智方便
iAM Smart

"iAM Smart" Sandbox Programme

Mobile App Integration, Encryption, Decryption

智方便 iAM Smart | SANDBOX Programme

Agenda

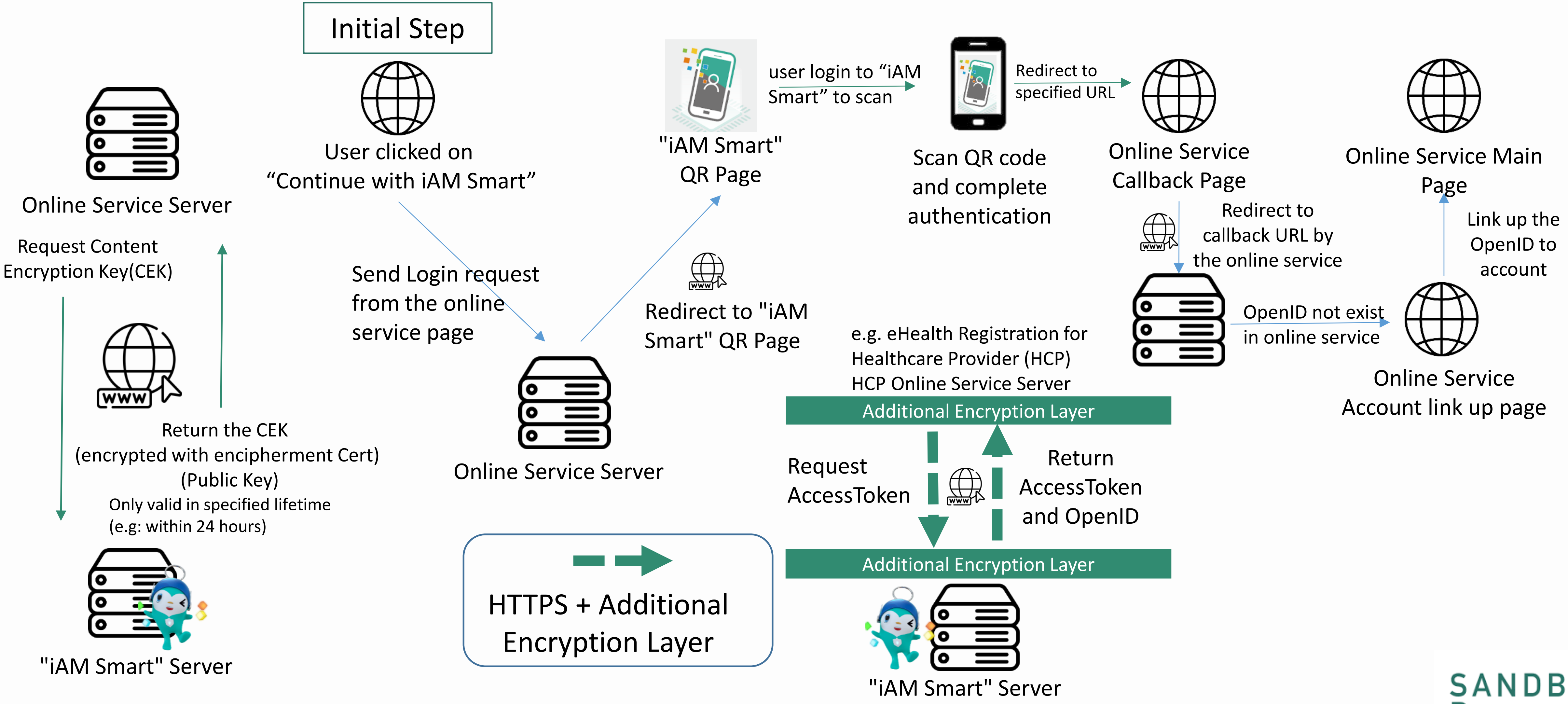
- API Structure Overview
- Mobile App Integration (Android/iOS)
- Self-Service Portal and Testing App
- Encryption and Decryption (KEK/CEK)
- Practical Tips
- Quiz

Disclaimer

The video is intended for preliminary introduction. It shall not be followed as the technical instruction. “iAM Smart” Sandbox Programme would not guarantee the correctness and timeliness of data which could be possibly affected by the modification of development. Development team shall follow the guidelines and policies or enquire to related professionals if any safety apprehension.

API Structure Overview

"iAM Smart" API Structure



Initial Step
Online Service Server
User clicked on "Continue with iAM Smart"
"iAM Smart" QR Page
user login to "iAM Smart" to scan
Scan QR code and complete authentication
Redirect to specified URL
Online Service Callback Page
Online Service Main Page
Request Content Encryption Key(CEK)
Send Login request from the online service page
Redirect to "iAM Smart" QR Page
Redirect to callback URL by the online service
Link up the OpenID to account
OpenID not exist in online service
Online Service Account link up page
WWW
Return the CEK
(encrypted with encipherment Cert)
(Public Key)
Only valid in specified lifetime
(e.g: within 24 hours)
Online Service Server
e.g. eHealth Registration for Healthcare Provider (HCP)
HCP Online Service Server
Additional Encryption Layer
Request AccessToken
Return AccessToken and OpenID
Additional Encryption Layer
"iAM Smart" Server
HTTPS + Additional Encryption Layer
"iAM Smart" Server

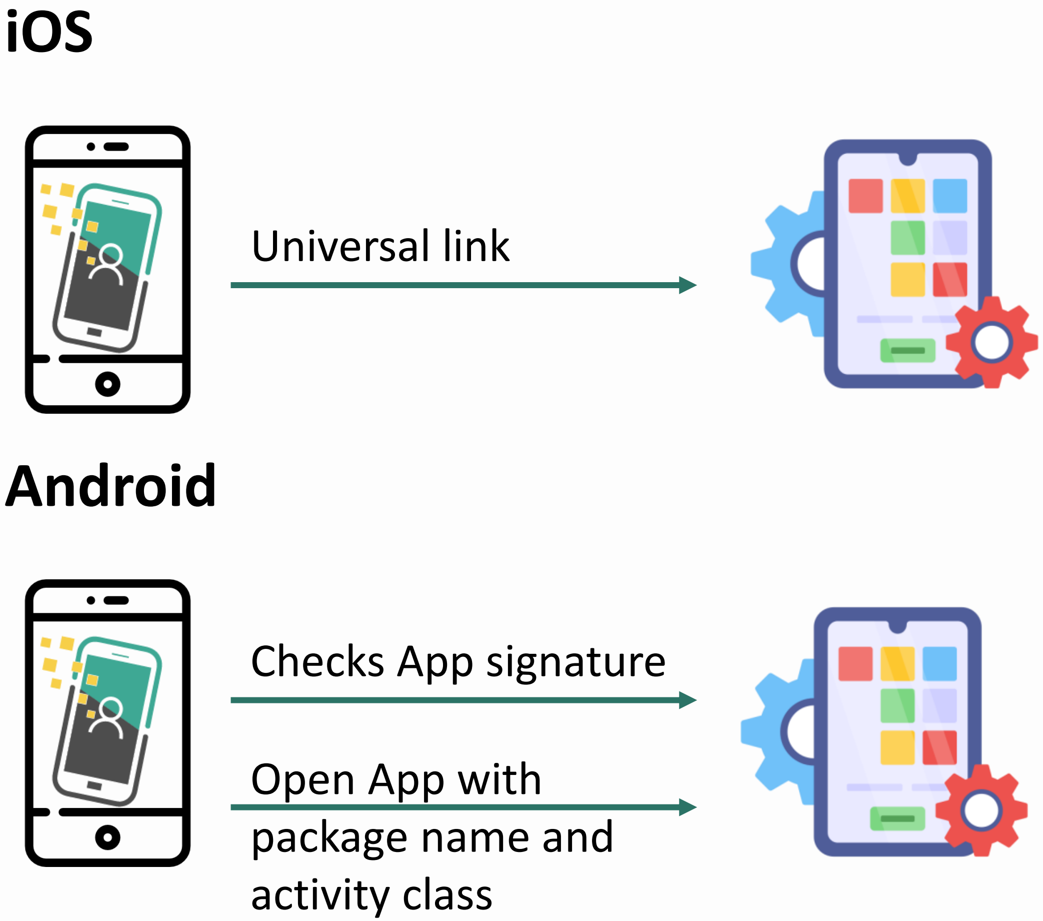
Mobile App Integration (Android/iOS)

Mobile App Integration with “iAM Smart” App

iOS - Universal Links

Universal Links are Apple's solution for deep linking on iOS, allowing a single link to direct users to specific content within an app or a webpage.

Android - Package name
it does not rely on App Link, making it compatible with both Android devices that have and do not have Google Mobile Services (GMS) enabled.



iOS

Universal link

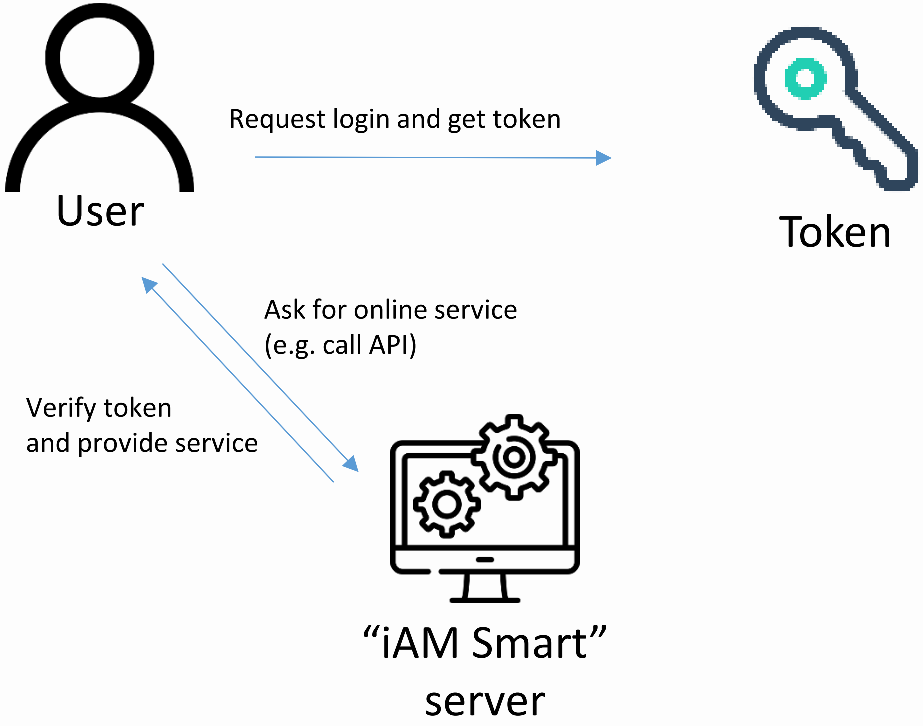
Android

Checks App signature

Open App with package name and activity class

OAuth 2.0 Like Flow

OAuth 2.0 authentication framework



Introduction

“iAM Smart” APIs are implemented by making reference to OAuth 2.0 having similar flow on authorisation with custom parameter.

FAQ

1. Does “iAM Smart” support OpenID Connect?
>> No.

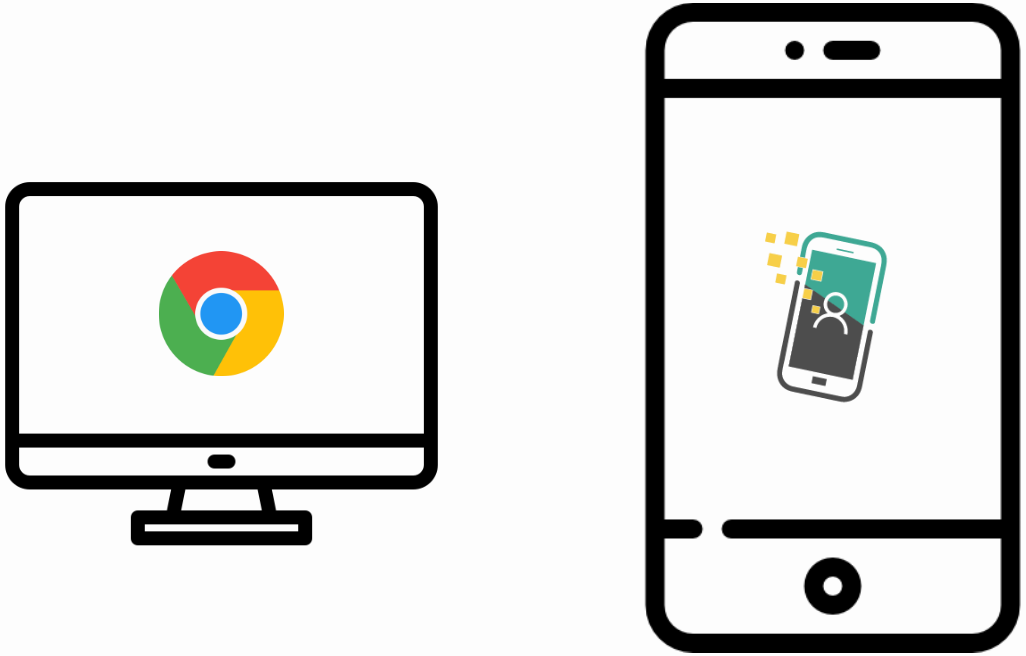
2. Could we re-use the existing OAuth library/ integrate with the identity solutions?
>> No. Online service shall develop the connector to support other identity solutions.

智方便 iAM Smart

Same Device and Different Device for “iAM Smart” Integration

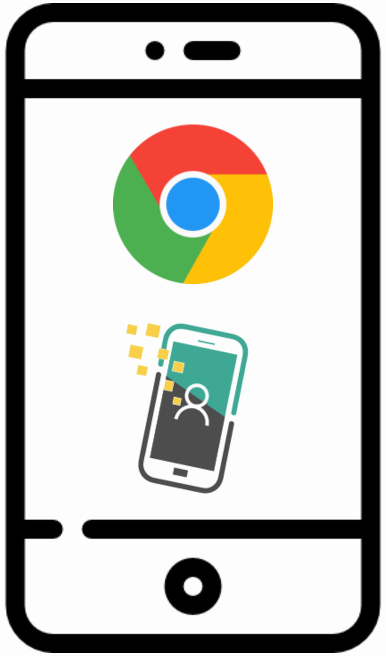
Different Device

Online Service and “iAM Smart” App are not installed in the same mobile phone.



Same Device

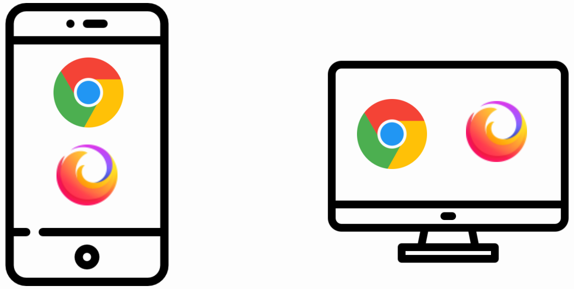
The online service and “iAM Smart” App are installed in the same mobile phone.



Online Service Web vs App

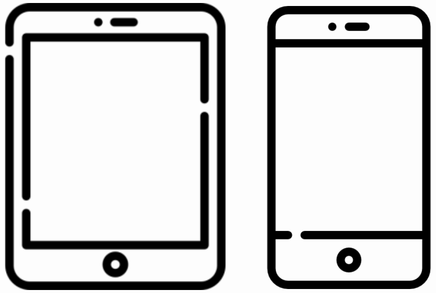
Online Service Website

User accesses the online service with an external browser and triggers "iAM Smart" function in the external browser.



Online Service Mobile App

The online service triggers "iAM Smart" function from App which supports **universal link/ explicit intent**.



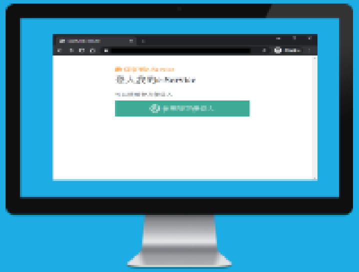
Note:

- Different API flow and APIs for online service website and online service mobile app.
- In-app browser/ Webview/ Mini-APP/ SFSafariViewController/ Android Custom Tabs also are considered as App and should follow the mobile app integration.
- Online Service Mobile App shall not call broker page for integration, which will introduce broken journey. (unable to return to Online Service Mobile App)

智方便 iAM Smart

High level Overview

A) Online Service Website and "iAM Smart" Mobile App in Different Devices


Online Service Website

"iAM Smart" Mobile App

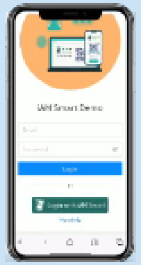
B) Online Service Website and "iAM Smart" Mobile App in Same Mobile Phone

Single mobile Phone with :

1. "iAM Smart" Mobile App
2. Browser to access Online Service webpage

C) Online Service Mobile App and "iAM Smart" Mobile App in Different Devices

"iAM Smart" Mobile App in one device


Online Service Mobile App in another device

D) Online Service Mobile App and "iAM Smart" Mobile App in Same Mobile Phone

Single mobile Phone with :

1. "iAM Smart" Mobile App
2. Online Service Mobile App

High level Overview

The mobile integration through the system and mobile benefits from security, functionality, and stability.

- Improved Functionality: Allows the app to leverage external services, enhancing capabilities (e.g., real-time data, location services).

