A2.1.10 Omninet Test Plan

1953067 宋潇歌 2052225 张勤杭 2051840 梁厚 1950389 季艺

Test Plan Identifier

- **Name**: Omninet Test Plan
- **Version**: v1.0
- **Date**: 2023.05.19

1. INTRODUCTION

1.1 Objectives

To test the functionality and features of the Omninet kiosk system, and to clarify the test tasks, test contents and test standards at different test levels.

1.2 Testing Strategy

- **Test the Welcome screen**: verify that the welcome message appears properly and is visible to the user.

- **Test the Payment screen**: verify that the payment options, including cash, credit cards, and debit cards, are available and functional.

- **Test the Internet Browser**: verify that the latest version of Netscape, Opera, or Internet Explorer is available and can be selected by the user.

- **Test Performance**: verify that users are provided with the appropriate connection speed depending on their connection type.

- **Test Localization**: verify that the kiosk can be configured to operate in the primary local language for its installed locale.

1.3 Scope

This document covers the test plan for the Omninet system, including the kiosks, payment systems, browser, performance, localization, content control, session termination, and confidentiality requirements.

1.4 Reference Material

- *IEEE Standard for Software Test Documentation(Std 829-2008)*
- *CPUX-UT Usability Test Report Example v0133 EN*

1.5 Definitions and Acronyms

- **Acceptance Criteria**

  The criteria that a user, customer, or authorized entity must approve for a component or system to be accepted. [Adapted from IEEE 610]

- **Adaptability**

  The ability of a software product to function in different specified environments without requiring any additional actions or means beyond what is provided for its intended purpose. This concept is closely related to portability testing. [Adapted from ISO 9126]

- **Agile Testing**

  Testing practice for a project using agile methodologies, such as extreme programming (XP), treating development as the customer of testing and emphasizing the test-first design paradigm.

- **Beta Testing**

  External acceptance testing is commonly carried out through, where potential or current users/customers evaluate a component or system at an independent location that is not affiliated with the developers. The aim is to assess whether the product meets their requirements and integrates effectively into their business processes. The feedback received from this kind of testing is critical for acquiring market insights.

- **Black Box Testing**

  Testing, either functional or non-functional, without reference to the internal structure of the component or system.

2. TEST ITEMS

- **Payment**: Test the kiosk's acceptance of cash, American Express, Visa, Mastercard, PLUS, and Cirrus networks.

- **Performance**: Test that users have greater than 50 KBPS connection speed on kiosks operating with a PSTN connection and greater than 128 KBPS connection speed on kiosks operating with DSL or cable connections.

- **Browser**: Test that the latest version of Netscape, Opera, or Internet Explorer is available on the kiosk.

- **Localization**: Test that the kiosk is configured to operate in the primary local language for its installed locale.

- **Content Control**: Test that pornographic, objectionable, lewd, obscene, or violent material is blocked.

- **Session Termination**: Test that users can terminate sessions by logging out or allowing time to expire.

- **Confidentiality**: Test that all cookies and other downloaded files are cleared, the URL history is cleared, the browser is exited, and the browser is restarted at the Welcome screen once a session terminates.

- **Software Updates**: Test that updates for operating system or browser patches, new network, modem, or graphics drivers, new logos, updated per-minute payment rate tables, virus, worm, malicious code, or other firewall definitions, and blocked web sites are pushed to the kiosk.

- **View Kiosks**: Test that call center agents can browse a list of kiosks and view information such as the current operating system version, current browser version, total uptime since installation, total update since last software update, and number of crashes, reboots, or other hard failures since last software update.

- **View Users**: Test that call center agents can view current and past URLs, credit or debit card number (if applicable), name (if available from credit card validation), amount paid for this session, blocks of time purchased, previous session (if available from credit card number and name), and paid time remaining.

- **Modify User**: Test that call center agents can modify a user's session by adding blocks of time.

- **Terminate User**: Test that call center agents can terminate a user's session and the user receives a refund for any unused time at the point of termination.

