

APPLICATION AND CONTENT CERTIFICATION (ACC) GUIDE

This certification guide describes the process and criteria that will be used for the certification of applications and content submitted by current or prospective Nextel International partners.

Last revised: November 2008

Introduction	4
Submission Certification Process	5
<i>Becoming a candidate for certification</i>	5
<i>Executing a Non-Disclosure Agreement</i>	5
<i>Submission of materials required for ACC testing</i>	5
For all submissions	5
For applications	5
For digital media assets (e.g. ringtones, wallpapers, themes, etc.)	6
For OEM devices (e.g. black boxes, AVL equipment or other solutions with iDEN technology integration)	6
<i>Verification and validation of submission package</i>	7
<i>Issues raised during testing and waiver processes</i>	8
<i>Post-certification launch or partnership activities.</i>	8
For business or enterprise solutions:	9
For digital media offerings:	9
Application and Content Certification Criteria	11
<i>Documentation and printed materials</i>	11
<i>Applications</i>	12
<i>Non-application Digital Media</i>	19
<i>Non-application OEM devices or other specialized hardware</i>	20
Appendices	21
<i>Self-testing Checklist</i>	21
<i>Demo Accounts and Web-based Application Data</i>	34
<i>Handset and Service Compatibility Checklist</i>	35

<i>Technical Support Contact Information</i>	<i>37</i>
<i>Known error messages and resolutions</i>	<i>38</i>
<i>Estimated Data Usage</i>	<i>39</i>
<i>Code Signature Request Form</i>	<i>40</i>
<i>Waiver Request Form</i>	<i>41</i>

Introduction

We are very pleased that you have chosen to work with us. This guide is our effort to communicate the process we will use to certify that your applications and content create a consistent experience for users, that the operation of solutions we commercialize jointly meet certain standards for operation and quality, and generally, to ensure that both NII Holdings, our operations in Latin America, and you deliver the most beneficial experience with the least amount of foreseeable difficulties.

The process for application and content certification (ACC) is the same for all types of content and applications, whether they are business-focused or aimed at consumers, although the criteria used for obtaining ACC approval may vary depending on the type of application or content. To make this process simpler to understand, this guide is organized as follows:

Part 1 describes the ACC process for all types of submissions for certification

Part 2 describes the criteria used to certify each type of submission

The requirements and process described in this guide are meant to be an aide to both you and Nextel so that we can take you from idea to certification as smoothly and efficiently as possible.

The ACC process is not a substitute for your own quality assurance processes.

Certification of your solution is not a requirement for you to commercialize your solution, and this is a voluntary process. However, if you do choose to commercialize your application or content without our certification, you are on your own. Obtaining ACC approval will give you access to all of the benefits that come from having been certified, including visibility of your submissions along with all other certified submissions, possibilities (although not guaranteed) for Nextel billing of your solution, and an ongoing relationship with Nextel that can be important for your long-term success.

I. Submission Certification Process

The process we follow for certification has the following end objectives:

- ensure that the range of applications enabled through Nextel provide a consistent experience and only deviate from our usability and style guidelines when reasonable;
- ensure that submissions comply with technical requirements or constraints that may be applicable to the submission type to ensure that submissions can operate properly and are also good citizens within Nextel networks and devices;
- ensure that foreseeable errors in the use or operation of a submission are known to Nextel to facilitate customer care operations;
- ensure that submissions handle unforeseeable error conditions gracefully;
- ensure that submissions are properly documented for end users and system administrators, if appropriate.

The following steps outline the process for generating a submission for ACC.

1. Review this document

Our certification criteria are detailed completely in this document. Developing your application to ensure that they will meet these criteria is important to make sure you do not experience delays or retesting of your application.

2. Submission of materials required for ACC testing

When you seek certification, we will be verifying a series of items and materials together. Ensuring that you have included *and reviewed* all materials before submitting them will make the process move smoothly, and not doing so will introduce delays to the launch of your application, service or content.

Not submitting all your materials will cause all testing of your application to stop until you submit them. This may result in a test restart fee assessed by the certification lab.

A complete ACC submission consists of the following:

A. For all submissions

- Completed self-testing checklist ([Appendix A](#)).
- Payment to the ACC testing lab *or* written documentation that Nextel has agreed to subsidize the testing in whole or in part.

B. For applications

- End user guide, ready for publication, in PDF format, if applicable.
- Final administrator guide, ready for publication, in PDF format, if applicable.
- Compiled and pre-tested binaries for handset clients

This includes the appropriate combination of JAR and JAD files for MIDlets or JAD, JAR, COD and ALX files for BlackBerry applications, or other relevant compiled binaries, compliant with Nextel requirements for formatting of descriptor files.

- URLs for web-based and WAP-based applications or for any web components of mobile client/server hybrid applications, as well as demo account information for end user and administrator views to be used during testing ([Appendix B](#)). Please be sure to have meaningful sample data in your systems so that certification can be done in a scenario that is close to real operation.
- Handset compatibility chart ([Appendix C](#)).
- Technical support contact information checklist ([Appendix D](#)).
- List of known error codes and conditions ([Appendix E](#)).
- Estimated Nextel packet data usage for one user for one device for a month ([Appendix F](#)).

This should be a realistic estimate of how much packet data traffic an average user is expected to generate in one month, including protocol headers (if using HTTP as a transfer protocol). This information is important to Nextel since it helps us project network capacity.

- Request for MIDlet code signing if a MIDlet for a Motorola iDEN device requires code signing ([Appendix G](#)).

For MIDlets for Motorola iDEN devices, all signature lines generated during development should be removed from JAD files before submission.

C. For digital media assets (e.g. ringtones, wallpapers, themes, etc.)

- Binary audio, video, image or theme packages in formats that will be distributed through Nextel distribution systems.
- Handset compatibility chart ([Appendix C](#)).

D. For OEM devices (e.g. black boxes, AVL equipment or other solutions with iDEN technology integration)

- End user guide, ready for publication, in PDF format.

