide a simplified sample program that will allow a participant to register for logbook and submit manually entered QSL records. This program will be provided in source code form as an example for logbook programmers. It will also be made available in executable form for users who do not have a computer log program.

2.4 Logbook Processing

2.4.1 Introduction

This section describes the main processing sequence for the Logbook of the World. An overview of the log submission and processing sequence is presented, followed by detailed specifications for log submission, log verification, QSL confirmation and awards credit. Additional services available via the ARRL website are discussed.

2.4.2 Logbook Processing Overview

Figure 2.2 illustrates the main processing sequence for the Logbook of the World. Although the diagram shows processing for the DXCC awards program, later sections will show how the system is designed to support any awards program.

The sequence begins with submission of a log extract containing one or more digitally signed QSL records. The log extract is submitted via e-mail or through an ARRL web page.

The Verification Processor uses the Certificate Database to verify that the digital signature attached to each QSL record is valid and that the record has not been altered since signing. The Verification processor also checks each QSL record for correct formatting. If QSL record passes verification, it is appended to the Log Database and a status message is returned to the submitter. If errors are detected, the QSL record is discarded and an error message is returned to the submitter.

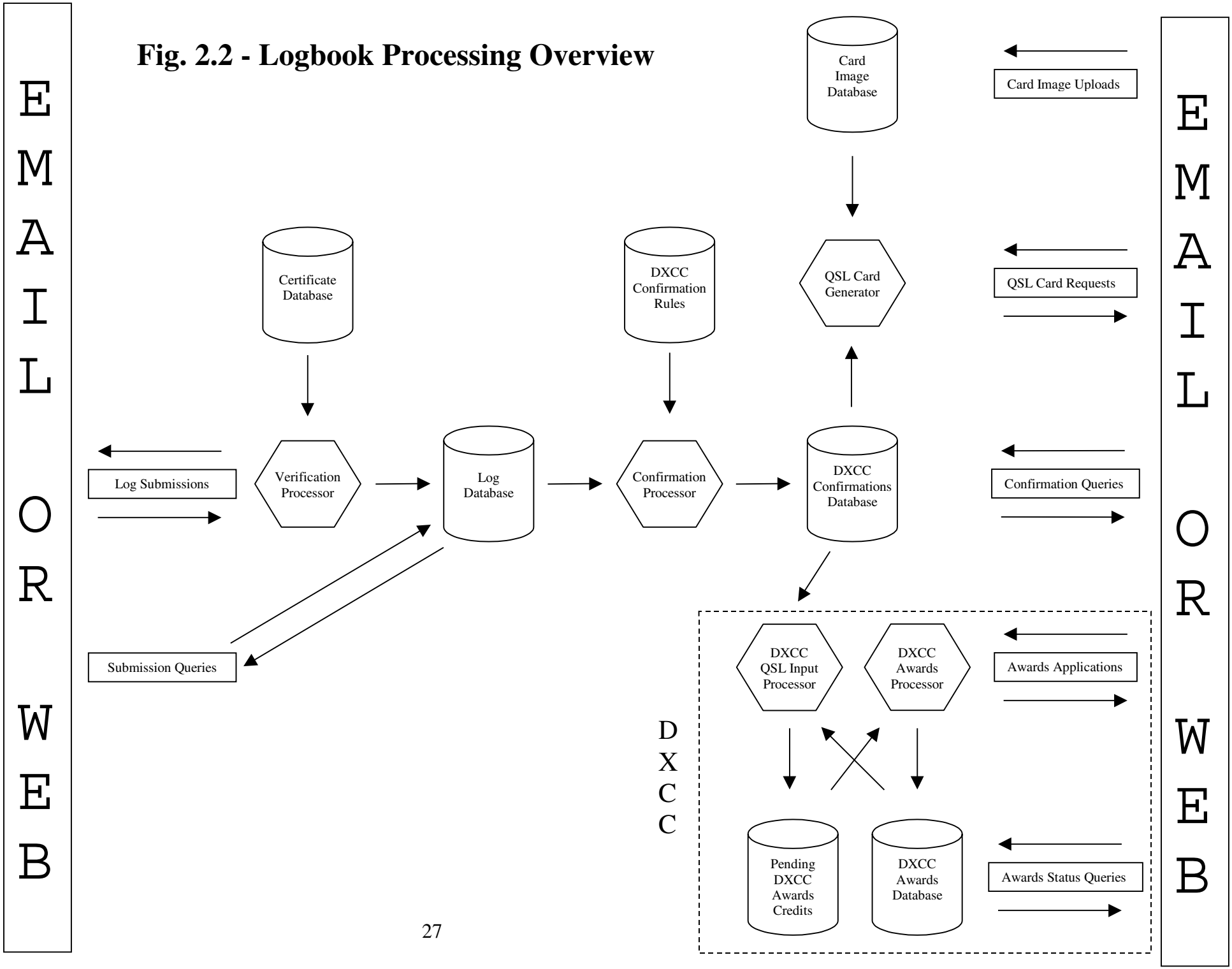
The Confirmation Processor scans each new log extract for matching unconfirmed QSL records previously written to the Log Database. Match rules are defined for each awards program. If a match is found, the QSL is written to a Confirmation Database specific to that award.

Confirmation records are exported to the DXCC QSL Input Processor. The input processor creates pending awards credit records. When a participant applies for DXCC credit and renders payment, the awards credits are written to the DXCC Awards Database.

A number of services are available via the ARRL website:

Service	Action
Log Submission	Submit log extract
Submission Query	Display log submission status and dates
Confirmation Query	Display confirmed QSLs
QSL Card Request	Generate QSL image from confirmed QSL
Upload QSL Card Image	Submit QSL card graphic image for storage
Awards Application	Apply and pay for credits and awards
Awards Status Query	Display awards summary and QSLs

Fig. 2.2 - Logbook Processing Overview



2.4.3 Verification Processing

This section describes verification and storage of incoming log extracts. Please refer to figure 2.3, "Verification Detail."

2.4.3.1 Certificate Lookup and Validation

The Verification Processor must obtain the submitter's certificate in order to validate the digital signature attached to the log extract. The Verification Processor will use the participant's call or certificate number in the uploaded QSL record to lookup the submitter's certificate in the Certificate Database.

Once the correct certificate is obtained, the Verification Processor will use standard PKI procedures to validate the certificate. This involves checking the issuer's signature on the certificate, and checking the certificate's validity dates. If the certificate fails the validity tests, the log will be rejected and an error message will be returned to the submitter (see section 2.4.3.8, "Status Messages".)

2.4.3.2 Digital Signature Verification

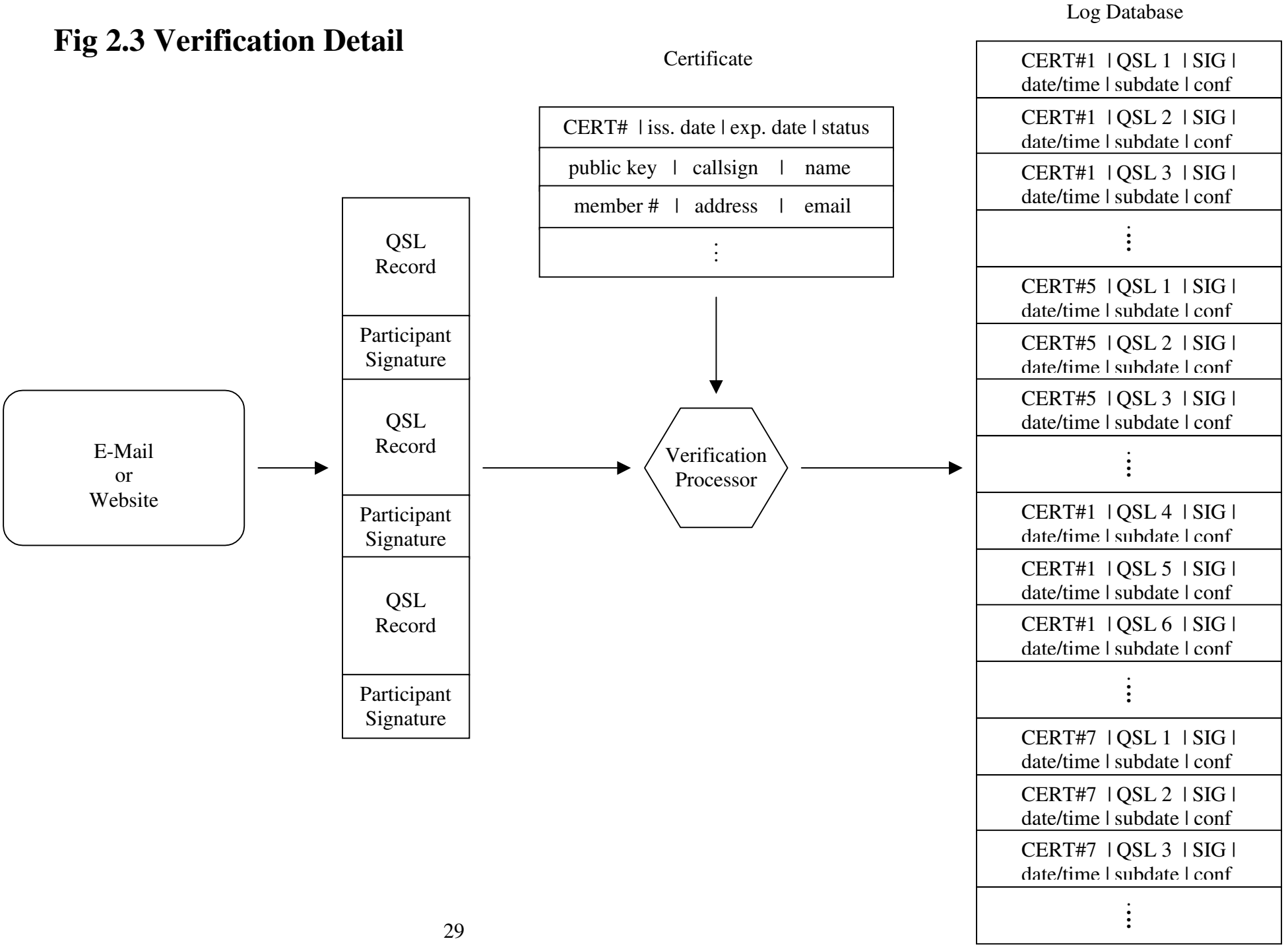
After a valid certificate has been obtained, the Verification Processor will use the digital signature algorithm defined in section 2.2.3, "Certificate Specifications" to validate each signed QSL record (also see Appendix A, "Public Key Infrastructure".)

First, the digital signature will be decrypted using the public key from the submitter's certificate (see section 2.4.3.1, "Certificate Lookup and Validation".) This will produce an unencrypted fingerprint of the QSL record.

Next, the QSL record will be put through the message digest function (one-way hash algorithm) to produce a fingerprint.

The two fingerprints must compare in order to validate the QSL record. If the fingerprint headers differ, the public and private keys do not match (invalid or forged signature.) If the fingerprints do not match, the QSL record was altered after it was signed. In either case, the QSL record will be rejected and an error message will be returned to the submitter.

Fig 2.3 Verification Detail



2.4.3.3 QSL Record Format Validation

After the signature has been validated, the QSL record extract will be examined for proper formatting. If format errors are detected, the QSL record will be rejected and an error message will be returned to the submitter.

2.4.3.4 Log Database

After verification and archive, the QSL record will be appended to the Log Database. This database contains all verified QSL records submitted to the Logbook system.