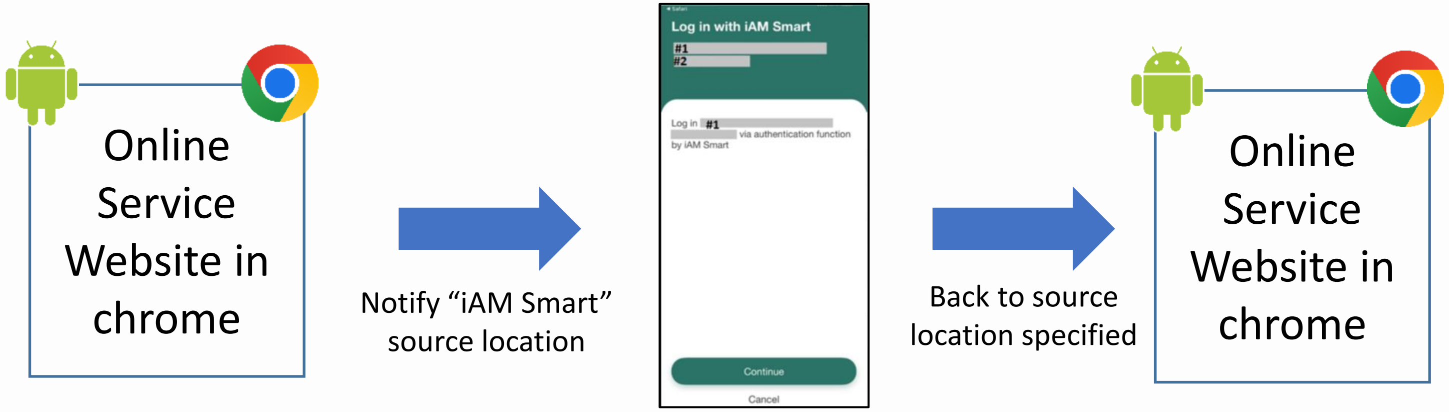
- Streamlined Workflows: Automates processes and reduces manual intervention, improving efficiency.

- Enhanced User Engagement: Provides personalized experiences by integrating user data and preferences.

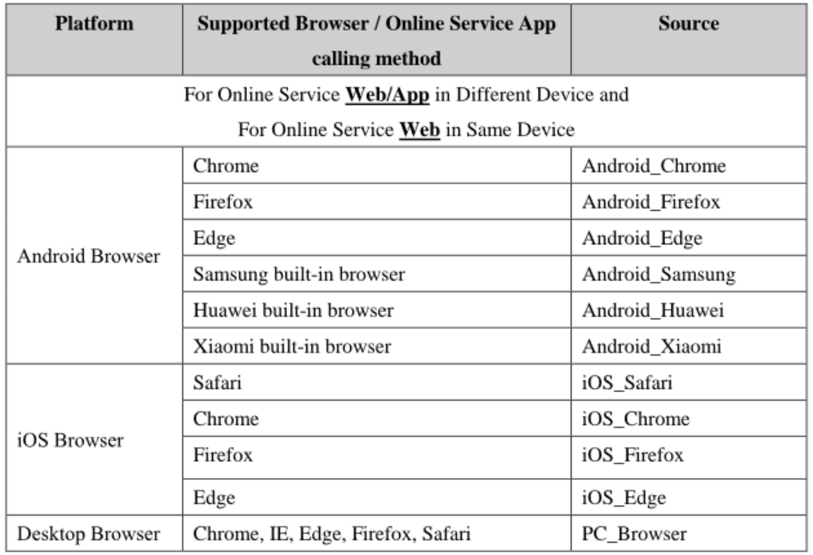
Parameter - Source

Online Service shall detect the user's devices for the sources parameter. The parameter is for "iAM Smart" App redirect to which app/ platforms.

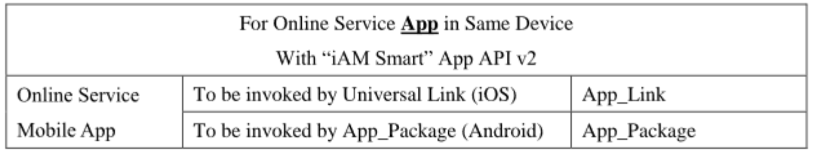
Misconfiguration will introduce broken user journey.


Online Service Website in chrome
Notify "iAM Smart" source location
Log in with iAM Smart
Continue
Cancel
Back to source location specified
Online Service Website in chrome

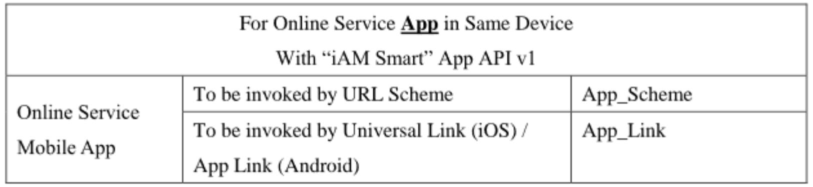
"iAM Smart" broker page & App



Platform	Supported Browser / Online Service App calling method	Source
For Online Service **Web/App** in Different Device and For Online Service **Web** in Same Device		
Android Browser	Chrome	Android_Chrome
	Firefox	Android_Firefox
	Edge	Android_Edge
	Samsung built-in browser	Android_Samsung
	Huawei built-in browser	Android_Huawei
	Xiaomi built-in browser	Android_Xiaomi
iOS Browser	Safari	iOS_Safari
	Chrome	iOS_Chrome
	Firefox	iOS_Firefox
	Edge	iOS_Edge
Desktop Browser	Chrome, IE, Edge, Firefox, Safari	PC_Browser



For Online Service **App** in Same Device With "iAM Smart" App API v2		
Online Service Mobile App	To be invoked by Universal Link (iOS)	App_Link
	To be invoked by App_Package (Android)	App_Package



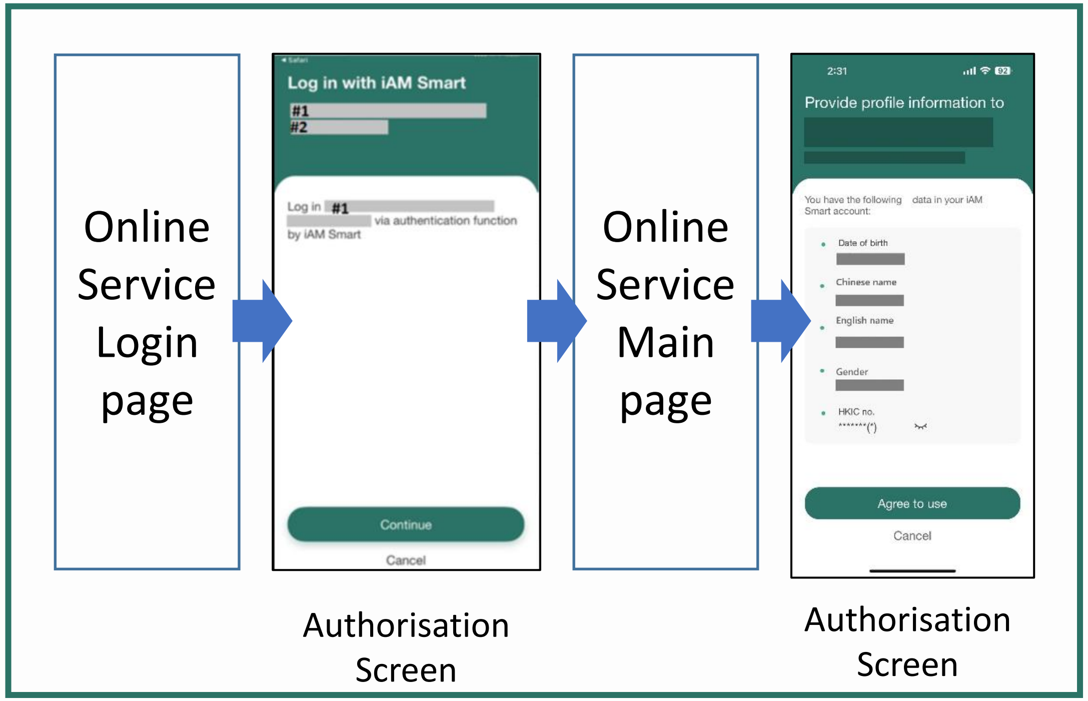
For Online Service **App** in Same Device With "iAM Smart" App API v1		
Online Service Mobile App	To be invoked by URL Scheme	App_Scheme
	To be invoked by Universal Link (iOS) / App Link (Android)	App_Link

Reference:
Section B: Supported Value at Source Parameter" in "iAM Smart" API Specification

API with Service Login vs Anonymous APIs

"iAM Smart" APIs with Service Login

The APIs design for the online service **support** login with "iAM Smart".



Log in #1 via authentication function by iAM Smart

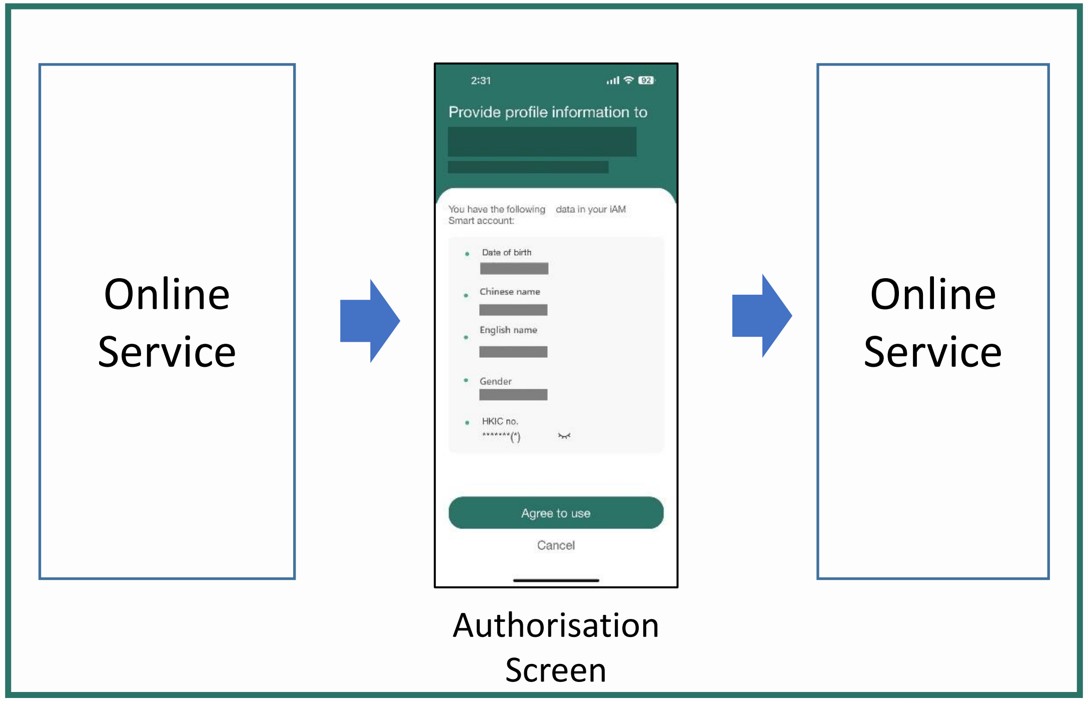
Provide profile information to

You have the following data in your iAM Smart account:

*******(*)

Anonymous APIs (without Service Login)

The APIs design for the online service that **do not support** login with "iAM Smart".



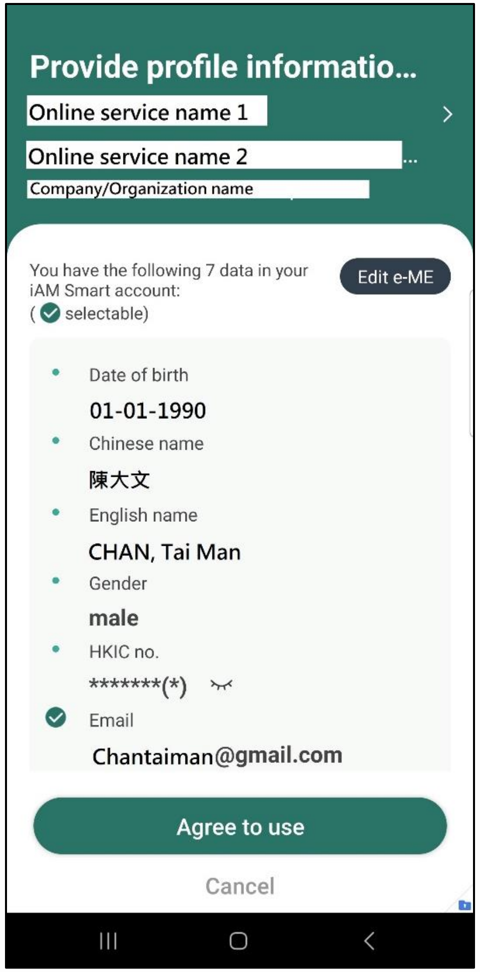
Provide profile information to

You have the following data in your iAM Smart account:

*******(*)

智方便 iAM Smart

Profile Fields & e-ME Fields



Provide profile informatio...

Online service name 1

Online service name 2

Company/Organization name

You have the following 7 data in your iAM Smart account:
(✓ selectable)

Edit e-ME

- Date of birth
  01-01-1990
- Chinese name
  陳大文
- English name
  CHAN, Tai Man
- Gender
  male
- HKIC no.
  *******(*)
- ✓ Email
  Chantaiman@gmail.com

Agree to use

Cancel

"iAM Smart" App Authorisation Page
(with profile fields)

←Profile Fields: (for identity verification)

Profile fields are the "iAM Smart" users' account information captured and verified during the registration. Requesting profile information for identity verification purpose should result in displaying as non-editable in the online service. Those information could be:

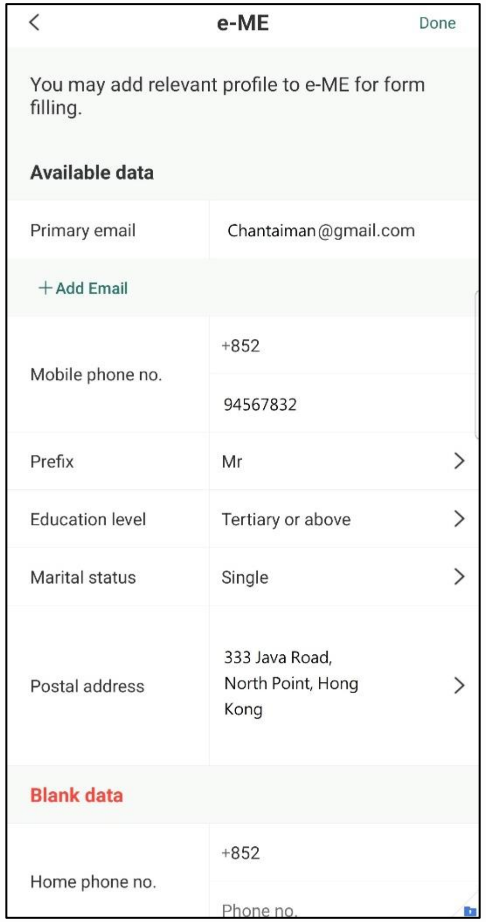
- Account opening
- Account matching
- Remote account opening

e-ME Fields: (for Form Filling)→

The e-ME fields contain profile fields and additional information that user voluntarily input for better online form filling experience. The data fill by "e-ME" fields shall editable by users.

Full list of "iAM Smart" data fields:
https://www.iamsmart.gov.hk/tc/about.html#this

Edit e-ME Page



< e-ME Done

You may add relevant profile to e-ME for form filling.

Available data

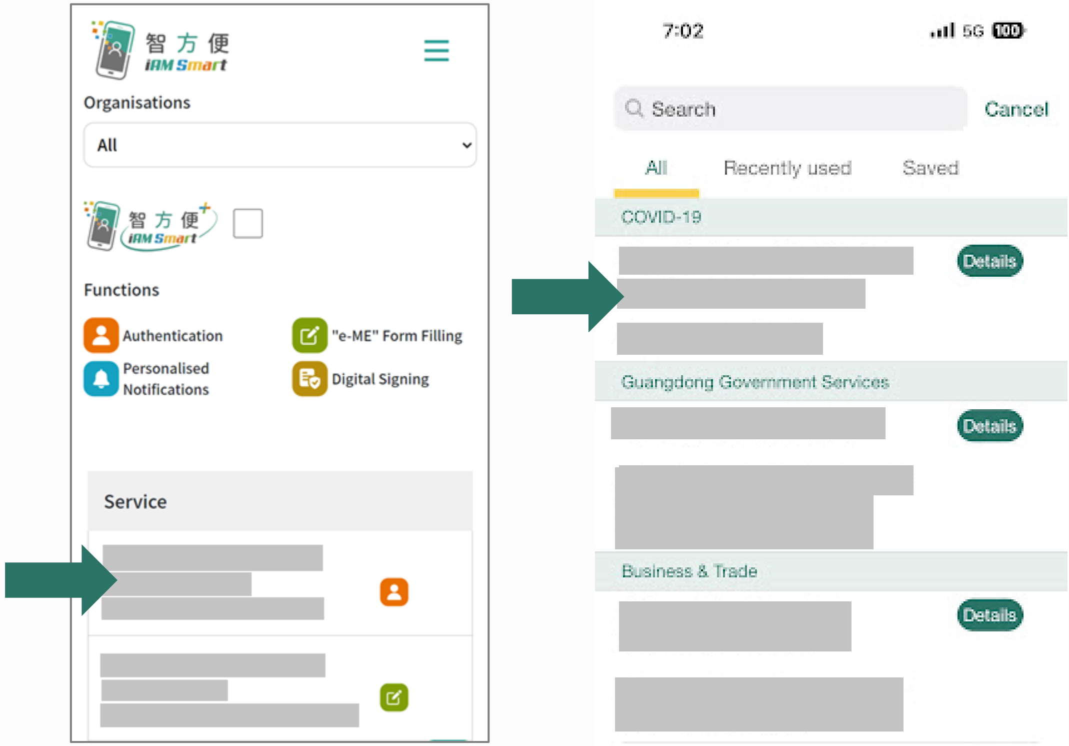
Primary email	Chantaiman@gmail.com
+ Add Email	
Mobile phone no.	+852 94567832
Prefix	Mr >
Education level	Tertiary or above >
Marital status	Single >
Postal address	333 Java Road, North Point, Hong Kong >

Blank data

Home phone no.	+852 Phone no.