- Final administrator guide (if applicable), ready for publication, in PDF format.
- Equipment integration guide (if applicable), ready for publication, in PDF format.
- Two samples of the device.
- Desktop or web-based client test harness to verify communication between device and a back end system.
- Technical support contact information checklist ([Appendix D](#)).
- List of known error codes and conditions ([Appendix E](#)).

3. Verification and validation of submission package

Our testing lab will validate the contents of your submission package and run your application or content through the appropriate technical test suite.

After testing, you will receive a report that indicates what the status is for a specific certification test case. The statuses indicated are as follows:

- **Passed:** solution has completed certification successfully
- **Failed:** solution has not completed certification successfully and will need to be resubmitted for certification.
- **Green:** during certification, no issues were identified that have a significant impact on end users or the network.
- **Yellow:** during certification, issues were identified that may have an end-user impact, but that are not significant enough to prevent usage of the submission.
- **Red:** during certification, issues having sever impacts on network features, connectivity, functionality, configuration or end-user experience were identified. The issue is significant enough that the application will not be launched until issues are resolved and the application has been resubmitted for testing.
- **Waived:** issues that were identified during certification were waived upon request of the submitter and with approval of the appropriate Nextel contact.

If your submission receives a **passed** status, it is considered certified. If it receives a **failed** status, then you must revise, retest and resubmit the components that failed for re-certification.

When you send us a submission, you are representing to us that it is your completed work, not a version in progress. Easily verified errors in your submission suggest to us that your own internal quality control is insufficient, puts you and your company in a bad

light, and is a poor use of everybody's time. As a result, *repeated failure of ACC testing can jeopardize your relationship with Nextel.*

4. Issues raised during testing and waiver processes

Our ACC criteria are designed to facilitate compliance with our standards, not to prevent situations that make sense. If, after reviewing the certification results, there are areas that do not meet ACC criteria (that is, they receive Yellow or Red status) but these are either part of the design of your application or they are not something you can fix because it is out of your control, then it may be possible to obtain a waiver. If you feel that you require a waiver, you at this point should submit a waiver request through the ACC portal for the test case you wish to waive. The waiver request will be verified and if the waiver is approved, the waiver will be recorded. If all Yellow or Red status items are waived, your application will be considered certified with waivers. If the waiver is denied, the issue will need to be addressed before the submission can be certified.

5. Post-certification partnership

The ACC process is one part of becoming our partner and is a critical component of completing a partnership. Depending on the nature of your application or service, building a partnership could be as simple as completing ACC and having it loaded on a content catalog, or as complex as defining sales education tools, defining pricing schedules, creating marketing collateral, and creating special customer care processes.

A. Becoming a candidate for partnership

You can become a candidate for partnership in one of three ways:

- be sponsored by NII or Nextel marketing or sales staff in one of our markets in Argentina, Brazil, Chile, Mexico or Peru. In this case, **your contact throughout the process will be the person sponsoring you.**
- be submitted for certification by a Nextel partner approved to be an aggregator or publisher. **In this case, your contact during the certification process will be the partner or aggregator submitting your application.**
- submit a Partner Interest Form through our developer website (<http://programa.nii.com>). Nextel staff will review the Interest Form and, if there is a fit for your offering within our activities, we'll initiate the process to establish a partnership with you. It is important to emphasize that *partnership is separate from certification, but is closely linked--* you can have a certified solution without being a partner, but you cannot complete the partnership process without having certified your submission(s). **In this case, your contact during the certification process will be communicated to you once a person is assigned.**

B. Executing a Non-Disclosure Agreement

Executing a proper non-disclosure and confidentiality agreement with us is important to protect both your intellectual property and confidential information as well as confidential information that NII or Nextel country operations may give you during the process. If you have a current NDA signed with NII Holdings, Inc. or one of our subsidiaries (Nextel Communications Argentina S.A.; Nextel Telecomunicações Ltda.; Nextel Chile S.A.; Nextel de México S. A. de C. V. or Nextel de Perú, S. A.), you have already met this requirement.

C. Launch activities

Your contact will work with you to define a list of the items that will be required for launching the product. These could include, but are not limited to, the following:

A. For digital content offerings:

- Screenshots or splash screens for content catalogs
- Content catalog text snippets
- Demo/teaser versions of games and consumer applications
- Revenue or billing agreements
- Known error and resolution listings
- Copyright and trademark verification

B. For business or enterprise solutions:

- Quick user guides
- Sales training presentations and materials
- Sales demonstration instructions
- Field user, administrator, or integration/installation training material
- Known error and resolution listings
- Sales support collateral
- Lists of professional and integration services offerings and price schedules
- Electronic or print marketing collateral
- Screen and print logos
- Revenue or billing agreements

- Information for Packet Network Operating Centers (PNOCs) on Nextel-specific web services or network APIs used by the solution.
- Copyright and trademark verification

II. Application and Content Certification Criteria

The criteria used to certify your submission package will vary depending on the nature of your submission and the technologies that it uses. For ease of explanation, we will divide this section into two parts, one defining the criteria used for certifying all printed materials and documentation, the other describing the criteria used for technical validation for each type of technology involved.

The items listed in this section represent the complete and comprehensive list of testing criteria, and will be the source used by Nextel certification teams to validate your submission.

1. Documentation and printed materials

- 1.1. Documentation must be accurate and consistent in functionality with the software.
- 1.2. Help screens within the application are considered part of the documentation and must be accurate and consistent with the functionality of the application.
- 1.3. Any URL links contained in the documentation or application are correct at the time of testing.
- 1.4. If a User's Guide is included, all major functions of the application will be tested against how the document describes the feature to work, and how screenshots portray the application.

The test will use the Table of Contents from the Application's User's Guide as a guide for testing. We recommended that the User's Guide be contained in a single PDF file when possible.

