Implementation Guide

Core Retailer Web-Based Applications

Version 1.0, May 2007

NASPL

THE Open GROUP
Making standards work™

Implementation Guide

Core Retailer Web-Based Applications

Version 1.0, May 2007

Document Number: IG0703

Published by The Open Group, May 2007.

Comments relating to the material contained in this document may be submitted to:

nsi-specifications@opengroup.org

Contents

Preface

North American Association of State and Provincial Lotteries (NASPL)

The NASPL Standards Initiative (NSI) was approved and funded by NASPL and the vendor community as a collaborative development effort with participation from the lotteries, gaming vendors, and retail associations. Project management and facilitation services for standards development and certification are provided by The Open Group in conjunction with NASPL.

The NSI vision is to provide an interoperable lottery environment that is based on a set of open Technical Standards, approved Best Practices, Certification and Verification programs that, when implemented, will improve the quality and integrity of the lottery environment, and will provide increased efficiencies, resulting in reduced costs and increased profit margins for lotteries, vendors, and lottery retailers.

The NSI mission is to establish a resilient organizational structure, set of processes, and procedures that will engage all constituents (lotteries, vendors, and retail representatives) in an environment of open discussion and cooperative development.

Further information about NASPL is available at www.naspl.org.

The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service, including UNIX certification. Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards, Best Practices, and Guides. Full details and a catalog are available at www.opengroup.org/bookstore.

Readers should note that all published NSI Technical Standards and Best Practices, and any updates, in the form of Corrigenda, are available at www.opengroup.org/naspl/published.

1 Introduction

1.1 Purpose and Scope

This document is the Implementation Guide for the Core Retailer Web-Based Applications Best Practice. It has been developed by The Open Group.

This guide is designed to help lottery vendors and lotteries implement web-based technologies to support lottery-retailer operations consistent with the Best Practice. In short, this entails implementation of a secure website that retailers can access to obtain financial information about their lottery-based activities.

The Best Practice builds on the NSI Technical Standard for XML Retail Accounting Reports in the Lottery Industry by defining the minimum technical requirements for delivery of the accounting reports. Additionally, the Best Practice establishes the overall type, frequency, and retention of data contained within the XML format defined by the Technical Standard. This guide will supplement the details of the Best Practice by providing possible implementation strategies and approaches.

1.2 About This Document

The structure of this document is as follows:

- Chapter 1: Introduction

  This section introduces the document and describes the purpose and scope of the Implementation Guide.

- Chapter 2: Why Implement the Best Practice?

  This section addresses the business rationale and operational issues that are driving the implementation of the Best Practice.

- Chapter 3: How to Implement the Best Practice

  This section provides a guide to implementing the Best Practice.

- Chapter 4: Certification/Verification Process

  This section looks at what comes after the implementation of the Best Practice, with a focus on moving toward formal certification/verification; that is, NSI Verification for lotteries and NSI Certification for vendors.

- Chapter 5: Contact Information

2 Why Implement the Best Practice?

This section sets the operational context and describes the business drivers and objectives for implementing the Best Practice.

The Core Retailer Web-Based Applications Best Practice is focused on improving communications between lotteries and retailers, specifically in the area of financial activity. The lottery-to-retailer relationship is a fundamental part of the business model for all lotteries, as graphically shown in Figure 1 of Section 2.1.1 of the Best Practice. The retailer is the bridge between the lottery and the final customer, the player.

Currently, all lotteries provide financial information to retailers. Most jurisdictions are in fact providing all of the information the retailers need. Most are even providing chain information electronically. So why implement this Best Practice? The answer to this question requires a look at the broader picture of the retailer's world.

Web technologies have become the mainstay of most business-to-business communication. The technology is affordable, reliable, and most importantly prevalent thought the business world. This is the technology that enables retail chains to grow and operate in wider geological locations. It also allows smaller retailers to be more efficient in the back-office portion of their business. Most of the suppliers to retailers provide web-based access to accomplish everything from ordering to accounting. Many larger retailers have a requirement to receive financial information in this form that currently precludes them from offering lottery products.

The key to the success of web technologies is the consistency of approach and delivery. Successful suppliers have adopted standardized means to communicate with retailers allowing retailers to buy and build supporting infrastructure to efficiently utilize the data. The NSI efforts in this Best Practice are designed to provide the roadmap for lotteries to leverage this trend. Additional benefits include:

- Consistency for retailers across jurisdictions
- Standards-based approach for lotteries
- Potential for new retailers requiring web-based financial data
- Foundation for future improvements in lottery-retailer communications

3 How to Implement the Best Practice

3.1 Read the Best Practice

The Best Practice was developed within the NSI Best Practice Working Group and was subjected to a wide review open to all NASPL lotteries and NSI vendors. Following the review, it was approved by the NSI Steering Committee and ratified by the NASPL Executive Committee.

In order to implement the Best Practice, you must read the Best Practice. In particular, you should become very familiar with Chapter 4 in the current version of the Core Retailer Web-Based Applications Best Practice, which can be found at www.opengroup.org/naspl/published. The requirements specified in Chapter 4 of the Best Practice must be adhered to as part of conformance to the Best Practice. It is important to note that all of the prescriptive terms found in that chapter must be interpreted according to the definitions in Section 1.3 (Terminology) of the Best Practice.

In this Best Practice there is additional information to consider in Chapter 5, Design Considerations. This section does not extend or provide any additional requirements for compliance; however, it is a summary of some of the real-world experience of the team members that participated in the development of the Best Practice.

For quick reference purposes, each Best Practice contains a Requirements Checklist in Appendix A. The Requirements Checklist contains all of the requirements listed in the Best Practice, each with a reference to the specific section in the Best Practice where the requirement is specified in greater detail, and each indicating which constituent is responsible for meeting the requirement as well as the level of prescription associated with the requirement.

3.2 Implement the Best Practice

The following is a roadmap on how to implement the Best Practice. It is a guide and not necessarily mandatory, but will help with correct implementation of the Best Practice within your organization. Practitioners should refer to the Best Practice to understand what the mandatory requirements are. Practitioners may choose to explicitly follow the steps as outlined in this guide, or they may choose to combine them or do them in a different order, depending on their particular circumstances. For example, some practitioners will already have in place procedures, templates, working methods, and technology (where appropriate) that will merely need to be updated to reflect the Best Practice; others may need to create these from scratch. The approach to implementing the Best Practice may also be influenced by where an organization currently is in the lifecycle of activities defined by the Best Practice. Regardless of a practitioner's current state of readiness, following all the steps as written in their entirety in the order stated will provide a deterministic roadmap to successful implementation of the Best Practice.

3.2.1 Familiarization and Commitment

This is the starting point to implementation. It is very difficult to implement requirements that are not understood or to which staff may object on the basis of “that’s not how we do things here”.

All staff that will be responsible for operating under the Best Practice or working with technology that incorporates the Technical Standard should familiarize themselves with the content of the Best Practice. It is unlikely that each individual will understand every requirement initially. There are recourses that can help with this. Team meetings will help to ensure common understanding and it is possible that a requirement which may appear obscure to one individual is clear to another. A group discussion at this stage can help to establish common ground for the changes that will need to be made to implement the Best Practice and can feed into the next stage in the process – the Gap Analysis.

Most importantly, the familiarization exercise should be used to identify any requirements that need explanation or clarification. The first resource to be consulted should be the Best Practice FAQ (see Section 3.3). If an issue remains, then the next resource is to contact the Best Practice support contact. It is far more efficient for all concerned – both the practitioner and the Certification/Verification Authority – when a requirement can be implemented correctly the first time, rather than need corrective action after formal assessment. Spending the time to fully understand the Best Practice before starting to implement it is likely to save time overall by avoiding the need for rework.