智 方 便 iAM Smart Service Catalogue and Landing Page Design

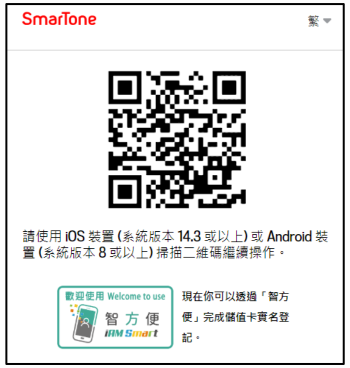
Both service catalogues in “iAM Smart” App and “iAM Smart” website will list the online services for user to trigger. Online Service shall submit the design of landing page of this trigger in early stage for comment.



Design 1: “iAM Smart” Badge

It explains how “iAM Smart” is integrated into the system with the “iAM Smart” badge.

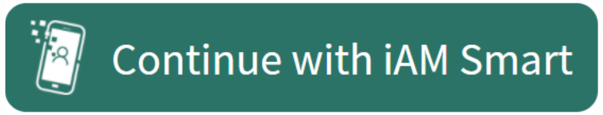
歡迎使用 Welcome to use
智 方 便
iAM Smart

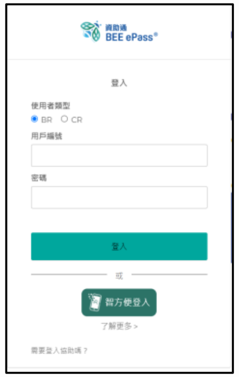


請使用 iOS 裝置 (系統版本 14.3 或以上) 或 Android 裝置 (系統版本 8 或以上) 掃描二維碼繼續操作。

現在你可以透過「智方便」完成儲值卡實名登記。

Design 2: Trigger “iAM Smart” functions

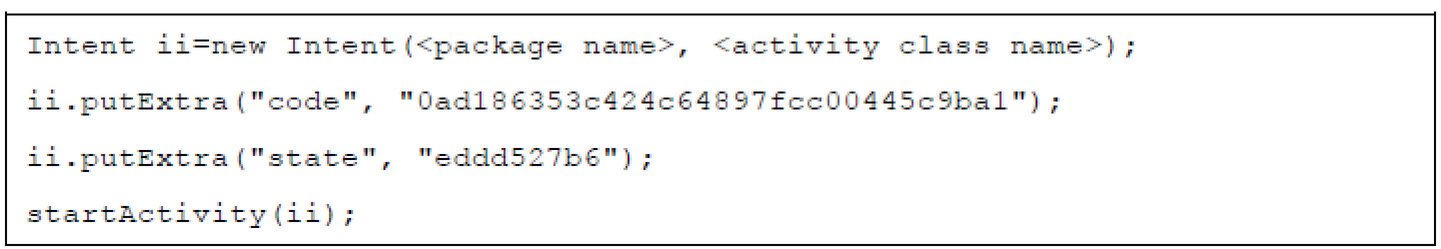




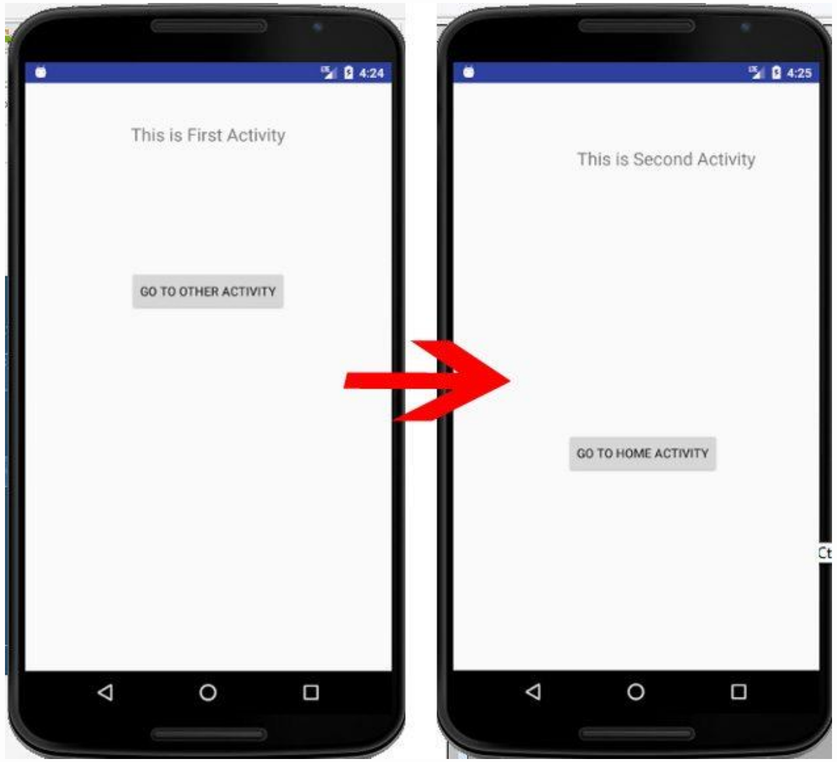
Ref: https://www.iamsmart.gov.hk/en/e-service-non_gov.html

Android – Package Name

By creating the intent with package name and activity class, the specific target activity would be invoked.



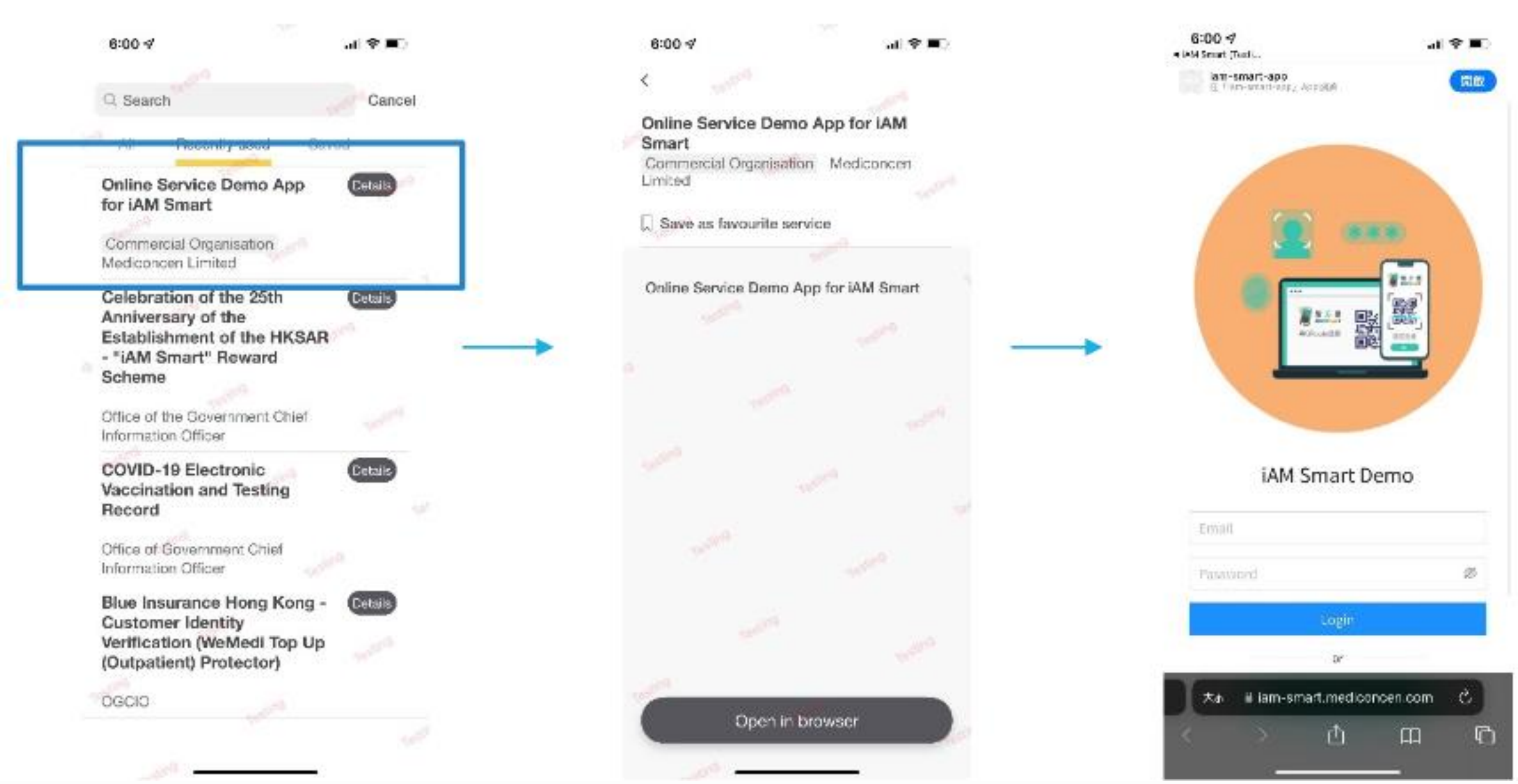
```
Intent ii=new Intent(<package name>, <activity class name>);
ii.putExtra("code", "0ad186353c424c64897fcc00445c9ba1");
ii.putExtra("state", "eddd527b6");
startActivity(ii);
```



For proper management of the application, the package name shall be provided 3 months before.

iOS - Universal Link

Universal Link would be similar to the package name in Android which allows user to open the service through iAM Smart.



Online Service Demo App for iAM Smart
Commercial Organisation
Mediconcen Limited

Celebration of the 25th Anniversary of the Establishment of the HKSAR - "iAM Smart" Reward Scheme
Office of the Government Chief Information Officer

COVID-19 Electronic Vaccination and Testing Record
Office of Government Chief Information Officer

Blue Insurance Hong Kong - Customer Identity Verification (WeMedi Top Up (Outpatient) Protector)
OGCIO

Online Service Demo App for iAM Smart
Commercial Organisation Mediconcen Limited

□ Save as favourite service

Online Service Demo App for iAM Smart

iAM Smart Demo

The Universal Link shall be submitted before the application onboarding.

Once the link is approved by the self service portal. It would be available within a short effective time.

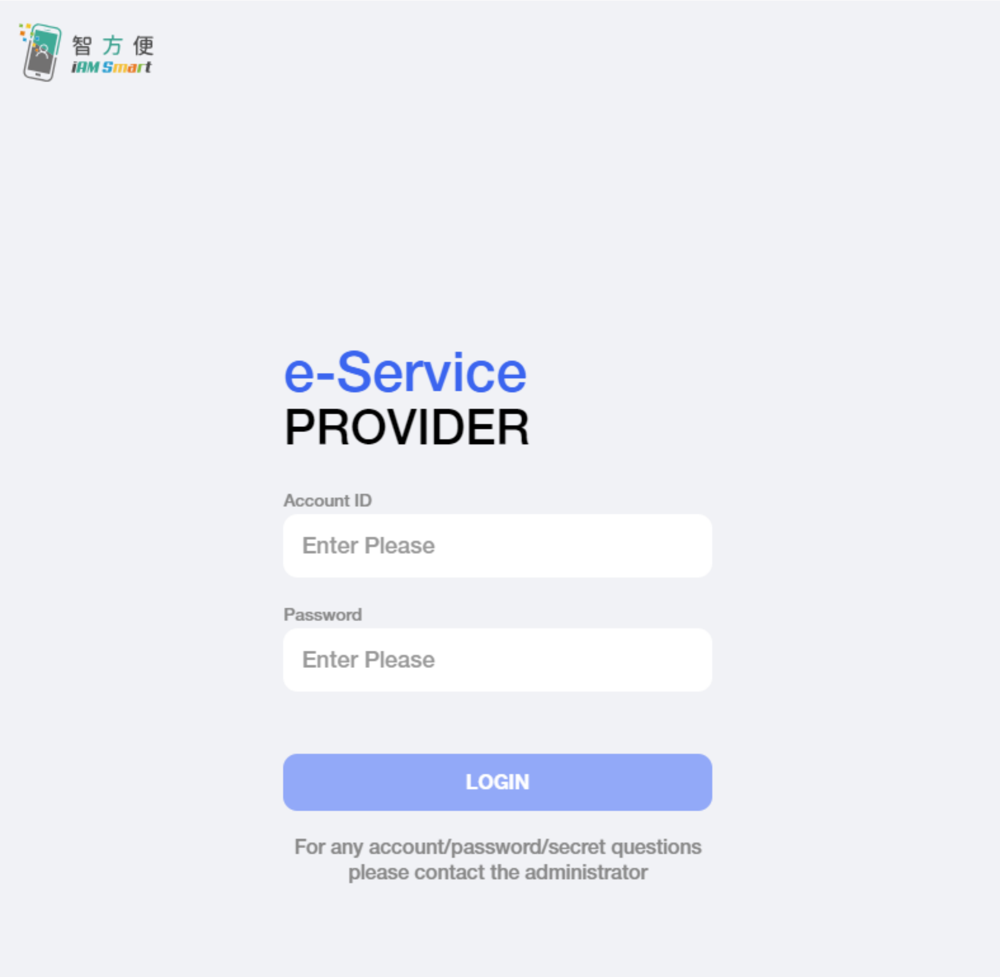
SANDBOX Programme

Self-Service Portal and Testing App

Self Service Portal

Major Functions:

- View integration information:
  - E.g. Client ID, Client Secret, approved API scopes, Service Catalogue records, etc.
- Each application (online service) has two set of accounts (1 set for Testing and 1 set for Production environments)
- Upload Encryption Certification (KEK)
- Maintain the whitelist for callback URI (RedirectURI)
- Maintain Creator and Approver Accounts



e-Service
PROVIDER

Account ID

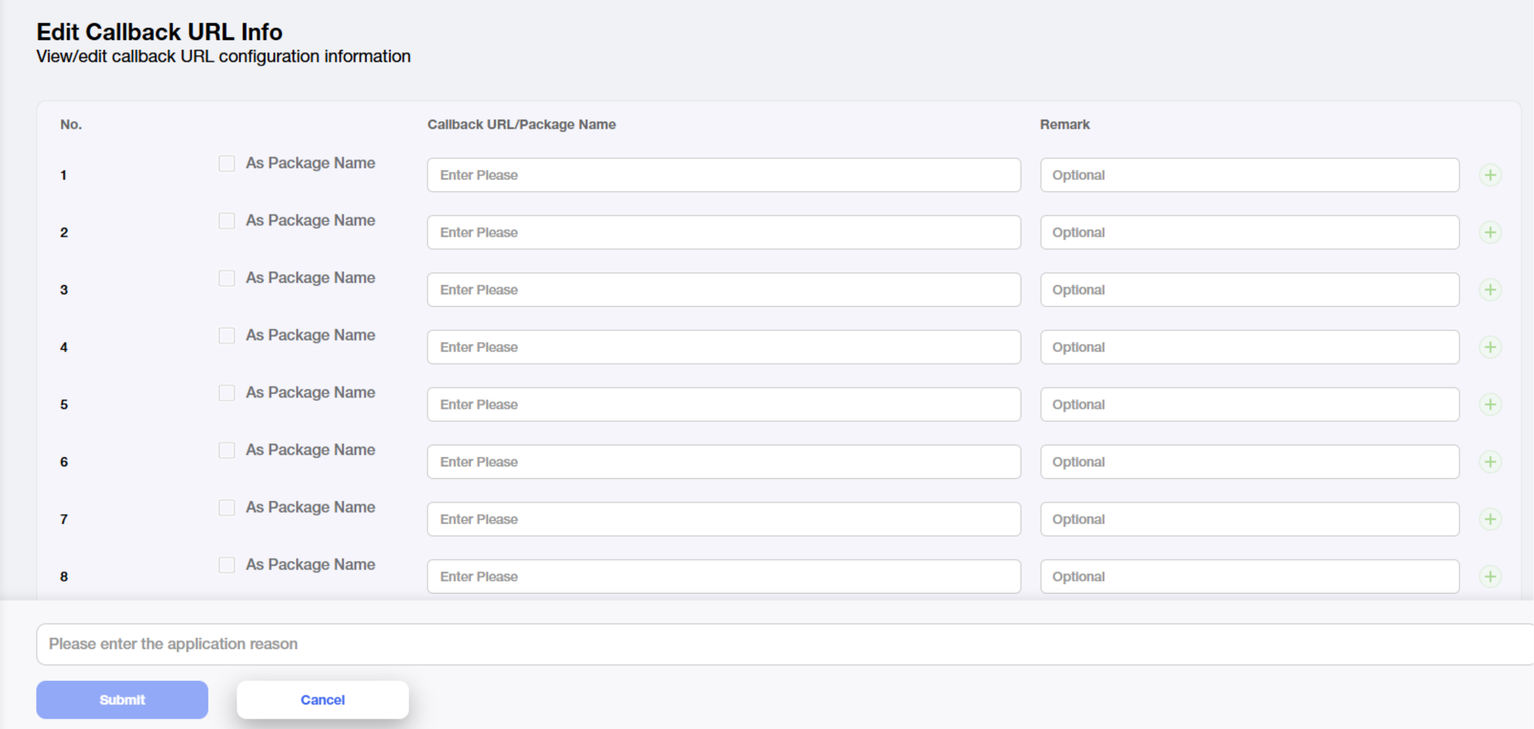
Enter Please

Password

Enter Please

For any account/password/secret questions please contact the administrator

Self Service Portal - Setup Callback URL



Edit Callback URL Info

View/edit callback URL configuration information

No.		Callback URL/Package Name	Remark	
1	□ As Package Name	Enter Please	Optional	+
2	□ As Package Name	Enter Please	Optional	+
3	□ As Package Name	Enter Please	Optional	+
4	□ As Package Name	Enter Please	Optional	+
5	□ As Package Name	Enter Please	Optional	+
6	□ As Package Name	Enter Please	Optional	+
7	□ As Package Name	Enter Please	Optional	+
8	□ As Package Name	Enter Please	Optional	+

Please enter the application reason

Online Service is required to implement its own callback APIs to support the return of asynchronised API response from the iAM Smart System when invoking the corresponding iAM Smart APIs. Online service provider can setup their callback URL via Self Service Portal

Self Service Portal - Accounts and Roles

Administrator

The administrator for an online service (Client ID), nominated and specified in the application form. The administrator is responsible for managing the creator and approver accounts.