- 1.5. If an application is a MIDlet suite, documentation must be in a single, unified document incorporating all MIDlets within the Suite in one Help section or User's Guide if provided.
- 1.6. Documentation must inform the user that other services will be blocked during data transfer if the application supports network packet data transmissions.
 - 1.6.1. **For Mexico-targeted applications:** Documentation uses the wording for service blockages provided by Nextel de México.
- 1.7. Help screens (and User's Guide if provided) must indicate that other services, (e.g. phone and SMS messages, etc.), will be blocked while the port is in use by the application, e.g. during sending/receiving data.
 - 1.7.1. **For Mexico-targeted applications:** Documentation uses the wording for service blockages provided by Nextel de México.
- 1.8. Documentation must include contact and technical support information for the content provider or developer.

- 1.9. Documentation for applications that rely on country-specific APIs or Web Services (such as local web data marts or other data warehouses) must specify that any features that rely on these APIs are available only in those markets.
- 1.10. Documentation must include references to application memory requirements.
- 1.11. Documentation must include release notes for bug fixes or enhancements between major releases (e.g. 1.2 to 1.3).
- 1.12. Help screens must include contact and technical support information for the content provider.

2. Applications

2.1. All applications

- 2.1.1. Application can be installed over the air through Motorola iFUN B2B APIs or MCDS.

The iFUN B2B APIs or MCDS systems are not directly available to external developers. This will be tested in practice by the ACC testing lab. For the purposes of completing the self-certification checklist, the developer can list this as passed if the application can be installed using a data cable and approved Motorola iDEN Java Application Loader software.

- 2.1.2. Application can be installed using a data cable and Motorola iDEN Java Application Loader.
- 2.1.3. Application launch time does not exceed 15 seconds.
- 2.1.4. Application launches properly on the device.
- 2.1.5. Entry point for the application is consistent when launched.
- 2.1.6. Text displayed is not truncated in the application.
- 2.1.7. Text displayed has no noticeable typographic or spelling errors in language.
- 2.1.8. Text and graphics used by the application are not offensive, inappropriate or discriminatory.
- 2.1.9. Dates and numbers are properly localized to the market:

	Number	Date
Mexico	1,000,000.00	DD/MM/YYYY
Perú	1,000,000.00	DD/MM/YYYY
Argentina	1.000.000,00	DD/MM/YYYY
Brazil	1.000.000,00	DD/MM/YYYY
Chile	1.000.000,00	DD/MM/YYYY

- 2.1.10. For applications that are supported in multiple languages, the application automatically displays the proper language based on the locale settings of the device.
- 2.1.11. For applications that are supported in multiple languages, the application offers an option for the user to switch the display language from within the application, overriding the locale settings of the device.
- 2.1.12. Application graphics and user interface are appropriate for the screen size and resolution of the device.
- 2.1.13. Applications that require or integrate with external peripheral devices (i.e. barcode scanners, printers, etc.) interact properly and as described with the peripheral device.

For this kind of application, the developer shall provide the proper peripherals on loan for execution of this test.

2.2. Java ME applications

- 2.2.1. JAD and JAR file names are no longer than 16 characters, including period and suffix.
- 2.2.2. JAD file contains iDEN properties specifying language-specific suite names for Spanish and/or Portuguese, as appropriate:
 - 2.2.2.1. For Spanish-language applications:
 - 2.2.2.1.1. iDEN-MIDlet-Name-es: Aplicación X
 - 2.2.2.1.2. iDEN-MIDlet-Vendor-es: Corporación X
 - 2.2.2.1.3. iDEN-MIDlet-es-1: Aplicación, <icon>, com.company.path
 - 2.2.2.2. For Portuguese-language titles:
 - 2.2.2.2.1. iDEN-MIDlet-Name-pt: Aplicativo X
 - 2.2.2.2.2. iDEN-MIDlet-Vendor-pt: Corporação X
 - 2.2.2.2.3. iDEN-MIDlet-pt-1: Aplicativo, <icon>, com.company.path
- 2.2.3. Version/build number for the submission is unique and has not been used before by the application.
- 2.2.4. Individual applications within a MIDlet suite contain a separate version number accessible by the user within the application.
- 2.2.5. Version/build numbers are provided in descriptors (JAD or JAD & ALX files) and the JAR manifest (if applicable).
- 2.2.6. All submissions for certification testing must have an individual unique build/version number in the JAD file and in the JAR manifest.
- 2.2.7. File size reported in the MIDlet-Jar-Size property of the JAD file matches the actual size of the JAR file.

- 2.2.8. Application uses only Java ME classes and APIs as defined in the Java ME MIDP and CLDC specs supported by the target device or as OEM APIs for the device developed by the manufacturer.
- 2.2.9. Application ends and resumes properly from suspend (paused) mode.
- 2.2.10. For a MIDlet that uses the external display of a clamshell-style device, the MIDlet behaves properly when installed on a clamshell-style device that does not have an external display if such devices are supported.
- 2.2.11. Application has a customized icon for display in main screens of the device.

2.2.12. Security requirements

- 2.2.12.1. Application that stores personal or secure information provides proper methods for masking that information so that unauthorized users cannot see it in its totality.
 - 2.2.12.1.1. Any sensitive personal information stored by the application must not be displayed in plain text without the use of a password or PIN of at least four characters
 - 2.2.12.1.2. For applications that store credit card numbers, neither the PIN nor the expiration date of the card must be stored
- 2.2.12.2. Application uses secure protocols or encrypts data to transmit personal or secure information.

2.2.13. Network requirements

- 2.2.13.1. Application handles error conditions and messages gracefully, ensuring that error messages display properly and that the application regains control after being dismissed.
- 2.2.13.2. Application handles data transactions appropriately to ensure that, in case network connectivity is interrupted during a transmission, data corruption does not take place either on the handset or on back-end systems.
- 2.2.13.3. Application shuts down network connections properly upon application exit.

To test this requirement, after exiting the application, an interconnect (telephone) session, a dispatch session, an SMS, an MMS, and a WAP session as available will be established to determine that all services are functional and available.