Finally, at a team meeting it will be necessary to remove roadblocks to implementation. Many of us become fixed in the way we approach our work and can be resistant to change. For the implementation to be a success, everyone responsible for operating in accordance with the Best Practice or working with technology that incorporates the Technical Standard needs to be committed to it. This may mean certain customs and practices or technical approaches have to be abandoned or modified. It is the business practice or technical manager’s duty to ensure all staff affected by the Best Practice are committed to making it work within their organization and in their day-to-day work.

3.2.2 Gap Analysis

The gaps are the differences between the way things have been done, and are currently done, and the requirements of the Best Practice. A gap may be a requirement of the Best Practice which is handled some other way, is only partly met, or may not be addressed at all in the current practice.

It is recommended that, in the case of a Best Practice, a current project and/or a recently completed project, or, in the case of a Technical Standard, the current technology, be used as the basis for the gap analysis. The gap analysis is an internal informal method to establish to what extent the Best Practice is currently applied, and to what extent existing custom and practice and/or technology must change to implement all the requirements of the Best Practice.

Requirements Checklist as a Tool for Gap Analysis

Gap analysis is most readily approached by a compliance matrix between each Best Practice requirement on the one hand, and the way things are currently done on the other.

In the case of a Best Practice, this would be a comparison of the requirements with the current project procedures, plans, specification, records, and general documentation.

In the case of a Technical Standard, this would be a matrix of the requirements and the current technology (hardware or software programs) that is currently being deployed.

Fortunately, the Requirements Checklist, found in Appendix A of the Best Practice, can form the basis of this matrix and has already done the job of deconstructing the Best Practice into a set of discrete stand-alone requirements.

For each requirement listed in the Requirements Checklist, the practitioners should determine which of the following categorizations apply. At this point in time it is not necessary to consider whether the requirement is categorized as "must", "should", or "may" in the Best Practice; that will come later in the process.

1. **Compliant**: The practitioners believe that the processes or technical approach they normally use comply with the Best Practice requirement and they have documents, records, or technology in which the requirement is instantiated.
2. **Partly-compliant**: The practitioners believe they meet the spirit of the requirement but they omit some of the detail or they do it in a slightly different way.
3. **Non-compliant**: They do not do it.

In addition, for every requirement the practitioner should determine if (as applicable):

1. It is realized in planning documentation and/or standard templates.
2. It is realized in project records.
3. It is realized in technology.

Finally, the practitioner or technical manager should note the status of each requirement marked partly-compliant or non-compliant.

- If its status is "must", then this is a deficiency that has to be corrected for the organization's implementation of the Best Practice to be compliant.
- If the status is "should", then the practitioner or technical manager should treat this as a strong recommendation to implement; however, if the practitioner or technical manager has a compelling reason to use an alternative method of meeting the requirement, this will not necessarily be a barrier to compliance in the future. It should be noted, though, that rationale such as "at the moment that requirement may just not be the way it is done in custom and practice" is not in itself a compelling reason to depart from the Best Practice.
- If the status is "may", then implementation is optional and the practitioner or technical manager might want to decide whether implementation is desirable or not.

By methodically going through each requirement in this way, it should be possible to identify the areas where the Best Practice is not currently followed and whether there are documented processes, templates, or technology (if applicable) that need to be created or modified to ensure that the Best Practice is followed in future projects.

3.2.3 Implementation of the Best Practice

This section focuses on how to implement the Best Practice requirements with an eye to being ready to apply to the formal validation program.

Lotteries are at different points in the use of web technologies. Most have some form of web presence. Some have already implemented a retailer-focused website that provides information to retailers about game offerings, promotional activities, and other marketing data. A few others have websites that provide the information required by this Best Practice.

With the diversity of existing implementations, this part of the guide is organized as follows:

- Section 3.2.3.1 provides general information about considerations for implementing the Best Practice and covers the basic information needed no matter where the lottery is in implementation.
- Section 3.2.3.2 identifies three common starting points for lotteries, based on the existing environment of the lottery.

3.2.3.1 General Implementation Considerations

3.2.3.1.1 Overview of Implementation Options

The bottom-line focus of the Best Practice is to establish a financially-focused retailer website that provides retailers with the financial information they need to successfully deal with lottery products. Projects to implement are therefore either building or modifying a website to provide this information consistent with the Best Practice. The Best Practice provides the guidelines needed to implement this web-based technology consistently.

So, the first decision is probably to establish the level of conformance that the project will implement. The Best Practice defines two: one for lotteries, and the other for web-based technology vendors. The requirements for the technology vendors require a higher level of standardization than the requirements for lotteries. This was done to establish the intended future direction of the overall web focus of future NSI activities. So which should be implemented? This depends on the state of the lottery’s web presence. The lower level of the Best Practice should be used if the lottery already has a financially-focused website implemented. The lower level of requirements will allow an existing website to be brought into compliance with minimal effort.

If your lottery is going to create a new retailer-focused website, the higher level should be used even though it is not required. This is accomplished by including the “should” status requirements as well as the “must” status. Working to the higher level will add only an incremental cost to the project, while upgrading in the future will require another project.

The second decision that needs to be made in any implementation is what resources are going to do the work. This is generally driven by the resources available, the qualifications of the resources available, and general lottery policy. The two ends of this spectrum are:

1. Lottery IT staff implements the application.

2. Contract resources implement the application. This also contains a subset where the lottery purchases a new gaming system and includes the retailer web-based applications as part of the requirements.

Between these two ends of the spectrum, there are various hybrid configurations where a combination of lottery IT staff and contract resources are applied to build the application. There is also another potential that at some point a third-party certified retailer web-based application could be purchased as a package. Whichever approach is taken, the lottery personnel involved with the project will need to understand some additional factors covered in the remaining sections.

3.2.3.1.2 Understanding the Technologies Involved

The Best Practice divides the technology involved into the following sections:

- Website (Section 4.1.1.1 of the Best Practice)
- Website Security (Section 4.1.1.2 of the Best Practice)
- Alternate Website Formats (Section 4.1.1.3 of the Best Practice)
- Website Help and Support Features (Section 4.1.1.4 of the Best Practice)
- Alternate Language Support (Section 4.1.1.5 of the Best Practice)

The Best Practice establishes the requirements for compliance within each of the referenced sections above. This guide will provide some real-world examples of websites that meet those requirements, some possible approaches for each section, and some search guidelines to gather more information via the Internet. Additional details on implementation considerations will be explored in Section 3.2.3.2.

Website

The term “website” references the fundamental technology that allows an application to be on the Internet. A website is a combination of hardware, network connection, software, and a registered Internet domain name. The next few paragraphs further explain these components, but for the most part modern websites are purchased or leased as a package, or specialized personnel will set up the website. This can be either lottery or contract personnel. Additionally, the decision on what website to utilize will be determined by the supporting development environment used for the web-based applications. For instance, if the retailer web-based application is developed in a Microsoft environment, then the website structure will generally be Microsoft-based as well.

The simplest form of hardware is the computer. Most websites utilize a specialized computer known as a “server”. This type of computer generally has more CPU power, larger amounts of memory, and more disk space than the typical desktop. Usually a server will also feature power supplies and cases that are designed to run 24 hours a day 7 days a week without downtime. They feature redundant components to prevent a single point of failure.