In order to prevent browsing for QSO dates/times or busted calls, the Log Database must not be directly accessible to participants. [Optionally] Participants may be allowed to display call, mode and band information.

Records will be converted to an internal database format with the following fields:

2.4.3.4.1 Submitted QSL Data

This is a set of fields containing the original QSL data submitted by the participant. Includes fields added by the log program, such as submitter's call, certificate number, etc.

2.4.3.4.2 Date/Time Conversion

The date and time fields in each QSL record may be converted to an internal representation to facilitate confirmation matching. The minimum requirement for the date and time fields is to express any time since 00:00 Jan 1, 1900 with a resolution of no more than 1 minute. [Optionally], the earliest date accepted by any supported awards program may be used.

2.4.3.4.3 Digital Signature

This is the verified digital signature received with the QSL record.

2.4.3.4.4 Submission Date

The submission time and date facilitates submission status messages and troubleshooting.

2.4.3.4.5 Confirmation Status Field

A confirmation status field will be added to each QSL record. This field is discussed in section 2.4.4.2, “Confirming a Contact”.

2.4.3.5 Status Messages

The Verification Processor will return a status message to the submitter of each log extract. The following messages may be returned for each QSL record:

1. QSL Record Accepted on <date> at <time>: <number> records
2. Incorrect Submission Format: <details>
3. Invalid Digital Signature
4. Log Modified after Signature

2.4.3.6 Audit Trail [Optional]

[Optionally], the Verification Processor will generate a chronological log of its activities. This will be useful for detecting participant-generated format problems, forged signatures, altered logs, and programming errors.

2.4.4 Confirmation Processing

This section describes confirmation of QSLs in the Log Database and creation of the Confirmation Database. Please refer to figure 2.4, “Confirmation Detail.”

2.4.4.1 The Confirmation Processor

The Confirmation Processor is run 1) whenever a new log extract is appended to the Log Database, or 2) manually, to scan the entire Log Database for confirmed contacts (for example, when support for a new awards program is added.)

2.4.4.2 Confirming a Contact

Each unconfirmed entry is compared with the other unconfirmed QSLs in the Log Database. If a match is found, a Confirmation Record is written to the Confirmation Database and both QSL records in the Log Database are flagged as confirmed. It is recommended that this be done by loading the confirmation status field with a pointer to the confirmation record in the Confirmation Database.

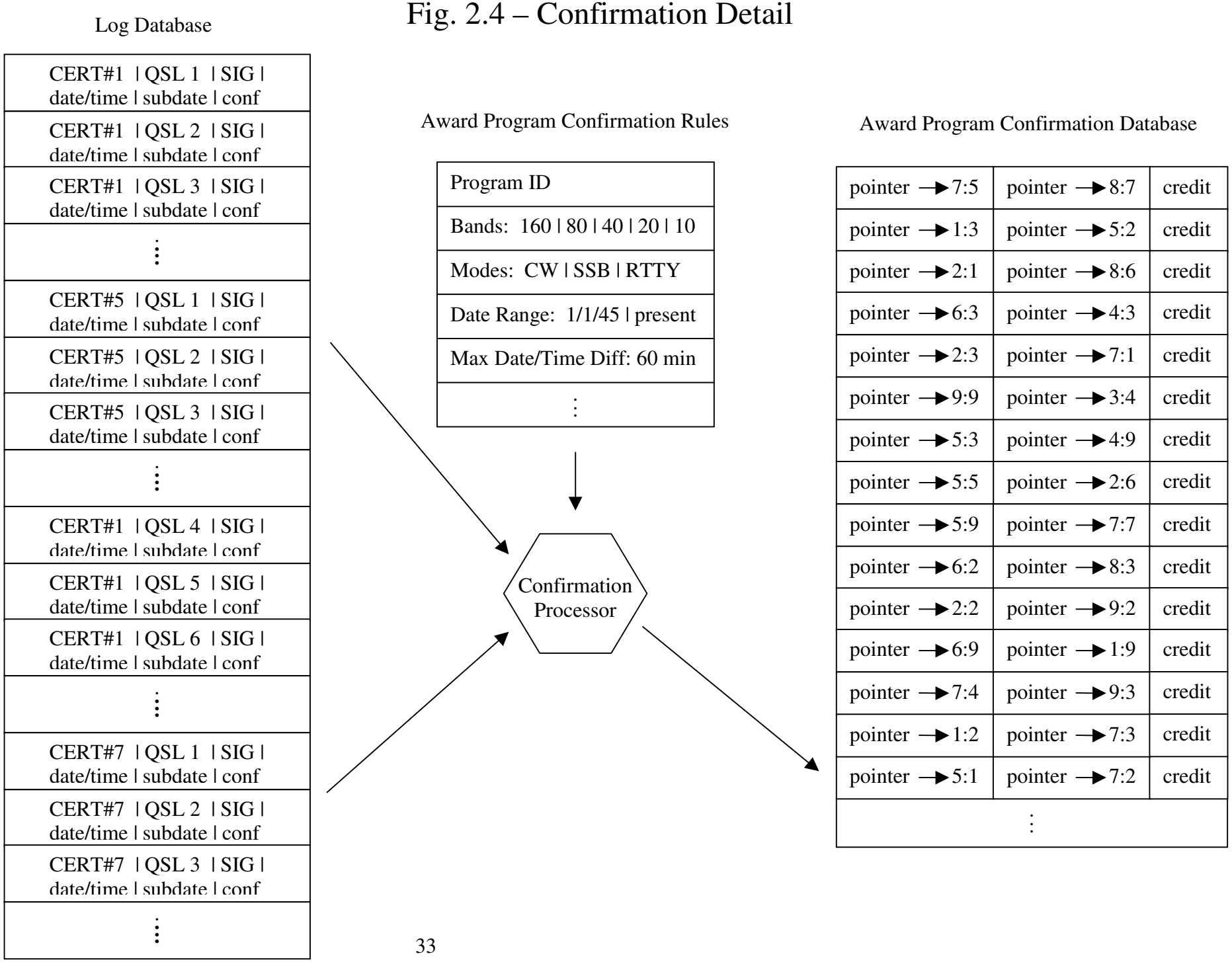
The system will not confirm two Log Database records that have the same certificate number.

2.4.4.3 Awards Program Confirmation Rules

Different awards programs may have different rules for confirming a QSL. For example, different programs may allow larger or smaller differences in the QSO time. The rules for each program will be defined in a file called the Awards Program Confirmation Rules File.

For each pair of records in which the calls match, the Confirmation Processor will apply at least one set of awards program confirmation rules. The rules will determine whether or not the QSL is confirmed for that award. The Confirmation Processor can be configured to support multiple awards programs. When multiple awards programs are supported, each set of rules will be applied to each potential confirmed contact.

Fig. 2.4 – Confirmation Detail



2.4.4.3.1 Awards Program Confirmation Rules File Parameters

Suggested parameters for the Awards Program Confirmation Rules file are:

1. Program ID
2. Allowed Bands
3. Allowed Modes
4. Valid Date Range
5. Maximum Time/Date Difference Allowed

2.4.4.4 Awards Program Confirmation Database

Each awards program has its own Confirmation Database. The information in this database is used to generate credit for awards. In addition, each participant may query the database for lists of his/her confirmed contacts.

2.4.4.4.1 Log Database Pointer Pairs

Each record in the database contains a pair of pointers to two records in the Log Database that represent a confirmed QSL. The format and contents of the pointer fields is implementation dependent.

The pointer pairs in the Confirmation Database are used by the awards program to determine awards credits. They are also used by the website services to obtain lists of confirmed contacts and generate QSL card images, etc. See section 2.4.6, “Website Services”.

2.4.4.4.2 Awards Credit Field

Each record in the database must contain an awards credit field to indicate whether the contact has been processed by the awards program software.

2.4.5 Awards Credit

Immediately after creation, the Log Database records pointed to by each new confirmation record are exported to the awards program QSL Input Processor and the Awards Credit Field in the confirmation record is set to show that the records have been exported. The QSL input processor is designed to accept machine-readable records representing confirmed contacts. The QSL input processor is part of the software for each awards program and is not part of the Logbook implementation project.

2.4.5.1 Special Requirements for DXCC Software

1. The DXCC QSL input processor must be capable of using the confirmed contacts received from the Logbook system to create pending awards credit records for each participant. Credits remain pending until a participant applies for official credit (see section 2.4.6.4, “Awards Applications”.)

2. Awards credit records in the DXCC database will provide space for a pointer back to the Confirmation Database record that generated the credit.

3. The DXCC awards credit process will ensure that the certificate number on log entries submitted for all “rare” entities matches the certificate supplied with documentation for the operation (see section 2.1.2, “Logbook Registration Rules”.

4. The DXCC awards credit process will check for an abnormal percentage of confirmations from the same certificate number or from the same Logbook participant.

2.4.6 Website Services

This section provides general descriptions of Logbook services available through the ARRL website. More information may be found in section 2.6, “User Interfaces”.

2.4.6.1 Confirmation Queries

A participant may query the Confirmation Database to display a list of confirmed QSLs. Selection criteria will include:

1. Call
2. Date Range
3. Time Range
4. Mode
5. Frequency
6. “ALL”

A query may be submitted by filling out a search form on the ARRL website. Results of the search will be displayed on the screen, and may be cut-and-pasted into other applications.

Participants will be allowed to display only their own confirmed contacts.

2.4.6.2 QSL Card Requests

If a station with which the participant has a confirmed contact has previously uploaded a QSL card image, the participant may request a printable QSL card for that contact. See section 2.4.6.3, "Card Image Uploads".

The QSL card request function will be available after each search that returns one or more confirmed contacts (see section 2.4.6.1, "Confirmation Queries".) Each confirmed QSL will be displayed with a check box if the corresponding station has uploaded a card image. If the corresponding station has not uploaded a QSL card image, then the check box will not be available. The participant will check all QSLs for which a card is desired.

The participant may download all selected cards by clicking a button labeled "Download QSL Cards." The server will then provide a PDF file that contains the selected card image(s).

2.4.6.3 Card Image Uploads

Each participant may upload one QSL card graphic image via the website for storage. The image must be constructed according to strict standards prescribed by ARRL. The graphic format will support automated merging of QSL data with the card image. Participants are limited to one image per certificate.

There will be a generic card image that may be used by any participant without uploading an image.

Note that accepting QSL card images for storage and retrieval may create content control problems for the ARRL.

2.4.6.4 Awards Applications

Awards applications may be submitted via the ARRL website. The Awards Application Processor is part of the software for each awards program and is not part of the Logbook implementation project. For more information, see section 2.6.3.1, "DXCC Awards Credit Status Query."

In the case of the ARRL DXCC program, when a participant applies for awards credit through the ARRL website, the system will report the number of pending

new awards credits, the charge for making the credits official, and the charges for any certificates, stickers, pins or plaques for which the participant has qualified. The participant will be allowed to choose the desired awards and render credit card payment. The system will then make the credits official and produce an order for the awards paraphernalia.

2.4.6.5 Awards Status Queries

A participant may query an Awards Database to display a program status summary or to obtain a list of confirmed QSLs that have been accepted for awards credit. This function will be provided by the software system specific to each awards program, and is not part of the Logbook implementation project. For more information, see section 2.6.3.2, “DXCC Awards Application Interface”.

2.5 Awards Processing

This section describes awards processing for ARRL sponsored awards such as DXCC, WAS and VUCC, as well as potential awards processing services for non-ARRL sponsored awards.

