

For **3-step authentication** to strengthen the security of information assets

BaroPAM Solution Integration Summary (Java)

Jan, 2024

III. Integration with BaroPAM application

1. BaroPAM integration API

1) Check JDK version

```
[root]# java -version
java version "1.7.0_121"
OpenJDK Runtime Environment (rhel-2.6.8.1.el5_11-x86_64 u121-b00)
OpenJDK 64-Bit Server VM (build 24.121-b00, mixed mode)
```

2) Integration API "barokey.jar" is located in ~/lib directory or set in classpath

```
[root] /home/tomcat/lib > ls -al
Total 4908
drwxr-xr-x 2 root root 4096 May 8 11:25 .
drwxr-xr-x 5 root root 4096 May 9 15:12 ..
-rw----- 1 root root 116 May 13 2015 .bash_history
-rw-r--r-- 1 root root 26074 Jun 20 20:49 barokey.jar
```

3) Set the "BAROPAM" environment variable used in the integration API "barokey.jar" in ".bash_profile"

```
export BAROPAM=/home/tomcat/conf/.baro_nurit
```

4) OTA key verification method

```
boolean bauth_key = barokey.verifyKEYL(String login_id, String phone_no, String cycle_time, String auth_key);
boolean bauth_key = barokey.verifyKEYP(String secure_key, String cycle_time, String auth_key);
```

Parameter	Description	Etc
login_id	Set the ID entered in the Login-ID field of the login screen.	
phone_no	Set smartphone numbers for each user only by numbers.	
secure_key	Set the secure key provided by the vendor.	
cycle_time	Set the generation cycle (3-60 seconds) of OTA key specified for each user.	
tkey	Set the OTA key entered in the password on the login screen.	

If the generation cycle of the OTA key specified for each user and the smartphone number is different from the generation period of the OTA key, verification may fail because the OTA key is different. information must match.

Since the OTA key, which is the authentication code used by BaroPAM, is written based on Java, the latest JDK 6.x or higher must be installed.

If it is not installed, you must install the latest JDK.

III. Integration with BaroPAM application

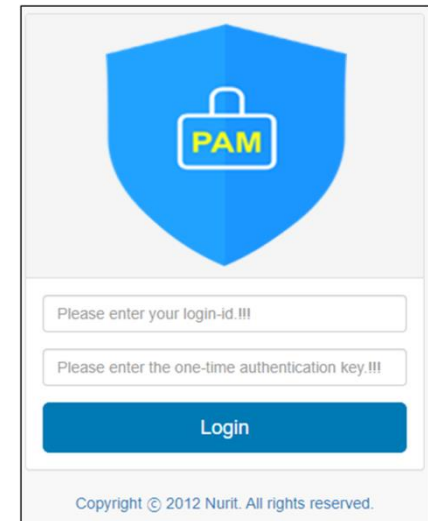
2. Ex) Application login program

When logging into the application, the user phone number (USER_PHONE), OTA key generation cycle (CYCLE_TIME), and last login time (LOGIN_TIME) columns must be added.

```
USER_PHONE    VARCHAR2(50) NOT NULL ,
CYCLE_TIME    VARCHAR2(2)  DEFAULT '30' ,
LOGIN_TIME    VARCHAR2(10) DEFAULT '0' ,
```

The reason for adding the login final time is to prepare for reuse and man-in-the-middle attacks by restricting only one user to log in to the same login-ID within the OTA key generation cycle, and the login is successful. In this case, the last login time must be updated.

```
.....
import com.barokey.barokey;
.....
try {
    // User information inquiry.
    bdto = udao.read(user_id);
    // When user information exists.
    if (bdto != null) {
        // Last login time Edit.
        long login_time = barokey.get_logintime(bdto.getCycle_time());
        // When the login last time is longer than the creation cycle.
        if (login_time > bdto.getLogin_time()) {
            // OTA key verification.
            bauth_key = barokey.verifyKEYL(bdto.getUser_id(), bdto.getUser_phone(), bdto.getCycle_time(), auth_key);
            // When the login last time is less than or equal to the creation cycle.
        } else {
            bauth_key = false;
        }
        // OTA key verification(Ok).
        if (bauth_key == true) {
            // Update last login time..
            udao.updateLoginTime(user_id, login_time);
        }
    }
}
.....
} catch(Exception e) {
    logger.info("Exception = [" + e + "]);
    e.printStackTrace();
} finally {
}
```