Network connections are varied. Most commercial connections for websites are high-speed dedicated connections that provide access to the Internet. This access takes the form of a physical connection, and a registered Internet or IP address. These connections are provided by an Internet Service Provider (ISP), usually a telecommunications company or a company specializing in Internet connections. Typical terms for service can refer to the physical connection, such as T1, DS1, DS3, etc. More commonly, the service is now referred to in terms of bandwidth. This is quoted in terms of general capacity and often in terms of capacity used in a month. Typical terms are 1.5 megabytes (abbreviated mb; the speed of a T1), 3mb, 10mb, etc. Monthly capacity is typically quoted in gigabytes (gb) such as 5gb, 10gb, etc.

The software that runs on the server to provide the basic foundation for a website is called the “web server”. There are many different types of web server software. Typical names are Apache, Red Hat, BSD, IIS, etc. The web server software, in simplest terms, provides the operating environment that allows the hardware and network connection to be accessed by other systems via the Internet, most typically a web browser. Web servers also incorporate other basics of an operating environment such as security, storage or disk access, database access, etc.

The registered Internet domain name is something used everyday by anyone who uses the Internet. The most recognizable form is the “dot com” format or www.domainname.com which is the way websites are accessed by clients. The process of registering a domain name has been greatly simplified. There are multiple services that will assist in this registration. There are formal guidelines for proper use of domain names, but practically speaking these have been largely ignored. For instance, the “.com” extension of the domain name was originally intended for business websites. The “.org”, “.net”, and “.gov” extensions, for example, were intended to serve as extensions for non-profit organizations, network providers, and government websites respectively. Since domain name extensions were not strictly enforced, “.com” has become the default name expected by most users. Lotteries are often governed by jurisdictional requirements, policies, regulation, and/or law on the domain name they use.

In summarizing this section, this is a very high-level overview of the primary components of a website. This may seem complicated, and does require specialized knowledge to set up and maintain; however, this technology is widely used and has become a commodity much as phone or cellular service. A simple phone connection commonly taken for granted is perhaps more complicated to establish than a website. The widespread use and common ways to accomplish this make getting and using a phone line almost mundane. The same is true with websites. If you search the following terms on the Internet, you will get hundreds of thousands of references. Typical search terms include:

- Domain Names
- Internet Service Provider
- Web Hosting

Website Security

In terms of the Best Practice, security takes two forms. The first is the way the Internet connection is established, and the second is how users are allowed access. Keep in mind that this is the minimum point for security on the website, and levels that apply more security will also be in compliance with the Best Practice. The Best Practice has one underlying assumption that is the foundation of this relatively straightforward approach to security: it assumes that the website does not have a direct connection to the lottery gaming or back-office system that is accessible via the Internet. So the risk of information compromise is simply access to retailer billing information stored on the website and security should be appropriate to that level. The focus of security is then the type of information on the website, and since this is financially-focused data, a security scheme to protect that type of data is required.

Specifically, the Best Practice sets the bar at Secure Socket Layer (SSL) 128-bit encryption. Searching on that phrase returns many links that provide information on the specifics of SSL encryption and the meaning of the 128-bit mode. For purposes of this guide, it is only necessary to understand what this is at a high level and some of the rationale for choosing this approach to security. In short, SSL encryption is a process where the data passed between a web server and a client is encrypted using a trusted key. The key is obtained by a registration service and consists of two parts: a public key and a private key. The public key is shared with the client, and is used by the client's browser to encrypt or hide the actual message. Only the private key can decode the message and that only resides on the server. Messages sent by the server are also encrypted and the browser uses a process that includes the public key to decode that information.

To comply with this portion of the Best Practice, a lottery only needs to obtain the SSL key information from a registration service and utilize that as part of the web server setup. By searching on "SSL 128-bit encryption registration" many of the more popular registration services can be found. The registration service adds another layer of trust, since it maintains information about to whom the key is issued and ensures they are who they claim to be. This approach is commonly used to secure financial transactions. It is used by banks, stock brokers, mortgage companies, etc. to provide clients with a secure means to access their financial data.

The second part of security covered by the Best Practice is focused on how individuals access the website. It establishes a best practice approach for user access that is consistent with most security plans and requirements for secured systems. The foundation of this approach is to have a unique way for the system to identify a user. Once identified, the user can be granted rights to access information based on the role or group to which the user belongs. All access to the website is assigned by the role, and documented. This keeps access clear and documented. No one-off or special access has to be maintained.

Implementing this approach is best handled using some form of directory. Security directories are a specialized form of directory that maintain the roles and access rights as one function, and the user information including assigned roles as another function. It is simply a storage mechanism that allows the web server to allow access to a user. In simple terms it is just like a phone directory. A name can be found and the associated number identified based on that name. Most web server software has some form of directory or provides access to a directory. Examples of directories include Microsoft's Active Directory, Novell's eDirectory, and OpenLDAP.

Alternate Website Formats

The Best Practice defines the website as the primary means for retailer access to lottery financial data. The focus is therefore on the way that most websites are accessed – a web page served to a browser upon request. There are other ways in which websites can be accessed. One of the most important ways is accommodating a system-to-system interface that will allow the retailer's system to access the retailer website directly without the need for a person to be involved. This automated approach allows the retailer's accounting system to automatically get the financial information based on parameters, rather than requiring a person to navigate to the website and download the data, then process that data into the accounting system. The Best Practice recommends the use of the XML Remote Procedure Call (XML-RPC), details of which can be found at www.xmlrpc.com.

Other formats that may be considered include ADA access, for web users that have special access needs. Primarily this is an alternative format for people who cannot see or navigate graphical interfaces such as a common web browser.

The last category of alternative formats deals with direct access to files in various formats. This simply establishes the need to keep these formats as secure as the website and to base alternate formats on conversion from XML rather than maintaining multiple files of different types. For instance, if retailers are currently getting files from the lottery in csv format, rather than store csv files, the recommendation is to produce these files dynamically from the core XML. This will be covered in more detail in the specific implementations below.

Website Help and Support Features

The Best Practice also requires some very basic user help and support features. The primary support feature is a search function capable of returning the necessary information for a retailer to navigate the website. This is a very limited search capability focused only on the ways to find information, and not a search of the data or information itself. The Best Practice goes on to suggest providing a Frequently Asked Questions (FAQ) section. This will be worth the time and investment needed to implement as the FAQ becomes the first level of support for users, avoiding a phone call to the lottery by the retailer to get an answer to a simple question.

Alternate Language Support

Providing alternate language support is suggested, not required by the Best Practice. The best rule of thumb for alternate language support is the lottery's current practice on their terminals. If sales terminals support alternate languages, the website should also support the same alternate languages provided at the terminal.

3.2.3.1.3 Implementation of the NSI Technical Standard for XML Retail Accounting Reports

This Best Practice requires that the lottery complies with the NSI Technical Standard for XML Retail Accounting Reports in the Lottery Industry. This Technical Standard defines a format for data that acts as a defined container, namely XML. The data can then be accessed by a retailer using tools that will work consistently across lottery jurisdictions. The Technical Standard does not define a required type or frequency of data; it simply defines the XML container.

The Best Practice leverages the work from this Technical Standard and adds requirements for both the type and frequency of data. In summary, the Best Practice requires three types of data, each with a specific frequency. These are:

- Invoice Data – produced for each invoice period as defined by the lottery
- Summarized Financial Data – for each business day as defined by the lottery

- Point-in-time Scratch Inventory Levels – at the end of each business day as defined by the lottery

Details on how to produce these XML files are included in the Implementation Guide for NSI XML Retail Accounting Reports (available at www.opengroup.org/naspl/published).

