

Developer Guide for CorpID enabled e-Services

Version: 1.0

June 2026

© The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

The contents of this document remain the property of and may not be reproduced in whole or in part
without the express permission of the Government of
the Hong Kong Special Administrative Region of the People's Republic of China

1. DOCUMENT REVISION HISTORY

Version No.	Release Date	Section Affected	Summary of Changes
1.0.0	30-06-2026		Initial version

2. TABLE OF CONTENTS

1.	Document Revision History	2
2.	Table of Contents	3
3.	Terms and Conditions	6
4.	Definitions	7
1.	INTRODUCTION	8
1.1	OVERVIEW	8
1.1.1	Introduction of API functions	9
1.1.2	CorpID Profile	9
1.1.3	Authorisation Scope and Access Token	12
1.1.4	Authentication for e-Service Login and Authorisation for Anonymous CorpID APIs	14
1.1.5	Callback API and Transient Input Data	14
1.1.6	Data Protection for CorpID API	15
1.1.7	Identification Code and Result Notification for Digital Signing	15
1.1.8	Streamline Workflow	16
1.2	ASSUMPTIONS AND CONSTRAINTS	16
1.3	E-SERVICE REGISTRATION TO “CORPID” SYSTEM	17
1.4	POTENTIAL BUSINESS CASES USING “CORPID”	17
1.4.1	e-Service Onboarding	19
1.4.2	User Authentication	20
1.4.3	Form pre-filling with Service Login	21
1.4.4	Digital Signing with Service Login	21
1.4.5	Anonymous Form pre-filling	23
1.4.6	Anonymous Digital Signing	24
2.	SYSTEM WORKFLOW USING “CORPID”	25
3.	IMPLEMENTATION PROCEDURE	25
3.1	PREREQUISITE	25
3.2	e-SERVICE AND “CORPID” SYSTEM INTERACTION DESIGN	26
3.2.1	Interaction between e-Service and CorpID Mini-program	26
3.2.2	Process of Common API Request and Response Parameters	29

3.2.3	Process of Common Errors Returned from CorpID APIs	31
3.3	API DATA ENCRYPTION AND DECRYPTION	34
3.3.1	Workflow for Encryption and Decryption	34
3.3.2	Encryption & Decryption Scope and Examples	37
3.3.3	Proper Handling of Encryption and Decryption.....	37
3.4	WORKFLOWS FOR AUTHENTICATION	38
3.4.1	Scenario 1: Authentication with iAM Smart (e-Service Website in Different Device)	38
3.4.2	Scenario 2: Authentication with iAM Smart (e-Service Website in Same Device).....	50
3.4.3	Scenario 3: Authentication with iAM Smart (e-Service App in Different Device)	58
3.4.4	Scenario 4: Authentication (e-Service App in Same Device)	65
3.4.5	Switching Corporation	71
3.5	FORM PRE-FILLING WITH SERVICE LOGIN (Profiles).....	74
3.5.1	Obtain Profiles Information (EXT-005, FOR B/D AND GOVERNMENT BUREAU ONLY) 74	
3.5.2	Scenario 1: Form pre-filling (e-Service Website/App in Different Device)	75
3.5.3	Scenario 2: Form pre-filling (e-Service Website in Same Device).....	81
3.5.4	Scenario 3: Form pre-filling (e-Service App in Same Device)	84
3.6	FORM PRE-FILLING WITHOUT SERVICE LOGIN (Anonymous Form Pre-Filling)	87
3.6.1	Scenario 1: Anonymous Form Pre-filling (e-Service Website in Different Device)	87
3.6.2	Scenario 2: Anonymous Form pre-filling (e-Service Website in Same Device)	95
3.6.3	Scenario 3: Anonymous Form pre-filling (e-Service App in Different Device).....	100
3.6.4	Scenario 4: Anonymous Form pre-filling (e-Service App in Same Device)	105
3.7	WORKFLOWS FOR DIGITAL SIGNING WITH SERVICE LOGIN	111
3.7.1	Scenario 1: Digital Signing (e-Service Website/App in Different Device)	111
3.7.2	Scenario 2: Digital Signing (e-Service Website in Same Device)	125
3.7.3	Scenario 3: Digital Signing (e-Service App in Same Device)	133
3.8	WORKFLOWS FOR DIGITAL SIGNING WITHOUT SERVICE LOGIN (Anonymous Digital Signing).....	140
3.8.1	Scenario 1: Anonymous Digital Signing (e-Service Website in Different Device)....	140
3.8.2	Scenario 2: Anonymous Digital Signing (e-Service Website in Same Device).....	153
3.8.3	Scenario 3: Anonymous Digital Signing (e-Service App in Different Device).....	161
3.8.4	Scenario 4: Anonymous Digital Signing (e-Service App in Same Device).....	169
3.9	DOCUMENT SHARING WITH SERVICE LOGIN	178

