Requirements for ARRL Logbook of the World Trusted Partners

The purpose of this document is to resolve some security issues concerning the interaction of third-party web sites with LoTW. Some sites have begun offering to store users' logs, passwords and LoTW certificates and manage users' LoTW accounts for them. Without adequate security, such sites would compromise the security of LoTW. ARRL has created this minimum security standard which a third-party site would have to meet, in order to maintain the same level of security as LoTW. Third parties may request acceptance to this Trusted Partners certification program and submit details as required to ensure their practices meet the standards. Sites meeting these requirements will be listed on ARRL's LoTW site.

To obtain and retain ARRL certification as a Logbook of the World (LoTW) Trusted Partner, the provider of a web-based service must satisfy the following requirements:

1. Private keys (and .p12 files which contain private keys) shall not be stored unencrypted ("in the clear") on a Partner's systems
2. Private keys (and .p12 files which contain private keys) may be stored on the Partner's systems provided that:
   2.1. The private key shall be encrypted using a cryptographic method having a strength equal to or greater than a 1024-bit asymmetric key (DSA/RSA) or an 80-bit symmetric key (2TDEA),
   2.2. The data protection (encryption) key which is used to encrypt the private key shall:
      2.2.1. be unique per private key;
      2.2.2. be known only to the user;
      2.2.3. be supplied by the user (or the user's computer) for each log that is signed;
      2.2.4. only be transmitted between a user's and a Partner's system by means of a secure (encrypted) protocol, e.g. HTTPS;
      2.2.5. not be stored on the Partner's systems.
3. A Partner may choose to store a user's private key in the user's web browser by means of a persistent, secure cookie.
4. For data protection keys that are derived by means of a password-based key derivation procedure, §2 in its entirety shall also apply to the input "secret value" (password, passphrase) as well as to the master key and all data protection keys produced as a result of the application of a such a procedure. (Reference: NIST SP 800-32).
5. A Partner shall ensure that the guessing entropy (calculated per Appendix A of NIST SP 800-63-2) of a password and derived data protection key used to encrypt a private key satisfies §2.1.
   5.1. A Partner who accepts a .p12 file which has already been "password protected" by a user shall have some means of verifying that the entropy of the user-supplied password and derived data protection key complies with §2.1 before the Partner may store the file on its systems.
6. Initially, and annually thereafter, a Partner shall provide the ARRL with written documentation describing how LoTW users' private keys (and .p12 files that contain private keys) are processed by and stored on the Partner's system.
7. All Partner's systems that access LoTW users' private keys shall pass a user-level inspection conducted by ARRL using a non-privileged account.

The following pages provide specifics and rationale for the above requirements.

Definitions

LoTW certificate	This is an X.509 format object. In LoTW this certificate is most often exchanged in *gzip* compressed format with a ".tq6" filename extension. A certificate does not constitute a "secret" and may be freely shared without restrictions.
Private key	This is the secret part of an asymmetric key pair. The private key is intended to be kept as a "secret": known only to, and in the sole control and possession of, the LoTW end-user.
.p12 file	A file in PKCS #12 archive format. This format provides a container for storing X.509 certificates and private keys.

Background

The authentication protocols employed by ARRL Logbook of the World (LoTW) assume:

1. some communications methods that may be used for the transmittal of logs will be inherently insecure and not trustworthy, e.g. e-mail;
2. the originator of a log cannot be reliably determined via the method used to transmit the log, e.g. e-mails can be forged.

To counter these limitations, participation in LoTW requires that a user authenticate their logs by means of something that only the user possesses. For LoTW, this something is a software authenticator (token) from the public-key infrastructure (PKI): the secret part of an asymmetric key pair — the private key (https://msdn.microsoft.com/en-us/library/windows/desktop/bb427432%28v=vs.85%29.aspx).

The PKI supports "non-repudiation," meaning that an individual cannot successfully deny his involvement in a transaction authenticated by his private key. The most basic requirement for non-repudiation is that the private key being used to authenticate shall be generated and securely stored in a manner that is *under the sole control of the user at all times*. The primary threat to such an authentication scheme is that users' authenticators (private keys) are copied with or without the users' knowledge.

