

Nintendo Wi-Fi Connection

Independent Game Server Usage Manual

Version 1.4

**The content of this document is highly confidential
and should be handled accordingly.**

Confidential

These coded instructions, statements, and computer programs contain proprietary information of Nintendo and/or its licensed developers and are protected by national and international copyright laws. They may not be disclosed to third parties or copied or duplicated in any form, in whole or in part, without the prior written consent of Nintendo.

Table of Contents

1	About This Document	5
1.1	Contents.....	5
2	How to Use an Independent Server.....	6
2.1	Authentication Process with the Nintendo Authentication Server.....	6
2.2	NAT Negotiations	6
2.3	Using Both the GameSpy Server and an Independent Server	6
2.4	Using an Independent Server Without Using the GameSpy Server.....	8
2.5	Security of Communications with an Independent Server.....	8
2.6	Authentication Token Specifications	8
2.7	SSL Server Certificate.....	9
2.8	Application to Use the Independent Server	9
2.9	Note Regarding Lotcheck	10
2.10	Contact Information when Service Goes Down	10
2.11	End of Service.....	10

Figures

Figure 2-1	Connecting to the GameSpy Server and an Independent Server.....	7
Figure 2-2	Connecting to an Independent Server Without Connecting to the GameSpy Server	8

Revision History

Version	Revision Date	Description
1.4	2011/07/15	Deleted the section 2.6 Confirming the Service Operating Status because it is no longer required to implement a webpage and submit the URL to report the service operating status. Deleted "URL and method of checking server operating status" and "When to use the server and frequency of use" from the list in section 2.8 Application to Use the Independent Server.
1.3	2010/08/16	Corrected entry in Table 2-3.
	2009/02/19	Deleted description in section 2.3 Using Both the GameSpy Server and an Independent Server that the Wi-Fi connection is valid until disconnected. Added a statement that the authentication token must not be saved to Save Data or other locations.
1.2	2008/10/01	Added support for WMS.
1.1	2008/03/31	Added support for Wii console. Added text about security of communications with independent servers. Detailed specifications for authentication token. Added explanation of SSL server certificate.
1.0	2006/09/11	Initial version.

1 About This Document

1.1 Contents

This document provides guidelines, precautions, and other essential information on how to use your own game server (independent of that operated by Nintendo and GameSpy) to run game software that supports Nintendo Wi-Fi Connection.

2 How to Use an Independent Server

2.1 Authentication Process with the Nintendo Authentication Server

Any game software that supports Nintendo Wi-Fi Connection must first go through the authentication process with the Nintendo Authentication Server, even when using an independent server. If you use the DWC library supplied by Nintendo, the entire process from connecting to the access point to authenticating can be performed seamlessly.

There are two ways to perform this authentication process when using an independent server.

You can perform a single set of steps to:

- Authenticate with the Nintendo Authentication Server to connect to the GameSpy server.

OR

- Authenticate with the Nintendo Authentication Server, but not connect to the GameSpy server.

If you plan to connect to the GameSpy server, use the **DWC library** to develop your game. If you do not plan to connect to the GameSpy server, use the **DWC-DL library**.

2.2 NAT Negotiations

To better support users, games that use P2P (person-to-person) communications must use the DWC library for matchmaking. If you were to use your own NAT negotiations for matchmaking (for example, if you were to use UPnP), your game would not be consistent with other games that support Nintendo Wi-Fi Connection and users might become confused.

Nintendo has verified the compatibility of the GameSpy NAT negotiation features with many wireless LAN access points, and the Nintendo Wi-Fi Connection home page provides a list of confirmed operation types.

2.3 Using Both the GameSpy Server and an Independent Server

In a single set of tasks, you can use the DWC library to connect to an access point, authenticate with the Nintendo Authentication Server, and connect to the GameSpy server. After that, you can use the DWC library to use the Nintendo server and the GameSpy server features.

Before connecting to an independent server, use the service locator feature of the DWC library to receive an authentication token for the server. Once received, this authentication token remains valid for 24 hours. If the service locator feature is used once at the start of gameplay to receive an authentication token, the token remains usable until the valid period expires. Storing the authentication token in save data or other locations is prohibited. For details about the service locator feature, see the *DWC Function Reference*. For more information, see section 2.6 Authentication Token Specifications.