3.2.3.1.4 *Approaches to Frequency and Data Retention on the Website*

The Best Practice defines the requirements for both frequency of data and retention of that data. These requirements were based on several factors. The primary factor was a basic knowledge of what a retailer needs to balance and control lottery-based activities in their store. This is currently reflected in the accounting reports available to the retailer via the gaming terminal. This can be enhanced using the web technologies referenced in the Best Practice. The retention factors were established by communicating with lottery accounting departments about the nature and types of calls they receive from retailers about past financial data. Both the frequency and retention were vetted with active retailers as part of the process and with several lottery field representatives that dealt directly with retailers.

To get this data requires converting the existing financial information present on either the lottery gaming system or back-office system into the XML format as discussed in Section 3.2.3.1.3 above. Retention means storing the financial data required by the Best Practice in a manner that allows a retailer to retrieve the information on the website without lottery assistance. Storing XML files has two basic approaches. One is via a file system on the website. The other is via a database. The database has several clear advantages over the file system approach.

Database operations pose less of a security risk than file system operations. Because the database does not provide a means to access the core file system, there is less risk of modifying or inserting files onto the server. Databases can also limit access based on the user’s roles without the need to modify the underlying file structure of the web server. Databases are more scalable than file systems. The sheer number of retailers and the number of XML files required for each retailer can make a file system very complex. Databases were designed to handle the volume without taxing file system resources. Databases support searchable queries and sorting. To accomplish this with a file system would require specialized code that will be an existing part of a database.

3.2.3.2 Specific Implementation Considerations

The intent of the following sections is to detail some of the issues to consider based on state of the lottery’s web presence. To some degree, these sections will build upon each other. For instance, lotteries with no web presence will start with what needs to be done to get a web presence. Once the web presence exists, that lottery would do much the same thing as a lottery with no retailer web focus, and so on.

3.2.3.2.1 *Lotteries with No Web Presence*

If a lottery has no web presence at all, then implementing this Best Practice will be the foundation of future websites as well. This adds some additional considerations that should be taken into account.

Generally, lotteries have developed websites of four general types, as follows:

- Jurisdiction-Focused

  The jurisdictional focus is a way of providing the general public with information about how a lottery functions in light of it being a governmental entity. This generally includes information required by law about the location of the lottery, the governance structure, contact information, and other information similar to other agencies of the jurisdiction. This type of website usually has a jurisdictional mandated look-and-feel to provide a consistency across agencies. It may also require a specific hosting arrangement so the lottery would simply submit content or pages. These websites may include some retailer-focused content, primarily in the form of how to become a retailer.

- Marketing-Focused

  Marketing-focused websites primarily target players. This is information about the games, how to play, where to play, and new games and/or concepts. These websites usually feature the way lottery proceeds are utilized by the jurisdiction and other ways the lottery contributes to the community. There may be a portion of this type of website focused on the retailer. Generally, retailer-focused marketing is in the same vein as player-focused marketing; i.e., information about the games and promotions available from the lottery.

- Game Focused

  The web has a natural attraction for gaming activity. Some lotteries are venturing into the web as a way to enhance the gaming experience. This takes the form of second chance opportunities where the website provides an entry mechanism, generally tied to entry of a losing ticket number for participation in a second chance draw. Other approaches enhance the scratch product by providing a visual gaming experience based on codes entered from scratch tickets. The winning and losing scenarios are played out online *versus* the traditional removal of the latex from the ticket. These websites are largely experimental and almost exclusively aimed at players of the games.

- Retailer Business-to-Business (B2B)

  Retailer-focused websites are created to conduct business. The core features of this type of website are covered by this Best Practice. Users will consist of the retailer base and traffic is related to the information available on the website. This website may also provide the appropriate links or content that may be available on the types of website detailed above.

When a lottery plans its whole web presence, the main consideration is which types of website are likely in the short, mid, and long term. Usually a B2B or retailer-focused website is not going to be the first web presence. But if it is, then there is still the consideration of the roles the other types of websites may provide in the mix. Also, some types of websites may seem totally unlikely, such as the gaming-focused website. But in long-term design you should still consider the possibility. In short there are four steps to getting a web presence for the lottery in place. These are:

- Domain Name

  Domain names are often overlooked in initial planning, but some thought and planning here can provide a solid foundation for flexibility down the line. If your jurisdiction requires the use of a specific domain name for the lottery, then this section may not apply; however, this may also provide some concepts that may provide a basis for use of additional domain names.

Domain names were originally conceived to provide two types of information. The first part is who the organization is; this is the root of the domain name. The second part is the type of organization; this is the extension of the domain name. With this intent in mind, the lottery can leverage domain naming to reflect the types of website provided. For instance, the domain lottery.gov or lottery.org can provide the jurisdictional-focused information. Lottery.com can be the business side of the lottery, defaulting to the marketing focus. A brand-focused name can be created for the gaming website, such as playlottery.com (the marketing staff will drive the actual name).

The retailer-focused website can also be identified via domain name. By using a sub-domain, any of the root domains can be specialized in purpose. As an example, retailer.lottery.com can be the place retailers go for B2B information. One other approach is to utilize a secure connection for the B2B website. For example, http://lottery.com would go to the marketing website, while https://lottery.com would resolve to the B2B website. The difference is the type of connection which will be covered in Section 3.2.3.2.2.

Acquiring a domain name is fairly simple. There is a multitude of domain registration organizations on the web. A simple search on "domain name registration" in any search engine will return millions of hits. Fees start around US $4 and go up based on the services offered. Normal services include auto-renewal.

Domain names also provide another major service. The domain name is the glue that ties the various hosting services that may be present into a single presence on the web; see Hosting below.

- Hosting

  Hosting is the basic service that allows a website to exist. There are two aspects that must be considered: who will provide the web hosting services and what is required. Section 5.1 of the Best Practice actually details design considerations. This includes a formula for calculating needed space to security requirements. Use this section to determine what is required. A similar type of analysis should be done for all of the other types of websites the lottery plans to implement in the short and mid terms so that hosting options can scale to meet those needs without requiring a re-engineering process.

  When considering who will provide the hosting service, the need for maintenance should also be considered. The ongoing maintenance requirements will far outstrip the initial setup costs and efforts over time. Basic maintenance considerations are detailed in Maintenance below.

  A primary factor in who will provide hosting services may be the jurisdictional legal or policy requirements in place. If the lottery jurisdiction is prescriptive in how web services are provided, that will generally drive the hosting decision. However, best practice web environment design may provide a means of justifying a change from policy requirements. Some of the basics are considered here.

First, a lottery web presence will generally require web hosts that are dedicated to the lottery's needs. The only exception to this is the jurisdictional type of website. Traffic to the marketing website will generally be the driving factor that requires a marketing website to be separately hosted. The security requirements will drive the retailer website in a different direction. The graphical volume will also drive specific needs for a gaming-focused website. This divergence in the nature of the possible websites drives a basic design consideration, namely separation of the websites.

Best practice design would isolate the web services provided based on the type of service required. For instance, the marketing website would be either physically or logically separated from the retailer-focused B2B website. This design allows the needed features for each type of service to be specifically tailored to the service. Physical separation requires the use of two separate web servers. Logical separation uses a specialized type of hosting known as "virtual web hosts". This allows a logical separation to be in place that is as robust as a physical separation, but utilizes the same hardware. The factor that determines whether logical or physical separation should occur is basically volume. Two services that require large amounts of processor and storage access should be physically separated. Services that do not can be logically separated. For the most part, the only service that will truly drive physical separation will be the gaming style of the website based on the graphical nature of the games.

