Manual Test Cases for Secure P2P File Sharing

April 04, 2025

Peer Discovery Tests

Test Case ID	PD-001
Description	Verify automatic peer discovery on local network using mDNS
Preconditions	• Two instances of the application running on different devices on same network • Both instances freshly started
Test Steps	1. Start application instance on Device 1 2. Start application instance on Device 2 3. Wait 30 seconds 4. Observe "Discovered Peers" list on both devices
Expected Results	• Each device should automatically discover the other • Device 1 should display Device 2's username in its "Discovered Peers" list and vice versa • No manual configuration should be required for discovery

Test Case ID	PD-002
Description	Verify peer information is updated when peer changes details
Preconditions	• Two devices with application running on same network • Peers already discovered each other

Test Steps	1. On Device 1, close application 2. Restart application with a different username 3. Wait 60 seconds 4. Observe peer listing on Device 2
Expected Results	• Device 2 should update Device 1's information • New username should be displayed in Device 2's peer list

Authentication Tests

Test Case ID	AUTH-001
Description	Verify mutual authentication between two peers
Preconditions	• Two applications running on same network • Peers discovered each other
Test Steps	1. On Device 1, select Device 2 in the peer list 2. Click "Connect to Peer" button 3. On Device 2, accept the connection request 4. Verify fingerprint matches when prompted 5. Check connection status on both devices
Expected Results	• Connection request appears on Device 2 • Both devices display fingerprint for verification • After acceptance, both devices show connected status • Both peers appear in "Verified Contacts" list on respective devices

Test Case ID	AUTH-002

Description	Verify rejection of connection with incorrect fingerprint
Preconditions	• Two applications running on same network • Peers discovered each other
Test Steps	1. On Device 1, select Device 2 in peer list 2. Click "Connect to Peer" button 3. On Device 2, when prompted to verify, claim fingerprint doesn't match 4. Reject the connection
Expected Results	• Connection should be rejected • Peers should not be added to each other's verified contacts list • Warning/error message should appear about fingerprint mismatch

File Sharing Tests

Test Case ID	FS-001
Description	Test sharing and listing files
Preconditions	• Two connected peers • Test file available on Device 1
Test Steps	1. On Device 1, click "Share New File" 2. Select test file to share 3. On Device 2, select Device 1 in contacts list 4. Click "View Peer Files"

Expected Results	• Shared file appears in Device 1's shared files list • Device 2 should see the file in Device 1's shared file listing • File size and hash information should be correct

Test Case ID	FS-002
Description	Test file download without consent
Preconditions	• Two connected peers • Device 1 has shared a file
Test Steps	1. On Device 2, view Device 1's shared files 2. Click "Download" on a file 3. Observe file transfer progress
Expected Results	• Device 1 shows succesfull transfer • Device 2 shows download progress • File is successfully downloaded and appears in Device 2's received files • Hash verification succeeds

Test Case ID	FS-003
Description	Test file transfer rejection
Preconditions	• Two disconnected peers • Device 1 has shared a file
Test Steps	1. On Device 2, view Device 1's shared files 2. Click "Download" on a file 3. On Device 1, it will automatically reject the download request

Expected Results	• Device 1 shows consent prompt • After rejection, notification displayed on Device 2 • File is not transferred

File Integrity Tests

Test Case ID	FI-001
Description	Test hash verification of downloaded files
Preconditions	• Regular peer and malicious peer running • Client connected to malicious peer
Test Steps	1. Connect to malicious peer 2. View peer's shared files 3. Attempt to download a file that will be altered during transfer 4. Wait for download process to complete
Expected Results	• Download should start • Hash verification should fail • Error message should indicate hash verification failure • Tampered file should be deleted and not stored in received files

Key Management Tests

Test Case ID	KM-001
Description	Test key rotation and notification to contacts
Preconditions	• Two connected and authenticated peers

Test Steps	1. On Device 1, click "Rotate Keys" button 2. Enter confirmation if prompted 3. Wait 30 seconds 4. Check connection status on Device 2
Expected Results	• Device 1 generates new keys • Device 2 receives notification about key change • Fingerprint on Device 2 updates to match new fingerprint • Connection remains established with new keys

Test Case ID	KM-002
Description	Test manually adding a contact by fingerprint
Preconditions	• Two applications running on network • Peers can discover each other
Test Steps	1. On Device 1, get fingerprint (from settings or info page) 2. On Device 2, click "Add Contact" 3. Enter Device 1's username and fingerprint 4. Attempt to connect to newly added contact
Expected Results	• Device 1 appears in Device 2's contacts list • Connection can be established without additional fingerprint verification

Security Tests

Test Case ID	SEC-001
Description	Test file encryption at rest

Preconditions	• Application installed with shared and received files
Test Steps	1. Share a text file with known content 2. Navigate to the shared files directory in the filesystem 3. Try to open the file with a text editor 4. Navigate to received files directory 5. Try to open a received file with a text editor
Expected Results	• Files in shared and received directories should be encrypted • Content should not be readable with standard text editors • Files should have different content than the original

Test Case ID	SEC-002
Description	Test perfect forward secrecy
Preconditions	• Two connected peers • Network packet capture software running
Test Steps	1. Capture network traffic during file transfer 2. After transfer completes, extract session keys (simulating compromise) 3. Perform another file transfer 4. Attempt to decrypt the second transfer with the first session's keys
Expected Results	• Session keys from first transfer should not be able to decrypt second transfer • Each file transfer should use different encryption keys

Test Case ID	SEC-003
Description	Test encryption during file transfer
Preconditions	• Two connected peers • Network packet capture software running
Test Steps	1. Share a text file with known plaintext content 2. On second device, download the file 3. Analyze captured network traffic 4. Search for plaintext content in the capture
Expected Results	• Plaintext content should not be visible in network traffic • File transfer should show encrypted data only

User Interface Tests

Test Case ID	UI-001
Description	Verify decrypted file viewing functionality
Preconditions	• Application with previously received encrypted files
Test Steps	1. Navigate to "Received Files" list 2. Click "View Decrypted" on a file 3. Observe what happens
Expected Results	• File should be decrypted temporarily • Appropriate application should open to display the file • After closing, temporary file should be removed • No decrypted copy should remain in the filesystem