3.9.1	Scenario 1: Document Sharing (e-Service Website in Different Device).....	178
3.9.2	Scenario 2: Document Sharing (e-Service Website in Same Device).....	182
3.9.3	Scenario 3: Document Sharing (e-Service App in Different Device).....	185
3.9.4	Scenario 4: Document Sharing (e-Service App in Same Device).....	188
3.10	WORKFLOWS FOR DIRECT LOGIN & DIRECT ACCESS.....	191
3.10.1	Scenario 1: Direct Login with e-Service Website (Direct Login v2).....	191
3.10.2	Scenario 2: Direct Access with e-Service Website	197
3.10.3	Scenario 3: Direct Login with e-Service Website (Fallback Mechanism).....	198
3.10.4	Scenario 4: Direct Login with e-Service App (Direct Login v2).....	199
4.	Appendix	205
A.	REFERENCE APPLICATIONS.....	205
A.1	Overview	205
A.2	Software Directory Structure.....	205
A.3	Implementation Reference.....	207
B.	STREAMLINE WORKFLOW SCENARIOS	209
B.1	Scenario 1	209
B.2	Scenario 2	210
B.3	Scenario 3	212
B.4	Scenario 4	213
B.5	Scenario 5	214
C.	4-digit identification code generation algorithm	215

3. TERMS AND CONDITIONS

The Government of the HKSAR (“HKSARG”) has the sole discretion to amend or vary the Reference Application and the Developer Guide for CorpID enabled e-Services (“Developer Guide”) from time to time.

The Reference Application 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 HKSARG. Information provided by the Developer Guide and all the associated intellectual property rights are retained by HKSARG.

e-Service Providers and their contractors (and sub-contractors, if applicable) (“users”) may use the Reference Application and the Developer Guide for the purpose of designing, developing, testing and running of their e-government applications. By using the Reference Application 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 Application 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 Application and information provided by the Developer Guide.

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

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

4. DEFINITIONS

The following terms and abbreviations are used in this document.

Terms / Abbreviations	Definition
CorpID System	The CorpID backend services that provide CorpID APIs and trigger e-Service callback APIs to return results to e-Service applications.
e-Service server	The e-Service backend services that trigger CorpID APIs and provide e-Service callback APIs to receive results from the CorpID System.
e-Service client terminal	The browser (Desktop PC or mobile) or e-Service mobile application that provide user interface for CorpID users to interact with e-Service server, “iAM Smart” mobile application, CorpID mini-program or CorpID System.
e-Service Website	It is the webpage generated by the e-Service server and displayed by a browser (Desktop PC or mobile).
CorpID e-Cert	Digital certificate issued by Recognized Certification Authority for e-Service account with digital signing function enabled. The usage and maintenance of the CorpID e-Cert are managed by CorpID System for the CorpID account.
Content Encryption Key or CEK	Symmetric encryption key to be exchanged with CorpID System for API data encryption and decryption.
Key Encryption Key or KEK	The public key of encipherment certificate prepared by e-Service for encrypting the CEK by the CorpID System.
Cross-Site Request Forgery or CSRF Attack	CSRF is an attack that forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated.