Bandwidth is not generally a consideration in web host separation, since bandwidth is most often a shared resource available to all physical and logical hosts. Bandwidth does have an influence on who would provide the service. This will be the primary driving force behind outsourcing the web hosting service. To buy and maintain a web connection, a lottery has to plan on capacity that will meet the bursting needs of the website. For instance, plans would need to anticipate the big volume hit that will most likely occur immediately after an invoice is available on the website. That would have to be factored in with the expected volume of all other websites the lottery provides. This burst capacity, if not provided, will cause very noticeable delays or even timeouts in web accesses by retailers and/or players, which will eventually dry up usage.

To meet that burst capacity, the lottery will in effect over-buy the needed bandwidth for most of the normal operations. Hosting services buy large capacity bandwidth and subdivide it for resale. They allow for burst beyond the "normal" size commit and generally price on average use over a period of time, most generally a month. Add into that the fact that the hosting company will provide maintenance of the bandwidth, upgrades, monitoring, etc. and the package becomes even more attractive. Add in the same types of service for the basic hosting hardware that offers both physical and virtual hosting capacity on a scalable basis and the reason for outsourcing by most companies becomes clear.

The driving factor behind internal hosting is generally based on one of two issues. These are security or legal requirements. Since the design suggested by the Best Practice specifically addresses the major security risk, that factor is mitigated. If there is a legal requirement that the lottery or jurisdiction must host themselves, then this decision is already made. Most businesses now recognize that providing their own hosting services is equivalent to providing their own phone service and similar decisions are being made to outsource.

- Content Plan

  Content is the heart of the website. In the case of the retailer-focused B2B website, the Best Practice defines the content, frequency, and retention of the base content. For all other websites, a content plan should be developed. This plan details what content will be made available by the website, who is the authoritative source for the content, who creates the content, and who is responsible for getting the content on the website. The authoritative source is the person or entity that provides the credibility to the content. In the case of the B2B website, this source is normally the accounting department of the lottery since this is financially-focused information. The other types of website will have other authoritative sources.

  Also note that the person or people in the organization who create the content may not be the people responsible for putting the content on the web. The creators are responsible for ensuring accuracy, consistency, and alignment. Those charged with putting the content on the website are technically-focused.

- Maintenance

  Websites require maintenance. Even the most basic static page website needs to be updated when a major change occurs. Additionally, there is a need to monitor the website to ensure it is available and functioning. Practically speaking there are other basic things that should be done to ensure the website is performing as expected.

  The retailer-focused website has some specific areas where maintenance will be critical. The Best Practice requires a daily update to content. The retention of data also requires a planned approach. Finally, the website must be available when retailers need it, which requires 24/7 availability.

  Other areas that should be considered include activity reporting, which is the tracking of who is using the website and how often. Additionally, logs need to be reviewed to ensure that no unauthorized or improper events are occurring. And as with any public website, the threats of attack, tagging, hacking, etc. are present and need to be monitored.

With the basics of the web hosting in place, the next series of steps are detailed in Section 3.2.3.2.2.

3.2.3.2.2 Lotteries with No Retailer-Focused Web Presence

Establishing a retailer-focused website is an effort of coordinating the sections listed above for a specific lottery or vendor solution. Specifically, the effort involves coordinating the following:

- Content
- Technology
- Maintenance

The required content is outlined in Section 3.2.3.1.3. In practical terms, there are many resources available now to assist in implementing the Technical Standard. These include an Implementation Guide, coordinated NSI/PCATS pilot programs, and a growing body of experience of lottery and vendor implementations. When establishing a retailer-focused website, rely on these resources. The intent and purpose of this Best Practice and the Technical Standard are to provide a consistent facing of lottery-to-retailer accounting information. This is best achieved by leveraging the work already in existence.

The technology involved is covered in detail in Section 3.2.3.1.2. Section 3.2.3.2.1 detailed consideration on how to coordinate hosts within the overall lottery web presence. The retailer-focused website defined in this Best Practice has a straightforward list of requirements. The Checklist in Appendix A of the Best Practice provides a straightforward list of necessary requirements for the website. Use this as core set of requirements for an RFP if you are purchasing the technology or a specification listing for in-house/contractor-focused development efforts.

Maintenance was mentioned above, and is often the most overlooked portion of a website. Consider early on how the data will be updated, what regular maintenance activities need to occur, and which resources will be used.

There are many possible ways to implement a retailer-focused website. This guide is designed to provide the general steps needed to comply, but leaves room for multiple types of implementations. However, a specific focused example is often useful in a planning process. Rather than cover a specific implementation, the body of this guide has remained general. Appendix A is utilized to detail a specific implementation that complies with the Best Practice and details the underlying decisions that drove the design. This is intended as an example only, and not a specific checklist for implementation.

3.2.3.2.3 Lotteries with an Existing Retailer-Focused Website

In this case, the work is focused on evaluating what the lottery provides against the requirements of the Best Practice and then closing any gaps. This area is covered in earlier parts of this document, specifically Section 3.2.2. However, Section 3.2.4 also provides information to not only identify and close gaps but also ensure through validation that the lottery retailer website complies.

3.2.4 Validation Ready Steps

In becoming validation-ready, it is helpful for the practitioner to have an understanding of what is required during the certification or verification process as it will help to prepare more effectively for validation. For the Core Retailer Web-Based Applications Best Practice, the current validation procedures call for verification that the underlying technology complies with the Best Practice, completion of a questionnaire about data availability and retention, and compliance with the NSI Technical Standard for XML Retail Accounting Reports in the Lottery Industry.

This Validation-Ready period is, in a sense, preparation for these future assessments, and during that period, practitioners should be attempting to determine whether they have met the Best Practice requirements and whether they are ready to apply for the formal validation process.

The first step is to finalize the verification process for XML Retail Accounting Reports or utilize a system that has been certified by the lottery’s vendor.

The next step is to test the lottery's implementation with the requirements of the Best Practice Checklist and ensure that all required aspects are met. This step can be accomplished by purchasing an application from a vendor that has been certified as compliant with NSI Core Retailer Web-Based Applications.

Finally, apply for verification and run the verification software with the lottery's website to ensure that all infrastructure requirements are met. Then complete the questionnaire to cover the retention and frequency requirements and submit the results to be verified.

3.3 Corrigenda, Interpretations, & Frequently Asked Questions

Often, during implementation, practitioners will have questions that others have asked before them and for which there is already a response in the Frequently Asked Questions (FAQ) document, which can be found at www.opengroup.org/naspl/conformance/docs/faq.html.

If the questions and answers are not in the FAQ, the practitioner should submit their questions as follows:

- For questions about the Best Practice or Technical Standard:
  nsi-specifications@opengroup.org

- For questions about the certification or verification process:
  naspl-cv-auth@opengroup.org

In addition to the FAQ, it is worth noting that once an NSI Best Practice or Technical Standard has been published, changes may be needed from time-to-time. Change requests may occur when, for example:

- The relevant Working Group raises issues about the Best Practice or Technical Standard.
- An ambiguity or inconsistency is discovered when implementing the Best Practice or Technical Standard.
- The certification process results in approved interpretations against the Best Practice or Technical Standard.
- Changes in technology or operations at the lottery, vendor, or retail sites affect the Best Practice or Technical Standard as it was originally defined.