Creator

The creator created by administrator, who responsible to create change request for redirectURI (callback URI) and encryption certificate.

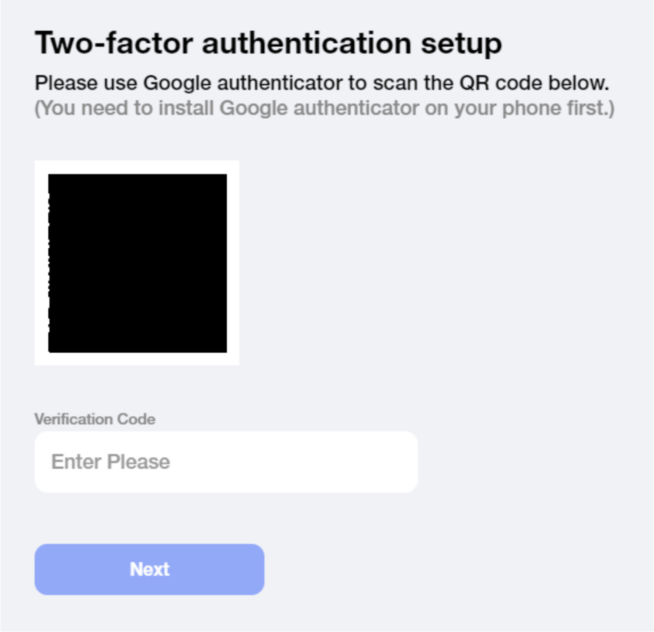
Approver

The approver created by administrator, who responsible to approver the change request created by creator.

Note: the account shall own by different team members.

Self Service Portal - Password for Setup Admin Accounts

1. Administrator, Creator and Approver will receive a password setup email.
2. Use (download if necessary) an authenticator mobile app to setup two-factor authentication.



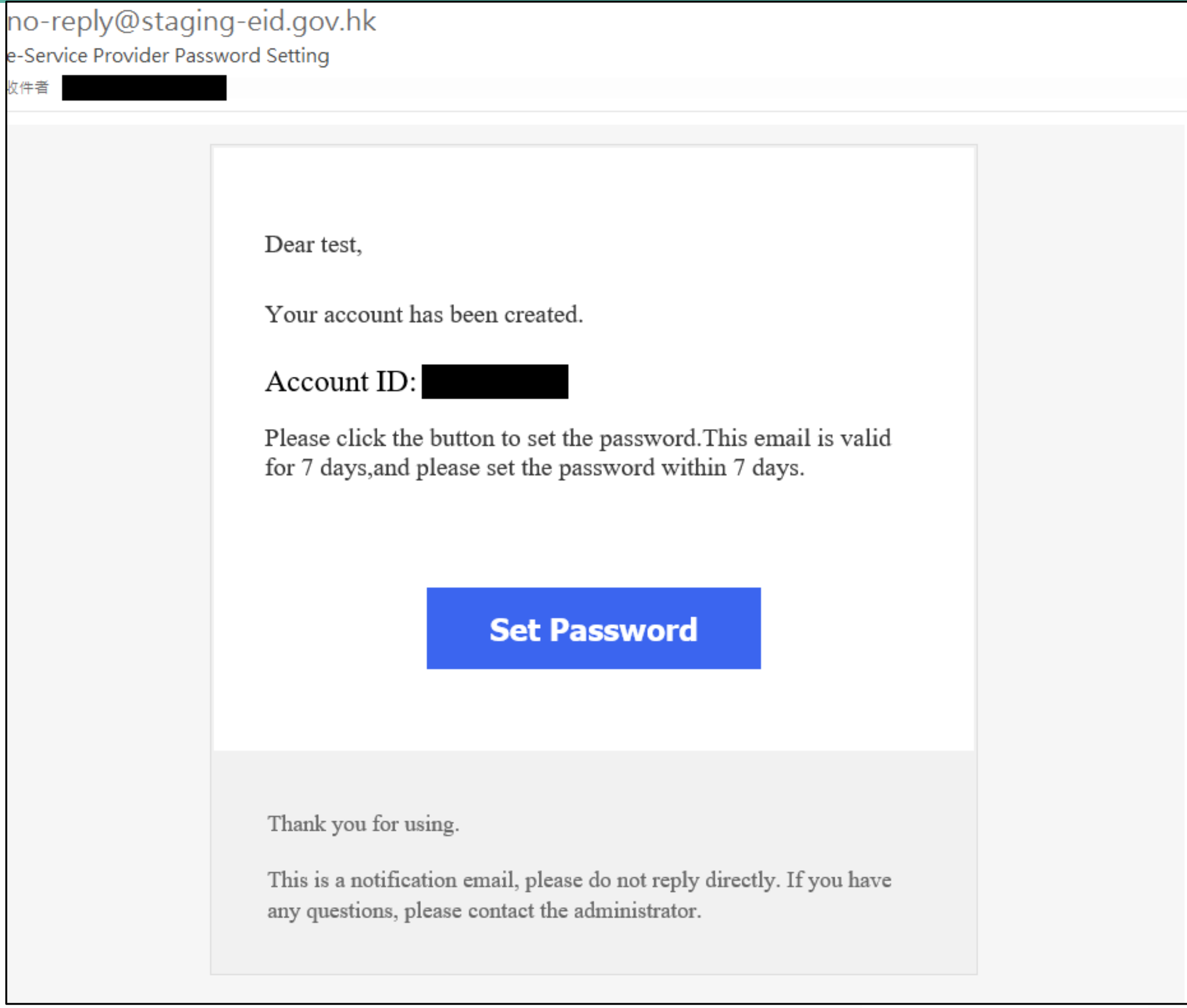
Two-factor authentication setup

Please use Google authenticator to scan the QR code below.
(You need to install Google authenticator on your phone first.)

[redacted]

Verification Code

Enter Please



no-reply@staging-eid.gov.hk
e-Service Provider Password Setting
收件者 [redacted]

Dear test,

Your account has been created.

Account ID: [redacted]

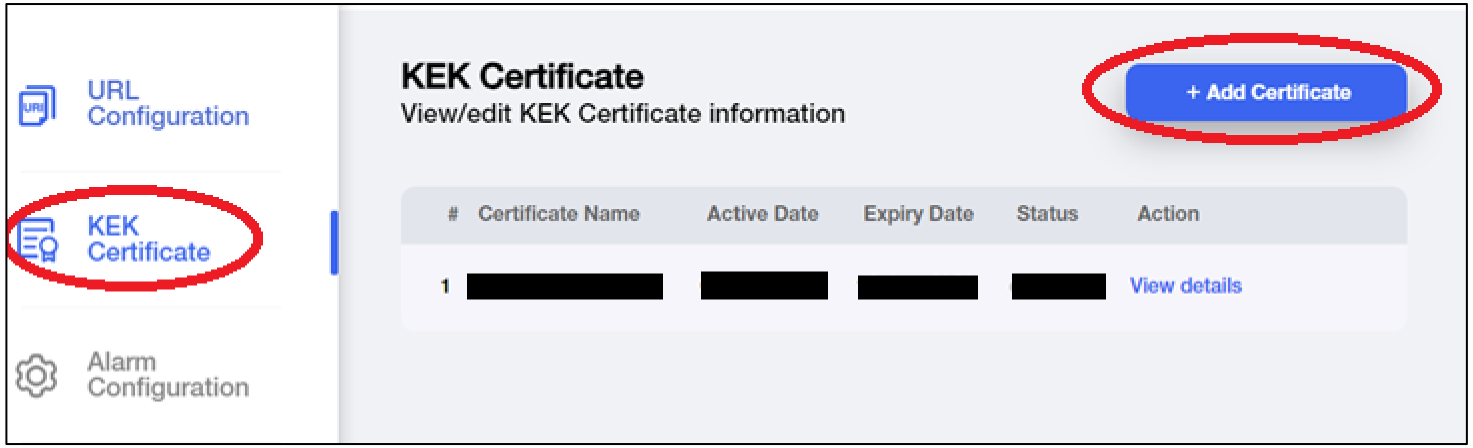
Please click the button to set the password.This email is valid for 7 days,and please set the password within 7 days.

Thank you for using.

This is a notification email, please do not reply directly. If you have any questions, please contact the administrator.

Self Service Portal - Creator: Upload Certificate (KEK) for Encryption

1. Select the KEK Certificate
2. Click “+ Add Certificate” button to proceed.

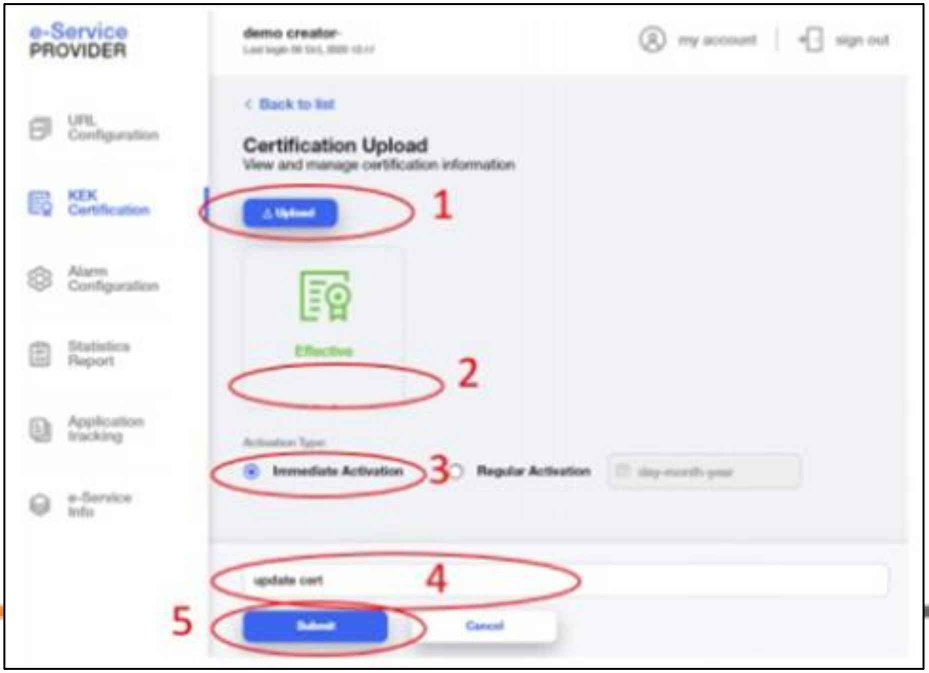


KEK Certificate

View/edit KEK Certificate information

#	Certificate Name	Active Date	Expiry Date	Status	Action
1	[redacted]	[redacted]	[redacted]	[redacted]	View details

1. Click the “Upload” button to select the certificate.
2. Verify the uploaded file.
3. Select the activation type.
4. Enter the description for reason
5. Click the “Submit” button for submitting the request to approver



demo creator

Certification Upload

View and manage certification information

Activation Type:

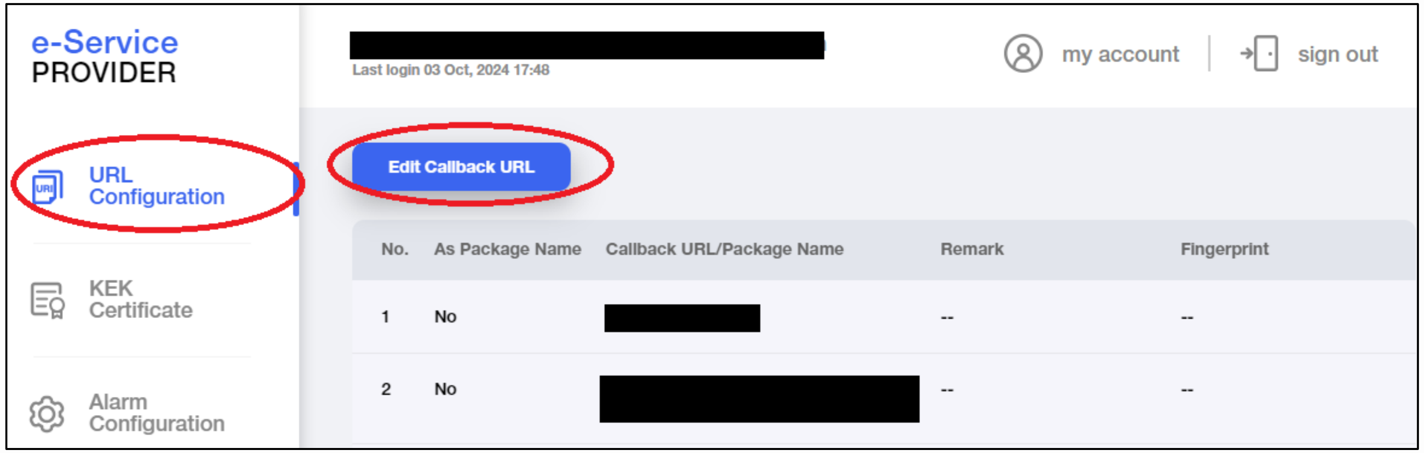
● Immediate Activation ○ Regular Activation day-month-year

update cert

Self Service Portal - Creator: Update redirectURI whitelist

Manage the redirectURI whitelist

1. Select the “URL Configuration” section.
2. Click the “Edit Callback URL” button to edit



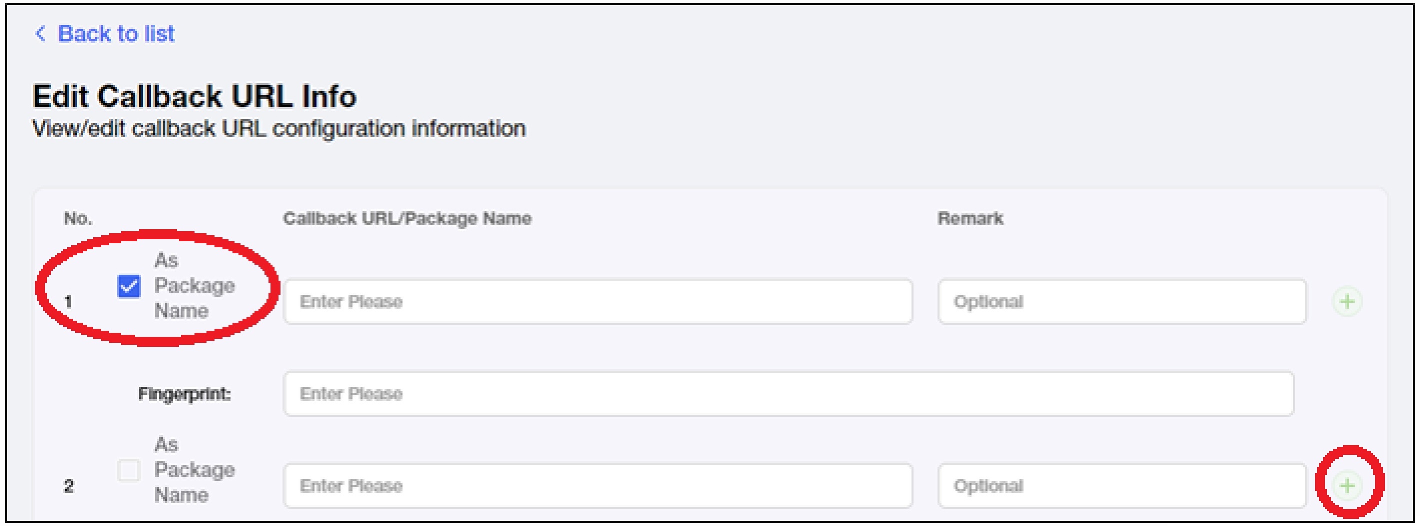
[redacted]