Note that awards processing is not part of the Logbook of the World system. Recommendations for awards processing discussed in this section apply to software implementations for individual awards processing systems, such as DXCC.

2.5.1 Processing for ARRL Sponsored Awards

The Logbook Confirmation Processor will initially be used only for DXCC (see section 2.4.4, "Confirmation Processing".). However, Logbook includes the functionality required to handle other awards such as WAS and VUCC. The details described here apply mostly to the DXCC program, but it is expected that processing techniques will be similar for the other awards programs.

2.5.2 Current Awards Applications

Currently, awards applications consists of three parts:

1. An application for one or more awards or award endorsements. The DXCC application form can be found at http://www.arrl.org/awards/dxcc/dxccapp.txt or http://www.arrl.org/awards/dxcc/dxccapp.pdf.

2. A list of QSLs being submitted for awards credit. DXCC forms for listing the QSLs can be found at http://www.arrl.org/awards/dxcc/dxccrec.txt or http://www.arrl.org/awards/dxcc/dxccrec.pdf

3. A set of paper QSL cards.

2.5.3 Online Awards Applications

Online awards applications consist of two parts:

1. An application for one or more awards or awards endorsements.

2. A set of confirmed QSL records.

The online application is similar to the paper application. The only significant difference is that it is in electronic form. The list of confirmed QSLs, however, is quite different. Paper QSLs require manual processing and postal return, while electronic confirmations require neither.

2.5.3.1 Submitting an Online Awards Application

Online awards applications can be submitted by logging on to an ARRL web page.

2.5.3.1.1 Application Submitted via Web Page

A participant can retrieve awards credit status from an ARRL web page (see section 2.4.6.5, "Awards Status Queries"). The participant can then supply application information and mark QSLs for which credit is desired (see section 2.4.6.4, "Awards Applications".)

2.5.4 Processing for non-ARRL Sponsored Awards

The Logbook of the World is capable of accommodating a wide variety of awards, including awards sponsored by organizations other than the ARRL. There are numerous examples of prestigious awards sponsored by other organizations, including WPX, IOTA, and WAZ.

Revenue opportunities may be available to the ARRL by partnering with other organizations that provide awards programs. Pricing models for such partnerships are beyond the scope of this document.

There are several different processing models for non-ARRL awards. Three possibilities are described below. Other models may be more appropriate for specific awards.

Note that all of the models described below require that signed QSL data be submitted to the Logbook of the World system. In other words, the ARRL acts as the Certificate Authority and verifies the signatures on all submitted QSL records. This ensures the security and integrity of all awards programs.

2.5.4.1 Award Confirmation and Credit Service

In this model, Logbook creates and maintains an award-specific Confirmation Database on behalf of an award sponsor.

The confirmation database is generated by the Confirmation Process using a set of confirmation rules supplied by the award sponsor in an ARRL-defined format (see section 2.4.4, "Confirmation Processing".)

The pointers in the Confirmation Database are used to generate a machine-readable list of band/mode/QTH credits for each applicant identified by the award sponsor. This will require implementation of a new program, but it is likely that substantial code can be reused from the DXCC system.

The credit list is returned to the awards sponsor. To ensure privacy, only the credit information is returned: the actual QSO information is not returned to the awards sponsor.

2.5.4.2 Database Licensing

The ARRL can provide Logbook data to legitimate award sponsors, either by providing copies of the data or by allowing access to copies on an ARRL server. The licensed data could be the Log Database, the DXCC Confirmation Database, or a specific Confirmation Database created using confirmation rules supplied by the award sponsor.

Note that this model has security issues. It is widely agreed that in order to prevent "fishing expeditions", log data should not be openly available. If the ARRL allows direct access to the QSL data, there is a chance this could happen. Even if the organization licensing access to the data has ethics beyond reproach, there is no guarantee that its internal security measures are adequate.

2.5.4.3 Outsourcing of Awards Programs to the ARRL

An organization could outsource the handling of its awards program to the ARRL. This could even include mailing the award certificates and/or plaques directly to the recipients. There is precedent for this model, as the Worked All Continents Award (WAC), sponsored by the International Amateur Radio Union, is currently handled by the ARRL for US amateurs.

The award sponsors would supply confirmation rules for their specific awards, and a specific Confirmation Database would be created (see section 2.4.4, "Confirmation Processing".) Alternatively, the "default" DXCC Confirmation Rules and DXCC Confirmations Database could be used. QSLs that require human intervention for validation could either be sent back to the award sponsor for approval, or an ARRL employee could be trained to perform appropriate validation services.

A mixture of electronic and paper QSLs would be submitted for most awards. If ARRL does not want to process the paper QSLs, they could be processed by the award sponsor, who would then submit them to the Logbook system. In this case, the award sponsor would sign the QSL records. The Verification Process would require special programming to handle this situation (see section 2.4.3, "Verification Processing".)

Outsourcing of an awards program to the ARRL could be advertised publicly, perhaps touting "Powered by ARRL Logbook" or "World Class Security and Integrity provided by ARRL Logbook"). Alternatively, outsourcing could be transparent to the awards program participants.

2.6 User Interfaces

2.6.1 Introduction

General descriptions of Logbook user interfaces are presented in this section. No attempt has been made to provide screen shots, or to specify interactive sequences or graphic appearance. The implementation team is expected to create detailed specifications for all user interfaces.

The importance of a good user interface cannot be overstated. Many otherwise excellent applications have failed due to poorly designed and/or tested user interfaces. As the expected users of these interfaces are an international group with extremely varied backgrounds, the importance of good user interface design is even more critical.

All user interfaces should be designed using standard techniques. All user interfaces should be tested by representative users in a low pressure setting. Direct or observed feedback should be used to make the user interfaces easier to use and navigate. There should be an attempt to have the test user population consist of persons with different native languages and backgrounds.

The user interfaces described in this section are divided into three groups: Logbook of The World Participant Interfaces, DXCC Participant Interfaces, and Administrative User Interfaces.

2.6.2 Logbook of The World Participant Interfaces

Logbook of The World participant interfaces will be available via log programs and the Logbook website. Section 2.3, “Log Program Specifications” details the features recommended for log programs. Section 2.4.6, “Website Services”, details the features recommended for the Logbook website.

2.6.3 DXCC Participant Interfaces

DXCC participant interfaces will be available via the DXCC website.

2.6.3.1 DXCC Awards Credit Status Query

The DXCC Awards Status Query will display the user’s credited DXCC entity totals and awards received. For each DXCC entity, the awards, bands and modes that have been credited will be displayed.

This is a combination of information that is currently shown in the “DXCC Award Credit Slip” and “DXCC Awards Credit Listing.”

The additional awards and endorsements for which the participant has qualified, but for which credit has not been purchased, will be displayed.

2.6.3.2 DXCC Awards Applications Interface

The DXCC Awards Applications Interface will allow a participant to apply for a new DXCC award or endorse an existing award.

- The participant will be allowed to choose the DXCC awards to be issued or endorsed.
- Participants will be able to include or exclude specific confirmed QSLs. For example, a participant may not want credit for QSOs made by a guest operator.
- The cost of the application will be displayed, and the participant will be prompted for payment information.
- The user will receive timely feedback on the application, including which QSLs have been credited for which awards, which QSLs are not allowed and why, and what will be sent to the participant via postal mail, if anything (award certificates, endorsement stickers, etc).

2.6.4 Administrative Interfaces

Administrative Interfaces will be available only on the internal ARRL network. They will NOT be externally accessible.

2.6.4.1 Certificate Lookup and Display

The Certificate Lookup and Display interface allows an operator to enter a certificate number, call or name to retrieve and display a certificate in the Certificate Database.

2.6.4.2 Certificate Authorization

The Certificate Authorization interface is the mechanism used to authenticate a non-U.S. call after the operator has verified the documentation mailed by the applicant. The operator first uses the Certificate Lookup and Display interface to enter the certificate number from the printout supplied with the license and ID documents. When the matching certificate is displayed, the operator verifies the that the call is correct and uses the Certificate Authorization interface to instruct the Logbook server to sign the certificate, store it in the Certificate Database, and send a copy to the applicant via e-mail or a browser query.

2.6.4.3 Certificate Revocation Interface

The Certificate Revocation interface allows an operator to instruct the Logbook server to revoke a selected certificate. The operator may optionally request that a notice be sent to the e-mail address in the certificate.

2.6.4.4 Postcard Printing Interface

In the event that the system is designed to buffer postcard data, this interface allows the operator to dump all pending postcards to a printer setup to print them.

2.6.4.5 Database Interface

The Database interface will allow access to the raw records in the Log Database, Confirmation Database and Certificate Database. It will provide the ability to search for records, display and modify them. If an off-the-shelf database package is used to implement the Logbook system, it will provide these capabilities.

Section 3 — Logbook Security

3.1 General Security Issues

This section reviews general security issues for Logbook of the World, including identification, authentication, verification, server security and attack recovery.

3.1.1 Identification

The primary means of identification in Amateur Radio is the call sign. The call is what we send on the air to tell everyone who we are and it is what we put on our QSL cards to identify who made the contact. The integrity of the Logbook system depends on being able to make sure that QSL information submitted under a given call was in fact submitted by the owner of that call. It should be impossible or very difficult for someone other than the rightful owner of the call to submit QSL data for that call. In order to ensure this, Logbook must have a secure and convenient way to identify the owner of a call.

An ideal identification system requires three "physical" proofs of identity:

- Something you are
- Something you have
- Something you know

"Something you are" generally means a unique physical characteristic, such as the appearance of your face, your fingerprint pattern or your iris pattern. This is known as *biometric* information and is considered very reliable. But the ideal system does not rely on biometrics alone because very clever people can fake it (e.g., wear makeup, make rubber fingerprints, hack the iris scanner, etc.)

"Something you have" is usually a physical token, such as a key, a credit card with a magnetic stripe or a smartcard containing a cryptographically protected private key. But the ideal system doesn't rely on a token alone, because someone can steal or counterfeit it.

"Something you know" is usually a user ID, a password or a PIN number. In some systems, the PIN is used to gain access to the private key on a smartcard. User IDs, passwords and PINs by themselves are not very secure because they are too easy to guess, especially with computers that can try thousands or millions of combinations.

Even though each type of physical proof can be compromised, the probability is very low that *all three* can be compromised at the same time.

Of course, fingerprint scanners and smartcards are not practical for Logbook. But we can still use the principals of physical proof of identity to design a more friendly and cost-effective system. The "something you are" can be "a person who gets mail at the address listed on the radio license". The "something you have" can be your radio license document or a private key stored only on your computer. The "something you know" can be an ARRL member ID number, a member account user ID and password, a certificate activation password or a PIN that protects the private key.

3.1.2 Authentication

Authentication is the process of validating the identity of a person who registers for access and issuing that person some type of "key" that enables access. Once the person has the key, it is the key itself that establishes identity (see section 3.1.3, "Verification Issues.) Since the authentication protocol establishes the link between identity and the key, it is a critical factor for preventing unauthorized access, impersonation and submission of false data.

3.1.2.1 Online Authentication

Validation of identity in an online authentication system is particularly challenging because there is no person-to-person contact. How can a server know that someone at a remote computer claiming to own a call is the rightful owner of the call? Even if biometric scanners, smartcard readers and PINs are used, a physical identification step is first necessary in order to validate the biometric information before it is loaded into the server and before a smartcard and PIN can be issued. In other words, the high-tech devices can confirm identity only after an initial physical check is made.