As a corollary to the assumption that all communications channels are inherently insecure, LoTW's design also presumes that all network-connected computer systems are inherently insecure. Therefore, as a mitigation against the "duplication threat", LoTW private keys are by design not stored in a central repository by ARRL, i.e. ARRL has chosen not to maintain a key backup and recovery server as a part of the LoTW PKI. The existence of a repository of private keys from multiple users was originally —and continues to be — viewed as constituting an unacceptable and unnecessary risk for LoTW and the integrity of the awards programs which it supports.

LoTW private keys are intended to be stored only on a computer system which is in the user's possession and control; and, in normal operation, a LoTW private key never leaves the user's possession or control. Such dispersal is meant both to limit the extent of the damage that would result in the event

of key compromise to a single user at a time and to clearly define the party responsible for keeping the private key secret.

ARRL policy specifies what happens should a private key be discovered to have been compromised: all contacts submitted by the holder of the key will be removed from LoTW, all confirmations generated by those contacts will be invalidated, and all award credit generated by those confirmations will be revoked. Users who allow their keys to be compromised, or who knowingly exploit compromised keys, may lose their privileges of using LoTW and participating in ARRL-sponsored award programs including DXCC.

Because the consequences are potentially so dire for an individual user, the ARRL does strongly recommend that LoTW users who store their private keys on shared or public computers protect their keys by means of password-based encryption.

The consequences for a user whose LoTW private key is compromised are clearly spelled out in existing policy. However, it is impossible to determine how or when a private key became compromised or whether a private key was compromised while that key was in the user's possession or while the key was entrusted to the care of another. Therefore, if a compromised key was shared with another individual in order for that second person to act as a QSL Manager, due consideration would have to be given as to whether that QSL Manager personally as well as all of that Manager's other clients would also be subject to similar consequences and sanctions as the user whose key was discovered to be compromised.

A web-based service which authenticates logs on behalf of its users is choosing to play the same role as the QSL Manager traditionally has. If it were learned that a user whose private key had become compromised had ever provided that key to a web-based service for the purpose of authenticating a log, such a situation would then present a very serious dilemma for ARRL, the service provider, as well as all of the users of the service.

ARRL wishes to encourage the widespread adoption and use of Logbook of the World; simultaneously ARRL needs flexibility to act in protecting the integrity of its awards programs and Logbook of the World. There are users who desire to use a web-based logging service in preference to a desktop application; these users would be dismayed to discover that they could be placing their long-term participation and investment in an award program such as DXCC at risk by having chosen to use such a service. Web developers want to offer their customers a reliable service; developers do not want their product and their customers exposed to risks due to events which may be outside of the developer's direct control.

To address the risks and uncertainties represented by these competing interests, ARRL has created the Logbook of the World Trusted Partners program. ARRL requests that LoTW Trusted Partners cooperate by not doing anything that would either:

i. conflict with the basic assumptions made in the design LoTW's authentication method; or
ii. compromise the functioning of LoTW's method of authentication.

And in return the ARRL agrees that no blanket consequences will be applied to all the users of a Partner's service in the event that the private key of a user of a Partner's service is found to have been compromised.

Frequently Asked Questions (FAQ)

1. **What are examples of "strong" passwords considered acceptable for securing a LoTW private key by means of password-based encryption?**

   For a password from which a data protection key is derived, a Trusted Partner needs to ensure that the password has at least 80-bits of "information entropy." Some examples of suitable passwords include:

   a. A randomly generated password 13-characters in length composed of characters chosen from the set of all ASCII printable characters (95 symbols);
   b. A randomly generated password 14-characters in length composed of characters chosen from the set of case-sensitive alphanumeric ASCII characters (a-z, A-Z, 0–9; 62 symbols);
   c. A randomly generated password 16-characters in length composed of characters chosen from the set of case-sensitive alphanumeric ASCII characters (a-z, 0–9; 36 symbols);
   d. A passphrase consisting of a sequence of six (6) words randomly chosen form a list of O(10,000) dictionary words, e.g.:
      http://world.std.com/~reinhold/diceware.html
      https://xkcd.com/936/

2. **How should random passwords be generated?**

   To ensure that a password is truly random, a Partner has the responsibility for generating the random password and then supplying it to their user. While a Partner may choose to make use of its own systems to generate random passwords on behalf of the user, a Partner shall never permanently store any password that it generates on any of its systems.