Last login 03 Oct, 2024 17:48

No.	As Package Name	Callback URL/Package Name	Remark	Fingerprint
1	No	[redacted]	--	--
2	No	[redacted]	--	--

Fill the form

1. Enter the callback URL(s) of the online service (including universal links/ verified applinks/ callback for authcode/ callbacks)
2. For Mobile App integration, please check “Package Name” and fill the package name and fingerprint



Edit Callback URL Info

View/edit callback URL configuration information

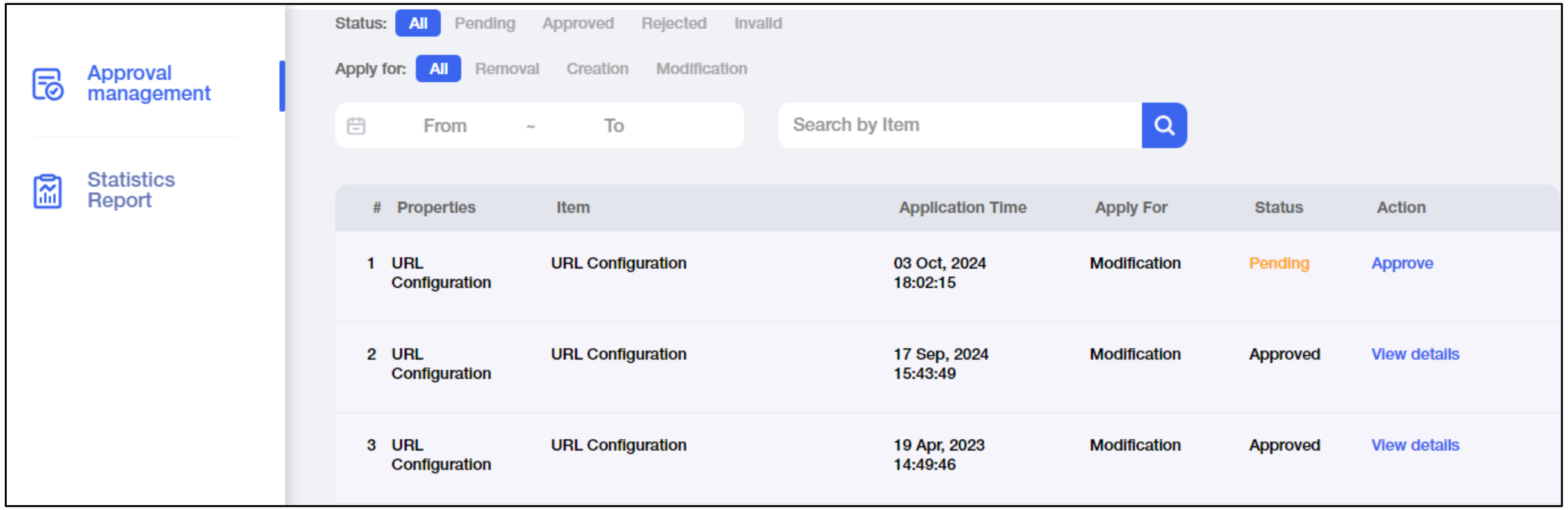
No.		Callback URL/Package Name	Remark
1	☑ As Package Name	Enter Please	Optional
	Fingerprint:	Enter Please	
2	☐ As Package Name	Enter Please	Optional

Self Service Portal – Approver

Approver approves the changes

1. The approver login and review the changes.

2. Approver approves the changes with remarks.



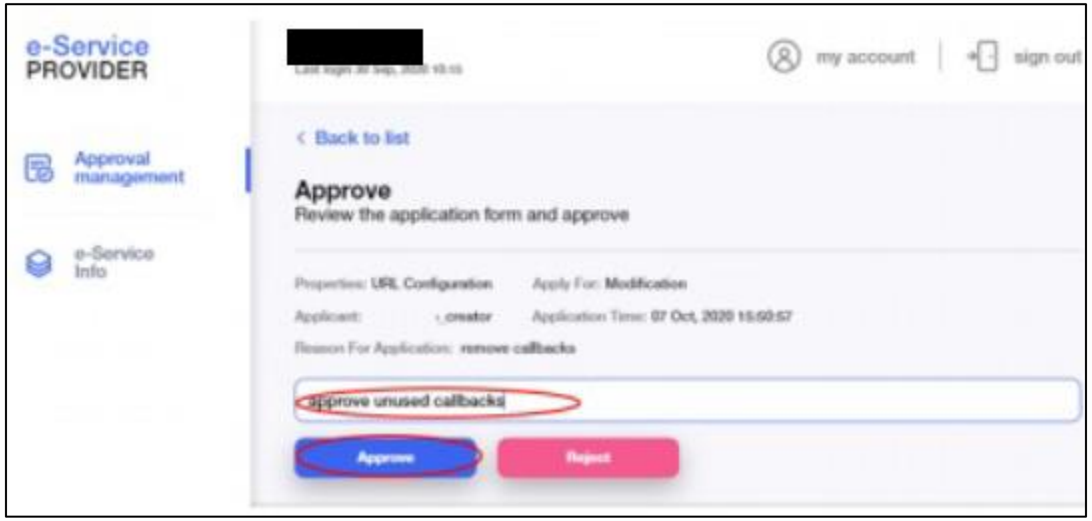
Status: All Pending Approved Rejected Invalid

Apply for: All Removal Creation Modification

From ~ To

Search by Item

#	Properties	Item	Application Time	Apply For	Status	Action
1	URL Configuration	URL Configuration	03 Oct, 2024 18:02:15	Modification	Pending	Approve
2	URL Configuration	URL Configuration	17 Sep, 2024 15:43:49	Modification	Approved	View details
3	URL Configuration	URL Configuration	19 Apr, 2023 14:49:46	Modification	Approved	View details



[redacted]

Last login 30 Sep, 2020 15:15

< Back to list

Approve

Review the application form and approve

Properties: URL Configuration Apply For: Modification

Applicant: _creator Application Time: 07 Oct, 2020 15:50:57

Reason For Application: remove callbacks

approve unused callbacks

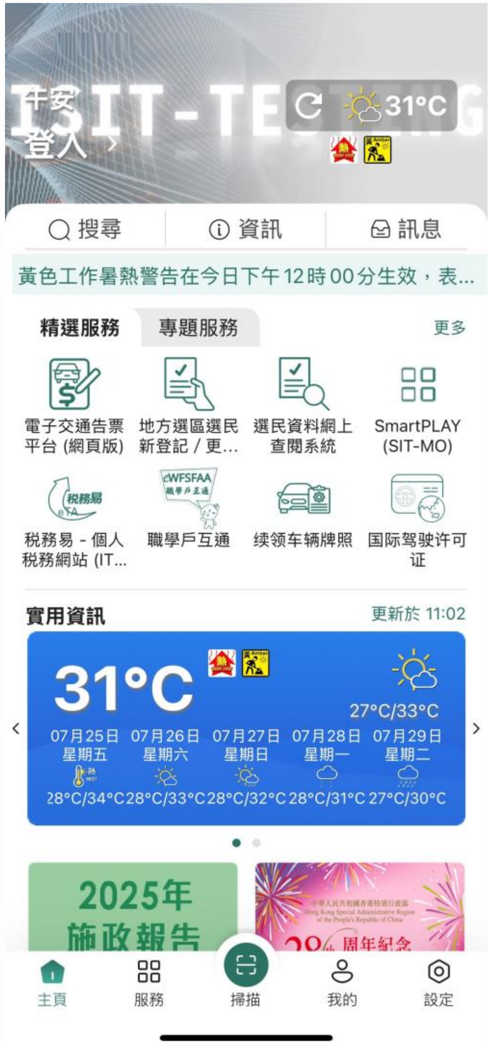
智方便 iAM Smart

"iAM Smart" Testing App

What is “iAM Smart” Testing App?
Testing environment version of “iAM Smart” App with pre-assigned testing account to **simulate** “iAM Smart” user in testing environment.

Supported Platforms:
iOS (TestFlight) and Android (PlayStore)

How to download :
By invitation only, please refer to the testing environment application form for nomination details.



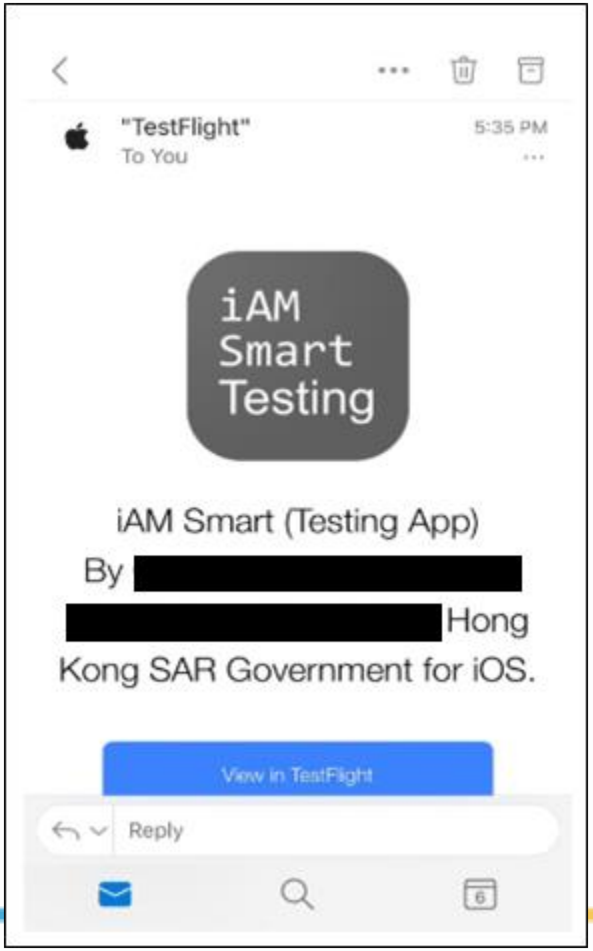
黃色工作暑熱警告在今日下午12時00分生效，表...

精選服務
專題服務
更多
電子交通告票平台 (網頁版)
地方選區選民新登記 / 更...
選民資料網上查閱系統
SmartPLAY (SIT-MO)
税務易 - 個人税務網站 (IT...
職學戶互通
续领车辆牌照
国际驾驶许可证
實用資訊
更新於 11:02
31°C
27°C/33°C
07月25日 星期五 28°C/34°C
07月26日 星期六 28°C/33°C
07月27日 星期日 28°C/32°C
07月28日 星期一 28°C/31°C
07月29日 星期二 27°C/30°C
2025年 施政報告
28th 周年紀念
主頁
服務
掃描
我的
設定

智方便 iAM Smart

"iAM Smart" Testing App - How to download

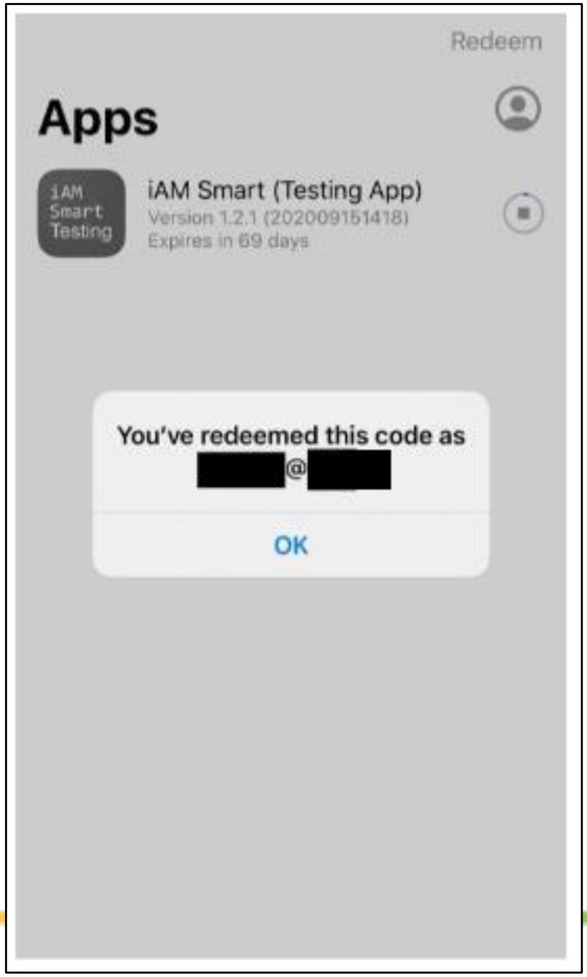
iOS (TestFlight)


"TestFlight" 5:35 PM
To You

iAM Smart Testing

iAM Smart (Testing App)

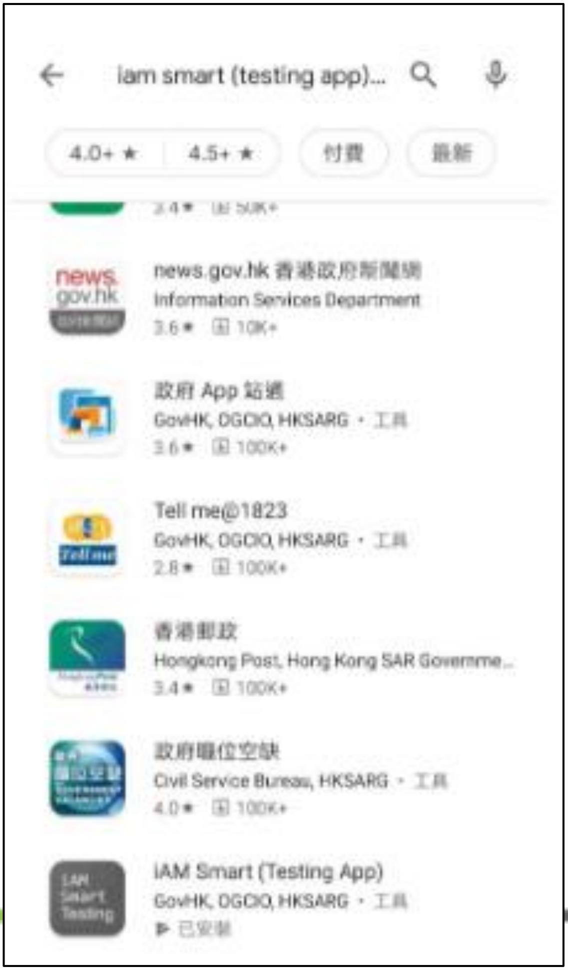
By [redacted] Hong Kong SAR Government for iOS.



iAM Smart (Testing App)
Version 1.2.1 (202009151418)
Expires in 69 days

You've redeemed this code as [redacted]@[redacted]

Android (PlayStore)



3.4★ 50K+

news.gov.hk 香港政府新聞網
Information Services Department
3.6★ 10K+

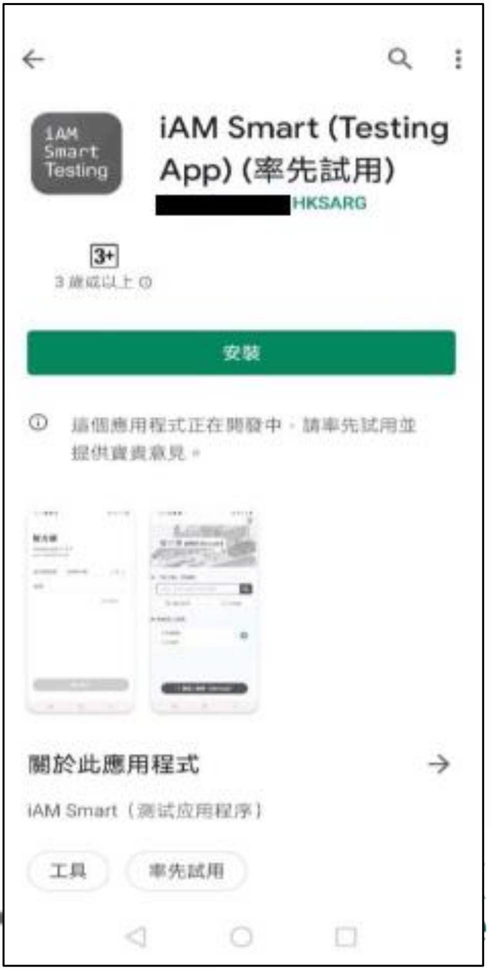
政府 App 站通
GovHK, OGCIO, HKSARG · 工具
3.6★ 100K+

Tell me@1823
GovHK, OGCIO, HKSARG · 工具
2.8★ 100K+

香港郵政
Hongkong Post, Hong Kong SAR Governme...
3.4★ 100K+

政府職位空缺
Civil Service Bureau, HKSARG · 工具
4.0★ 100K+

iAM Smart (Testing App)
GovHK, OGCIO, HKSARG · 工具
已安裝


iAM Smart (Testing App) (率先試用)
[redacted]HKSARG

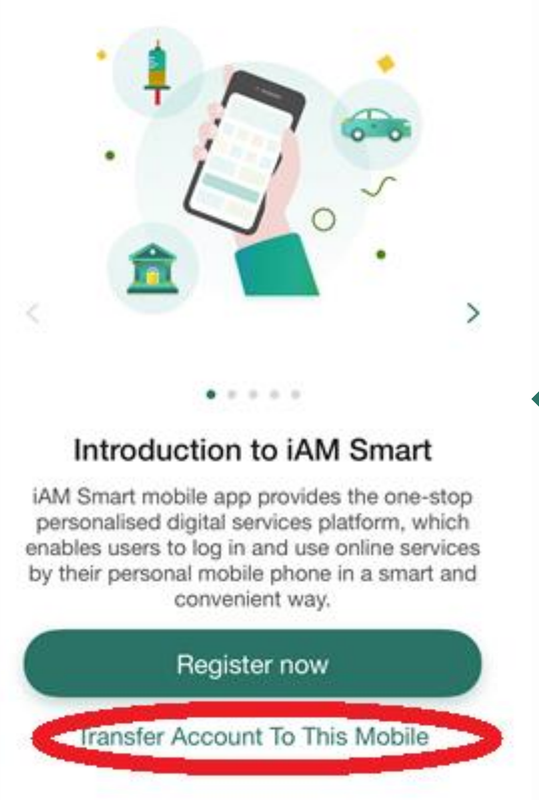
3+
3 歲或以上

這個應用程式正在開發中。請率先試用並提供寶貴意見。

關於此應用程式

iAM Smart（测试应用程序）

"iAM Smart" Testing App – QR code of testing account



Introduction to iAM Smart

iAM Smart mobile app provides 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.