- 2.2.13.4. Application does not cause any adverse effects to the network, such as obstruction of network traffic or services, during the test cycle.

This test requirement confirms whether the application behaves as a good citizen on the network. If during the testing performed by Nextel it becomes apparent that the application is behaving disrupt-

tively, this test case will be considered FAILED until the cause can be identified. For the purposes of completing the self-certification checklist, the developer can list this as PASSED if, in good faith, the developer believes *and can demonstrate if subsequently required to do so* that the protocol choices and data transfer mechanisms used are as efficient as possible given the nature of the application.

2.2.14. Stress Tests

- 2.2.14.1. Application launches and shuts down appropriately, or generates appropriate error messages, under restricted memory conditions.
For this test, Nextel will fill up the device's data space with voice-noices or media such as video files until there is 1k left of available memory, and will launch the application up to 5 times to determine proper behavior.
- 2.2.14.2. Application can send and receive data during restricted memory conditions.
- 2.2.14.3. Application starts up within a reasonable time period, not exceeding 15 seconds.
- 2.2.14.4. Application releases unneeded resources when in paused state.
- 2.2.14.5. Application does not generate any inappropriate behavior or operational errors during normal operation of the application such as unexpected restarts, exceptions, or unusual error messages.
- 2.2.14.6. Application handles interruptions gracefully and resumes proper functionality after the interruption. Tested interruptions include:
 - 2.2.14.6.1. Incoming Interconnect Phone Calls;
 - 2.2.14.6.2. Incoming Private Phone Calls (Dispatch and Alerts);
 - 2.2.14.6.3. Incoming SMS, MMS, Net Alert and Two-Way Message (as available).

2.2.15. Additional Requirements for MIDlets for Motorola iDEN devices

- 2.2.15.1. iDEN Program Space and iDEN Data Space values are listed in the JAD file, using the following syntax:
iDEN-Program-Space-Requirement: *n*
iDEN-Data-Space-Requirement: *n*
 - 2.2.15.1.1. **NOTE:** For Zeus-based devices (i876 and beyond), the iDEN-Program-Space-Requirement property is no longer required.
- 2.2.15.2. Program Space and Data Space in the JAD file match those listed in the About screen of the phone and in the User Guide (if applicable).
- 2.2.15.3. MIDlets that require privileged access to protected APIs under Operator (OPA) or Trusted Third Party (TTP) security domains list all

packages covered under Motorola security parameters in the MIDlet-Permissions property of the JAD file.

- 2.2.15.4. MIDlets that require privileged access to protected APIs and that use packages that are covered under security domains but that do not require the privileges allowed under OPA or TTP security domains list said packages in the MIDlet-Permissions-Opt property of the JAD file.
- 2.2.15.5. The MIDlet-Certificate-1-1 and MIDlet-Jar-RSA-SHA1 properties of the JAD file are empty or do not exist.

This test verifies that applications that were signed using Motorola SDKs during testing do not include those signatures when submitted. Such signatures are handset-specific and subject to expire within 48 hours of signature and will cause errors during testing. If your application requires a digital signature, the testing lab will apply this before beginning the testing process and return the signed files to you if testing passes. **If your application has already been signed permanently by Motorola or NII before submission, please note this so that the testing lab can waive this requirement.**

- 2.2.15.6. MIDlet-Install-Notify, MIDlet-Delete-Notify and Midlet-Delete-Confirm properties point to valid URLs or are omitted.
 - 2.2.15.7. Applications that use CallReceive API must handle incoming phone calls within the time allotted by the Java Application Manager of the device so that they do not lose permission to handle incoming calls.
 - 2.2.15.8. Servers that support HTTPS sessions from a MIDlet must use SSL certificates that are supported by Motorola for Java ME-based HTTPS sessions.
 - 2.2.15.9. MIDlet has icons for all four supported sizes, properly formatted for Iconic, Standard, Compressed and Zoom views with the appropriate resolutions for the devices supported and with correct settings for icon transparency.
- 2.2.16. Additional Requirements for Java applications for BlackBerry devices*
- 2.2.16.1. Submission includes an ALX file for installation using the Blackberry Desktop Client.
 - 2.2.16.2. Applications handle Security Policy Variations appropriately
Applications may be run on BlackBerry devices that are connected to tightly restricted BlackBerry Enterprise Servers (see <http://programa.nii.com/en/node/248> for more details). These test cases verify known conditions that hinge on security policy configurations.

- 2.2.16.3. On applications that require the features of the Mobile Data Service of the BlackBerry Enterprise Server (BES), the application generates an appropriate alert when run on a device that is not connected to a BES.
- 2.2.16.4. Applications do not generate split pipe alerts when connected to a BES with “Allow-Split-Pipe Connections” security policy set to false. This tests that one application does not attempt to establish connections using both direct TCP *and* MDS.
- 2.2.16.5. Application behaves gracefully when run on a device connected to a BES with security policies that could restrict its network access:
 - 2.2.16.5.1. application attempts connection through MDS (*device-side=false*) and BES Security policy Allow Internal Connections is set to FALSE.
 - 2.2.16.5.2. application attempts connection through direct TCP (*device-side=true*) and BES Security policy Allow External Connections is set to TRUE.
 - 2.2.16.5.3. application attempts HTTPS connection and and BES Security Policy “TLS Devices Side Only” is set to TRUE.
 - 2.2.16.5.4. If TLS through BES is required, HTTPS sessions must use *deviceside=true*.