3. FEATURES TO BE TESTED

- **Welcome**: The kiosk will be tested to ensure the welcome message is displayed correctly

- **Payment**: The kiosk will be tested to ensure payment can be made in 5-minute increments up to 1 hour

- **Browser**: The kiosk will be tested to ensure the correct browser is displayed

- **Performance**: The kiosk will be tested to ensure it meets the specified connection speeds

- **Localization**: The kiosk will be tested to ensure it supports all languages supported by the operating system and browser
- **Content Control**: The kiosk will be tested to ensure it prevents the display of objectionable material
- **Session Termination**: The kiosk will be tested to ensure it logs out correctly and allows time to expire
- **Confidentiality**: The kiosk will be tested to ensure it clears cookies and URLs correctly

4. FEATURES NOT TO BE TESTED

Based on the outcome of risk analysis, certain defects in the specified modules may not pose significant risks or have severe consequences given the time restriction. Meanwhile, some features remain out of the testers' tasks because they might be the user's responsibility. Thus, it is paramount to identify and enumerate such defects.

Here is an example of features not to be tested.

Level	Aim	Features Not to Be Tested
Unit Level	Performance	1. Scalability 2. Stability
	Usability	1. Learnability 2. Memorability
	Maintainability	1. Analyzability 2. Modifiability
System Level	Performance	speed of every response within the back-end side
Acceptance Level	Performance	speed of every response within the back-end side

5. APPROACH

5.1 Component Testing

Component Testing: Test individual components and evaluate how they interact with each other.

- Verify that kiosks have the latest version of Netscape, Opera, or Internet Explorer

- verify payment options are working correctly

- verify that the kiosks are connected to the appropriate network, and test the kiosk's ability to connect to the server farm

5.2 Integration Testing

Integration Testing: Test the system as a whole to ensure all components are working together properly.

- Verify that the kiosk is able to connect to the server farm, that the kiosk is able to receive and process software updates, and that the kiosk is able to properly display the welcome screen.

5.3 Conversion Testing

Conversion Testing: Test the conversion of existing data into the new system.

- Verify that the kiosk is able to support the languages of the installed locale

- verify that the kiosk is able to block objectionable material

- verify that the kiosk is able to properly process payments from the customer

5.4 Job Stream Testing

Job Stream Testing: Test the job streams that run the system.

- Verify that the kiosk is able to properly process payments from the customer

- verify that the kiosk is able to clear cookies and other downloaded files

- verify that the kiosk is able to restart the browser at the Welcome screen

5.5 Interface Testing

Interface Testing: Test the interfaces between the system and external systems.

- Verify that the kiosk is able to properly communicate with the server farm

- verify that the kiosk is able to properly communicate with customers

- verify that the kiosk is able to properly communicate with call center agents

5.6 Security Testing

Security Testing: Test the security features of the system.

- Verify that the kiosk is able to protect against sending or receiving a virus, worm, or other malicious code

- verify that the kiosk is able to block access to pornographic, objectionable, lewd, obscene, or violent material

- verify that the kiosk is able to properly process payments from the customer

5.7 Recovery Testing

Recovery Testing: Test the system's ability to recover from crashes and other malfunctions.

- Verify that the kiosk is able to properly restart after experiencing a crash or other hard failure

- verify that the kiosk is able to properly resume a session after a power outage

5.8 Performance Testing

Performance Testing: Test how the system performs under different load levels.

- Verify that the kiosk is able to maintain a greater than 50 KBPS connection speed on PSTN connections

- verify that the kiosk is able to maintain a greater than 128 KBPS connection speed on DSL or cable connections

5.9 Regression Testing

Regression Testing: Test to ensure that existing features are not broken after changes are made.

- Verify that the kiosk is able to properly process payments from the customer

- verify that the kiosk is able to properly display the Welcome screen

- verify that the kiosk is able to properly terminate sessions

5.10 Acceptance Testing

Acceptance Testing: Test to ensure the system meets the requirements specified in the requirements document.

- Verify that the kiosk is able to properly process payments from the customer

- verify that the kiosk is able to properly display the Welcome screen

- verify that the kiosk is able to properly terminate sessions

5.11 Beta Testing

Beta Testing: Test the system with real users to ensure usability and performance.