How can I get the testing account for testing?
Please click "Transfer Account To This Mobile) and scan the QR code provided by support team to access the testing account.

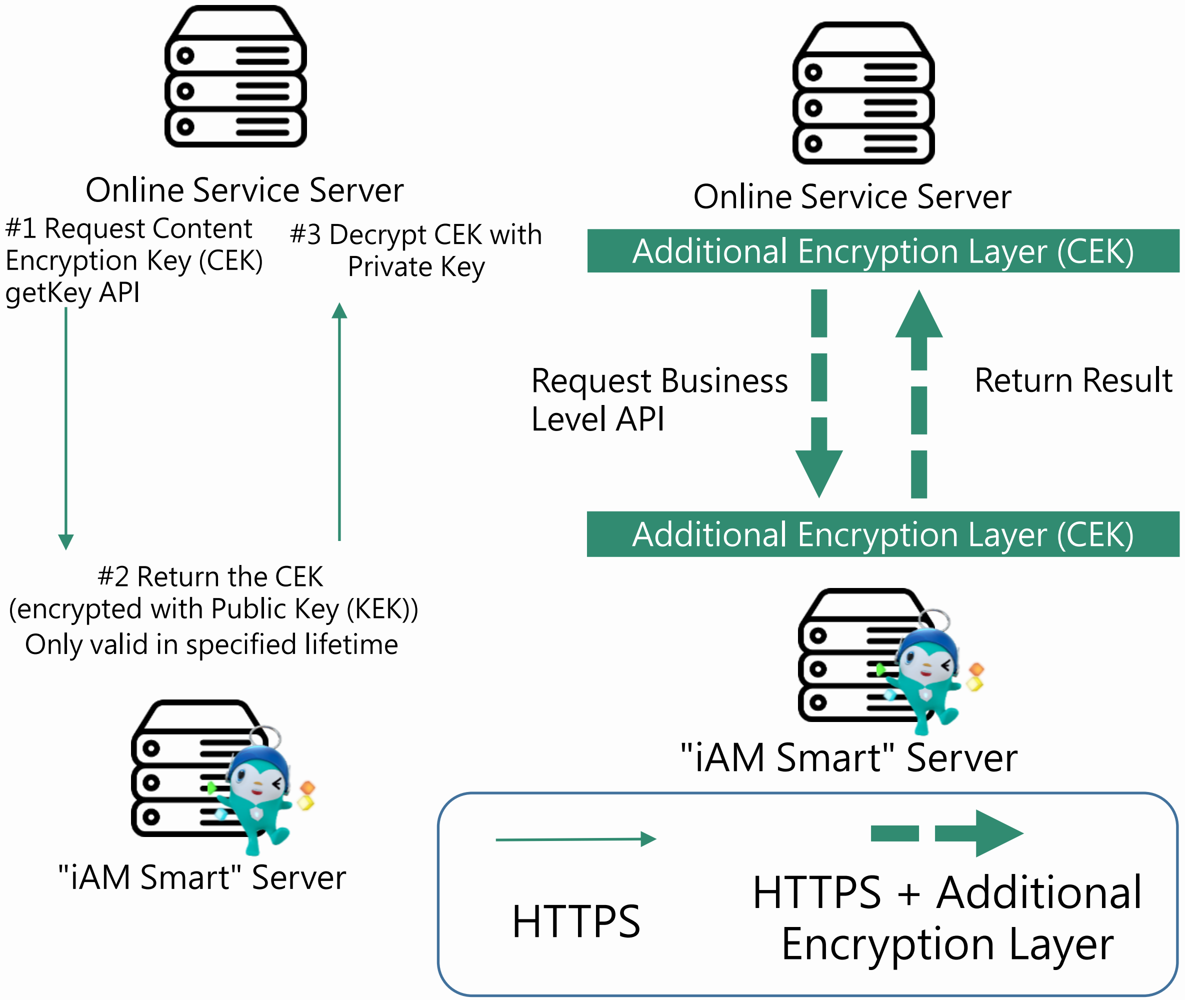
Can I install the Testing App with production app in the same device?
No. The support team suggests you to install either one to avoid any confusion for your use of production app.

Can I request custom accounts with specified HKIC no. and name?
Online service shall use the pre-assigned accounts only.

Encryption and Decryption (KEK/CEK)

智方便 iAM Smart

Additional Encryption Layer (KEK + CEK)



Online Service Server

#1 Request Content Encryption Key (CEK) getKey API

#3 Decrypt CEK with Private Key

#2 Return the CEK (encrypted with Public Key (KEK)) Only valid in specified lifetime

"iAM Smart" Server

Online Service Server

Additional Encryption Layer (CEK)

Request Business Level API

Return Result

Additional Encryption Layer (CEK)

"iAM Smart" Server

HTTPS

HTTPS + Additional Encryption Layer

Highlight

- All traffics between online service Server and “iAM Smart” Server protect by HTTPS
- All business level APIs protect by KEK + CEK

Key Encryption Key (KEK)

- The public key for encrypting CEK from “iAM Smart” Server uploaded by online service.
- Protect CEK

Content Encryption Key (CEK)

- AES256 symmetric encryption key
- Generate by “iAM Smart” Server (valid for period of time) for each online service. (per client id)
- Protect all business APIs

Key Encryption Key (KEK)

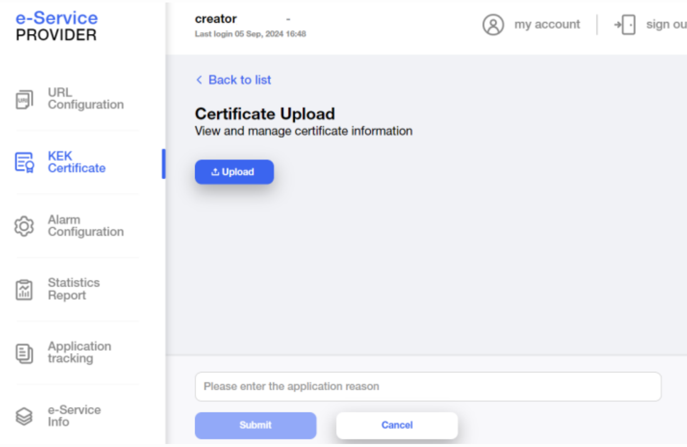
Requirements

- Apply from HKRCA (HKPost / DigiSign)
- 1 for “iAM Smart” testing environment (Trial Cert)
- 1 for “iAM Smart” production environment (Production Cert)

Reference:
Hong Kong Recognized Certification Authorities (HKRCA)
https://www.digitalpolicy.gov.hk/tc/our_work/digital_infrastructure/legal_framework/regulation/eto/ca/disclosure_records/

HongKong Post
https://www.ecert.gov.hk/support/faq/index.html#C35

Configuration



creator -
Last login 05 Sep, 2024 16:48

Certificate Upload
View and manage certificate information

Please enter the application reason

- Upload to self-service portal (.cer file)
- Configured by creator account

  Effective Time: Immediate/ Schedule
- Approved by approver account

Reference:
Self-service Portal
https://<“iAM Smart” domain for testing/ production environment>/ESP/index.html

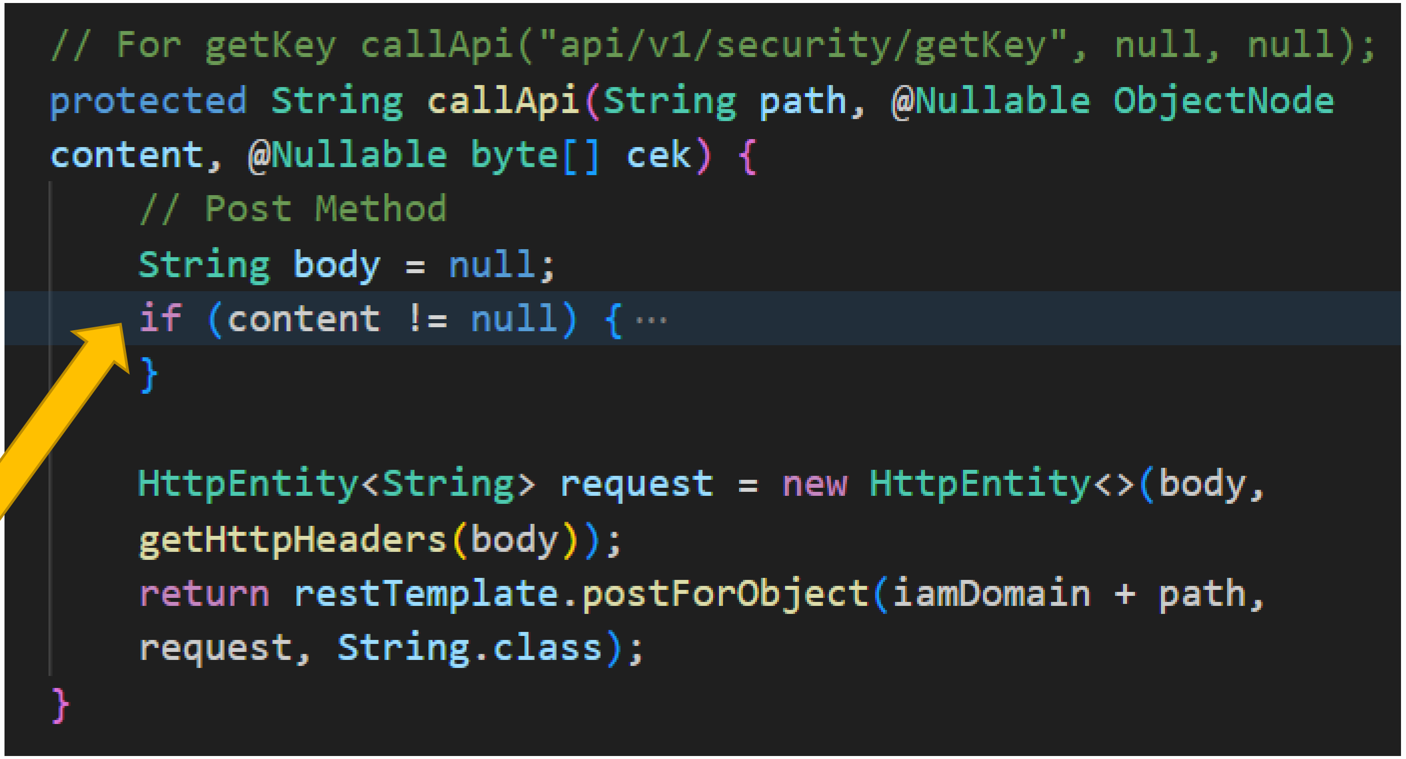
Request Content Encryption Key (CEK) - 1

Common parameters

- clientID
- signatureMethod
- nonce
- timestamp
- Signature
  - Sometimes the responsebody could be empty

For Other APIs

- All parameter shall be encrypted by CEK and put into request body.



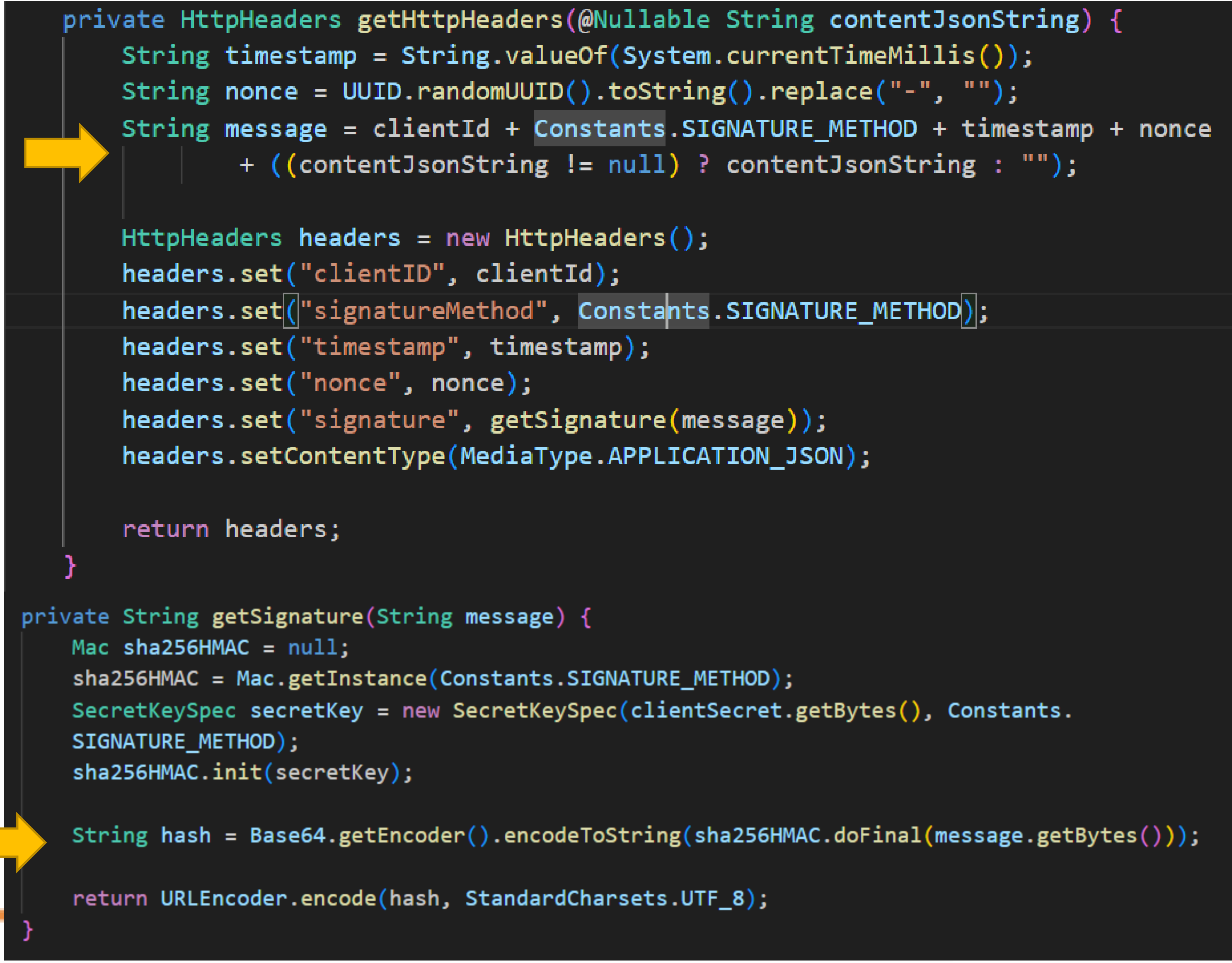
```
// For getKey callApi("api/v1/security/getKey", null, null);
protected String callApi(String path, @Nullable ObjectNode
content, @Nullable byte[] cek) {
    // Post Method
    String body = null;
    if (content != null) {…
    }

    HttpEntity<String> request = new HttpEntity<>(body,
    getHttpHeaders(body));
    return restTemplate.postForObject(iamDomain + path,
    request, String.class);
}
```

Request Content Encryption Key (CEK) - 2

Common parameters / Headers

- clientID
- signatureMethod
- nonce
- Timestamp (sync with HKO)
- Signature

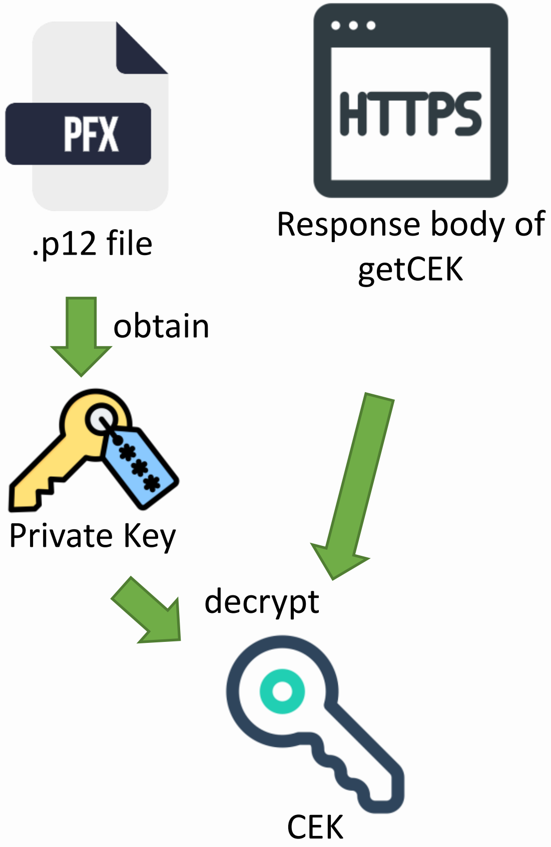
  Sha256(clientId + “HmacSHA256” + timestamp + nonce + requestContent)