III. Integration with BaroPAM application

2. Ex) Application login program(BLE inteconnection)

To automatically log in to the application, the following Javascript must be added to the login screen.

```
<script type="text/javascript">
var bleWorker; // BLE worker
var isRunBleWorker = false;
let BaroBLE_SYSTEM = "BaroWEB"; // Application name

window.onload = function() {
  startBleWorker();
}
function startBleWorker() {
  var frm = document.frm_login;
  if (!window.Worker) {
    if (bleWorker) {
      stopBleWorker();
    }
    bleWorker = new Worker('./js/bleWorker.js');
    if (!isRunBleWorker && bleWorker) {
      isRunBleWorker = true;
    }
    bleWorker.postMessage({action:'start', system_name:BaroBLE_SYSTEM});
    bleWorker.onmessage = function(e) {
      const {action, user_id, password, auth_key} = event.data;
      if (action != "start") {
        frm.user_email.value = user_id;
        frm.password.value = password;
        frm.auth_key.value = auth_key;
        login(); // Validate input items when clicking the login button
      }
    };
  }
}

function stopBleWorker() {
  if (bleWorker) {
    bleWorker.postMessage({action:'stop', system_name:BaroBLE_SYSTEM});
    bleWorker.terminate();
    bleWorker = null;
    isRunBleWorker = false;
  }
}
.....
```

BaroPAM application plan

Password alone is never safe when logging in to all information assets, and **new application methods (additional authentication, password replacement, new password)** that can replace or additionally authenticate the password (secondary authentication) are required each time it is used.

1. Additional authentication

Apply OTA key as additional authentication (secondary authentication) other than login-ID and password (ID/PW/OTA)

```
frm.user_email.value = user_id;
frm.password.value = password;
frm.auth_key.value = auth_key;
```

2. Password replacement

Remove the password and replace it with a OTA key(ID/OTA)

```
frm.user_email.value = user_id;
frm.auth_key.value = auth_key;
```

3. New password

By combining the password and the OTA key, a new OTP is generated and applied for each OTA key generation cycle(ID/PW+OTA)

```
frm.user_email.value = user_id;
frm.password.value = password + auth_key;
```

III. Integration with BaroPAM application

3. Install the BaroPAM app and set up information

BaroPAM App Download

The BaroPAM solution is a security-optimized solution based on a Pluggable Authentication Module method that anyone can easily and directly apply to various OS and applications that require self-authentication to strengthen the security of information assets!

제한 횟수(1~10 times): 3
제한 시간(15~600 sec): 30
인증 방식(Key method): app512
인증 주기(Cycle time, 3~60 sec): 30
Secure key: [a]clchBvQdpj7b4PzBpM2DleBvmtHFV/

ACL 구분(Acc): BaroPAM setup - Application information
종간자(man-): 시스템명 BaroWEB
출급 일회용: 아이디 mc529@nurit.co.kr
비밀번호: 94720258, 12271111, 36534076, 26650119, 40762665

추가기능: 서버명 BaroPAM, Username WORKGROUP\wbaropam, 확장설정 Share, BLE 적용, 자동로그인, 화면잠자기, 데이터베이스 연동, 애플리케이션 BLE 연동, HTTP 연동

Register application information
System name: BaroWEB
Identify: mc529@nurit.co.kr
Auth key cycle time(3~60 Sec): 20

사용자 정보
성명: 이종필
회사: 누리아이티
부서: 기술지원부
직역: 이사
이메일: mc529@nurit.co.kr
휴대전화: 01027714076
생성주기: 20초
사용기간: 2021-06-29-9999-12-31
등록일시: 20210629141935653654 이종필
변경일시: 20220621085448204001 이종필

BaroPAM app can be used on Android 6.0 (Marshmallow) API 23, iOS 13.0 or higher, and does not support landscape mode. After installing the **BaroPAM** app, After installing the **BaroPAM** app, run the **BaroPAM** app, click the "One Time Auth key" button on the menu selection screen, and enter the "Cycle time, ID, and system name" set in the Application information in the "Register application information" screen of the **BaroPAM** app. You must enter the same information. If you set the app code (kr: Korean, en: English, jp: Japanese, cn: Chinese) on the **BaroPAM** app settings -> change screen settings screen, the **BaroPAM** app changes accordingly.

Message: The "OTA key" is incorrect because the date and time of the Android phone or iPhone are different from the current time.

Cause: This is caused by not using the time provided by the network for the Android or iPhone's date and time.