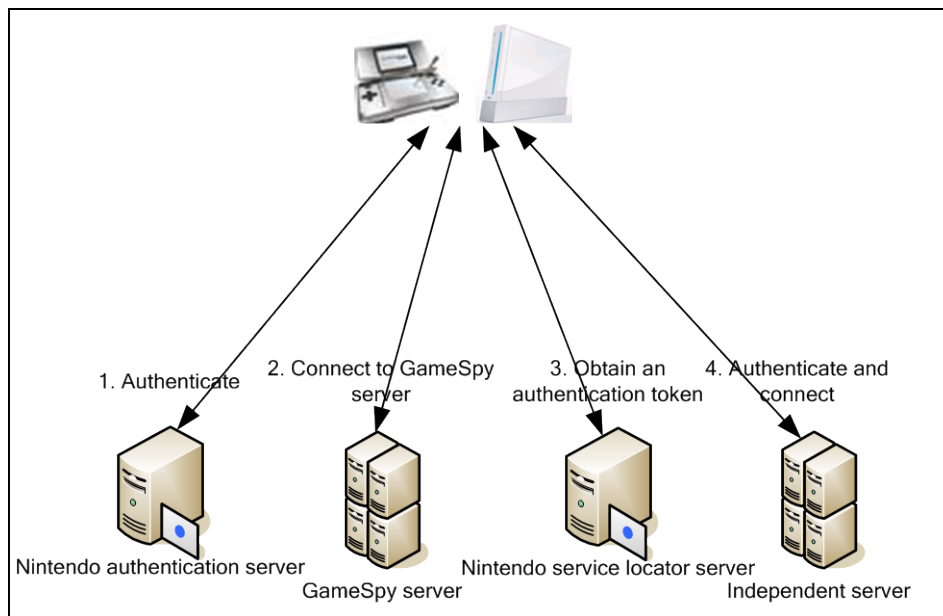
When you receive the authentication token, send it to the independent server and then verify on the server side that the value is correct. There is no set method for sending the authentication token, but you should encrypt the communications route to prevent packets from being intercepted and the tokens from being used in unauthorized ways.

Nintendo provides a sample of the program that the independent server must use to verify the authentication token packaged with the DWC(_DL) library. This authentication token incorporates the Wi-Fi Connection ID, Wii number, and the Wii console's MAC address and time of creation; the server program allows the independent server to get these values. The server also uses values to identify Nintendo DS systems and Wii consoles.

If an application connects to the same independent server multiple times, the authentication token only needs to be verified the first time; on subsequent connections, you can use your own methods for authentication and session management. However, if there is no problem with performance, you can choose to verify the authentication token every time. The specification is the same even when connected to multiple servers, but you must verify the authentication token with the first server with which the connection is made.

Verifying the authentication token confirms that the connection is coming from a device that has gone through the authentication process with the Nintendo server. There are no restrictions regarding authentication between servers, so it is technically possible to connect to an independent server without using this authentication token. However, always use the authentication token to protect the security of the server itself.

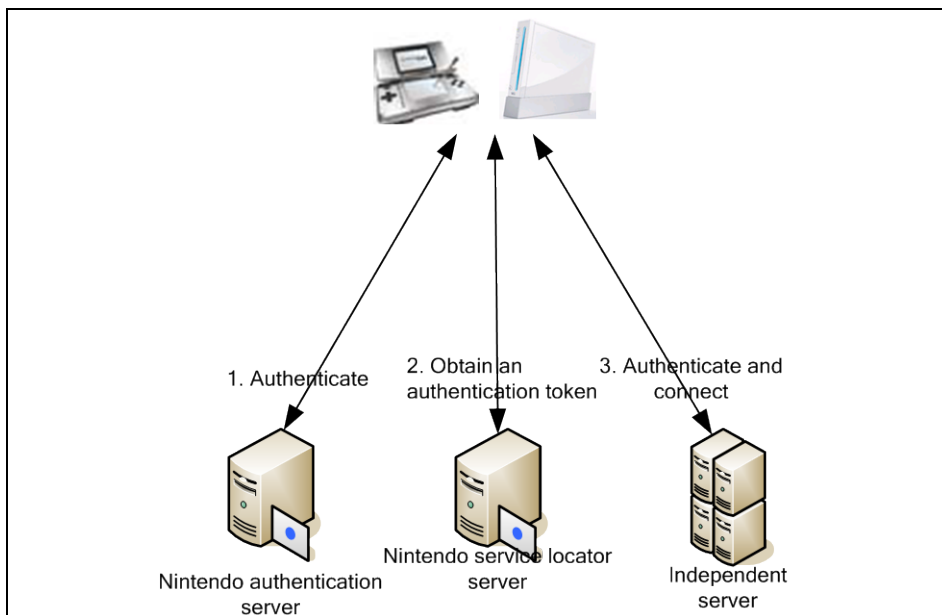
Figure 2-1 Connecting to the GameSpy Server and an Independent Server



2.4 Using an Independent Server Without Using the GameSpy Server

In a single set of tasks, you can use the DWC-DL library to connect to an access point and authenticate with the Nintendo Authentication Server. Similar to the process described in the previous section, you then use the service locator feature of the DWC-DL library to receive an authentication token for your server. After that, the details for connecting to and using the server are the same as those described in section 2.3 Using Both the GameSpy Server and an Independent Server.