The following sections analyze some of the ways we can perform a physical identity check without imposing excessive cost or inconvenience:

3.1.2.2 Something You Are: A Person with a Mailing Address

One way to validate the identity of an online registrant claiming to own a given call is to mail the access key to the address of the person who owns the call. But how do we know the correct address? Could someone who does not own the call fool us into believing that *his* address is the address of the call sign owner? If so, then he can intercept the access key and impersonate the owner of the call.

The issue then becomes, "How can we determine the true address of the call sign owner? If we can do this, and an impersonator tries to register, then the password will be sent to the rightful owner of the call and not to the impersonator.

Of course, we can't use the address supplied by the applicant because we have no way to know whether it is indeed the address of the person who owns the call.

Instead, the system must independently determine the address of the person who owns the call. There are several ways to do this:

1. For ARRL members, use the address in the member record
2. Lookup the address in a published call sign database
3. Lookup the address in the license authority database
4. Examine copies of the radio license and other identifying documents
5. Examine the original radio license and other identifying documents

There are several problems with relying on the address in the ARRL member database. First, the addresses are supplied by member and are not independently verified. Someone could impersonate the owner of a call simply by signing up for membership under that call and supplying his own address. The only barriers to this attack are the cost of membership and the chance that the rightful owner will signup for membership and discover that his call is already in use. Second, a member address can be temporarily changed by anyone who can gain access to the member account of the call sign owner (see section 3.1.2.5.4, "Cracking Member ID Numbers.") If the address can be changed, the access key can be diverted to an impersonator.

Unfortunately, the addresses in published call sign databases are not secure and are not very reliable. In general, publishers of call sign databases allow anyone to change the address associated with a call, without proof of ownership. Again, if the address can be changed, the access key can be diverted to an impersonator.

License authority databases offer perhaps the most secure and convenient means of obtaining the address of the rightful owner of the call. In general, it is difficult for an impersonator to change the address associated with a call, and doing so is most likely a serious crime in most jurisdictions. However, there are some drawbacks to this approach. First, licensees are not always diligent about updating their address with the license authority. In order for authentication and registration to be successful, the applicant must ensure that the license authority has the correct address. This could result in delays. Second, the United States is the only country for which a license authority databases is currently available (fortunately, the United States is where the majority of potential Logbook users reside.)

If there is no license authority database, then we can require the applicant to send in a paper copy of the license documentation, along with a copy of at least one other government-issued identification document. Although the best procedure would be to mail the access key to the address on the license, it would be reasonable to accept any address accompanied by a copy of the license and other identifying documents. The presumption here is that it would be very difficult for an impersonator to obtain copies of the documents or fake them.

If there is fear that copies of the documents will be forged, then we could require originals. However, it is no easy task to forge even a copy of an official document, and few people would try.

3.1.2.2.1 Authorization via E-mail

Mailing the access key imposes a delay of several days or more, and adds postage and handling costs. If we could send the access key to an e-mail address instead of a mailing address, we could offer users faster online authentication and avoid postage and handling costs.

In order to take advantage of e-mail, we need to be able to correlate an e-mail address with the owner of the call. An e-mail address by itself is not sufficient proof of identity, so we need some independent means to establish the link.

Since we have already established that we can accept any mailing address accompanied by license and identity documentation, there is no reason why we cannot accept an e-mail address submitted in this fashion. We don't have to worry about the e-mail address getting stale because presumably it will be valid between the time the documentation is sent and the time we authenticate, and it will be used only once.

3.1.2.3 Something You Have: A Radio License

Our method for authentication via mail or e-mail effectively requires proof that the applicant possesses a valid radio license. This satisfies the requirement for something you have.

3.1.2.4 Something You Know: A Password or Passphrase

Once the applicant receives the password via mail or e-mail, the private key and certificate can be activated. Although it is not strictly required, the private key can be protected by a password or passphrase. Whenever the private key is used to sign a log extract, the user will be prompted for a password or passphrase. This is a standard feature of all PKI implementations and prevents impersonation by someone who gains physical access to the computer that contains the private key. A password or passphrase satisfies the requirement for something you know.

3.1.2.5 Security of the Members-Only Website

Another method for online authentication would be to require proof of ARRL membership. This could be accomplished by the applicant supplying his or her ARRL member ID, or by logging on to the Members-Only website (establishing access to the Members-Only website requires knowing one’s member ID.) In both cases, identity is established by something you know: your member ID or your

Members-Only logon ID and password. Once identity is established through proof of membership, the address in the member record can be used for mailing the activation password.

Unfortunately, there are problems with this approach.

3.1.2.5.1 General Security of UserIDs and Passwords

Many websites protect access via userID and password pairs, the security of which is generally considered safe for non-critical applications. However, this form of protection has always been vulnerable to computer programs that guess the userID, the password, or both. This is called "cracking".

The simplest form of cracking entails a "brute force" attack: trying every combination of characters that could make up the userID and/or password. If the userID and password are made up of randomly selected characters, the guessing process is entirely dependent on the number of characters that must be guessed and the speed of the computers and networks involved. As computers have increased in speed, brute force attacks have become much more feasible.

In general, the greater the number of characters, the longer it takes to try all the combinations. One of the best defenses against a brute force attack is to use a large number of randomly selected characters. Unfortunately, this is inconvenient for users. Left to their own devices, users normally choose short userIDs and passwords that contain words or phrases that are easy to remember. Sophisticated cracking programs take advantage of this lapse by utilizing large databases of common words and phrases.

Another good defense is for the server to insert a time delay between each unsuccessful attempt, and to disconnect the user after a small number of unsuccessful attempts. Unfortunately, this attack can be defeated easily by spoofing IP addresses and/or using large numbers of Internet-connected computers to guess in parallel (sometimes effected by viruses without the knowledge of those who own the computers.) Note that the latter approach dramatically increases the compute power available for guessing.

Cracking attacks used to be rare, but now there are many sophisticated cracking programs publicly available on the Internet.

3.1.2.5.2 Security of Member Numbers and Members-Only Accounts

The authentication system can be compromised if an impersonator gains access to someone else's Members-Only website account. This can be accomplished in one of three ways: crack the member's ID number, crack the Members-Only account password or change the call in one's own member record.

3.1.2.5.3 Cracking Member ID Numbers

Registration for access to the Members-Only website requires entry of a valid call sign and matching member number (a 10-digit number printed on the label of QST.)

The easiest attack is to steal the call sign and label off a friend's copy of QST.

In addition, there are several cracking attacks that allow access to a very large number of Members-Only accounts. The simplest attack is to start with a valid member ID number (one's own, for example) and increment by one. Since member ID numbers have been issued sequentially, this will likely result in a valid ID number. Then a cracking program can be used to try all possible call sign combinations to determine the one that matches. Another attack is to select any valid call sign and try all combinations for the 10-digit number. It helps to know if the call sign belongs to someone who is an ARRL member, and whether that member has already registered for access to the Members-Only website, but this is not strictly necessary. These attacks require trying a large number of combinations, and can be detected (see section 3.1.2.5.5 "Detecting Cracking Attacks".)

Note that the Members-Only registration process currently allows registration under the same call more than once. This means an attacker who determines someone's member ID number can gain access to that person's member's account, even if it has been registered already.

3.1.2.5.4 Cracking Members-Only Account Passwords

Another approach is to crack the password for an existing Members-Only account. The password can be as few as four characters (approximately 65 combinations per digit), and most users will pick something easy to remember. The cracker must use a call sign for an ARRL member who has registered for access to the website, but there are already 80,000 such accounts available. Once an account has been cracked, the attacker can

temporarily change the mailing address, register for Logbook, then change the address back to its original value.

3.1.2.5.5 Detecting Cracking Attacks

The Members-Only website keeps track of failed registration and logon attempts, and could be programmed to flag and invalidate any account for which an unusually large number of failed attempts have been made. However, this will likely inconvenience the rightful owner of the account and repeated attacks cannot be prevented.

3.1.2.5.6 Changing the Call Sign in the Member Record

It isn't necessary to crack a member ID number or a logon password to compromise the Members-Only website. Registered members are allowed to change their member data online, including the call sign. Thus, a member can temporarily change the call sign in his or her member record to *any* call sign, register for Logbook under that call sign, then change the member record back to the original call sign. Although there is a several-day delay while the change is processed by the circulation department, personnel in that department are not currently trained to detect unusual call sign changes.

3.1.2.5.7 Enhancing Members-Only Security

The Members-Only system could be changed to enhance security for Logbook registration, but this would make it more difficult and inconvenient to register for access and use the features of the Members-Only website. The Members-Only website is very popular and very valuable to ARRL, so any change that would make the system less attractive to use would be undesirable.

3.1.3 Verification Issues

Verification takes place when access is requested, and is the process of making sure the "key" fits the lock and is being used by the person to whom it was issued.

3.1.3.1 Passwords versus Private Keys

3.1.3.1.1 Security of Passwords

A user ID and password could be used to gate ongoing access to the Logbook system, but they are highly vulnerable to cracking attacks (see section 3.1.2.5.1 "General Security of UserIDs and Passwords".) In

addition, user IDs and passwords do not provide a reliable means for permanently tagging data with proof of its origin.

3.1.3.1.2 Security of Digital Signatures

Digital signatures are much more secure than userIDs and passwords. The public keys used for digital signatures are considered to be virtually impervious to cracking. They are typically at least 1024-bits in length (approximately 128 characters) and are randomly generated. Digital signature technology uses encryption algorithms that are considered, for all practical purposes, unbreakable.

3.1.3.1.3 Other Major Benefits of Digital Signatures

Digital signatures provide an excellent mechanism for regulating access to a system, but unlike UserIDs and passwords, digital signatures also can be used to provide proof that a particular piece of data was submitted by the owner of the private key, and that the data has not been altered since signing.

In the Logbook context, this allows us to permanently tag each submitted log record with ownership information, and to conclusively prove that the log record has not been altered by a hacker or an insider.

In addition, digital signatures provide the only mechanism for future implementation of an EQSL system. In such a system, a participant would send an email to another station requesting a confirmation. The station would return a digitally-signed log record, which would be forwarded by the requesting station to DXCC.

3.1.4 Special Security Checks

Security of the Logbook system can be considerably enhanced if the following special checks are made during processing:

1. The same call may not be registered for Logbook more than once for the same time frame of activity (VP5 example of call sharing)
2. The mailing address must match the country that issued the call
3. More than 10 certificates issued to the same mailing address triggers staff review
4. No self-confirmations (both log records cannot come from the same certificate)
5. DXCC checks for unusual percentage of confirmations from same certificate
6. DXCC requires valid cert with required documentation for "rare" entity

Note that additional checks will be necessary if the Members-Only system is used for authentication (for example, ensuring that the member record address and call sign have not been changed recently.)

3.1.5 Server Security

Like most networked applications, the Logbook system is vulnerable to attacks on the server.

3.1.5.1 Server Attack Sources

3.1.5.1.1 Inside Attacks

An inside attack could be carried out by an ARRL employee or a visitor who gains physical access to the server or who is able to access it over the internal network. Inside attacks can be prevented by imposing strict internal procedures for physical access to the server and by utilizing strict internal network security techniques.

3.1.5.1.2 Hacker Attacks

A hacker is someone who gains unauthorized access to the server over the Internet. The probability of hacker attacks can be lowered by using state-of-the-art website protection facilities. It is recommended that the Logbook server not be directly connected to the Internet.