There is a documented process called the Corrigenda Process for dealing with change requests and updates to the Best Practices and Technical Standards. That process can be found at www.opengroup.org/naspl/published.

It is important that practitioners are aware that this process exists so they can check for any existing updates or interpretations they should know about while implementing the Best Practice or Technical Standard, and conversely if they have any questions during implementation, they know there is a process in place for resolution.

4 Certification/Verification Process

Once your organization has started implementing the Best Practice, your IT Manager should familiarize him/herself with the certification/verification processes, though of course you will not be able to register for certification/verification until you have completed the implementation and have determined that you are validation-ready.

The first step in the certification/verification process is for the IT Manager to visit the NSI Certification/Verification website at www.opengroup.org/naspl/conformance/cert. All of the NSI Best Practices, Technical Standards, and Certification/Verification Documents are available online and accessible from this website, including: Certification/Verification Policies, Conformance Requirements, Conformance Statement Questionnaires, Certification and Trademark License Agreements, Fee Schedule, Frequently Asked Questions, and User Guides.

The next step in the certification/verification process is to read the Guide to NSI Certification/Verification and the Supplement that applies to the Best Practice you will be certifying against. These documents should be read thoroughly prior to attempting to certify a best practice or technology as they describe the program and the process in its entirety.

The following documents should be read and understood prior to certification/verification, since you will be required to agree to them during that process:

- The **NSI Certification/Verification Policy and Supplements** define the policies that govern the operation of the NSI Certification/Verification program. These policies define what can be certified, what it means to be certified, and the process for achieving and maintaining certification/verification.

- The **NSI Certification/Verification Agreement** covers the terms and conditions of the certification/verification service.

For more details on the certification/verification process, please refer to the Certification Guide, available at www.opengroup.org/naspl/conformance/cert.

If you have additional questions, please contact the NSI Certification Authority at naspl-cv-auth@opengroup.org.

5 Contact Information

For further general information on the implementation process, please contact either of the following:

- Andy White (awhite@nasplhq.org)
- Norm Day (n.day@opengroup.org)

For questions about specific requirements of the Best Practice or the certification/verification process, please contact:

- naspl-cv-auth@opengroup.org

A Sample Lottery Implementation

A.1 Introduction

This appendix is included to provide a real-world example of how a lottery may comply with the Best Practice. This is by no means the only approach and should be used as a reference model only.

A.2 Assumptions

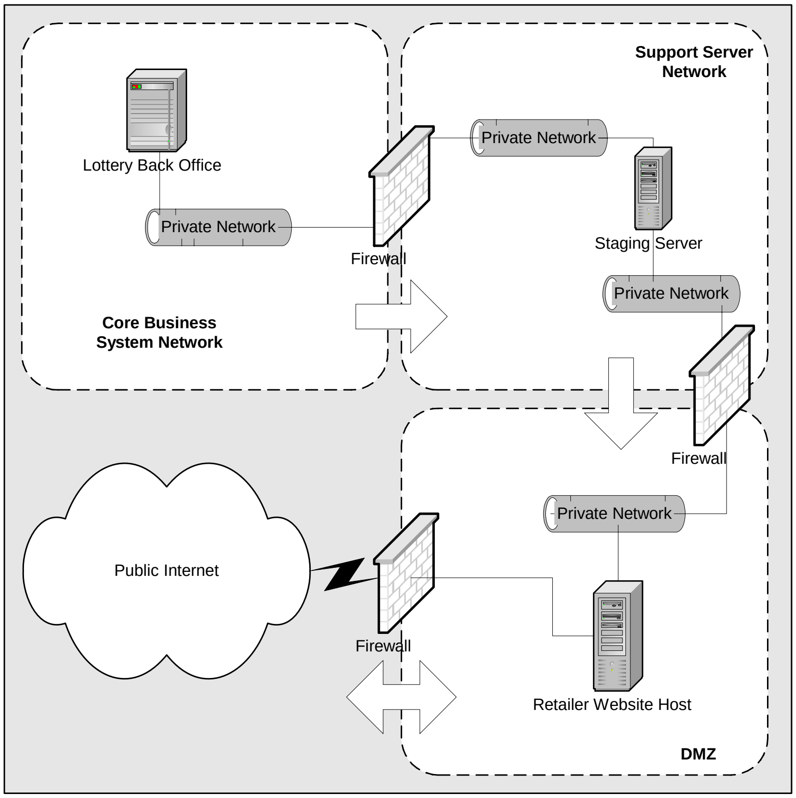
For purposes of this example, this appendix will examine Sample Lottery. Sample Lottery already has a web presence in both the governmental compliance type of website and a marketing website focused primarily at players. This appendix will focus on the implementation of the retailer-focused website for financial reporting compliant with the Best Practice. Further information about Sample Lottery is summarized in the table below.

Number of Retailers	3500
Business Day	Midnight to 11:59pm each weekday.
Invoice Cycle	Weekly from Monday through Sunday.
Invoice Date	Invoices are available Monday morning before 10:00am for the previous week.
Sweep Date	Sweeps occur on Wednesday of each week.
Online Gaming System	Vendor provided by Vendor A.
Scratch Support System	Vendor provided by Vendor B. Retailer access to the system via the terminal is currently handled by a pass-through approach where Vendor A passes all scratch-related transaction from the online system to the scratch system.
Accounting System	Vendor provided by Vendor C.

A.3 Basic Site Design

Overview

The diagram below shows a logical layout of the systems involved in the website.



This is a logical representation for purposes of explaining the infrastructure involved in the website. In actual implementation, Sample Lottery has chosen a rack-based blade server that handles the entire Support Server portion of this diagram. This blade server consists of several servers, each a single blade or card within the rack mount base. The private networks within the Support Server environment are provided by Virtual Private Networks established from within the blade rack and to all connecting hosts. Firewall services are also coordinated via a centralized management system managed by Sample Lottery staff.

The DMZ is actually a hosted service provided to Sample Lottery. This service provides a standardized firewall interface for web access to a Sample Lottery Dedicated Server. The server in this example is running a hardened version of Linux with an Apache web server. The hosting service maintains the web-faced firewall and provides all web-based bandwidth. The server is monitored by the hosting service for basic operational conditions and availability. Sample Lottery manages the actual server, including content.

There are three directional arrows in the diagram, each representing the basic policy for the firewall. Communications from the Core Business Systems are one-way, from the Business

Systems to the Support Server. This effectively isolates the Business Systems from any access outside of Sample Lottery. The Support Server also has a one-way communication channel out to the Website Host via a secured network. This isolates both the Support Server and all other access beyond the Support Server. Two-way accesses can occur between the Internet and the Website Host. This is necessary for normal web operations.

The sections below will utilize this diagram to explain and detail the function within each area.

DNS

Domain Name Service (DNS) is the means by which physical servers are found on the Internet based on domain names. Sample Lottery uses the following domain names for the various servers.

www.SampleState.gov/Lottery	The state-compliant, governmental-focused website.
www.SampleLottery.gov	The same state-compliant, governmental-focused website as above.
www.SampleLottery.com	The marketing-focused player-based website.
retailer.SampleLottery.com	The retailer-focused website.

Sample Lottery worked with the state DNS administrator to link the first domain name required by the state to the lottery-compliant governmental website. The DNS for the lottery-specific domain names are maintained by a hosting company. Sample Lottery has opted for an automatic renewal cycle on the lottery-specific domain names and has also reserved additional name extensions – such as .net, .info, etc. – to protect the naming brand. The hosting company also provides automatic forwarding of all of these additional domains back to the marketing-focused website.