Action: For Android phones, go to "Settings" -> "General management" -> "Date and time" -> "Automatic date and time" and "Automatic time zone" -> "Allow" For iPhone, go to "Settings" -> "Date & Time" -> "Set Automatically" -> "Allow"

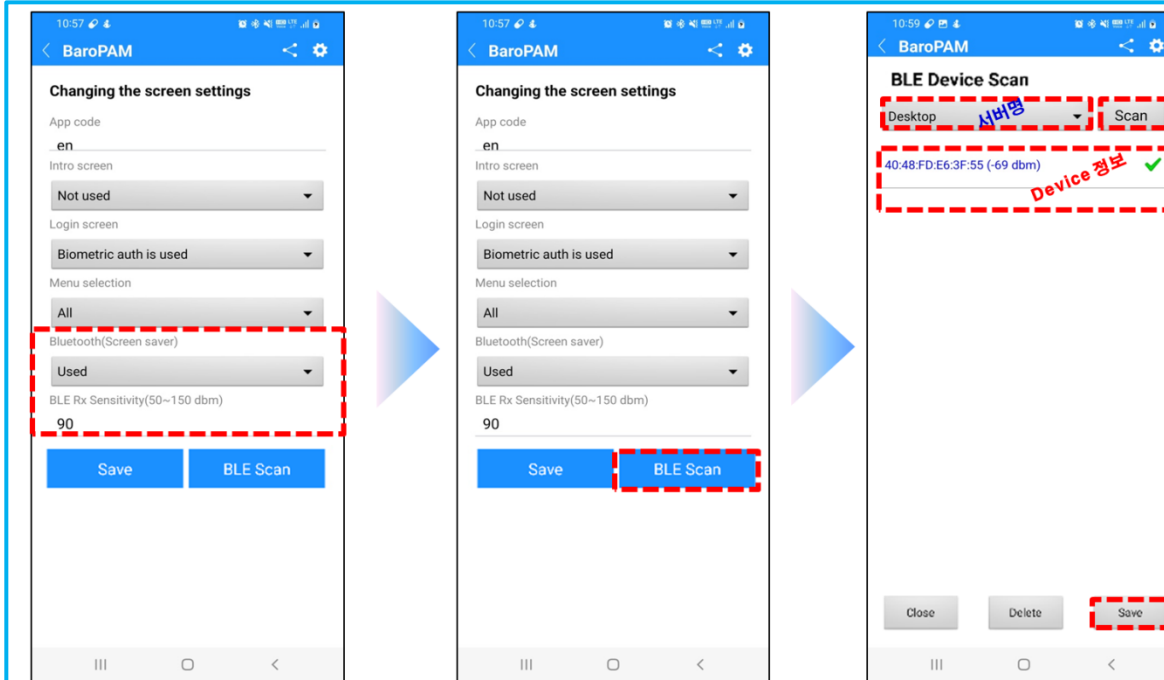
Message: If you cannot log in because the OTA key does not match.

Cause: BaroPAM is a time synchronization method, so the time of the phone and Server must be the same.

Action: Check if the phone and Servers time are correct.

III. Integration with BaroPAM application

4. USB Device Scan & Save



The image shows three sequential screenshots of the BaroPAM application interface. The first screenshot shows the 'Changing the screen settings' screen with the 'Bluetooth(Screen saver)' dropdown menu highlighted by a red dashed box. The second screenshot shows the same screen with the 'BLE Scan' button highlighted by a red dashed box. The third screenshot shows the 'BLE Device Scan' screen with a scanned device 'Desktop 시범용' and its MAC address '40:48:FD:E6:3F:55 (-69 dbm)' highlighted by a red dashed box. A red dashed box also highlights the 'Save' button at the bottom right of the scan screen.

Select the server name you want to scan (the server name registered on the server information registration screen) and click the "Scan" button to display the scanned BLE Device information at the bottom.

Click the "Save" button to save the scanned BLE Device information.

Click the "Delete" button to delete the saved BLE Device information.

Clicking the "Close" button closes the "BLE Device Scan" screen and returns to the "Change Screen Settings" screen.

Note) BLE reception sensitivity setting standard (unit: negative number)
PC/Notebook: 90 dbm, Thin client: 77 dbm

Message: When the BaroBLE function, screen saver lock prevention and automatic release functions do not work.

Cause: App permission is not set.

Action: Settings of the phone → Apps → BaroPAM → Permissions → Set permission allow in "Nearby Devices and Locations".