3.1.5.2 Primary Server Attacks

There are a number of attacks on the Logbook server that could be attempted. These include:

3.1.5.2.1 Falsely Authorizing a Call Sign

In one variation, the attacker registers under a desired call, breaks server security, and authorizes mailing of the activation password to a desired address. The attacker would simply use the same authorization application used by ARRL personnel when receiving documentation in the mail. The primary defenses against such an attack are to strengthen server security and limit access to the authorization application.

In another variation, the attacker accesses the server, creates an activated certificate containing the desired call, signs the certificate with the ARRL CA private key and inserts it into the certificate database. This attack requires access to both the server and the ARRL CA private key, and is quite difficult because it requires specialized software. The best defenses

are to strengthen security of the server containing the key and protect the key itself with an access password.

3.1.5.2.2 Modifying the Log Database

The attacker breaks server security and modifies the Log Database by adding or editing records containing false QSO information. The current design does not provide for each individual log record to be signed by the submitter, so this attack would not be detected unless and until an audit is performed. The audit consists of comparing the Signed Log Backup with the Log Database.

Strengthening server security and running regular audits will minimize the probability of this attack. The attack can be completely eliminated by requiring each log record to be individually signed and checking the signature before each operation involving the record. This will add considerable volume to the database (the length of a signature is longer than the length of a log record) and will add significant processing time.

3.1.5.2.3 Altering the Confirmation Database

The attacker breaks server security and modifies the Confirmation Database by adding or editing pointers to the same record in the Log Database. An audit would be required to detect that this attack had taken place. This attack can be prevented by adding checks to programs that use the Confirmation Database.

3.1.5.2.4 Destroying Data

The attacker breaks server security and deletes or alters records in the Log Database and/or Confirmation Database. The purpose of this malicious attack is to undermine the integrity of the Logbook system. This attack would not be detected until someone complains about awards credit not being received or until an audit is performed. The best defense is to strengthen server security and run regular audits.

3.1.5.2.5 Denial-of-Service Attacks

Denial-of-Service attacks seek to overload the server network connection, processor, and/or storage capacity. Typically, this is a hacker attack carried out over the Internet. All server-based systems are vulnerable to such attacks, and Logbook will share whatever means are used by ARRL

to protect its other server-based systems. In addition, at very little cost, and no inconvenience to users, Logbook can be designed to resist certain attacks (e.g., reject excessive data submissions from the same source.)

3.1.6 Attack Recovery

It is crucial that the system be designed so that it can recover from security attacks. It is required that the system be able to back out any records that are later deemed invalid. This means that a pointer trail must be maintained from each awards credit back to the Confirmation Database and Log Database records from which it was generated. The awards system must provide the ability for an authorized individual to remove an awards credit. This process should mark all associated records with information about the removal of credit.

The ability to reverse awards credit is essential not only to prevent attacks involving falsely authorized calls and/or theft of private keys and passwords, but also because it is not possible to anticipate all of the attacks that theoretically could be carried out against the Logbook system. The audit trail and recovery features are insurance against such attacks.

3.2 Authentication Analysis

This section analyses various authentication protocols that can be used for authorizing access to the Logbook of the World system. The protocols are listed, followed by a summary of attacks. Then each alternative is described step-by-step, followed by assumptions underlying the design, possible attacks, probability of attack, consequences of attack, usability/cost issues and comments. A summary table comparing the protocols may be found at the end of the section.

Please refer to section 3.1, "Logbook Security" for more background on issues affecting authentication. In particular, section 3.1.3, "Passwords versus Digital Signatures", section 3.1.2.2, "Something You Are: A Person with a Mailing Address", and section 3.1.4, "Special Security Checks" contain important information for understanding the possible attacks and how they can be limited.

3.2.1 Authentication Protocols

The following methods can be used to authenticate participants in the Logbook program. The methods are listed from weakest security to strongest security.

- Honor System – Instant Registration
- Honor System – Mail Password
- ARRL Membership – Instant Registration for Any Call
- ARRL Membership – Instant Registration for Call in Member Record
- ARRL Membership – Call in Member Record and Mail Password
- Call Book Database – Mail Password
- Photocopy of License
- Licensing Authority Database – Mail Password
- Original License

3.2.2 Authentication Attack Summary

The following is a summary of attacks that can be made on the Logbook authentication protocols listed in section 3.2.1:

A. Lie about owning call
B. Supply an untraceable address (e.g., Mailboxes, Etc.)
C. Steal any unregistered member's ID number from QST label
D. Crack any unregistered member's ID number
E. Crack any unregistered member's Members-Only site password
F. Change address in member record from Members-Only site
G. Change address on someone else's call in call book database
H. Alter call and signature on original or photocopy of license/ID
I. File false address change for someone else's license
J. Steal someone else's license and ID

3.2.3 Honor System – Instant Registration

Description:

1. The applicant visits an ARRL web page and supplies name, address and call.
2. The applicant is instantly registered and is given a username and password for access to the log submission website.

Assumptions:

- Applicant's claim of call sign ownership can be trusted

Attacks:

A. Lie about owning call

Probability of Attack:

Extremely High

Consequences:

- Attacker can register any call
- Attacker can register an unlimited number of stolen or made-up calls
- Attacker can register an unlimited number of stolen or made-up semi-rare DX calls without detection
- Attacker can give or sell unlimited false awards credit to self and others
- Bogus log records can be submitted, confirmed and processed for awards credit
- Attack cannot be detected until a rightful call sign owner complains
- Recovery from attack is difficult and expensive
- The attacker cannot be identified
- The attacker cannot be prevented from repeating the crime

Usability/Cost Issues:

None

Comments:

- It is so easy to register any call that the Special Security Checks are ineffective.
- A pure honor system provides no security at all.

3.2.4 Honor System – Mail Password

Description:

1. Applicant visits an ARRL web page and supplies name, address and call
2. Applicant is mailed a password for accessing the log submission website
3. A fee is charged for each call registered

Assumptions:

- Applicant's claim of call sign ownership can be trusted
- By requiring a valid address, we know who submitted the log records
- Registration fee limits the extent of attack

Attacks:

A. Lie about owning call
B. Supply an untraceable address (e.g., Mailboxes, Etc.)

Probability of Attack:

Very High

Consequences:

- Attacker can register any call (needs access to an in-country mailing address)
- Attacker can register stolen or made-up calls (limited by fee and addresses)
- Attacker can register semi-rare DX calls without detection
- Attacker can give/sell limited false awards credits to self/others (limited by fee and addresses)
- Wealthy, entrepreneurial, energetic attacker can give/sell large number of false awards credits to self/others
- Bogus log records can be submitted, confirmed and processed for awards credit
- Attack cannot be detected until a rightful call sign owner complains
- Recovery from attack is difficult and expensive
- The attacker cannot be identified
- The attacker cannot be prevented from repeating the crime

Usability/Cost Issues:

- User experiences a one-time delay of several days to two weeks
- Postcards and postage add to ARRL's program administration costs.

Comments:

- The assumption that the address tells us who submitted the log records is faulty.

3.2.5 ARRL Membership – Instant Registration for Any Call

Description:

1. Applicant must be an ARRL member
2. Applicant must be registered for ARRL Members-only website
3. Applicant logs on to Members-Only website using call and password
4. Applicant is instantly registered to participate in Logbook
5. Applicant may subsequently register up to ten calls

Assumptions:

- ARRL member's claim of owning any call can be trusted
- Member address tells us who submitted the log records
- Cost of membership is a sufficient deterrent against attack
- System Security Checks limit extent of attack

Attacks:

A. Lie about owning call
B. Supply an untraceable address (e.g., Mailboxes, Etc.)
C. Steal any unregistered member's ID number from QST label
D. Crack any unregistered member's ID number
E. Crack any unregistered member's Members-Only website password

Probability of Attack:

High

Consequences:

- Attacks A and B:
  - Any ARRL member can register any call (needs access to an in-country mailing address.)
  - Any ARRL member can register up to ten stolen or made-up calls for the same country
  - Any ARRL member can give/sell limited false awards credit to self/others (limited by membership fee and addresses)
  - Wealthy, entrepreneurial, energetic attacker can give/sell a large number of false awards credits to self/others
  - Attacker cannot be identified beyond a mailing address
  - Attacker can repeat the crime if willing to pay

- Attack C, D or E:
  - Anyone can register any call issued by a country matching the mailing address for an unregistered ARRL member
  - Anyone can register a very large number of stolen or made-up calls
  - Attacker can give/sell very large number of false awards credits to self/others
  - Attacker cannot be identified
  - Attacker cannot be prevented from repeating the crime
- All attacks:
  - Attacker can register semi-rare DX calls without detection
  - Bogus log records can be submitted, confirmed and processed for awards credit
  - Attack cannot be detected until a rightful call sign owner or member complains
  - Recovery from attack is difficult and expensive

Usability/Cost Issues:

None

Comments

- The assumption that members can be trusted is faulty.
- The assumption that the address tells us who submitted the log records is faulty.
- Protocol is very vulnerable to cracking attacks

3.2.6 ARRL Membership – Instant Registration for Call in Record

Description

1. Identical to "ARRL Membership - Instant Registration for Any Call", except the applicant is allowed to register only the call in his/her member record.

Assumptions

- ARRL member's claim of owning call in member record can be trusted
- Member's address tells us who submitted the log records
- Cost of membership is a sufficient deterrent against attack
- Cost of membership greatly limits the extent of attack
- System Security Checks limit extent of attack

Attacks:

A. Lie about owning call
B. Supply an untraceable address (e.g., Mailboxes, Etc.)
C. Steal any unregistered member's ID number from QST label
D. Crack any unregistered member's ID number
E. Crack any unregistered member's Members-Only website password

Probability of Attack:

Medium

Consequences:

- Attacks A and B:
  - Any ARRL member can register one call from any country in which member has access to a mailing address
  - Any ARRL member can give/sell false awards credits for one entity to others
  - Wealthy, entrepreneurial, energetic attacker can give/sell a large number of false awards credits to self/others
  - Attacker cannot be identified beyond a mailing address
  - Attacker can repeat the crime if willing to pay
- Attack C, D or E:
  - Anyone can register the call of an unregistered ARRL member, provided call was issued by the country in the member's mailing address
  - Anyone can register a large number of calls
  - Attacker can give/sell large number of false awards credits to self/others
  - Attacker cannot be identified
  - Attacker cannot be prevented from repeating the crime

- All attacks:
  - Attacker can register semi-rare DX calls without detection
  - Bogus log records can be submitted, confirmed and processed for awards credit
  - Attack cannot be detected until a rightful call sign owner or member complains
  - Recovery from attack is difficult and expensive

Usability/Cost Issues:

- Authentication for additional calls requires one of the stronger security methods described below

Comments

- The assumption that members can be trusted is faulty.
- The assumption that the address tells us who submitted the log records is faulty.
- Under attacks A and B, the one-call-per-member-record restriction significantly increases the amount of time, effort and money required to hand out a large number of false awards credits
- This protocol is very vulnerable to cracking attacks.

3.2.7 ARRL Membership – Call in Member Record and Mail Password

Description:

1. Identical to "ARRL Member – Instant Registration for Call in Record", except the password that allows access to the Logbook system is mailed to the address in the member record.

