Test Case 1: E-Government Password Authentication

- Scenario 1: The user selects the option to log in with his/her E-Government Password, enters his/her correct password, clicks on the "Login" button and successfully logs in.
- Scenario 2: User fails authentication with incorrect ID number with correct password
- Scenario 3: User, correct ID number with wrong password, authentication fails
- Scenario 4: The user changes their existing E-Government password for security and successfully creates a new E-Government password.
- Scenario 5: The user realizes that his/her account is temporarily locked due to many failed attempts and starts the "Password Recovery" process.

Test Case 2: Mobile Signature Verification

- Scenario 1: The user selects Mobile Signature as the authentication method with "TR Identity Number", "GSM Number" and "GSM Operator". The user completes the mobile signature process and accesses his/her account after successful authentication.

- Scenario 2: The user realizes that the signature app is not working or has access issues on their mobile device and cannot log in to resolve this issue.

- Scenario 3: The username realizes that the mobile signature code has expired and requests a new code. It then completes the verification process using the new code.

- Scenario 4: When the user forgets the password of the mobile signature application, the user takes action to reset or recover the password by initiating the relevant process.

- Scenario 5: The user cancels the authorization process during the mobile signature process or authorizes the process incorrectly, which makes the authentication process fail.

Test Case 3: Electronic Signature Verification

- Scenario 1: Users choose an electronic signature, known as E-Signature, to authenticate their identity. Thus, users can download the e-Government Gateway e-Signature Application on their computer and successfully access the E-Signature authentication.

- Scenario 2: The user cancels the authorization process during the e-signature process or authorizes the process incorrectly, which makes the authentication process fail.

- Scenario 3: When the user tries to log in with an electronic signature, if the information registered in the system does not match the information associated with the electronic signature, the login process fails.

- Scenario 4: The user realizes that the signature has expired and completes authentication by creating a new electronic signature or extending the time period.

- Scenario 5: The system warns the user when he/she enters the information required to create an electronic signature incorrectly. The user fills in the missing information and tries again.

Test Case 4: Turkish ID Card Verification

- Scenario 1: Users choose an electronic signature, known as a TC Identity Card, to authenticate their identity. Thus, users are linked to the Identity TC Number

system, download the e-Government Gateway Identity Card Application to your computer and successfully access E-Signature authentication.

- Scenario 2: The user finds that his/her ID Card cannot be read or recognized.

- Scenario 3: The user learns that his/her Turkish ID Card has expired and decides to get a new card.

- Scenario 4: The user realizes that his/her ID Card has been lost or stolen and reports the loss or theft.

- Scenario 5: The user realizes that his/her Turkish ID Card information does not match the information he/she entered into the system. If necessary, the user checks and updates their credentials.

Test Case 5: Internet Banking Authentication

- Scenario 1: Users prefer to use their existing Internet Banking credentials for authentication. Simply select the bank in the list and login with your Internet banking user account.

- Scenario 2: Authentication fails using an incorrect password, even if the user enters the correct username or ID number.

- Scenario 3: The user becomes unable to access their account or forgets their password. Creates a new password, enters the system and starts the password recovery process.

- Scenario 4: When using two-factor authentication, the user enters their username and password and then logs into the system via mobile app or SMS with the verification code.

- Scenario 5: After several login attempts, the user realizes that their account is locked and follows the steps to unlock it.

## Test Scenario Form

### General Information

| | | | |
|---|---|---|---|
| ID | 001 | Author. | Reza Dysta Satria |
| Name. | E-Government Incorrect Password Login | Related Requirement | Authentication in case the usernames enter the wrong password during password entry will fail. |
| Version | Version 20.11 | Commitments | TR Identity Number and password requirement |
| Objective | Whether the expected results are correct when usernames enter the wrong password to check that it is not. | | |

### Test Activities

| | |
|---|---|
| Test Environment | Testing should be done on a development or test server away from the live production environment. |
| Prerequisites | A correct ID number and a wrong password must have been created for the user. |
| Termination | • The test must be completed when authentication fails.<br><br>• The user notification or error message should indicate that authentication failed.<br><br>• The test result should be documented to inform the software developers or relevant teams about the error status. |

### Test Steps

1. Go to the E-Government login page.

2. Enter your Turkish ID Number.

3. After entering a valid ID number, enter an incorrect password.

4. After entering the password, click on "Login" or a similar button.

5. Review the response of the e-Government system. Record the user warning or error message.

6. If an error message appears, note the content of the message and the instructions given to the user. Also check that it is worded in a clear and understandable way that the user should understand that authentication has failed.

7. Verify that the system authentication failed due to incorrect password entry.

8. Save your records to save error conditions or test results.

## Test Results

| | |
|---|---|
| Expected Outcome | • Anyone entering an incorrect password should see an error message.<br>• The error message should indicate that the authentication process failed.<br>• Guidance should be given to assist the user to enter a correct password or reset their password. |
| Realized Result | • After entering an incorrect password, the error message is displayed as "Entering an incorrect password. Please review your password."<br>• The user was faced with the option to reset the password. |
| Result (Pass/Fail) | Passed |
| Error ID | EDH-001 |
| Test Conductor | Reza Dysta Satria |