“iAM Smart” Developer Guide
for
iAM Smart Personal Code Verifier

Version: *1.0.1*

APRIL 2025

Document Revision History

Ver. No.	Release Date	Section Affected	Summary of changes
1.0.0	20 August 2024		Initial release
1.0.1	24 April 2025	3.1, 3.2	Update screenshots

Table of Contents

Terms and Conditions

The Digital Policy Office ("DPO") has the sole discretion to amend or vary the Reference Sample Coding and the Developer Guide from time to time.

The Reference Sample Coding and the contents of the Developer Guide remain the property of, and shall not be reproduced in whole or in part without the express permission of the Government of the HKSAR ("HKSARG"). Information provided by the Developer Guide and all the associated intellectual property rights are retained by HKSARG.

Organisations and their contractors (and sub-contractors, if applicable) (hereafter referred as users) may use the Reference Sample Coding and the Developer Guide for the purpose of designing, developing, testing and running of their self-developed applications. By using the Reference Sample Coding and the Developer Guide, users agree not to sue HKSARG and agree to indemnify, defend and hold harmless HKSARG, its officers and employees from any and all third-party claims, liability, damages and/or costs (including but not limited to, legal fees) arising from the use of the Reference Sample Coding and the Developer Guide.

HKSARG will not be liable for any direct, indirect, incidental, special or consequential damages of any kind resulting from the use of or inability to use the Reference Sample Coding and information provided by the Developer Guide.

Modifications of the Reference Sample Coding by users may be required if any third-party libraries or technologies that the Reference Sample Coding adopted are no longer available due to product end of life, incompatibility issue, technology deprecation or other reasons.

During the implementation of self-developed applications, users shall observe and comply with the Personal Data (Privacy) Ordinance (Cap. 486) in handling personal data collected from the iAM Smart Personal Code, if any.

Users agree to abide the usage terms and conditions specified in this form before releasing the Reference Sample Coding and the Developer Guide to their contractors (and sub-contractors, if applicable).

Definitions

The following terms and abbreviations are used in this document.

Terms / Abbreviations	Definition
Digital Certificate for the Personal Code	Digital certificate issued by Recognized Certification Authority to sign for the Personal Code, Verifier can use the public key of this certificate to verify the integrity and authenticity of the digital signature embedded in the Personal Code.
"iAM Smart Personal Code", "Personal Code"	"iAM Smart Personal Code" facilitates "iAM Smart" users to present their partial personal data in the form of a QR code during verification and registration processes, without the need to disclose excessive personal details by utilizing an identity card.
"iAM Smart" System	The "iAM Smart" mobile app and backend services provide the one-stop personalised digital services platform, which enables users to log in and use online services by their personal mobile phone in a smart and convenient way.
Owner	"iAM Smart" users presenting the QR Code.
Reference Sample Coding	Sample code snippet presented in this Developer Guide.
Verifier	Third party scanning the Personal Code using the "iAM Smart" mobile app or third-party self-developed application.

1. Introduction

This developer guide aims to introduce the workflow from the aspect of the owner or verifier of the iAM Smart Personal Code ("Personal Code"), prerequisites and technical details of the Personal Code for the developer to implement their self-developed applications.

The Personal Code allows users to display their partial personal data for verification purposes, without the need to present their identity document and disclose excessive personal information.

There are two ways to verify the Personal Code:

1. iAM Smart Mobile Application
2. Third-party self-developed application

2. Adoption of Personal Code

Application is not required for the adoption of "iAM Smart Personal Code" but subscription to DPO for latest update is recommended. During the implementation, it is essential for developers to comply with the Personal Data (Privacy) Ordinance (Cap. 486) including the six data protection principles in the collection, holding, accuracy, retention period, security, privacy policy and access to and correction of personal data. The Digital Policy Office expressly disclaims and excludes any obligation, responsibility or liability of whatever nature for any loss, damage costs or expenses (whether direct, indirect or consequential) arising from the use of or failure to use of the "iAM Smart Personal Code".

To receive the latest updates regarding the "iAM Smart Personal Code" such as renewal of the public certificates for validation, please send an email to iamsmart_api@digitalpolicy.gov.hk with the subject line "Subscription to iAM Smart Personal Code." If you wish to unsubscribe, kindly use the subject line "Un-subscription to iAM Smart Personal Code". It is important to note that the registered email address is solely used for the purpose of processing subscription applications and receiving updates related to the "iAM Smart Personal Code".