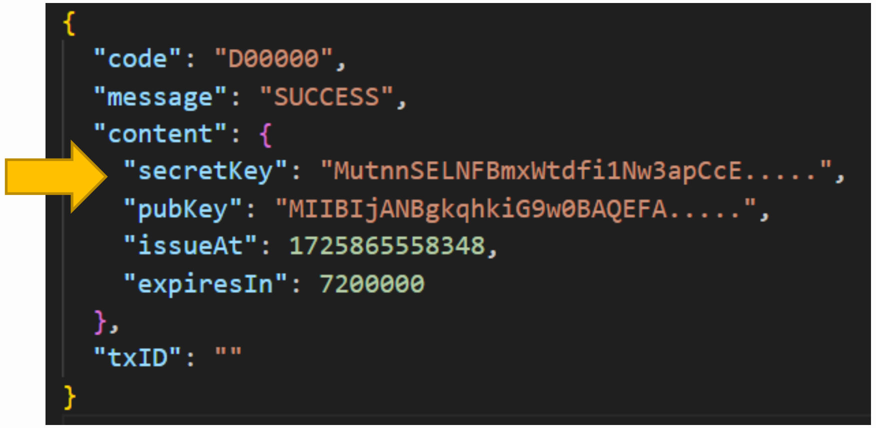
```
    private HttpHeaders getHttpHeaders(@Nullable String contentJsonString) {
        String timestamp = String.valueOf(System.currentTimeMillis());
        String nonce = UUID.randomUUID().toString().replace("-", "");
        String message = clientId + Constants.SIGNATURE_METHOD + timestamp + nonce
                + ((contentJsonString != null) ? contentJsonString : "");

        HttpHeaders headers = new HttpHeaders();
        headers.set("clientID", clientId);
        headers.set("signatureMethod", Constants.SIGNATURE_METHOD);
        headers.set("timestamp", timestamp);
        headers.set("nonce", nonce);
        headers.set("signature", getSignature(message));
        headers.setContentType(MediaType.APPLICATION_JSON);

        return headers;
    }
```

```
private String getSignature(String message) {
    Mac sha256HMAC = null;
    sha256HMAC = Mac.getInstance(Constants.SIGNATURE_METHOD);
    SecretKeySpec secretKey = new SecretKeySpec(clientSecret.getBytes(), Constants.
    SIGNATURE_METHOD);
    sha256HMAC.init(secretKey);

    String hash = Base64.getEncoder().encodeToString(sha256HMAC.doFinal(message.getBytes()));

    return URLEncoder.encode(hash, StandardCharsets.UTF_8);
}
```

Decrypt CEK from Response Body

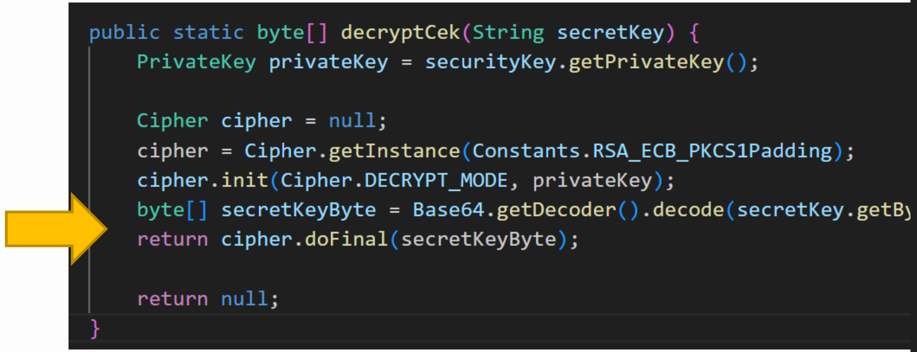


2. Reponses body of getKey



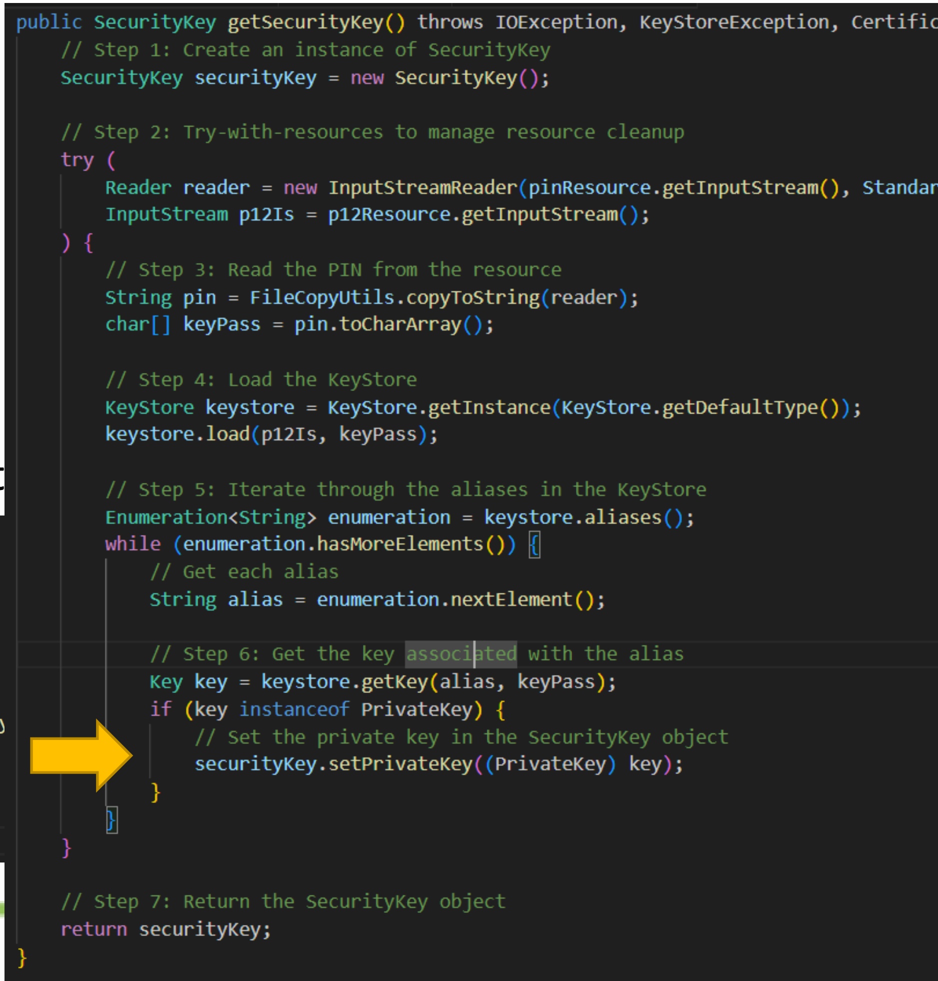
```
{
  "code": "D00000",
  "message": "SUCCESS",
  "content": {
    "secretKey": "MutnnSELNFBmxWtdfi1Nw3apCcE.....",
    "pubKey": "MIIBIjANBgkqhkiG9w0BAQEFA.....",
    "issueAt": 1725865558348,
    "expiresIn": 7200000
  },
  "txID": ""
}
```

3. Get the CEK using private key to decrypt



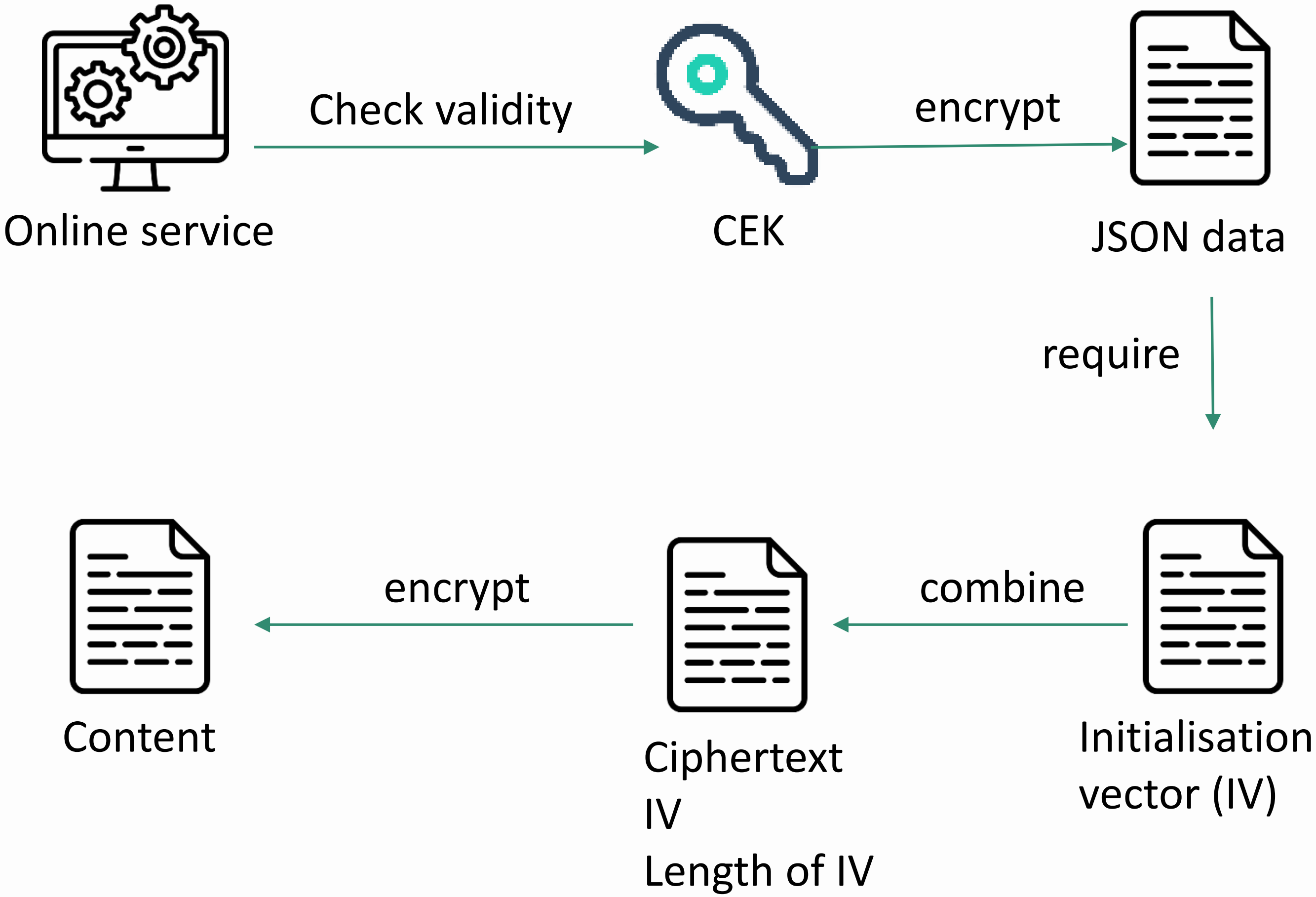
```
public static byte[] decryptCek(String secretKey) {
    PrivateKey privateKey = securityKey.getPrivateKey();

    Cipher cipher = null;
    cipher = Cipher.getInstance(Constants.RSA_ECB_PKCS1Padding);
    cipher.init(Cipher.DECRYPT_MODE, privateKey);
    byte[] secretKeyByte = Base64.getDecoder().decode(secretKey.getBy
    return cipher.doFinal(secretKeyByte);

    return null;
}
```

1. Extract the private key from p12 file



```
public SecurityKey getSecurityKey() throws IOException, KeyStoreException, Certific
    // Step 1: Create an instance of SecurityKey
    SecurityKey securityKey = new SecurityKey();

    // Step 2: Try-with-resources to manage resource cleanup
    try (
        Reader reader = new InputStreamReader(pinResource.getInputStream(), Standar
        InputStream p12Is = p12Resource.getInputStream();
    ) {
        // Step 3: Read the PIN from the resource
        String pin = FileCopyUtils.copyToString(reader);
        char[] keyPass = pin.toCharArray();

        // Step 4: Load the KeyStore
        KeyStore keystore = KeyStore.getInstance(KeyStore.getDefaultType());
        keystore.load(p12Is, keyPass);

        // Step 5: Iterate through the aliases in the KeyStore
        Enumeration<String> enumeration = keystore.aliases();
        while (enumeration.hasMoreElements()) {
            // Get each alias
            String alias = enumeration.nextElement();

            // Step 6: Get the key associated with the alias
            Key key = keystore.getKey(alias, keyPass);
            if (key instanceof PrivateKey) {
                // Set the private key in the SecurityKey object
                securityKey.setPrivateKey((PrivateKey) key);
            }
        }
    }

    // Step 7: Return the SecurityKey object
    return securityKey;
}
```

Make an API request with CEK?



Online service

Check validity

CEK

encrypt

JSON data

require

Initialisation vector (IV)

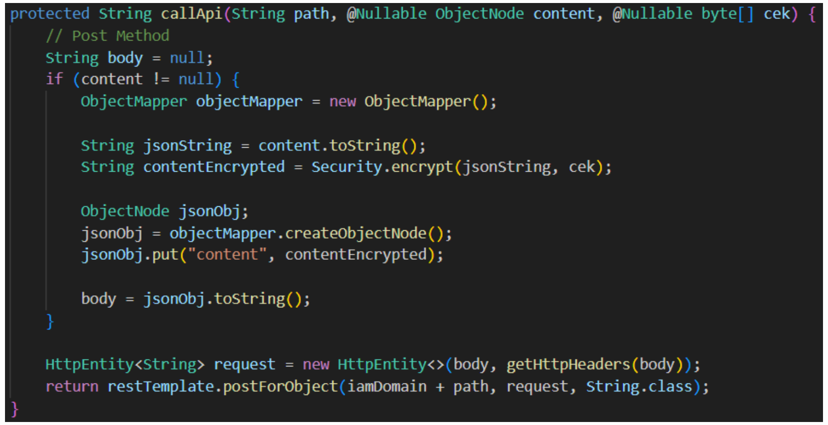
combine

Ciphertext
IV
Length of IV

encrypt

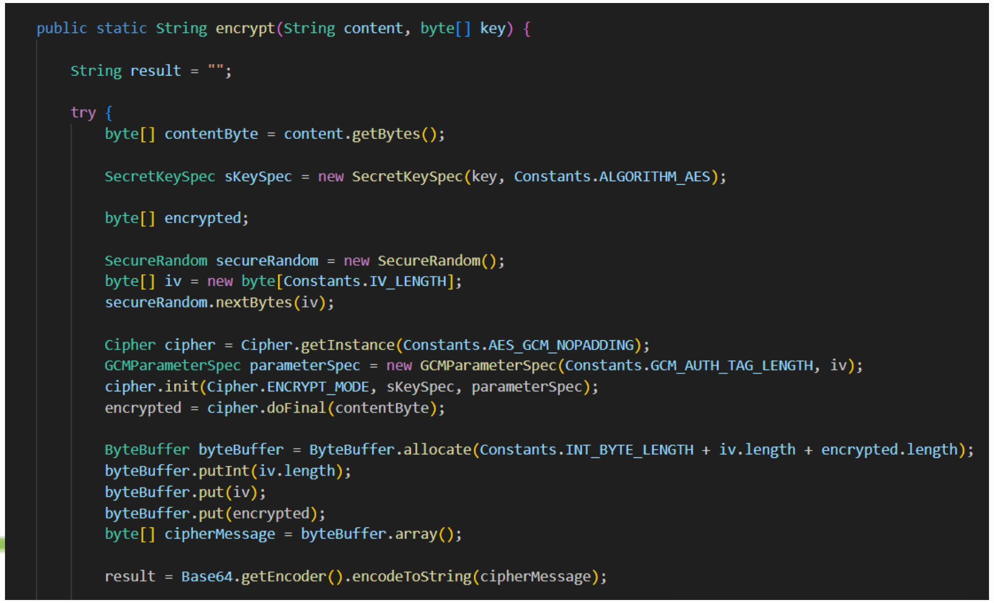
Content

1. Make API Request with CEK Encryption



```
protected String callApi(String path, @Nullable ObjectNode content, @Nullable byte[] cek) {
    // Post Method
    String body = null;
    if (content != null) {
        ObjectMapper objectMapper = new ObjectMapper();

        String jsonString = content.toString();
        String contentEncrypted = Security.encrypt(jsonString, cek);

        ObjectNode jsonObj;
        jsonObj = objectMapper.createObjectNode();
        jsonObj.put("content", contentEncrypted);

        body = jsonObj.toString();
    }

    HttpEntity<String> request = new HttpEntity<>(body, getHttpHeaders(body));
    return restTemplate.postForObject(iamDomain + path, request, String.class);
}
```