Message: A phenomenon in which the Bluetooth connection used by the mouse or keyboard of the desktop/notebook is disconnected.

Action: 1. How to use device manager

Run Windows Control Panel → Devices → Devices and Printers → Right-click on the connected USB icon 'Properties' → Select Bluetooth Low Energy GATT Ready HID Device → Uncheck Allow the computer to turn off this device to save power

2. Change power options

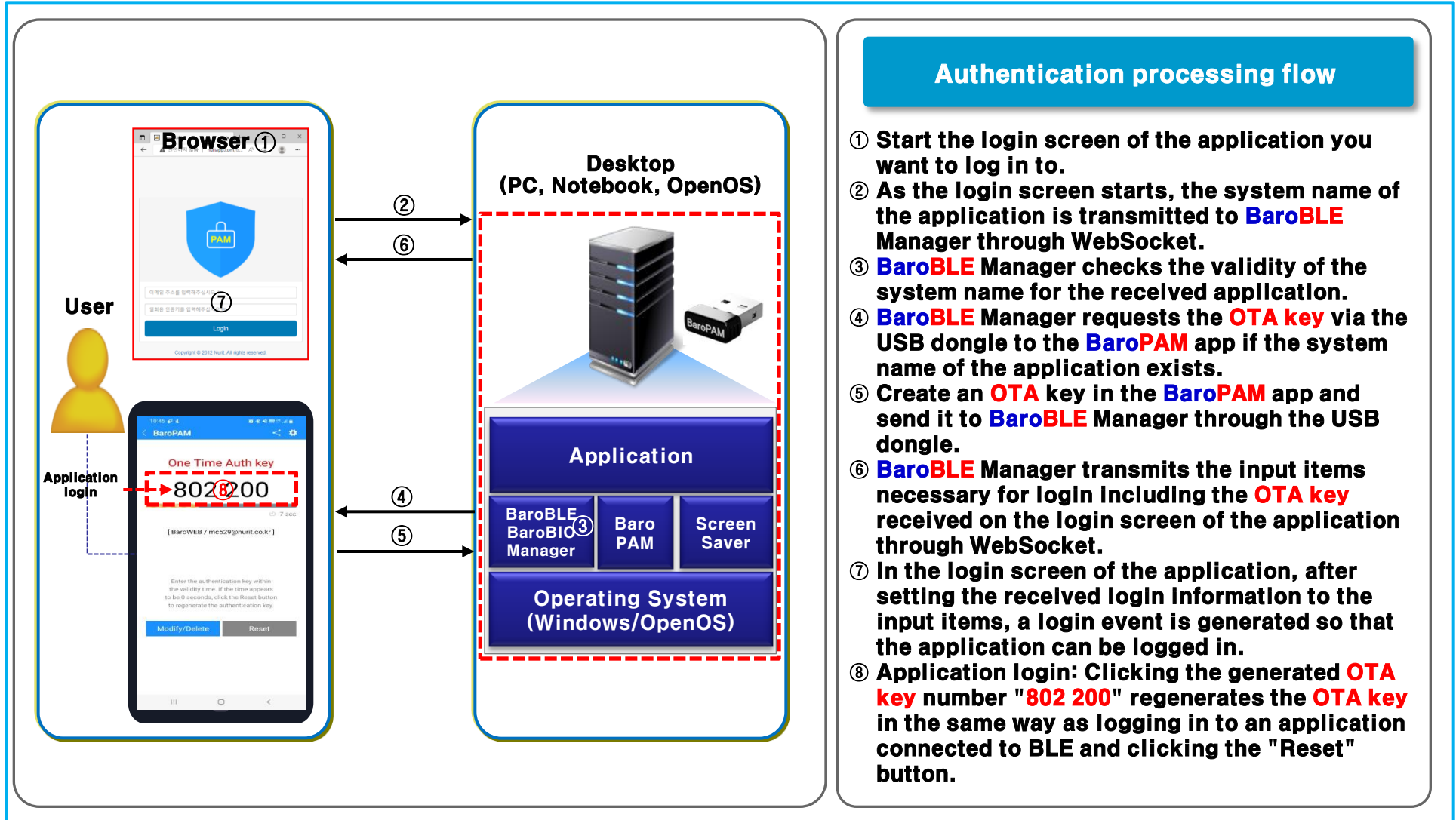
Run Windows Control Panel → Power Options → Change Settings → Change Advanced Power Management Options Settings → USB Settings (Set USB Selective Power Saving Mode) → Battery: Disabled / Power Usage: Disabled