Assumptions:

- An ARRL member's claim of owning call in member record can be trusted
- We can prevent identity theft by using the mail system
- Cost of membership is a sufficient deterrent against attack
- Cost of membership greatly limits the extent of attack
- System Security Checks limit extent of attack

Attacks:

A. Lie about owning call when joining ARRL
B. Supply an untraceable address (e.g., Mailboxes, Etc.)
C. Steal any unregistered member's ID number from QST label (requires F)
D. Crack any unregistered member's ID number (requires F)
E. Crack any unregistered member's Members-Only site password (requires F)
F. Change address in member record from Members-Only site (requires C, D, or E)

Probability of Attack:

Medium-Low

Consequences:

- Attacks A and B:
  - Any ARRL member can register one call from any country in which member has access to a mailing address
  - Any ARRL member can give or sell false awards credits for one entity to others
  - Wealthy, entrepreneurial, energetic attacker can give/sell a large number of false awards credits to self/others
  - Attacker cannot be identified beyond a mailing address
  - Attacker can repeat the crime if willing to pay
- Attack C, D or E (with attack F):
  - Anyone can register the call of an unregistered ARRL member, provided call was issued by the country in the modified mailing address
  - Anyone can register a large number of calls
  - Attacker can give or sell large number of false awards credits to self/others

    - Attacker cannot be identified
    - Attacker cannot be prevented from repeating the crime
- All attacks:
    - Attacker can register semi-rare DX calls without detection
    - Bogus log records can be submitted, confirmed and processed for awards credit
    - Attack cannot be detected until a rightful call sign owner or member complains
    - Recovery from attack is difficult and expensive

Usability/Cost Issues:

- User experiences a one-time delay of several days to two weeks
- Postcards and postage add to ARRL's program administration costs.
- Authentication for additional call requires one of the stronger security methods described below.

Comments

- The assumption that members can be trusted is faulty.
- The assumption that the address tells us who submitted the log records is faulty.
- The one-call-per-member-record restriction and mailing of password greatly increase the amount of time, effort and money required to hand out a large number of false awards credits
- Mailing the password eliminates identity theft via cracking attacks C, D or E, but attack F can be used to circumvent
- Probability of attack F can be reduced somewhat by adding a Special Security Check to detect recent member record address changes.

3.2.8 Call Book Database – Mail Password

Description:

1. The applicant logs on to an ARRL website and supplies the call.
2. If the call is found in a trusted call book database, a password for accessing the Logbook system is mailed to the address in the call book database
3. A fee is charged for each call registered

Assumptions:

- The name and address listed in certain callbook databases is reliable enough to establish call sign ownership
- We can prevent identity theft by using the mail system
- System Security Checks limit extent of attack

Attacks:

G. Change address on someone else's call in callbook database

Probability of Attack:

Medium-to-Low, depending on callbook selected

Consequences:

- Attacker can register any call (needs access to an in-country mailing address)
- Attacker can register multiple calls (limited by fee and addresses)
- Attacker can register multiple semi-rare DX calls without detection
- Attacker can give/sell limited false awards credits to self/others (limited by fee and addresses)
- Wealthy, entrepreneurial, energetic attacker can give/sell large number of false awards credits to self/others
- Bogus log records can be submitted, confirmed and processed for awards credit
- Attack cannot be detected until a rightful call sign owner complains
- Recovery from attack is difficult and expensive
- The attacker cannot be identified
- The attacker cannot be prevented from repeating the crime

Usability/Cost Issues:

- User experiences a one-time delay of several days to two weeks.
- Callbook address data may be unreliably out-of-date, requiring user to update.

- Callbook security against unauthorized address change may be minimal or non-existent
- Postcards and postage add to ARRL's program administration costs.

Comments

- The assumption that the address tells us who submitted the log records is faulty.
- It may be difficult to change addresses in certain callbooks

3.2.9 Photocopy of License

Description:

1. The applicant logs on to an ARRL website and supplies the call
2. The applicant mails ARRL a photocopy of the license, photocopy of identity document, an original signature and an e-mail address
3. ARRL staff member verifies the license and identity document; compares signatures
4. If the documents pass inspection, the applicant is authorized
5. A fee is charged for each call registered

Assumptions:

.

- It takes a fair amount of effort to alter the data on license and identity photocopy
- It takes some skill to alter the signature portion of license and identity photocopy
- It is difficult to obtain an original or photocopy of a radio license and identity document issued by another country
- It is very difficult and time consuming to produce forged license and identity photocopies for more than a handful of countries
- Forging even a copy of an official document may be a crime in some jurisdictions
- Stealing a license and official ID is a crime
- E-mail address can be accepted because the documentation proves it came from the owner of the call

Attacks:

H. Alter call and signature on original or photocopy of license/ID
J. Steal someone else's license and ID

Probability of Attack:

Very Low

Consequences:

- Attacker can register any call
- Attacker can register multiple stolen calls (limited by effort, skill, and fees)
- Attacker can register semi-rare DX calls without detection
- Attacker can give/sell limited false awards credits to self/others (limited by effort, skill, and fees)
- Wealthy, entrepreneurial, energetic attacker can give/sell large number of false awards credits to self/others
- Bogus log records can be submitted, confirmed and processed for awards credit

- Attack cannot be detected until a rightful call sign owner complains
- Recovery from attack is difficult and expensive
- The attacker cannot be identified
- The attacker cannot be prevented from repeating the crime

Usability/Cost Issues:

- User experiences a one-time delay of several days to two weeks.
- High labor cost at ARRL HQ to examine documents and authorize access.

Comments:

- Forgery attacks are unlikely
- Theft attacks are unlikely
- Successful forgery and theft attacks are most likely for calls within the attacker's own country.

3.2.10 Licensing Authority Database – Mail Password

Description:

1. The applicant logs on to an ARRL website and supplies the call
2. If the call is found in a machine-readable licensing authority database, a password required for access to the Logbook system is mailed to the address in the database
3. A fee is charged for each call registered

Assumptions:

- The name and address listed in a licensing authority's database establishes call sign ownership
- Defrauding Logbook requires making fraudulent representations to a government authority (i.e., committing a serious crime)

Attacks:

I. File false address change for someone else's license (divert reissued license)

Probability of Attack:

Extremely Low

Consequences:

- Attacker can register any call (needs access to an in-country mailing address)
- Attacker can register multiple stolen calls (limited by effort, skill, fee and addresses)
- Attacker can register semi-rare DX calls without detection
- Attacker can give/sell limited false awards credits to self/others (limited by effort, skill, fee and addresses)
- Wealthy, entrepreneurial, energetic attacker can give/sell large number of false awards credits to self/others
- Bogus log records can be submitted, confirmed and processed for awards credit
- Attack cannot be detected until a rightful call sign owner complains or fraud is discovered by licensing authorities
- Recovery from attack is difficult and expensive
- The attacker cannot be identified
- The attacker cannot be prevented from repeating the crime

Usability/Cost Issues:

- User experiences a one-time delay of several days to two weeks.
- Very few reliable databases for non-U.S. licensing authorities are available.
- Address in licensing authority database may be out-of-date, requiring user to update.
- Postcards and postage add to ARRL's program administration costs.

Comments:

- Attack requires submitting falsified documents
- Attack may require submitting an original or copy of license, which would require forgery
- Attack in some countries may require other proof of identity
- For U.S. calls, attack requires registering for the ULS before the rightful owner registers, or cracking the owner's logon ID and password
- False filing attack is extremely unlikely

3.2.11 Original License

Description:

1. The applicant logs on to an ARRL website and supplies the call
2. The applicant mails ARRL an original license, identity document, an original signature and an e-mail address
3. ARRL staff member verifies the license and identity document; compares signatures
4. If the documents pass inspection, the applicant is authorized
5. A fee is charged for each call registered

Assumptions:

- It takes great skill and effort to alter the data on an original license and identity document
- It takes great skill and effort to alter the signature portion of a license and identity document
- It is very difficult to obtain an original radio license and identity document other than one's own
- Forging or stealing an official document is a crime in every jurisdiction
- An e-mail address can be accepted because the documentation proves it came from the owner of the call

Attacks:

H. Alter call and signature on original or photocopy of license/ID
J. Steal someone else's license and ID

Probability of Attack:

Extremely Low

Consequences:

- Attacker can register any call
- Attacker can register multiple stolen calls (limited by effort, skill, and fees)
- Attacker can register semi-rare DX calls without detection
- Attacker can give or sell limited false awards credits to self and others (limited by effort, skill, and fees)
- Wealthy, entrepreneurial, energetic attacker can give/sell large number of false awards credits to self/others
- Bogus log records can be submitted, confirmed and processed for awards credit
- Attack cannot be detected until a rightful call sign owner complains or fraud is discovered by licensing authorities

- Recovery from attack is difficult and expensive
- The attacker cannot be identified
- The attacker cannot be prevented from repeating the crime

Usability/Cost Issues:

- User experiences a one-time delay of several days to two weeks.
- User must surrender original license, risking loss or theft, and possibly preventing operating.
- High labor cost at ARRL HQ to examine licenses and authorize access.

Comments:

- Forgery attacks are very unlikely
- Theft attacks are unlikely
- Successful forgery and theft attacks are most likely for calls within the attacker's own country.

3.2.12 Logbook Authentication Table

Protocol	Attacks	Probability	Limits	Usability Issues	Cost Issues
Honor – Instant	A	extremely high	none	none	none
Honor – Mail	A, B	very high	fee, address (weak)	delay	postage, cards
Member – Instant	A, B, C, D, E	high	A,B: fee, address C,D, E: none	none	none
Member – Instant One Call	A, B, C, D, E	medium	A,B: fee, address, one call C,D, E: address-call match	additional calls difficult	none
Member – One Call Mail	A, B, C, D, E, F	medium-low	A,B: fee, address, one call C,D,E,F: address-call match	delay, additional calls difficult	postage, cards
Call Book Database – Mail	G	medium-low	fee, address	delay, security, address correction	postage, cards
Photocopy of License	H, J	very low	fee, time, skill, availability, crime	delay, postage	labor
Authority Database – Mail	I	extremely low	address, database security, crime	delay, database availability, address correction	postage, cards
Original License	H, J	extremely low	fee, time, skill, availability, crime	delay, postage, lost originals	labor

Appendix A. Public Key Infrastructure

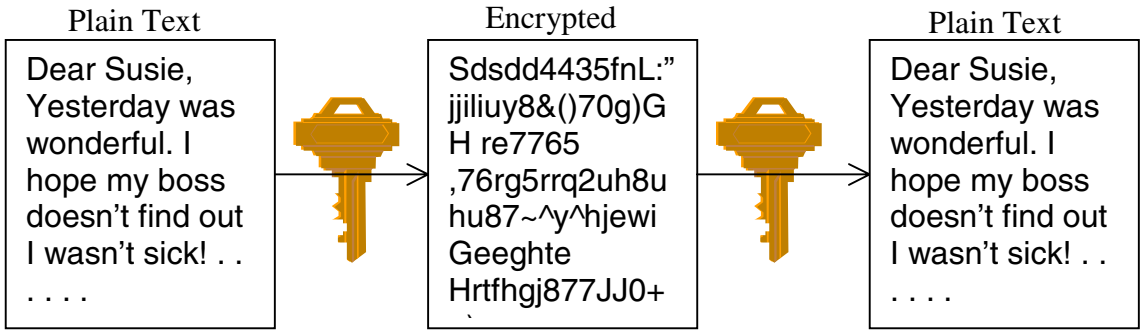
Public Key Infrastructure (PKI) services are important general purpose security services for Internet and Intranet applications, which include electronic commerce and secure messaging. This section explains the technologies and concepts involved in PKI, including Encryption (Secret Key and Public Key), Digital Signatures, Certificates and Certificate Authorities. PKI standards are also discussed.