Sample Lottery personnel utilize the hosting company's administrator's page that allows the DNS entries to be updated. In this way, the host IP addresses provided by the hosting company can be related to the proper domains. The use of an administrative page is very common for hosting services. Had Sample Lottery decided to maintain their own DNS server, the method for updates could be found easily via a web search. Keywords include DNS, setup, and operating system (i.e., Linux, Windows, etc.).

Sample Lottery decided to purchase a domain hosting service to leverage the service and avoid the cost and overhead of a lottery-specific DNS. The hosting service provides fast DNS updates across all major web DNS services and full redundancy to keep the service available.

Core Business Systems

Sample Lottery has several business systems that are integral to the retailer-focused website. In short, there are three business systems that deal with pieces of the retailer financial records. These are:

- Gaming System
- Scratch System

- Accounting System

During the work on the implementation of the XML Retail Accounting Reports, Sample Lottery decided to utilize a specialized system to gather and format the financial information needed to generate the XML files compliant with the Technical Standard. This process involved getting the raw data from each source and formatting that data into the XML files. On a daily basis, sales information is produced by the Gaming System and transferred to the XML support system. At the end of each business day, a snapshot file is produced by the Scratch System and transferred to the XML support system. At the end of each invoice cycle, the Accounting System transfers all adjustments, charges, commissions, and invoice summary data to the XML support system.

The XML support system then generates the XML file for each lottery. These files are generated every day recapping daily activity for the previous business day, and each Monday the invoice information for the previous week is included in the file. An XML file is produced for each retailer and then the automated process transfers each file to the retailer web-based application Support Server detailed below.

Support Server

Sample Lottery has two Support Servers for the retailer web-based application. These are:

- Retailer Web Application Database Support Server
- Retailer Web Application Support Server

The purpose of this design is to provide a secure, direct support system for the Retailer Accessible Web Server (see below). Everything on the Retailer Accessible Web Server will originate from these two servers. This provides a robust backup to the live website and includes a process to re-populate a base server should the need arise.

The Retailer Web Application Database Support Server provides a database that contains the XML files for retailers as required by the Best Practice. This server receives each file from the XML support server and files that XML file as an attribute along with key metadata about the file. Attributes for the database include the following:

1. Date of the file – The date the file was produced.
2. Retailer ID – The Sample Lottery unique identifier for the retailer.
3. Invoice Indicator – A simple Boolean filed true if this is an Invoice file.
4. XML String – The contents of the XML file stored as a string.

This Database Support Server utilizes a production quality database, consistent with other business systems within the lottery. The key factor in choosing the database was the common use of the database product in other Sample Lottery business systems. This server acts as the original source of XML financial data for the retailer-focused website. There is a regular back-up cycle, and design includes use of a RAID array (Redundant Array of Independent Disks) for disk storage and redundant server blades, power supply, and networks to ensure no single point of failure.

The Database Support Server has an automated process that updates the Retailer Accessible Web Server with new database entries. Specifically, this process selects all entries for a given day and generates transactions that place all of these entries onto the Retailer Accessible Web Server.

The Retailer Web Application Support Server is the source of all production code that resides on the Retailer Accessible Web Server. This includes the style sheets used for presentation, the supporting code for retrieval of database contents, and the actual web pages on the website. Sample Lottery has opted for a combination of web support for the retailer-focused website consistent with the practices on the other Sample Lottery sites. The look-and-feel is handled by the marketing group within Sample Lottery and a contract has been established with a specialized web design group to translate the marketing design to the look-and-feel aspects of the web page. This same firm has assisted with navigation and a basic search feature and website map.

There is additional content provided for the website by the internal retailer group, such as basic contact information, some procedural information, and regular updates on retailer-focused events. Sample Lottery expects more of this as time goes by and has established this support server to organize all updates to the website.

The role of the Retailer Web Application Support Server is to stage all updates to the website and then, via an automated process, update the live website. In this case, the various contributors to the website have a specific methodology to follow when adding content. The methodology includes steps that require the content provider to log in, and then place the content with additional metadata about when the content should be on the live website and for how long. The server then uses a process that will push the content to the live website as specified within the metadata.

DMZ or Secure Area with Limited Web Access

DMZ is a borrowed term in computing. The original term references a Demilitarized Zone which references a buffer zone to separate two opposing parties engaged in a military action. The idea also applies to the edge zone between an organization, such as the Sample Lottery, and the wide open Internet. This is usually formed via a firewall setting that limits access back into the organization while allowing controlled access to the Internet.

The existence of individuals and organizations that attempt to tag, break, or otherwise subvert legitimate websites is a simple fact of life in the Internet world. The concept of a DMZ is to limit the access for negative purposes while still providing the access required for the intended use of the website.

In the diagram, the DMZ is linked to the Support Server environment through a firewall. As previously stated, the firewall policy is basically a push out of the Support Server area and into the DMZ. In practice, Sample Lottery has established a firewall policy that only allows access to a specific IP address, which corresponds to the physical address of the Dedicated Server provided by the hosting company. This connect is web-based, limited to the ports utilized by SSL encryption; i.e., port 443. The SSL certificate is self-generated by the Sample Lottery since the only users of this IP address/port are the Sample Lottery Support Servers and administrative staff. File administration is handled via an SFTP (Secure File Transfer Protocol) connection that is also allowed from the Support Server environment to the Dedicated Server via port 22. The

SFTP is also limited by specific IP addressing with complimentary limits on the Dedicated Server.

Access to the Dedicated Server from a public point of view is also limited by a firewall. This firewall allows access via a domain name (retailer.SampleLottery.com) on either the general HTTP port 80 or on the SSL port 443. The port 80 access is redirected to the secure port. This limits the types of access to the server, and also removes most of the areas of potential threat. Since this is a static and simple firewall policy, Sample Lottery has opted to have this service provided by the hosting company. A complimentary policy for access is also enforced at the server level (see below).

Sample Lottery utilizes a registered SSL certificate for the public access. This was obtained at the same time as the domain name registration was purchased as part of the package provided by the Domain Name Registration service provider. Sample Lottery opted for a combined package so that renewals would be automatic, just like the domain service. By utilizing this approach, Sample Lottery met the requirements of the Best Practice for SSL encryption.

Retailer Accessible Web Server

The specification process for obtaining the Retailer Accessible Web Server is detailed in Section A.4. The design considerations, purpose, and use of this server are covered here.

Sample Lottery decided in the early design phase to keep the actual web server for the retailer website as generic and simple as possible. The purpose of this server is limited to providing web access to retailers to obtain their financial reports. By focusing the website on this single purpose, many potential security, capacity, and access issues were avoided. Sample Lottery also based design on the concept of limited access. Access is granted only for the focused purpose and nothing more.

This design does have some limitations. Primarily, the design makes updating and maintenance slightly more complicated. Support personnel must follow strict access guidelines and utilize the Support Server model for transfer of data to the website. This means that support staff need to learn this environment and cannot use some of the common and simple tools available to manage websites. This is a necessary trade-off to keep the website secure and focused.

In practice, the server has a total of two exposed services. The first is normal web access for retailers on ports 80 and 443. This compliments the firewall policy discussed above. The other service is IP address and port-specific for access from the Support Server area of Sample Lottery. This access adds the additional service of SFTP from the specific Sample Lottery address related to the Support Server.

Directory

Sample Lottery reviewed several options to control access to the retailer website. These options boiled down to three basic types, as follows:

- Operating System Controls
- Database of Roles and Users

- Directory Technology

The operating system was attractive at first glance; however, the means to maintain this level of user access would require that Sample Lottery system administrators would need to add and maintain the user list or the administration of the operating system would have to be distributed to so many users that the base operating system security would be compromised.