3. **Randomly generated and assigned passwords are very user unfriendly, can user-supplied passwords be employed by Trusted Partners in the password-based encryption of LoTW private keys?**

   Yes. The difficulty presented by user-supplied passwords is obtaining a reasonable estimate for the "guessing entropy" such passwords possess. One method for doing this is described in Appendix A of NIST Special Publication 800-63-2, *Electronic Authentication Guideline* (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>).

   Now, in that very appendix, the authors warn not to regard the method being described as being anything more than a "very rough rule of thumb." There is subsequent research that strongly suggests that the NIST procedure likely represents both an underestimate of the guessing entropy on the "easy" end and an overestimate on the "difficult" end. However, the NIST procedure is pretty much the only one out there in terms of an objective method for estimating the guessing entropy of a password. So, lacking a more suitable alternative, ARRL Trusted Partner requirements reference the NIST procedure.

   According to the NIST method, a user-chosen password with the specified 80-bits of guessing entropy requires a password with a length of 64 characters (if no checks are applied) or 58 characters (when both a dictionary check and composition rules are applied). ARRL recognizes

that is almost certainly an overestimate of the password length needed to meet the 80-bits of guessing entropy requirement as well as being an impractical length for a user chosen password — it is something that would be described more appropriately as a "passphrase".

4. What role do private keys and digital signatures play in Logbook of the World?

Private keys and digital signatures are the mechanism by which the origin of log entries which are submitted (uploaded) can be authenticated. In the narrowest technical sense, a digital signature is a method for authenticating that a log entry was "signed" by someone who has possession and control of a specific private key.

Because the private key is an item that could be stolen, leaked or shared — although it never should be — the digital signature does not "prove" the identity of the individual who signed a log entry. The digital signature only establishes that a log entry has been "signed" using an item which is expected to remain under the sole control of an LoTW user at all times.

An LoTW user who, for whatever reason, "loses control" of their private key can no longer be considered a "trustworthy" participant in Logbook of the World. So, any compromised or otherwise untrustworthy user must — at a minimum — "start over" in LoTW with a new private key and re-uploading all of their logs, etc.

5. In what way is non-repudiation important to users of Logbook of the World and to web application providers?

A LoTW user might attempt to explain the misuse of a private key by claiming that "my private key had to have been stolen." Whether true or not, by making a statement of that sort, the user is proving themselves "untrustworthy" to be a participant in LoTW — just as the misuse of a private key on its own could be taken as proof of untrustworthiness. Despite — or rather because of — any attempt at repudiation will result in the user being disavowed and their record of participation in LoTW expunged.

Participation by intermediaries — like a web service — in the chain of custody of a private key is not naturally a part of the public-key infrastructure (PKI) and it does obfuscate how the PKI goes about providing a "solution" to the non-repudiation problem.

Consequently, if a LoTW user's attempt to explain the misuse of a private key was instead that "my private key must have been leaked because I supplied my key to Brand-X's web site" then, just taking the user's statement at face value, suspicion must naturally fall upon all users of Brand-X's web site as having been similarly compromised.

The Trusted Partners program is an attempt to forestall the natural and logical progression of such suspicions — and their consequences — by pre-certifying that a Trusted Partner's web application meets certain minimum requirements for trustworthiness.

6. So, what's the worst that could happen if a web service provider doesn't become a Trusted Partner?

Imagine the scenario of a $1,000,000-class mega-DXpedition whose QSL manager sells confirmations or whose QSL printer siphons off a few blank cards for him and a few of his friends or ….

In such a scenario, whatever sanctions might be imposed on the parties directly involved, there would certainly also be a scandal, perhaps a personal and financial disaster for some of those involved, possibly great disappointment among the "deserving" expecting to get an all-time new one. But the extent of the disruption and the number of unhappy people is limited to just the one discredited DXpedition.

Now, imagine that one DXpedition plus 50 more like it all have used Brand-X's cloud signing service. And then some other individual user of Brand-X's service — a non-DXpedition, maybe even not a DXer — is found to have had his LoTW private key compromised.

Would any web service choose to put itself in Brand-X's position after having been informed of the possible consequences for its users and not become a Trusted Partner?