A.1 Encryption

A.1.1. Secret Key

Secret Key Cryptography is sometimes known as Conventional or Symmetric Cryptography. The same key is used for both encryption and decryption. This key is essentially a random number shared between the participants in a secure exchange.

In the example below, the plain text message is encrypted with a Secret Key. It can only be decrypted by someone who possesses that same Secret Key.

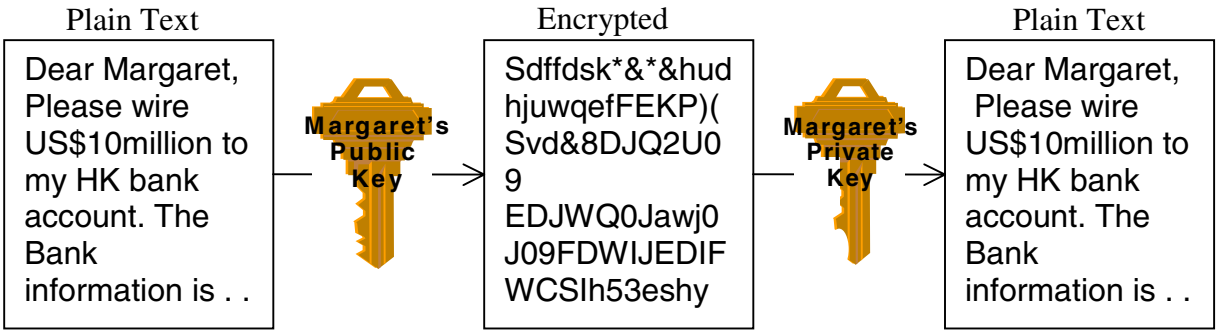


Note that the sender and the receiver of the message must both have the same key. Key distribution is a significant issue for Secret Key encryption.

A.1.2. Public Key

With Public Key encryption each entity taking part in secure communications has a Key Pair consisting of a Public Key and a Private Key. The Public and Private Key in the Key pair are mathematically related so that whatever is encrypted with the Public key can be decrypted with the Private Key, and vice-versa. The Private Key is kept private and never divulged. It may be stored on a smartcard or on a local hard drive. The Public Key is public knowledge and freely available, perhaps via a publicly accessible database on the Internet.

Below, a message to Margaret is encrypted with her Public Key. Since her Public Key is public knowledge, anyone can send her an encrypted message. Only Margaret possesses her Private Key. Hence only Margaret can read this message intended for her.

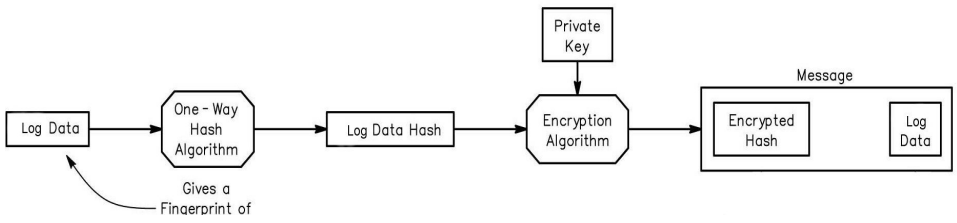


Public Key encryption is several orders of magnitude slower than Secret Key encryption. Systems that use Public Keys, yet must encrypt large amounts of data, typically are "Hybrid Cryptosystems" – they generate a Secret Key which is then passed using Public Key encryption. That Secret Key is then used to efficiently encrypt bulk data. For example, both Netscape's and Microsoft's email programs use Public Key security, yet they use a (randomly generated) Secret Key to encrypt email.

A.2 Digital Signature

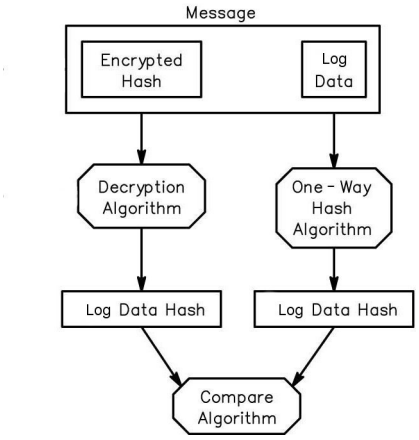
A Digital Signature is data that vouches for the origin and integrity of a message. To produce a Digital Signature, a "fingerprint" of the data to be signed is taken (using a Message Digest function). This "fingerprint" is encrypted by the signer's Private Key. This encrypted fingerprint is the Digital Signature. The Figure A.1 illustrates how Logbook would use the process:

Fig. A.1 Log Extract Digital Signature



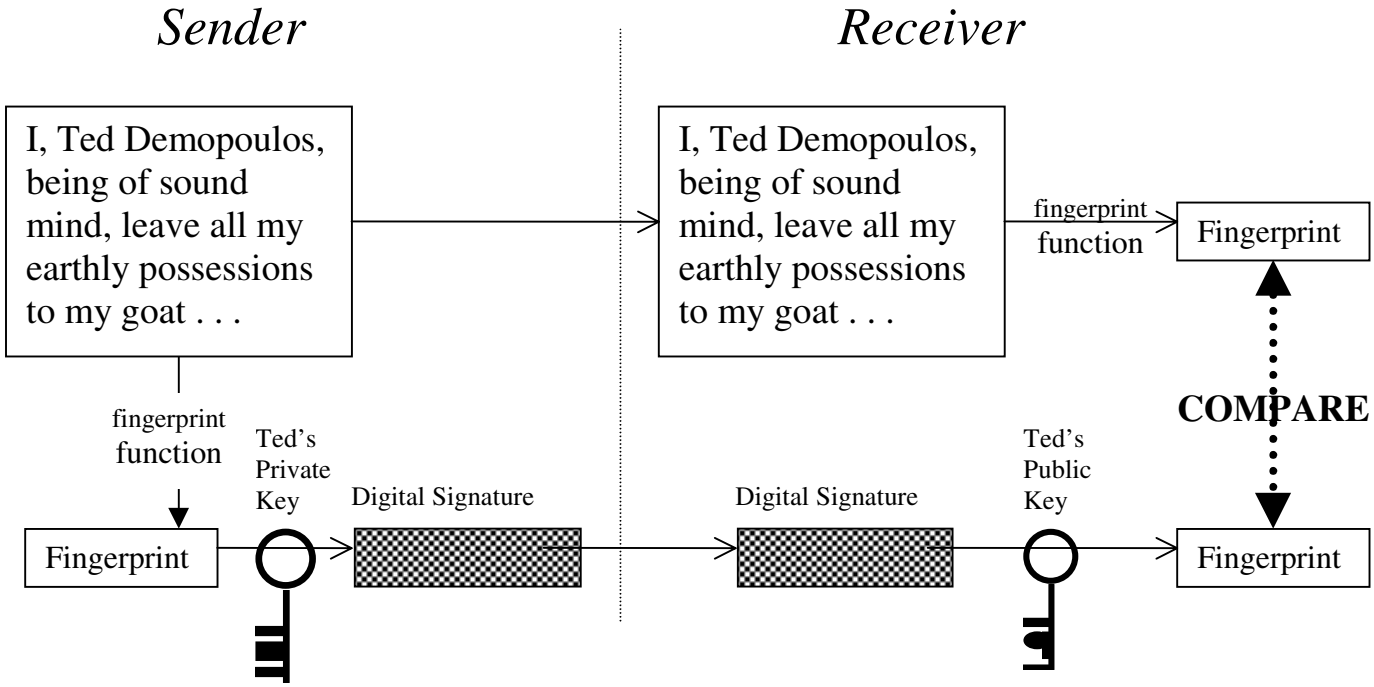
To verify a Digital Signature, it is decrypted by the signer's Public Key and compared to a "fingerprint" of the signed data. If they match, then the Digital Signature is valid. Figure A.2 illustrates how Logbook would use the process:

Fig. A.2 Digital Signature Verification



In the example below, Ted Demopoulos digitally signs a copy of his will and sends it to his attorney. His attorney can confirm that it was actually signed by Ted by verifying the Digital Signature. If the will has been modified at all, the two fingerprints to the right of the diagram will not match, and the Digital Signature's verification will fail.

Notice that the will itself is not encrypted. It could have been, for example using Ted's Attorney's Public Key. In that case, only Ted's Attorney, who presumably has his own Private Key, could decrypt the will.



A.3 Certificates

Rather than dealing with "raw" Public Keys, most software uses Certificates. A Certificate, sometimes called a "Digital Certificate," can be thought of as the digital equivalent to a Passport. Certificates contain a Public Key along with information about the entity who has the related Private Key, such as their name, who issued the Certificate, etc. The entire Certificate is Digitally Signed by a trusted party.

Some of a typical Certificate's fields are shown below:

Subject	-who this Certificate is issued to
Subject Public Key Information	-the Public Key and how it is to be used
Signature Algorithm Identifier	-algorithm used by the Trusted Party who signed this Certificate
Issuer	-who issued (and signed) this Certificate
Validity Period	-the period for which this Certificate is valid. Typically a year or less
.	
.	
Trusted Party's Digital Signature	

A Certificate is only as trustworthy as the "Trusted Party" which issued it. Using our passport analogy, some passports are very trustworthy.

For example, the USA will only issue passports to citizens, USA passports are hard to counterfeit, "blanks" are almost impossible to get, USA citizenship and passports are not for sale, and it is non-trivial to trick the US government into issuing a non legitimate passport. USA passports are very trustworthy.

There are some countries whose passports are far less trustworthy. Some countries (or in some cases their diplomats or officials) are willing to sell passports with any picture and passport details wanted. Some countries have official "Economic Citizenship" programs that allow you to become a citizen for a fee and be issued a passport. In some cases you are allowed to simultaneously change your name if desired and have it appear on the passport. These countries passports are not as trustworthy! (note that some of these passport programs ARE legitimate – often well educated, wealthy, non-criminal people who would make ideal citizens are encouraged to apply).

A.4 Certificate Authorities (CAs)

A Certificate Authority is defined as something that is trusted to sign certificates. Certificate Authorities accept Certificate applications, authorize them, issue Certificates and maintain status information about them. A Certificate is no more secure than the Certificate Authority that authorized it.

There are different types of Certificate Authorities:

Organization Specific or Internal CAs - A CA may be specific to a certain organization, such as IBM or The Red Cross. It might include only employees or perhaps customers as well. It may be internally operated or outsourced.

Public CAs - A number of CAs act as Public CAs. They issue Certificates to entities who apply for one, usually for a fee. Often Public CAs are contracted to issue all of the Certificates for a particular organization.

Verisign is the best known Public CA, and is essentially a Public Trust Utility.

A CA will have a Certificate. Some CAs have their Certificates signed by other CAs. Some CAs sign their own Certificates. These CAs with self signed Certificates are known as “Root CAs.”

In order to trust a CA we must have a copy of their Certificate in order to verify the Digital Signatures of Certificates they have issued. For example, both Microsoft Internet Explorer and Netscape Navigator come with a number of well-known and generally trusted CA’s Certificates.

A.5 Certificate Practice Statement (CPS)

A Certification Practice Statement (CPS) is a legal document issued by CAs. It describes their policies and procedures for issuing and revoking certificates. Certification Practice Statements may range from simple and almost trivial checks, to full-blown investigations and credit checks. A CA may have different CPSs for different types of Certificates it may issue.

A.6 PKI Standards

A PKI is a framework in which Public Key security is used. It is a set of standards, Certificate Authorities, relationships between the Certificate Authorities, protocols, etc to facilitate the use of Certificates.