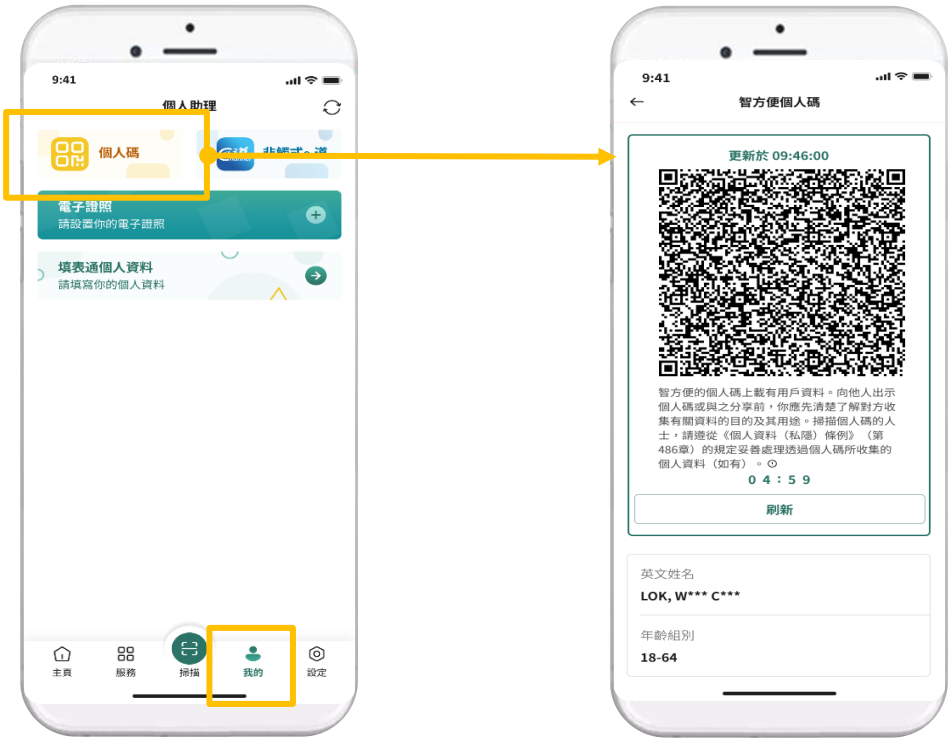
After subscription, we will inform you the latest development about the Personal Code, such as notice of certificate renewal, etc.

3. User Journey

This part will focus on the user journey for Personal Code in the aspect of owner and verifier. The following wireframes illustrate the detailed process for presenting and scanning the Personal Code.

3.1 Owner

1. User accesses the Personal Code function by clicking the “Personal Code” icon in the Personal Assistant page after logging in the “iAM Smart” mobile app.
2. Then "iAM Smart" System will generate the Personal Code and display it for identification purpose.



3.2 Verifier

(For “iAM Smart” mobile app)

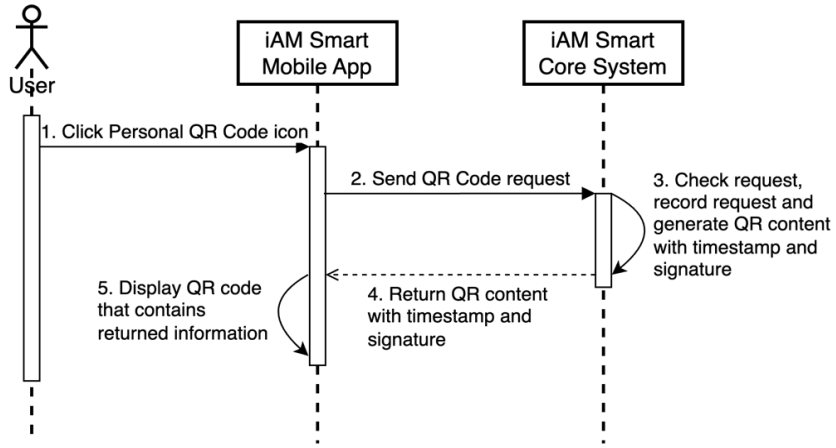
1. Verifier uses the scanner function embedded in “iAM Smart” mobile app to scan and verify the Personal Code.
2. “iAM Smart” will then display the partial identity information of the “iAM Smart” user. The information collected from the Personal Code should be handled in strict adherence to relevant provisions of the Personal Data (Privacy) Ordinance (Cap. 486).