Figure 2-2 Connecting to an Independent Server Without Connecting to the GameSpy Server



2.5 Security of Communications with an Independent Server

By using the method described above for the authentication token, you can deny connections from devices other than Nintendo DS systems and Wii consoles that have gone through the Nintendo authentication server, and thus ensure a certain level of security for your independent server.

To ensure security for Nintendo DS systems and Wii consoles, you should also take steps to prevent alteration of data packets and communications with bogus servers spoofing as your server. To do so, you can either add a digital signature (RSA signature, HMAC value, or other similar method) to the data transmitted from your server and verify the integrity of data received by your server, or use the HTTPS protocol for communications with your server to verify the server certificate at the start of communications.

2.6 Authentication Token Specifications

The authentication token is an encrypted value of different items, such as the ones listed below. A different encryption key is used for each game.

- The first 13 digits of the Wi-Fi Connection ID (only for Nintendo DS system)
- The Wii number (only for Wii console)
- The MAC address (in the case of the Wii console, the MAC address for the wireless LAN interface)
- The token creation date and time
- A hash value

Your independent server decrypts the authentication token and checks its validity. The decrypted character string is checked to confirm that the format and hash value are correct, and the token is not more than 24 hours old. For more details about how to decrypt, perform error checking, and extract the various values, refer to the sample program for checking authentication tokens packaged with the DWC(_DL) library. To perform the error check correctly, you should periodically adjust your server's system clock using a method such as NTP.

You will be informed of the decryption key (tokens for service locator development and for products) on the WMS once your application to use the independent server is approved.

2.7 SSL Server Certificate

If you will be using the SSL protocol for communications with your independent server, Nintendo's own certificate authority can issue the SSL server certificate for that server. If you want Nintendo to issue an SSL server certificate, apply using the WMS and provide Nintendo with the CSR file.

Nintendo-issued SSL server certificates provide the following features.

- The validity period of the server certificate is set to the maximum, so you do not need to worry about periodic updates.
- There is no fee charged for issuing the certificate.
- If you are using HTTPS for WiiConnect24 download tasks, you will need to use a certificate issued by Nintendo. (This is not necessary for HTTP. For details, see the *WiiConnect24 Programming Manual*.)
- Nintendo's certificate authority is not included in browsers such as Opera, Internet Explorer, and Firefox, so the SSL server certificate cannot be used by servers to which PCs also connect.

For communications other than WiiConnect24 download tasks, for your SSL server certificate you can use one of the commercial certificate authorities, such as VERISIGN®, CyberTrust, or RSA. You can also use your own certificate authority. If you are using your own certificate authority, be very careful administrating it.

2.8 Application to Use the Independent Server

Complete and submit the independent server application, which includes the items listed below. The information provided is used for technical verification, Lotcheck, and user support purposes. Be sure to apply using the WMS.

- Purpose of use
- Server host name or IP address
- Protocol to be used (port number)
- Encoding of transfer data/Use of signature
- Average size/maximum size of transfer data
- Certificate authority for SSL server certificate
- Uses for server other than Wi-Fi Connection
- Time of periodic server maintenance
- Game behavior when server is down
- Contact information when server goes down

2.9 Note Regarding Lotcheck

For Lotcheck, Nintendo uses an actual, operating server. Before submitting the master for your product, prepare the server environment and refrain from any server maintenance during the Lotcheck period. If for some reason an actual operating server is not available, inform Nintendo when submitting the master.

2.10 Contact Information when Service Goes Down

Contact Nintendo when you intend to halt service for some set time, or if the service stops unexpectedly. You can confirm contact information using the WMS.

2.11 End of Service

If you end a service that was being provided via your independent game server, be sure to inform Nintendo at support@noa.com. Nintendo will update the registration information in the Authentication Server and, in the first authentication process, issue a message stating that the service has ended.

All company and product names in this document are the trademarks or registered trademarks of their respective companies.

© 2006-2011 Nintendo

The contents of this document cannot be duplicated, copied, reprinted, transferred, distributed, or loaned in whole or in part without the prior approval of Nintendo.