A.6.1. Public Key Algorithms

There are a number of Public Key algorithms including Diffie-Hellman, RSA, El Gamal and Menezes-Qu-Vanstone Discrete Logarithm Algorithm. RSA is the most common Public Key algorithm, named after its inventors.

A.6.2. Certificate Standards

X.509v3 is a widely agreed upon standard for Certificates. X.509v3 Certificates are very similar to the Certificate shown in Appendix 3 (A.3). Each Certificate contains as a minimum the following information: to whom the Certificate was issued, Public Key information, a serial number, the validity period for the Certificate, the CA who signed this Certificate and their Digital Signature. The X.509v3 specification also allows Extensions, which allow arbitrary information to be included with Certificates. A number of standard extensions are defined.

A.6.3. Digital Signature Standards

There are two commonly used Digital Signature standards, RSA and Digital Signature Standard (DSS).

RSA Digital Signatures - until 1991, Digital Signatures based on RSA public key encryption were a defacto standard.

> DSS Digital Signatures - a proposed NIST (US National Institute of Standards and Technology) standard based on a variant of El Gamal signatures for signing and verification. The key length is restricted from 512 to 1024 bits. Uses the Digital Signature Algorithm (DSA). Optimized for smart cards. El Gamal is a Public Key Cryptography system based on the difficulty of computing discrete algorithms.

Appendix B. Glossary of Terms

Activation

Step in completing the registration process in which the certificate authority digitally signs the certificate. See *Activation Password, Digital Signature, Certificate, Certificate Authority, Registration.*

Activation Password

Password generated by certificate authority and sent to applicant. Applicant must send password back to the CA to activate the certificate and complete the registration process. The use of postal mail in this sequence serves to prove the applicant's identity. See *Activation, Applicant, Certificate Authority, Identity, Password, Registration.*

Applicant

A licensed amateur radio operator who wishes to register for participation in the Logbook of the World program. See *Registration.*

ARRL

American Radio Relay League. Sponsor of *Logbook of the World*, *DXCC* and the QSL *bureau* system.

ARRL HQ

ARRL headquarters.

Audit Trail

A machine-readable chronological list of all transactions in the Logbook of the World system. Facilitates troubleshooting, security investigation and deletion of false *QSL records*.

Authentication

Process of verifying the *identity* of an applicant registering for Logbook of the World. The applicant's ownership of the *call sign* to be registered is verified.

Awards

Certificates, plaques and stickers granted to amateur radio operators who prove contacts with stations in specified locations.

Awards Application

Request for *awards* credit. Contains identification information, list of claimed awards, list of claimed QSOs/credits, payment information, etc.

Awards Credit

Credit granted by an awards sponsor showing that the participant has proved a radio contact meeting specified requirements, such as *entity*, *frequency*, *mode*, etc.

Awards Sponsor

Organization offering a program granting awards for proof of radio contacts.

Bureau

Facility for providing bulk exchange of QSL cards.

Buro

See *Bureau*.

Call Book

Directory of amateur radio operators containing *call sign*, name, address and other information. May contain data collected from unofficial sources.

Call Sign

A short sequence of letters and numbers that identify a licensed radio station.

Card Image

Graphic representation of a QSL card.

Certificate

A machine-readable identification record used in *Public Key Infrastructure*. Contains *participant's* identifying information and *public key*. The certificate is digitally signed by the *Certificate Authority.*

Certificate Authority

Organization that issues and maintains certificates. Also known as the CA. Services include *authentication* and *revocation*. See *Certificate.*

Contest

Amateur radio activity in which each participant attempts to contact as many of the other participants as possible in a prescribed time period, usually 24-48 hours. Frequent contests and the large number of QSOs results in a significant percentage of total QSL traffic.

Confirmation

Condition resulting when two *QSL records* exactly match according to a set of *Confirmation Rules* for a particular awards program. Confirmation is required for *awards credit*.

Confirmation Rules

A set of rules for determining when two *QSL records* match.

Cracking

The act of guessing a *userID, password* or *passphrase.* Computerized attacks may involve attemting every possible character combination (brute force) or sophisticated mathematical or statistical guessing algorithms.

Digital Signature

Technology whereby machine-readable data can be signed. The signature proves who signed the data and that the data has not been altered since signing.

Direct QSL

QSL card sent directly to recipient via postal mail.

DSA

Digital Signature Algorithm. Standard created by the U.S. Government for creating a *digital signature*. Uses *Public Key Infrastructure*.

DXCC

DX Century Club. Awards program sponsored by ARRL for winning certificates, stickers and plaques for proving radio contacts with at least 100 entities. The most popular awards program in the world and the recipient of the most QSL cards.

DXing

Amateur radio operating activity in which participants attempt to contact as many different countries or *DXCC entities* as possible.

DXpedition

Amateur radio operating activity in which one or more operators sets up a temporary radio station in another country.

Electronic QSL

A machine-readable version of a paper QSL card. Can be used to confirm radio contacts.

Encryption

Technology for scrambling data to ensure secrecy and privacy. Used by some *digital signature* algorithms.

Entity

A location for which *DXCC* credit may be obtained. Usually a country or territory of a country.

EQSL

A *digitally signed* electronic QSL that is sent by one amateur radio operator to another. In order to confirm the conact, the receiving operator generates a matching signed *QSL record*. The pair of signed QSL records is then returned to the originating operator or forwarded to the awards sponsor. An EQSL system mimics the paper QSL system. Note the *Logbook of the World* is not an EQSL system.

Expiration

Date when a *certificate* is no longer valid.

FCC License Database

Machine-readable database containing *call sign*, name, address and other information for all currently-licensed amateur radio operators in the United States and its territories.

Fingerprint

See *Hash.*

Frequency

QSL data indicating the radio frequency on which a radio contact took place.

Hacker

A person who deliberately attempts to subvert a computer system.

Hash

A short set of data bits that uniquely identifies a larger set of bits, such as a character string, a data record or a file. Also known as a fingerprint. A special sequence, called a hashing algorithm, is used to create the hash. Secure hashing algorithms are one-way (i.e., the larger set of bits cannot be reverse engineered from the hash.) See *SHA*.

Honor Roll

Coveted award granted by the *ARRL DXCC* program for proving radio contacts with nearly all of the *entities* on the DXCC list.

Honor System

An *authentication* system that relies on the word of the *applicant*.

HQ

ARRL headquarters.

ID

Abbreviation for *identity* or *identification* information.

Identity

Who you are. In Logbook of the World, the person who owns a particular *call sign*.

Identification

Process of establishing *identity*. In Logbook of the World, process of establishing *call sign* ownership.

Identification Document

A paper document identifying a particular person, issued by an official entity such as a government agency or department. Required for authenticating DX call signs.

Insider

A person employed by the operator of a central server. A security risk exists if the person has access to the server. See *Logbook Server.*

IOTA

Islands on the Air. An awards program focused on radio contacts with operators located on Islands.

Key

A sequence of data bits required to encrypt or decrypt a message, or to generate or verify a *digital signature*. See *Key Distribution, Key Pair, Public Key Infrastructure, Public Key, Private Key, Secret Key.*

Key Distribution

Process of sending *keys* for *encryption* and/or *digital signature* to each participant in a secure network.

Key Pair

In *Public Key Infrastructure,* a mathematically related pair of *keys* used for *encryption* and *digital signatures*. One key is made public (see *Public Key*) and one key is kept secret (see *Private Key*). Provides a secure method of key distribution.

Library

A set of computer subroutines that can be used by a program to offer specific functionality. In Logbook of the World, a set of *ARRL*-supplied subroutines that can be used by a log program for *Public Key Infrastructure* and communications.

License

Official sanction of an amateur radio operator by a *Licensing Authority*.

License Authority

Government entity responsible for issuing amateur radio licenses. The Federal Communications Commission (FCC) is the licensing authority in the United States.

Log Program

A computer program allowing entry of radio contact information into a permanent database. Most popular log programs keep track of progress towards popular *awards*.

Logbook Server

The central computer system that runs the *Logbook of the World* application.

Logbook of the World

The ARRL central database of worldwide QSL and *confirmation* information. Allows electronic submission of QSL data for transmission to *DXCC* and other awards programs.

Member number

Unique number issued by *ARRL* to each of its members.

Mode

QSL data indicating the modulation mode (CW, SSB, AM, FM, RTTY, etc.) in which a radio contact took place.

Outsource

To retain another organization or individual to perform data processing tasks.

Participant

A licensed amateur radio operator who is registered to use *Logbook of the World*.

Passphrase

A set of words used to protect access to applications and/or data.

Password

A sequence of characters used to protect access to applications and/or data. See *Activation Password.*

PIN

Personal Identification Number. A short sequence of numbers used to protect a credit/debit card or a *smartcard*. Similar to a *password*.

PKI

See Public Key Infrastructure.

Pointer

A value that indicates the location of certain data within a database or file.

Portable Call

A *call sign* that is used in a location other than the official licensed location. For example, if NT1N operates in the seventh call district, he would sign NT1N/7. If NT1N operates in France, he would sign NT1N/F. NT1N/7 and NT1N/F are both examples of portable call signs.

Private Key

One of two mathematically related *keys* from a *key pair* used in a *Public Key Infrastructure* security system. The private key is always kept secret.

Public Key

One of two mathematically related *keys* from a *key pair* used in a *Public Key Infrastructure* security system. The public key may be published for all to see.

Public Key Infrastructure

A system using mathematically related *keys* to perform *encryption* and *digital signatures*. One key is public and one key is private. See *Key Pair, Private Key, Public Key.*

QSL

Confirmation of a radio contact. The information may be on paper or in machine-readable form.

QSL Card

A piece of paper or cardboard containing information and a signature confirming a radio contact.

QSL Record

A machine-readable set of data containing information that confirms a radio contact.

QSO

Abbreviation for a radio contact.

QTH

Abbreviation for location.

Rare Entity

A *DXCC entity* with which it is difficult to make and confirm a radio contact. Confirmations of contacts with rare entities require special scrutiny for authenticity.

Registration

Process of applying for and receiving authorization use *Logbook of the World*.

Reissued Call

A call sign originally issued to one person, then later reassigned by the *license authority* to another person. Frequently occurs as a result of the FCC vanity call sign program.

Renewal

Process of reinstating an expired *certificate*.

Revocation

Process of invalidating a *certificate*. Usually involves placing the certificate on a Certificate Revocation List (CRL).

RSA

Popular *digital signature* algorithm. Uses *SHA* plus *encryption* by exponentiation.

RST

Sequence of numbers representing received signal quality. “R” stands for Readability, “S” stands for Signal Strength and “T” stands for Tone (CW only.)

SHA

Secure Hash Algorithm. Widely-used standard for generating a hash. See *Hash.*

Secret Key

A sequence of data bits used for *encryption* and *digital signature*. Also known as a *Shared Key.* Both parties must posses a copy of the key and must not reveal it. This methodology presents security problems in key distribution that are not presented by *Public Key Infrastructure* systems.

Signature

See *Digital Signature.*

Smartcard

A plastic card, similar to a credit card, that contains a computer chip and/or memory chip. Some smartcards are used only to store data. Advanced smartcards can perform operations on data stored on the card, including *encryption* and *digital signature* operations.

Submission

Process of sending *QSL records* to *Logbook of the World*.

User ID

A sequence of characters identifying a user. May or may not be kept secret. Often used in conjunction with a *password* or *passphrase*.

Validation

Process of confirming *identity*.

Verification

Process of confirming a *digital signature*.

X.509

A widely-used format for *Certificates.*