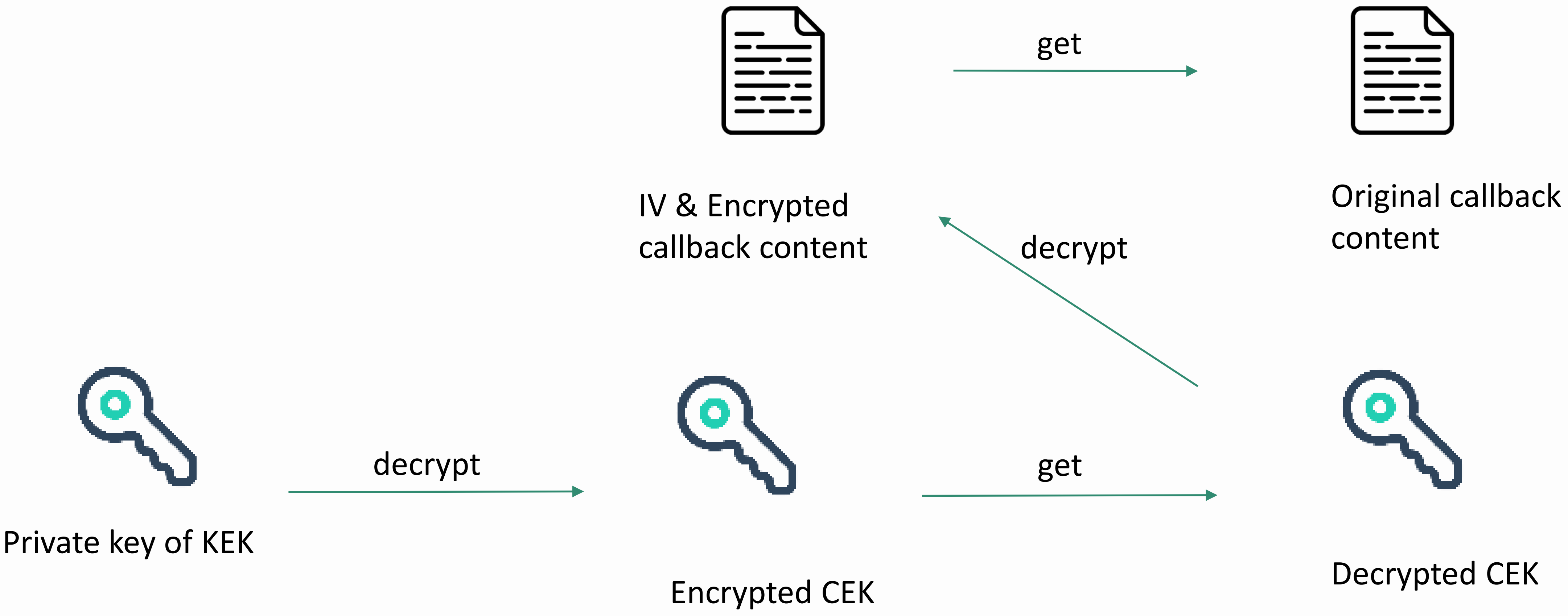
2. Encrypt JSON content with CEK



```
public static String encrypt(String content, byte[] key) {

    String result = "";

    try {
        byte[] contentByte = content.getBytes();

        SecretKeySpec sKeySpec = new SecretKeySpec(key, Constants.ALGORITHM_AES);

        byte[] encrypted;

        SecureRandom secureRandom = new SecureRandom();
        byte[] iv = new byte[Constants.IV_LENGTH];
        secureRandom.nextBytes(iv);

        Cipher cipher = Cipher.getInstance(Constants.AES_GCM_NOPADDING);
        GCMParameterSpec parameterSpec = new GCMParameterSpec(Constants.GCM_AUTH_TAG_LENGTH, iv);
        cipher.init(Cipher.ENCRYPT_MODE, sKeySpec, parameterSpec);
        encrypted = cipher.doFinal(contentByte);

        ByteBuffer byteBuffer = ByteBuffer.allocate(Constants.INT_BYTE_LENGTH + iv.length + encrypted.length);
        byteBuffer.putInt(iv.length);
        byteBuffer.put(iv);
        byteBuffer.put(encrypted);
        byte[] cipherMessage = byteBuffer.array();

        result = Base64.getEncoder().encodeToString(cipherMessage);
```

Decrypt the response body by Decrypted CEK

After receive the callback



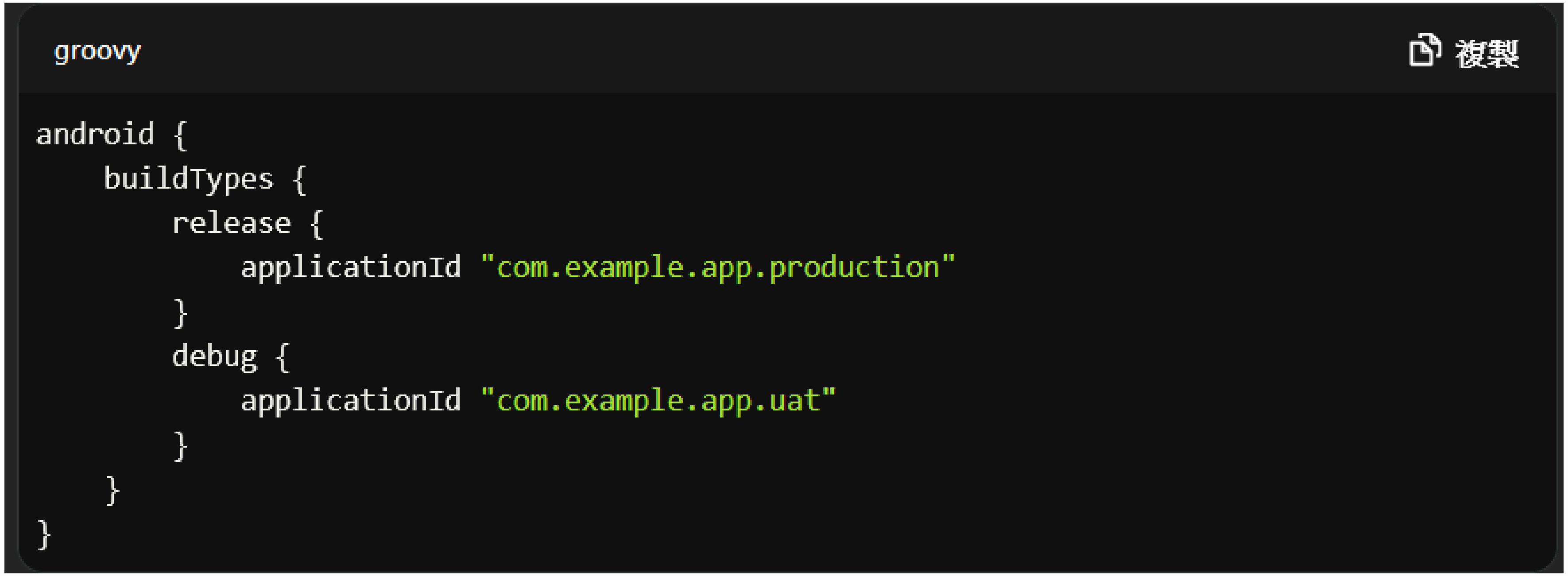
Practical Tips

智方便 iAM Smart

Tips 1: Online Service App has different package names in UAT and Production

Environment configuration:

- Use build configuration files to define different package names for different environments. For instance, in Android, you can use build.gradle to specify different application IDs for UAT and production builds.



```groovy
android {
    buildTypes {
        release {
            applicationId "com.example.app.production"
        }
        debug {
            applicationId "com.example.app.uat"
        }
    }
}
```

Tips 2: Broker Page is not applicable to App integration

Direct API Integration:

Use direct API calls to the backend services without involving a broker page. Ensure that your app is configured to handle these API endpoints directly.

Testing Procedures:

Ensure your testing strategy accommodates the lack of a broker page. This includes:

Unit testing of API calls.

Integration testing to ensure that your app functions correctly with the backend services.

Fallback Mechanisms:

If applicable, consider implementing fallback mechanisms in your app. For example, if an API call fails, you could provide cached data or a default response.

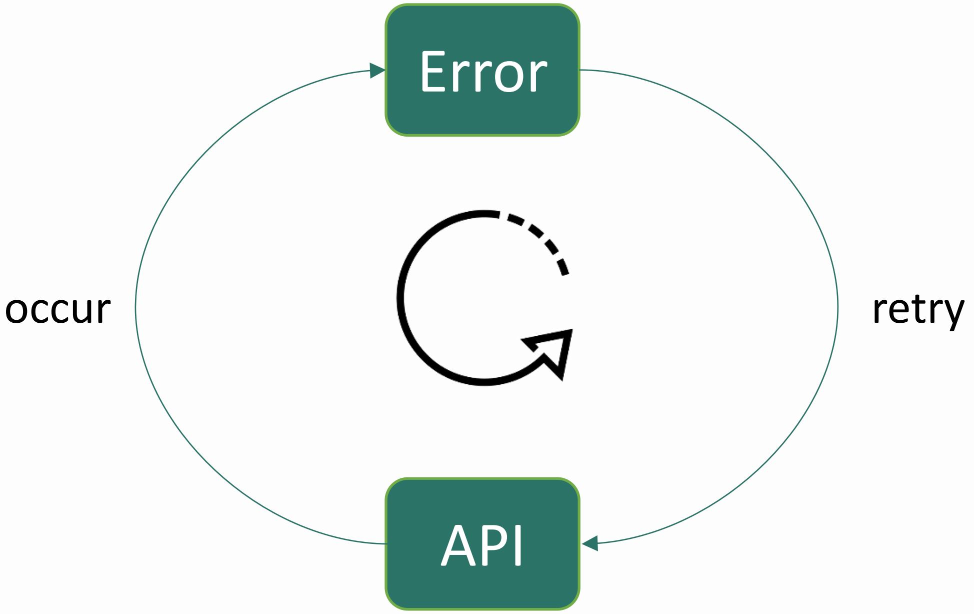
Security Considerations:

Ensure that all API communications are secure (e.g., using HTTPS) and that sensitive data is handled appropriately, especially without the broker page serving as an intermediary.

Tip 3: CEK calling for API

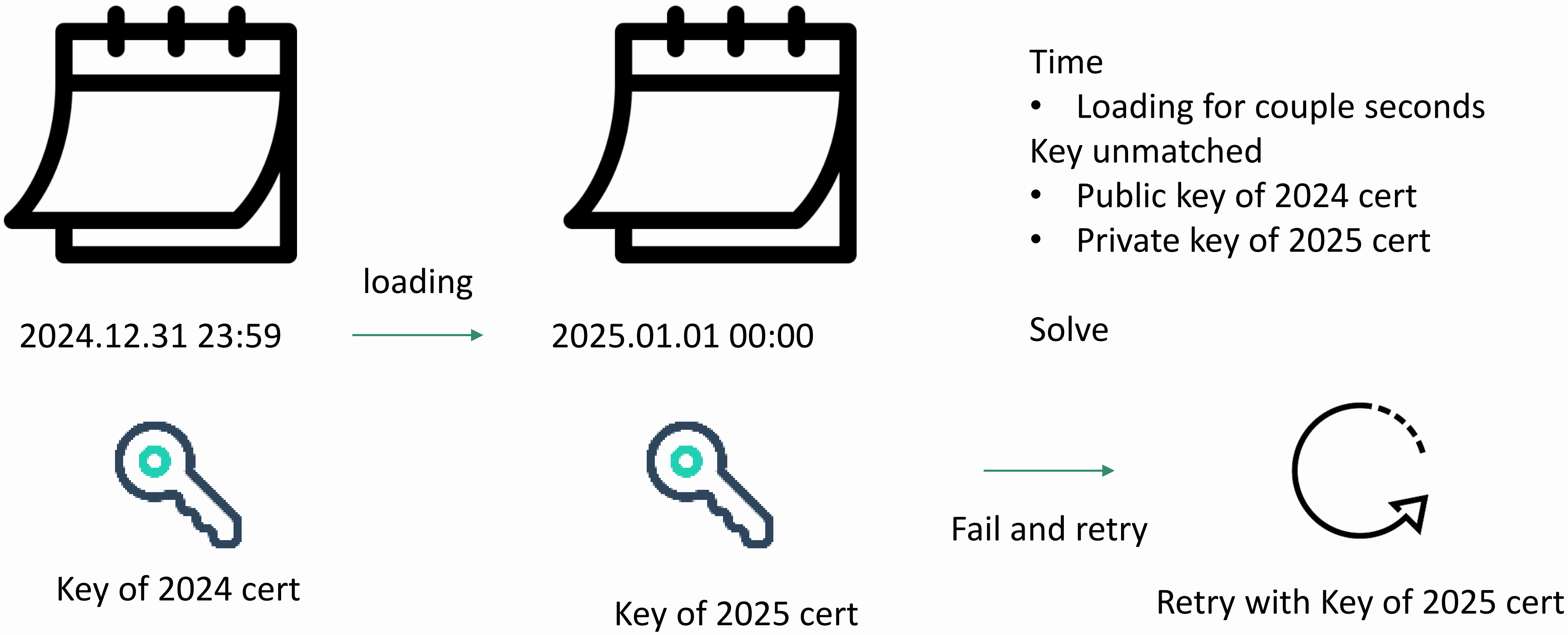
- Encryption/Decryption Error Code may be received due to unexpected reasons

- Online service shall retry the “Request Symmetric Content Encryption Key” API



- https://<iAM_Smart_domain>/api/v1/security/getKey

Tip 4: KEK expired



2024.12.31 23:59

loading →

2025.01.01 00:00

Key of 2024 cert

Key of 2025 cert

Time

- Loading for couple seconds

Key unmatched

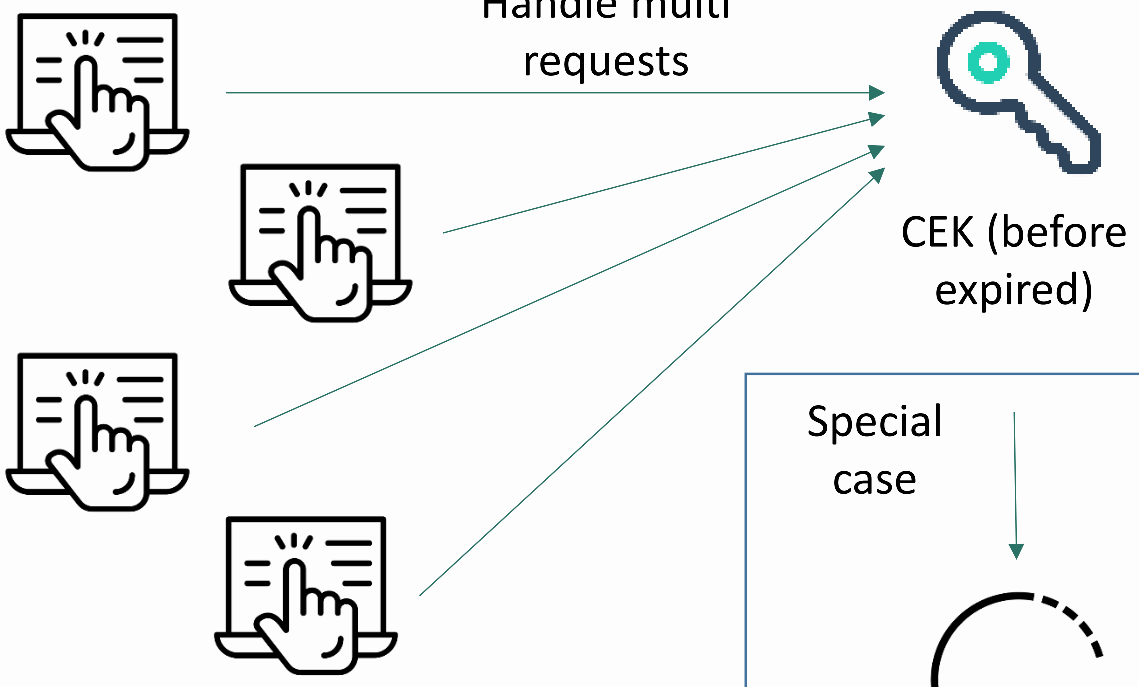
- Public key of 2024 cert
- Private key of 2025 cert

Solve

Fail and retry →

Retry with Key of 2025 cert

Tip 5: Excessive CEK request



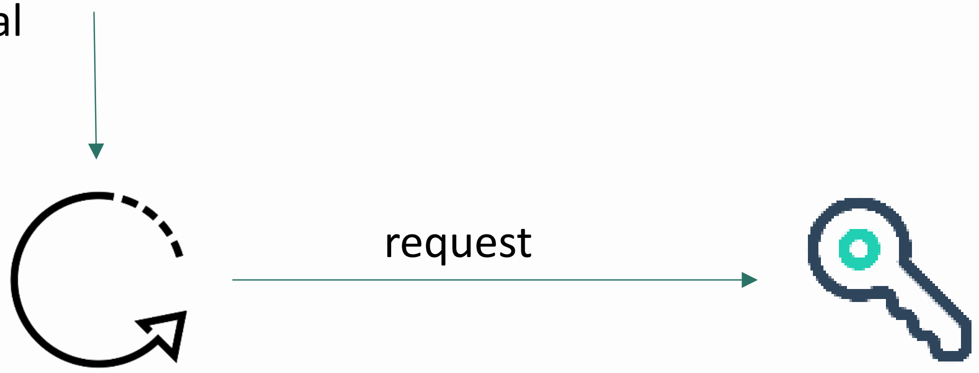
Handle multi requests

CEK (before expired)

Multiple requests

- A CEK would be applied into encryption/decryption for many times
- It is not supposed to generate a new CEK by request, unless
  - Encryption/Decryption fail
  - Other problems need retry
- Should not be request before expired

Special case



Retry

request

New CEK

Quiz

Question:
Which algorithm would be used for business data encryption?

A. HKRCA
B. AES-128
C. AES-256
D. HTTPS

Answer: C