(For third-party scanner)

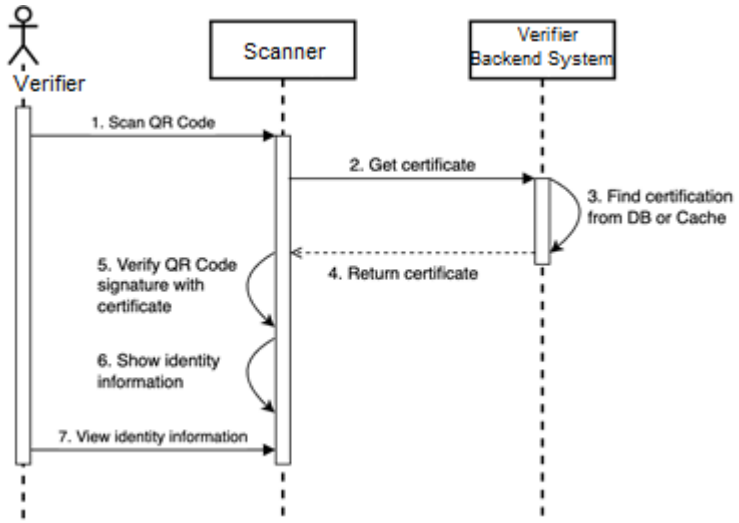
1. Verifier obtains and installs the latest Digital Certificate for the Personal Code from the Sandbox website (https://iamsmart.cyberport.hk).
2. Install the latest digital certificate into the self-developed QR code scanner.
3. Verifier uses the self-developed QR code scanner to scan the Personal Code.
4. The self-developed QR code scanner validates the scanned QR code content by verifying the digital signature embedded in the Personal Code using the pre-installed digital certificate.
5. The self-developed QR code scanner displays or stores the identity information of the “iAM Smart” user. The information collected from the Personal Code should be handled in strict adherence to relevant provisions of the Personal Data (Privacy) Ordinance (Cap. 486).

3.3 Sequential Diagrams

3.3.1 Get Personal Code Content



3.3.2 Validate and View Personal Code Content



4. Contents of the Personal Code

4.1 Data Specification

Field Name	Field Type	Field Description	Code Range	Format	Remark
body	Object	The JSON element representing the signed components including hash, engName, ageGroup and generatedDateTime		JSON Object	
hash	TEXT	Masked hash value for person identification			
engName	TEXT	Masked English name of the user			
ageGroup	TEXT	Age group of the user	11-17; 18-64; 65+		
generatedDateTime	TEXT	Date and time when the Personal Code is generated		dd/mm/yyyy HH:mm:ss	
sn	TEXT	Serial number of the digital certificate			
signature	TEXT	Digital signature of the Personal Code			
type	TEXT	QR code type	LPQR		Only one type of QR code at present
version	TEXT	The version number of the Personal Code	1		

5. Sample Personal Code for testing

Content of the above sample Personal Code:


```
{
    "body":{
        "hash":"OvwahDm8vN**********************************",
        "engName":"LOK, W*** C****",
        "ageGroup":"18-64",
        "generatedDateTime":"01/01/2024 09:00:00"
    },
    "signature":"A3y8M+se9SbNBm0BEPYjIK3tp7Z+TfFsr/SQNIjBPGhgBse
    a1IPgLdkVeXuRLIohGLtMy2UK0anSLmCznqmIMYTSm3nddij8EYfhzP
    Mtfjv2tAROv+uIupfTTGS4Ox70Gp8Ee6cP+JLZNsgcjvMD2zimdUYU5a
    DIUPoaPp6RJvkH4tbSOJbds0X4rsK1j775byKSLeHKZ1PYYhDNIIgpYW
    rClYCUii/Yz8CRx5kPZDJxTX+oNUvlUNEQpGxTcjSKp5r3/kW+oWKY
    cvQPAHQ6rdPr/PjibIotVE+jWC5/1kEJ74kXZbJffPljsP6iakDd3LuZO4Ml
    KoJ2mG0hxxZXPw==",
    "sn":"1sa8h8o",
    "type":"LPQR",
    "version":"1"
}
```


The above sample Personal Code is signed by testing certificate for illustration purpose only.

6. Validation of the Personal Code

6.1 Procedures to verify the QR Code text

1. Check the type and version number of the Personal Code

   (a) The type (Field Name = "type") must equal to "LPQR". At present, only "LPQR" type is available. More types will be introduced from time to time in order to support different business cases. Developers should refer to the data specification in the latest Developer Guide, and check the QR code type to be used for individual business cases.

   (b) The version (Field Name = "version") may change from time to time in order to support different business cases. The current version number is "1" and will be changed when more data is embedded in the body (Field Name = "body") representing the data elements to be signed. Developers should refer to the data specification in the latest Developer Guide, and check the minimum version required for individual business cases.