The next reviewed approach was to create a data structure in a database that would hold roles and users. Adding users for a particular retailer could be handled via a simple input screen that would be accessible to a specific retailer role. This approach was viable; however, it was discounted due to the need to code and build specific administration roles and screens that were unique to this application. Sample Lottery also felt that it may limit future plans that would require further user and role granularity.

The final decision was to utilize directory technology. There are several directory systems available in the market today. They feature rich administrative tools and the ability to interoperate at certain levels. Sample Lottery utilizes a directory for internal security as well, but it was decided to separate the retailer directory from the employee directory simply because they were focused at different purposes. To keep design simple, the retailer directory was created on the actual web server. The directory is periodically backed up via an automated process. To keep things portable and interoperable in the future, Sample Lottery followed the recommended approach of the Best Practice and utilized the Lightweight Directory Access Protocol (LDAP).

The actual roles developed in the Sample Lottery design are also simple and to the point of what is being implemented today. There are four retailer roles, as follows:

- Retailer Administrator

  The retailer administrator role is limited to one function only – maintenance of the retailer user base. This role allows the designated retailer administrator to add, change, and delete users that are authorized to access the retailer's financial reports. This role was initially populated by obtaining the user ID and passwords from the lottery system and populating this role for all retailers. This allowed the first adopters to access this account with a user ID and password they already knew and kept lottery staff involvement to a minimum. After that initial launch, a help screen was added to allow lottery retail support staff to add an authorized email address to the retailer's directory. Sample Lottery's retail support staff have the means to verify that they are speaking with an authorized retailer representative and can enter the retailer's valid email to start an automated sign-up process. The process allows the retailer to establish the administrator account via the provided email account.

- Invoice Access

  Invoice access is as simple as the name. A user that has invoice access can view and download the files pertaining to invoices. In a chain, this includes access to all invoices for all locations or the combined invoice.

- Balancing Access

  Balancing access allows access to the daily activity and scratch inventory levels for the retailer. Again, chains can access all balancing activity for all locations.

- Location-specific Access

  Location-specific access is a specialized access that allows a manager at a specific location to access the daily activity and scratch inventory levels for the specific retailer location.

A.4 Hosted Server Design Specifications

The purpose of this section is to provide the specifics on calculations, approaches, and requirements derived for the actual Retailer Accessible Web Server.

SSL Encryption

The main requirement for SLL encryption pertaining to the host is the ability of the hosting company to allow a domain name reference that is outside of the hosting company's control. In other words, Sample Lottery specified that the hosting company must provide a set IP address for the hosted server. Sample Lottery used this address as the resolution point for the retailer.samplelottery.com address. The SSL certificate was requested utilizing this specific domain name. The resulting Security Certificate was then installed on the hosted server.

Database/Storage Requirements

Sample Lottery opted to meet the Brest Practice required retention timeframes. The calculations used to develop the requirements for specifying storage are outlined below.

Report	Retailers	Frequency	Retention	Count	Average File Size	Required Space
Invoice File (including daily activity)	3500	Weekly	16 months	70	1mb	245gb
Daily Activity no Invoice	3500	Daily	13 weeks	91	0.5mb	160gb
Total Size						~450gb

Bandwidth Requirements

Bandwidth is also a mathematical factor consisting of the number of accesses and the average file size accessed. This calculation is based on an average month.

((3500 Retailers * 30 days * .5mb) + (3500 Retailers * 4 days * 1bb)) / 1000 = 66gb/month

HTML vs. XHTML vs. XSL

From a server specification standpoint, there are no specific requirements about how pages are served. This is a function of the browser that accesses the website. Sample Lottery utilizes XHTML (Extensible HyperText Markup Language) for all static pages and uses an XML format for dynamic pages that are formatted via XSL (Extensible Stylesheet Language). The XSL simply converts the XML into reference elements that are then formatted using style sheets that conform to the Cascading Style Sheet (CSS) standard. For samples of how XSL can display XML and a free tutorial, refer to www.w3schools.com/xml/xml_xsl.asp.

A.5 Operations

Sample Lottery began most of the operational task as manual processes to identify the rough areas in operations. Starting with manual processing allowed Sample Lottery to refine and perfect the process so that it could be automated. For purposes of illustration, some of the processes that are actually related to the XML processing are included. These XML processes are the trigger point for the retailer web-based application processes.

Typical Daily Activity

Each day, an operational run on the gaming system produces the summary of activity file which is automatically transferred to the XML Support Server. Part of the XML Support Server process transfers each completed XML file to the Retailer Web Support Server. As each file is received, the Retailer Accessible Web Server stores the file within its internal database and then transfers the file to the database on the actual retailer website via an automated process. Thus updates are all automated.

One additional process that runs on a daily basis is handling new retailers. When a new retailer has activity passed to the Support Server, a complimentary support entry is placed into the database. This also triggers the addition of the retailer into the directory located on the Retailer Accessible Web Server. This entry will be updated with a valid email address by Sample Lottery retailer support staff to initiate the new administrative account as detailed above.

Sample Lottery administrative staff review the log files from the Support Server and the Retailer Accessible Web Server on a daily basis. This review utilizes a log tool that classifies the log entries into “normal” and “exceptions”. Exceptions are closely reviewed and any necessary actions taken.

Invoice Day Activity

This follows the same processes as the daily activity. There is simply additional data that is combined into the XML by the XML Support Server. From the Retailer Accessible Web Server’s point of view, the file is simply larger than on other days and the additional metadata flag for an invoice is set to true.

Scheduled Maintenance

Maintenance is largely two-fold. First is the process that removes data based on the retention schedule. Second is updating any pages that have changed. The first process was implemented based on a retention timeframe. Sample Lottery utilizes a day count for each type of retention. In the case of daily files, the retention time is 13 weeks * 7 days per week or 91 days. Any file that is flagged false on the invoice metadata and older than 91 days is simply deleted. For invoices, the retention period is 16 months. Sample Lottery calculated the days as follows: 365days + (4 months * 31 days) to get 489 days. Any file flagged true on the invoice attribute older than 489 days is also deleted.

File updates are handled as they occur. The maintenance process stores the new file and then uses a metadata date to install on the Retailer Accessible Web Server. Both processes occur on a daily basis.

A.6 Future Considerations

Automated Access

Sample Lottery opted not to launch with a means for machine-to-machine access. However, this eventuality was considered in the design. Sample Lottery plans to utilize the XML-RPC approach for automated access. In short, the plan has three process requirements.

First is to allow an automated authentication. This will require a new role focused at automated access and will allow access to both invoice and daily activity.

The second process step requires the requesting system to provide the last file date that it received.

The final step is for the Retailer Accessible Web Server to retrieve the most recent activity report after the provided date and present it as an XML file stream. If no file is found, a graceful message is sent informing the requesting system that no further updates are available.

Two-Way Communication

Two-way communications will require some additional design considerations. The initial design provides a path out of Sample Lottery and to the retailer that ensures the business systems of the lottery are protected. This part of the design will stay the same. When Sample Lottery adds the capability for data to be submitted back from the retailer, an additional communication line will be established. This will come in the form of another Support Server to handle incoming data. The retailer website will have controlled access to this Support Server, through a firewall. Incoming data will take the form of an XML file that will contain predefined text. The additional design considerations are beyond the scope of this example. This section is included to simply validate the design, and describe the initial steps for expansion into two-way communications.