2.3. WAP or XHTML Applications

- 2.3.1. Application loads and operates properly on the following browsers, if application is supported on the target device:
 - 2.3.1.1. Openwave v4.1 (small-screen Motorola iDEN phones)
 - 2.3.1.2. Openwave v7.0 (large-screen Motorola iDEN phones, Falcon line)
 - 2.3.1.3. Openwave V7.2 (small- and large-screen Motorola iDEN phones, Phoenix line)
 - 2.3.1.4. BlackBerry Browser (BES-linked BlackBerry devices)
 - 2.3.1.5. BlackBerry Internet Browser (non-BES-linked BlackBerry devices)
 - 2.3.1.6. Pocket Internet Explorer (Windows Mobile devices)
- 2.3.2. Graphics linked into application are properly formatted for the target device.
- 2.3.3. Application does not attempt to link to image files in formats that are not supported on the target device.
- 2.3.4. Loading application does not generate load errors or alerts on browser.
- 2.3.5. Application does not generate unnecessary reloads or refreshes.
- 2.3.6. Applications relying on unique identifiers such as UP_SUBID for identification function properly on devices that do not provide such headers

(Pocket Internet Explorer and BlackBerry Browsers) if such browsers are supported.

2.4. Network-initiated Location applications using NII web-based location APIs

- 2.4.1. The solution issues and receives no more than one request every 10 minutes per enabled phone number.
- 2.4.2. If the solution requests a location for a subscriber that is not provisioned, the solution does not re-issue the a location request for that subscriber for one hour.
- 2.4.3. The XML request generated by the solution does not generate errors or alerts in the Openwave Location Studio consoles.
- 2.4.4. The solution uses the correct login credentials to access the platform.
- 2.4.5. The solution's connection to the API is done through secured channels (using HTTPS or a VPN connection).
- 2.4.6. In case of an unsuccessful fix or a fix that does not generate a horizontal accuracy that falls within 20% of the requested accuracy, the solution issues no more than two subsequent retry requests within the 10-minute period.
- 2.4.7. The solution issues no more than 72 requests per subscriber in a 24-hour period.
- 2.4.8. Each session request sent by the solution includes no more than 25 handsets.
- 2.4.9. The solution does not exceed the maximum number of concurrent requests.
- 2.4.10. The solution does not open more than 50 sessions concurrently.
- 2.4.11. Nextel IP N&S (Nextel engineering) validates that the production environments for the Network-Initiated API have capacity to handle the additional load that would be placed by migrating the solution into the production servers.

2.5. Additional requirements for all location based services

- 2.5.1. Any use of mapping or external location data used by the application must be authorized by the owner of the copyright for the data, if any.

NII's goal is to help cultivate and nurture a community of developers, platform providers, and customers. Our partners are part of that ecosystem; proper relationships with data providers ensure that data providers will continue improving their data in response to the demand that we generate for it.
- 2.5.2. Application does not rely on mapping or geoinformation APIs or Web Services that are in Beta, that are not made available in production by

their provider for enterprise or mobile use or that are not permitted to be used for resolution of coordinates originating from GPS systems.

As with map data, platform providers are a critical part of the location services ecosystem. Proper relationships with platform providers helps ensure that they will continue improving their platforms to better meet your needs as a developer, and respecting their terms of use is critical to that.

Furthermore, relying on free APIs that the provider explicitly states are not allowed for production or mission-critical applications etc. do not generally allow these services to be used for production applications and

- 2.5.3. Applications verify upon initial launch that the phone can receive assist data from Nextel servers, and notify the user that it will be necessary to subscribe to the appropriate GPS assistance product (*iLocation for Java* in Mexico, *aGPS* in Brazil, *aGPS Vertical* in Argentina, *LIE* in Perú) for optimal speed of GPS performance.
- 2.5.4. Applications fall back on triangulation APIs or use cell location when appropriate.
- 2.5.5. For applications using location services, documentation must include the following language:

English: “The availability and accuracy of applications and services using GPS- or triangulation-derived location information will vary depending on the environment in which the location feature is used. In some situations, where adequate signals cannot be obtained, the GPS system may not work at all. Read your user guide for information on enhancing GPS performance.”

Spanish: “La disponibilidad, precisión y validez de las aplicaciones y servicios dependientes en localización utilizando GPS o triangulación variarán de acuerdo al entorno en el cual se utilice esa función. En algunas situaciones, donde no sea posible obtener señales adecuadas, es posible que los sistemas de GPS o triangulación no funcionen. Vea su guía del usuario para saber maneras de aumentar el rendimiento del sistema de GPS.”

Portuguese: “A disponibilidade, precisão e validez dos aplicativos e serviços que dependem do sistema GPS ou da triangulação variarão de acordo ao entorno no qual sejam usadas essas funções. Em algumas situações, onde não fosse possível obter sinais adequadas, é possível que os sistemas de GPS ou triangulação não funcionem. Veja a sua guia do usuário para achar maneiras de aumentar o rendimento do sistema GPS.”

3. Non-application Digital Media

3.1. Ringtones

- 3.1.1. Monophonic and polyphonic MIDI files must be properly encoded for the iDEN handset they are meant for. Details on supported media formats are available on [NII's Developer Program Website](#).
- 3.1.2. MP3 files to be made available as real music ringtones must follow proper encoding and size constraints for the devices they are meant for.

3.2. Wallpaper

- 3.2.1. Images must use appropriate color depths and resolutions for the handset that they are meant for. Details on supported wallpaper maximum and minimum sizes and color depths are available at [NII's Developer Program Website](#).
- 3.2.2. Images must not block or impede the display of Nextel identifying information on the main or external displays.

4. Non-application OEM devices or other specialized hardware

- 4.1. Application or service operates automatically without requiring user intervention after device is powered on.

III. Appendices

A. Self-testing Checklist

Application Name:			
Version:			
Publication Date:			
Submission Date:			
Final status:		Test Date(s):	

Test #	Description	Self-test result	Nextel test result	Status
A	Sample Test	PASS	PASS	GREEN
A.1	Sample Test 2	PASS	PASS	YELLOW
B.1	Sample Test 3	PASS	FAIL	WAIVED

1	Documentation and Printed Materials			
1.1	Documentation must be accurate and consistent in functionality with the software.			
1.2	Help screens within the application are accurate and consistent with the functionality of the application.			
1.3	URL links contained in the documentation or application are correct.			
1.4	All major functions of the application described in documentation work as described and screenshots portray the application accurately.			