2. Check the Timestamp (Field Name = "generatedDateTime")

   To ensure the Personal Code is up-to-date, it is suggested to check the timestamp of the Personal Code. The validity period of the Personal Code should be set suitably addressing the requirements of individual business cases.

3. Check the serial number of the public certificate (Field Name = "sn")

   Each Personal Code will be digitally signed by the "iAM Smart" System using the Digital Certificate for the Personal Code. The subject of the current certificate is as below:

   CN = IAM SMART
   OU = IDREF
   OU = 21924873
   OU = OTH HKSARG-DPO
   OU = DIGITAL POLICY OFFICE, HKSARG
   O = DS ID-CERT CLASS 5 (488682)
   C = HK

   The serial number of the public certificate used to generate the Personal Code can be found in "sn" field of the Personal Code. The serial number format of the public certificate is converted from Hexadecimal to Base32Hex string. Developers are suggested to convert and check the serial number presented on the

Personal Code if see the Personal Code is genuine. The serial number of the current public certificate is "**78a54559**".

The current public certificate remains effective until **17:27:13 on 12 August 2027**. DPO will publish a new public certificate before the expiry, and announce the effective date when the certificate renewal will be conducted, through the subscription email. The developers shall develop their application to incorporate at least two (2) such public certificates at the same time for verification, and checking at least two (2) serial numbers in turn in order to maintain the serviceability to the public during the public certificate rollover..

4. Verify the digital signature

   To ensure the integrity and authenticity of the Personal Code, the scanner application should use the latest public certificate to verify the signature.

   The signature of the Personal Code adopts the "SHA256withRSA" algorithm. The content for the signature includes all data elements under the "body" element of the Personal Code:

```
{
    "hash":"HYDjCcrpJW**********************************",
    "engName":"LOK, W*** C****",
    "ageGroup":"18-64",
    "generatedDateTime":"01/07/2024 09:41:00"
}
```

   The developer shall retrieve the body element and sort the data elements inside the body object in ascending alphabetical order of the element name, and then generate the hash for verification.

   The following is the sample JAVA program code to verify the signature:

```
List<String> bodyKeyList = new ArrayList<String>(bodyMap.keySet());
Collections.sort(bodyKeyList, (key1, key2) -> key1.compareTo(key2));
StringBuilder sortedBodyString = new StringBuilder("{");
for (String key : bodyKeyList) {
sortedBodyString.append("\"" +
key).append("\":\"").append(bodyMap.get(key)).append("\",");
}
sortedBodyString.deleteCharAt(sortedBodyString .length() - 1);
sortedBodyString.append("}");
```

   where the "bodyMap" is composed of the value of the "body" object in map type; and sortedBodyString is a value used for signature verification.

```
Signature signature = Signature.getInstance("SHA256withRSA");
signature.initVerify(publicKey);
signature.update(hashedData);
boolean isValid = signature.verify(signedHash);
```

where the "hashedData" is composed of the value of " sortedBodyString" in string type, and hashed by SHA256.

6.2 Exception Handling

Scenario	Error Description	Suggested Action
Unrecognised Code	The QR Code is not Personal Code, or Personal Code with supported type and compatible version.	Show error message and remind user to present the correct Personal Code
Expired Code	The Personal Code has been produced beyond the validity period from the present time.	Show error message and remind user to refresh the Personal Code manually
Invalid Code	The QR code can be recognised but tampered. The integrity checking failed using digital signature validation.	Show error message

Unrecognised Code　　Expired Code　　Invalid Code

7 Appendix

7.1 Public Certificate

The most recent version of the public certificate for the Personal Code can be found on the iAM Smart sandbox programme website (https://iamsmart.cyberport.hk). To maintain the integrity and authenticity of the Personal Code, developers are advised it to use the valid public certificate for content verification along with the digital signature.

The public certificate details can also be accessed through HK DigiSign (https://www.dg-sign.com/eng/download_reg_cert.htm) by searching the English Name "IAM SMART". The certificate is valid for 3 years as usual. It is recommended to check the validity period and the latest version of the public certificate regularly.

The current public certificate remains effective until **17:27:13 on 12 August 2027**. DPO will publish a new public certificate before the expiry, and announce the effective date when the certificate renewal will be conducted, through the subscription email. The developers shall develop their application to incorporate at least two (2) such public certificates at the same time for verification, and checking at least two (2) serial numbers in turn in order to maintain the serviceability to the public during the public certificate rollover.