3. Change Bluetooth device settings

Run Windows Control Panel → Bluetooth and other devices → Add Bluetooth option on the right side of the screen → Check Allow Bluetooth devices to find this PC → Apply → OK

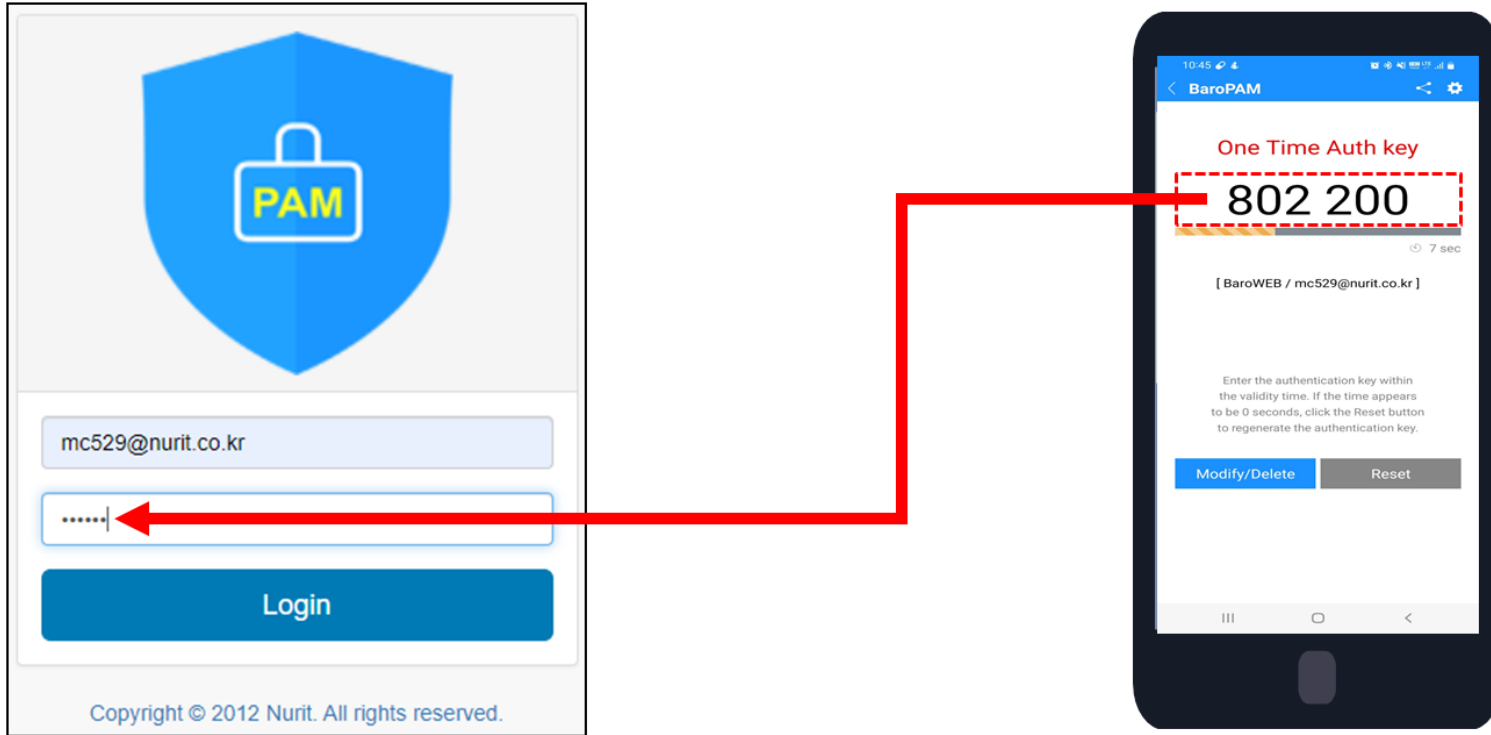
III. Integration with BaroPAM application

5. Integration with BaroPAM app and BaroBLE



III. Integration with BaroPAM application

6. Application login



When logging in to applications such as ERP/Groupware/Electronic payment/Portal, enter the login-ID and generate a **OTA key** in the **BaroPAM** app. After entering the generated **OTA key**, click the Login button to log in to the application.

Password you don't need to remember!
BaroPAM will be with you.

Thank You!

www.nurit.co.kr
mc529@nurit.co.kr