Test #	Description	Self-test result	Nextel test result	Status
1.5	If an application is a MIDlet suite, documentation is in a single, unified document incorporating all MIDlets within the Suite in one Help section or User's Guide.			
1.6	Documentation informs the user about service blockage possibility for data applications.			
1.6.1	Mexico only: Documentation uses the wording for service blockages provided by Nextel de México.			
1.7	Help screens and User's Guide indicate that other services will be blocked while the data port is in use by the application.			
1.7.1	Mexico only: Help screens and User's guide uses the wording for service blockages provided by Nextel de México.			
1.8	Documentation includes contact and technical support information for the content provider or developer.			
1.9	Documentation for applications that rely on country-specific APIs or Web Services (such as local web data marts or other data warehouses) specifies that any features that rely on these APIs are available only in those markets.			
1.1	Documentation includes references to application memory requirements.			
1.11	Documentation includes release notes for bug fixes or enhancements between major releases (e.g. 1.2 to 1.3).			
1.12	Help screens include contact and technical support information for the content provider.			
2	Applications			
2.1	<i>All Applications</i>			
2.1.1	Application can be installed over the air through Motorola iFUN B2B APIs or MCDS.			

Test #	Description	Self-test result	Nextel test result	Status
2.1.2	Application can be installed using a data cable and Motorola iDEN Java Application Loader.			
2.1.3	Application launch time does not exceed 15 seconds.			
2.1.4	Application launches properly on the device.			
2.1.5	Entry point for the application is consistent when launched.			
2.1.6	Text displayed is not truncated in the application.			
2.1.7	Text displayed has no noticeable typographic or spelling errors in language.			
2.1.8	Text and graphics used by the application are not offensive, inappropriate or discriminatory.			
2.1.9	Dates and numbers are properly localized to the market: Mexico: 1,000,000.00 DD/MM/YYYY Perú: 1,000,000.00 DD/MM/YYYY Argentina: 1.000.000,00 DD/MM/YYYY Brazil: 1.000.000,00 DD/MM/YYYY Chile: 1.000.000,00 DD/MM/YYYY			
2.1.10	For applications that are supported in multiple languages, the application automatically displays the proper language based on the locale settings of the device.			
2.1.11	For applications that are supported in multiple languages, the application offers an option for the user to switch the display language from within the application, overriding the locale settings of the device.			
2.1.12	Application graphics and user interface are appropriate for the screen size and resolution of the device.			

Test #	Description	Self-test result	Nextel test result	Status
2.1.13	Applications that require or integrate with external peripheral devices (i.e. barcode scanners, printers, etc.) interact properly and as described with the peripheral device. (the developer shall provide the proper peripherals on loan for execution of this test).			
2.2	<i>Java ME Applications</i>			
2.2.1	JAD and JAR file names are no longer than 16 characters, including period and suffix.			
2.2.2	JAD file contains iDEN properties specifying language-specific suite names for Spanish and/or Portuguese, as appropriate:			
2.2.2.1	For Spanish-language applications: iDEN-MIDlet-Name-es: Aplicación X iDEN-MIDlet-Vendor-es: Corporación X iDEN-MIDlet-es-1: Aplicación, <icon>, com.company.path			
2.2.2.2	For Portuguese-language titles: iDEN-MIDlet-Name-pt: Aplicativo X iDEN-MIDlet-Vendor-pt: Corporação X iDEN-MIDlet-pt-1: Aplicativo, <icon>, com.company.path			
2.2.3	Version/build number for the submission is unique and has not been used before by the application.			
2.2.4	Individual applications within a MIDlet suite contain a separate version number accessible by the user within the application.			
2.2.5	Version/build numbers are provided in descriptors (JAD or JAD & ALX files) and the JAR manifest (if applicable).			
2.2.6	All submissions for certification testing must have an individual unique build/version number in the JAD file and in the JAR manifest.			

Test #	Description	Self-test result	Nextel test result	Status
2.2.7	File size reported in the MIDlet-Jar-Size property of the JAD file matches the actual size of the JAR file.			
2.2.8	Application uses only Java ME classes and APIs as defined in the Java ME MIDP and CLDC specs supported by the target device or as OEM APIs for the device developed by the manufacturer.			
2.2.9	Application ends and resumes properly from suspend (paused) mode.			
2.2.10	For a MIDlet that uses the external display of a clamshell-style device, the MIDlet behaves properly when installed on a clamshell-style device that does not have an external display if such devices are supported.			
2.2.11	Application has a customized icon for display in main screens of the device.			
<i>2.2.12</i>	<i>Security Requirements</i>			
2.2.12.1	Application that stores personal or secure information provides proper methods for masking that information so that unauthorized users cannot see it in its totality.			
2.2.12.1.1	Any sensitive personal information stored by the application must not be displayed in plain text without the use of a password or PIN of at least four characters			
2.2.12.1.2	For applications that store credit card numbers, neither the PIN nor the expiration date of the card must be stored			
2.2.12.2	Application uses secure protocols or encrypts data to transmit personal or secure information.			
<i>2.2.13</i>	<i>Network Requirements</i>			
2.2.13.1	Application handles error conditions and messages gracefully, ensuring that error messages display properly and that the application regains control after being dismissed.			