- Verify that the kiosk is able to properly process payments from the customer

- verify that the kiosk is able to properly display the Welcome screen

- verify that the kiosk is able to properly terminate sessions

6. PASS / FAIL CRITERIA

6.1 Suspension Criteria

- Unacceptable performance level
- Unacceptable connection speed
- Unacceptable site blocking
- Unacceptable privacy
- Unacceptable software updates
- Unacceptable view kiosks
- Unacceptable view users
- Unacceptable modify user
- Unacceptable terminate user

6.2 Resumption Criteria

- Acceptable performance level
- Acceptable connection speed
- Acceptable site blocking
- Acceptable privacy
- Acceptable software updates
- Acceptable view kiosks
- Acceptable view users
- Acceptable modify user
- Acceptable terminate user

6.3 Approval Criteria

- All test cases must pass with no errors
- All features must meet the requirements

7. TESTING PROCESS

7.1 Test Deliverables

- Test results

- Test plans

- Test cases

- Test scripts

- Test reports

7.2 Testing Tasks

- Create a test plan

- Design test cases

- Execute test cases

- Analyze test results

- Document defects

7.3 Responsibilities

- Project lead: Create a test plan and assign tasks

- Software engineer: Design test cases and execute test cases

- Tester: Analyze test results and document defects

7.4 Resources

- **Automated Tools**

   Choose resources of tools by specifying availability.

- **Budget**

   Estimate costing and available fundings.

- **Human Resource**

Role	Capabilities
Test Analyst Team	1. Determine what to test and prioritize the tasks, and monitor the test coverage;

	2. Define specific tests, design test cases, and schedule test executions; 3. Develop test documentations and deliver them to the product owner; 4. Compare actual and expected results, checking whether a product meets the requirements.
Test Architect Team	1. Work out the ways to optimize the testing process at a high level; 2. Identify tools and technologies that align with business goals, company infrastructure and testers' skillsets; 3. Monitor the effectiveness of testing, and provide mentoring and suggestions to improve testing practices.
Test Manager Team	1. Prepare the test strategy for the project, and define the list of tasks for all; 2. Set metrics to measure the quality and progress of work and keeps track of everyone's performance.
Customer Representative Team	May take part in any process mentioned above. Help clarify requirements and provide customers' test opinions and expected results.

7.5 Schedule

- Test plan: 5 days
- Test design: 10 days
- Test execution: 10 days
- Test analysis: 5 days
- Defect documentation: 5 days
- Total: 35 days

8. ENVIRONMENTAL REQUIREMENTS

8.1 Hardware

- Kiosks will be tested in airports, malls, theaters, and other public places

- Verify that hardware is properly installed and configured to meet the system requirements.

- Verify that all kiosks are connected to the server farm.

- Ensure that all hardware is stable and reliable.

8.2 Software

- Verify that the latest versions of Netscape, Opera, and Internet Explorer browsers are installed on Windows kiosks.

- Verify that the operating system or browser patches, new network, modem, and graphics drivers are installed correctly.

- Verify that the kiosks are configured to operate in the primary local language.

- Ensure that the kiosks are configured to support all languages supported by the operating system and browser.

8.3 Security

- Verify that the site blocking feature is enabled to prevent display of pornographic, objectionable, lewd, obscene, or violent material.

- Verify that the kiosks are protected against sending or receiving a virus, worm, or other malicious code.

8.4 Tools

- Verify that the kiosks are equipped with the necessary tools to accept cash, credit/debit cards, and other forms of payment.

- Verify that the kiosks are equipped with tools to track and record user information.

8.5 Publications

- Verify that the kiosks are equipped with the necessary publications to inform users of payment and session termination options.

8.6 Risks and Assumptions

- Assume that the kiosks will be installed in airports, malls, theaters, and other public places.

- Identify any potential risks that may arise from installing kiosks in public places.

- Plan for contingency measures to minimize the risks.

9. CHANGE MANAGEMENT PROCEDURES

1. Verify that the customer service agents have the capability to update software on the Omninet kiosks.

2. Ensure that the kiosks can be updated with the latest version of the operating system and browser.

3. Validate that the kiosks are updated with the appropriate site blocking to prevent the display of objectionable material.

4. Confirm that the kiosks can be configured to operate in the primary local language.

5. Test that customer service agents can view the list of kiosks and their current operating system and browser versions.

10. PLAN APPROVALS

- Approval by the Project Manager
- Approval by the System Designer
- Approval by the Quality Assurance Manager
- Approval by the System Administrator
- Approval by the Release Manager