Test #	Description	Self-test result	Nextel test result	Status
2.2.13.2	Application handles data transactions appropriately to ensure that, in case network connectivity is interrupted during a transmission, data corruption does not take place either on the handset or on back-end systems.			
2.2.13.3	Application shuts down network connections properly upon application exit. To test this requirement, after exiting the application, an interconnect (telephone) session, a dispatch session, an SMS, an MMS, and a WAP session as available will be established to determine that all services are functional and available.			
2.2.13.4	Application does not cause any adverse effects to the network, such as obstruction of network traffic or services, during the test cycle.			
2.2.14	<i>Stress Tests</i>			
2.2.14.1	Application launches and shuts down appropriately, or generates appropriate error messages, under restricted memory conditions.			
2.2.14.2	Application can send and receive data during restricted memory conditions.			
2.2.14.3	Application starts up within a reasonable time period, not exceeding 15 seconds.			
2.2.14.4	Application releases unneeded resources when in paused state.			
2.2.14.5	Application does not generate any inappropriate behavior or operational errors during normal operation of the application such as unexpected restarts, exceptions, or unusual error messages.			
2.2.14.6	Application handles interruptions gracefully and resumes proper functionality after the interruption. Tested interruptions include:			
2.2.14.6.1	Incoming Interconnect Phone Calls;			

Test #	Description	Self-test result	Nextel test result	Status
2.2.14.6.2	Incoming Private Phone Calls (Dispatch and Alerts);			
2.2.14.6.3	Incoming SMS, MMS, Net Alert and Two-Way Message (as available).			
<i>2.2.15</i>	<i>Additional Requirements for MIDlets for Motorola iDEN devices</i>			
2.2.15.1	Program Space and Data Space values are listed in the JAD file, using the following syntax: iDEN-Program-Space-Requirement: n iDEN-Data-Space-Requirement: n			
2.2.15.1.1	NOTE: For Zeus-based devices (i876 and beyond), the iDEN-Program-Space-Requirement property is no longer required.			
2.2.15.2	Program Space and Data Space in the JAD file match those listed in the About screen of the phone and in the User Guide (if applicable).			
2.2.15.3	MIDlets that require privileged access to protected APIs under Operator (OPA) or Trusted Third Party (TTP) security domains list all packages covered under Motorola security parameters in the MIDlet-Permissions property of the JAD file.			
2.2.15.4	MIDlets that require privileged access to protected APIs and that use packages that are covered under security domains but that do not require the privileges allowed under OPA or TTP security domains list said packages in the MIDlet-Permissions-Opt property of the JAD file.			

Test #	Description	Self-test result	Nextel test result	Status
2.2.15.5	<p>The MIDlet-Certificate-1-1 and MIDlet-Jar-RSA-SHA1 properties of the JAD file are empty or do not exist.</p> <p>This test verifies that applications that were signed using Motorola SDKs during testing do not include those signatures when submitted. Such signatures are handset-specific and subject to expire within 48 hours of signature and will cause errors during testing. If your application requires a digital signature, the testing lab will apply this before beginning the testing process and return the signed files to you if testing passes.</p> <p>If your application has already been signed permanently by Motorola or NII before submission, please note this so that the testing lab can waive this requirement.</p>			
2.2.15.6	MIDlet-Install-Notify, MIDlet-Delete-Notify and Midlet-Delete-Confirm properties point to valid URLs or are omitted.			
2.2.15.7	Applications that use CallReceive API must handle incoming phone calls within the time allotted by the Java Application Manager of the device so that they do not lose permission to handle incoming calls.			
2.2.15.8	Servers that support HTTPS sessions from a MIDlet must use SSL certificates that are supported by Motorola for Java ME-based HTTPS sessions.			
2.2.15.9	MIDlet has icons for all four supported sizes, properly formatted for Iconic, Standard, Compressed and Zoom views with the appropriate resolutions for the devices supported and with correct settings for icon transparency.			
2.2.16	<i>Additional Requirements for Java applications for BlackBerry devices</i>			
2.2.16.1	Submission includes an ALX file for installation using the Blackberry Desktop Client.			

Test #	Description	Self-test result	Nextel test result	Status
2.2.16.2	Applications handle Security Policy Variations appropriately.			
2.2.16.3	On applications that require the features of the Mobile Data Service of the BlackBerry Enterprise Server (BES), the application generates an appropriate alert when run on a device that is not connected to a BES.			
2.2.16.4	Applications do not generate split pipe alerts when connected to a BES with "Allow-Split-Pipe Connections" security policy set to false. This tests that one application does not attempt to establish connections using both direct TCP and MDS.			
2.2.16.5	Application behaves gracefully when run on a device connected to a BES with security policies that could restrict its network access:			
2.2.16.5.1	application attempts connection through MDS (deviceside=false) and BES Security policy Allow Internal Connections is set to FALSE.			
2.2.16.5.2	application attempts connection through direct TCP (deviceside=true) and BES Security policy Allow External Connections is set to TRUE.			
2.2.16.5.3	application attempts HTTPS connection and BES Security Policy "TLS Devices Side Only" is set to TRUE.			
2.2.16.5.4	If TLS through BES is required, HTTPS sessions uses deviceside=true.			
2.3	<i>WAP or XHTML Applications</i>			
2.3.1	Application loads and operates properly on the following browsers, if application is supported on the target device:			
2.3.1.1	Openwave v4.1 (small-screen Motorola iDEN phones)			
2.3.1.2	Openwave v7.0 (large-screen Motorola iDEN phones, Falcon line)			

Test #	Description	Self-test result	Nextel test result	Status
2.3.1.3	Openwave V7.2 (small- and large-screen Motorola iDEN phones, Phoenix line)			
2.3.1.4	BlackBerry Browser (BES-linked BlackBerry devices)			
2.3.1.5	BlackBerry Internet Browser (non-BES-linked BlackBerry devices)			
2.3.1.6	Pocket Internet Explorer (Windows Mobile devices)			
2.3.2	Graphics linked into application are properly formatted for the target device.			
2.3.3	Application does not attempt to link to image files in formats that are not supported on the target device.			
2.3.4	Loading application does not generate load errors or alerts on browser.			
2.3.5	Application does not generate unnecessary reloads or refreshes.			
2.3.6	Applications relying on unique identifiers such as UP_SUBID for identification function properly on devices that do not provide such headers (Pocket Internet Explorer and BlackBerry Browsers) if such browsers are supported.			
2.4	<i>Network-initiated Location applications using NII web-based location APIs</i>			
2.4.1	The solution issues and receives no more than one request every 10 minutes per enabled phone number.			
2.4.2	If the solution requests a location for a subscriber that is not provisioned, the solution does not re-issue the a location request for that subscriber for one hour.			
2.4.3	The XML request generated by the solution does not generate errors or alerts in the Openwave Location Studio consoles.			
2.4.4	The solution uses the correct login credentials to access the platform.			

Test #	Description	Self-test result	Nextel test result	Status
2.4.5	The solution's connection to the API is done through secured channels (using HTTPS or a VPN connection).			
2.4.6	In case of an unsuccessful fix or a fix that does not generate a horizontal accuracy that falls within 20% of the requested accuracy, the solution issues no more than two subsequent retry requests within the 10-minute period.			
2.4.7	The solution issues no more than 72 requests per subscriber in a 24-hour period.			
2.4.8	Each session request sent by the solution includes no more than 25 handsets.			
2.4.9	The solution does not exceed the maximum number of concurrent requests.			
2.4.10	The solution does not open more than 50 sessions concurrently.			
2.4.11	Nextel IP N&S (Nextel engineering) validates that the production environments for the Network-Initiated API have capacity to handle the additional load that would be placed by migrating the solution into the production servers.			
2.5	<i>Additional requirements for all location based services</i>			
2.5.1	Any use of mapping or external location data used by the application must be authorized by the owner of the copyright for the data, if any.			
2.5.2	Application does not rely on mapping or geoinformation APIs or Web Services that are in Beta, that are not made available in production by their provider for enterprise use or that are not permitted to be used for resolution of coordinates originating from GPS systems.			

Test #	Description	Self-test result	Nextel test result	Status
2.5.3	Applications verify upon initial launch that the phone can receive assist data from Nextel servers, and notify the user that it will be necessary to subscribe to the appropriate GPS assistance product (iLocation for Java in Mexico, aGPS in Brazil, aGPS Vertical in Argentina, LIE in Perú) for optimal speed of GPS performance.			
2.5.4	Applications fall back on triangulation APIs or use cell location when appropriate.			
2.5.5	<p>For applications using location services, documentation must include the following language:</p> <p>English: "The availability and accuracy of applications and services using GPS- or triangulation-derived location information will vary depending on the environment in which the location feature is used. In some situations, where adequate signals cannot be obtained, the GPS system may not work at all. Read your user guide for information on enhancing GPS performance."</p> <p>Spanish: "La disponibilidad, precisión y validez de las aplicaciones y servicios dependientes en localización utilizando GPS o triangulación variarán de acuerdo al entorno en el cual se utilice esa función. En algunas situaciones, donde no sea posible obtener señales adecuadas, es posible que los sistemas de GPS o triangulación no funcionen. Vea su guía del usuario para saber maneras de aumentar el rendimiento del sistema de GPS."</p> <p>Portuguese: "A disponibilidade, precisão e validade dos aplicativos e serviços que dependem do sistema GPS ou da triangulação variarão de acordo ao entorno no qual sejam usadas essas funções. Em algumas situações, onde não fosse possível obter sinais adequadas, é possível que os sistemas de GPS ou triangulação não funcionem. Veja a sua guia do usuário para achar maneiras de aumentar o rendimento do sistema GPS."</p>			

Test #	Description	Self-test result	Nextel test result	Status
3	Non-application Digital Media			
<i>3.1</i>	<i>Ringtones</i>			
3.1.1	Monophonic and polyphonic MIDI files are properly encoded for the iDEN handset they are meant for.			
3.1.2	MP3 files to be made available as real music ringtones must follow proper encoding and size constraints for the devices they are meant for.			
<i>3.2</i>	<i>Wallpaper</i>			
3.2.1	Images use appropriate color depths and resolutions for the handset that they are meant for.			
3.2.2	Images do not block or impede the display of Nextel identifying information on the main or external displays.			
<i>3.3</i>	<i>Themes</i>			
4	Non-application OEM devices or other specialized hardware			
4.1	Application or service operates automatically without requiring user intervention after device is powered on.			

B. Demo Accounts and Web-based Application Data

User Type	Username or ID	Password	Other info	Demo URL (if applicable)
End user	DAT01	DAT01		
Admin	DAT01	DAT01		
Other (specify)				

Special instructions during testing:

Special instructions for demo:

C. Handset and Service Compatibility Checklist

Model		Minimum firmware version required (if any)
i205		
i265		
i275		
i290		
i335		
i355		
i530		
i560		
i605		
i690		
i710		
i730		
i730 ROM 9		
i733		
i760		
i776		
i830		
i830 R2		
i833		
i833 R2		
i850		
i860		
i870		

Model		Minimum firmware version required (if any)
i876		
i880		
i885		
i930		

Country	Services Required (if any) including necessary IP routing information (address ranges, public IP addresses, firewall configuration requirements, etc)
Argentina	
Brazil	
Mexico	
Peru	

Country	Certificates or keys required on servers for secure transactions, if any
Argentina	
Brazil	
Mexico	
Peru	

D. Technical Support Contact Information

Support tier	Name of contact(s)	Phone	Email	Pager
Tier 1				
Tier 2				
Tier 3				

E. Known error messages and resolutions

Error Code	Error Condition	Known Cause	Resolution

F. Estimated Data Usage

Protocol(s) Used:

Estimated two-way data transfers (including protocol headers) per user per month:

Other network routing requirements (if any):

For Network-Initiated Location Services:

Expected frequency of connection requests to API (in minutes):

Expected number of location requests per connection:

Expected number of location updates requested per handset per day:

Expected total number of handsets located by solution for 2, 6 and 12 months past launch

G. Code Signature Request Form

(Use only for Java ME applications running on Motorola iDEN devices)

Required Function Groups (from MIDlet-Permissions)	Requested Security Domain (TTP - Trusted Third Party or OPA - Operator)

H. Waiver Request Form

Test Case #	Nextel certification Status	Description of waiver request	Nextel approval of waiver