1. INTRODUCTION

1.1 OVERVIEW

To accelerate the digital economy development in Hong Kong through strengthening digital infrastructure and fostering digital transformation, the Digital Policy Office (“DPO”) is developing the Digital Corporate Identity (“CorpID”) Platform, thereby facilitating and bringing ease to corporations in their use of e-Government services. The DPO will launch the CorpID Platform in end 2026 and gradually extending the range of services.

CorpID can serve as a common digital key for identity authentication, enabling corporations to use the e-government services and conduct online business transactions at ease. Successful applicant will be issued a CorpID. The responsible person of the corporation can set the authorised representatives and authorise their personnels to conduct electronic commercial activities on behalf of the corporation.

The DPO launched the CorpID Sandbox Programme in December 2025 for corporations and government bureaux/departments interested in adopting CorpID to design their applications that can better meet the market demands. Typical use cases include remote account opening where corporate identities and authorisation of authorised representatives can be verified, login to various e-service platforms in a simple, secure and convenient manner, verifiable digital signing of application documents, funding agreements or contracts, and automatic form pre-filling without having to repeatedly provide corporate information, thereby reducing business processing time and human error.

The CorpID Sandbox provides a CorpID Developer Portal in which technical references such as this Developer Guide, CorpID Application Programming Interface (API) Specifications, CorpID sample applications, information on pre-requisites and relevant configurations are available for developers to understand the technical requirements, and test the CorpID APIs, facilitating smooth and efficient adoption of CorpID and deployment of real applications.

For implementation of production scale CorpID enabled application, a dedicated System Integration Test environment (“iSIT Environment”) with a CorpID mini-program is developed, offering a suite of API functionalities and workflows that mirror the actual operations for core CorpID functions (namely Corporate Identity Verification, Digital Signing, Form Pre-filling and Document Wallet). e-Services shall follow both the API Specifications and Developer Guide by CorpID Platform for its implementation.

1.1.1 Introduction of API functions

The core functions of the CorpID Platform as mentioned in Section 1 are built in form of RESTful APIs, which could be accessed by registered e-Services. CorpID makes reference to OAuth 2.0 for authentication and authorisation amongst CorpID users, e-Services, the iAM Smart and CorpID Platforms. The e-Services adopting CorpID are required to provide RESTful callback APIs to receive API responses from the iAM Smart and CorpID Platforms in order to complete the entire workflow.

The core CorpID functions include:

Corporate Identity Verification

- Corporate Identity Verification makes use of the Authentication API provided by the iAM Smart and CorpID Platforms to verify the identities of the users in a simple and secure way. The API can be used in various scenarios, such as user login, membership system, booking system, etc.

Digital Signing

- e-Service can make use of the Digital Signing API to enable a corporate user to perform digital signing with legal backing after the user has authenticated with e-Service using iAM Smart and CorpID Platforms. It can be used in many cases, such as digital signing an online application form and digital signing a contract and agreement.

Form Pre-Filling

- e-Service can make use of the Profiles API to retrieve data of “corpProfileFields” and “eCorpFields”. The API can be used in various scenarios, such as account opening, account linkup, form pre-filling, etc.

Document Wallet

- Through the Document Wallet API, e-Services can securely access digital certificates and documents submitted by the corporations and issued by government B/Ds as supporting documents. For verifiable certificates and documents, they are issued using the globally recognized Decentralized Identity (DID) and Verifiable Credential (VC) standards developed by the World Wide Web Consortium to ensure authenticity.

1.1.2 CorpID Profile

A CorpID Profile represents the corporation he/she represents. It contains the following corporate information.

Components	Information
------------	-------------

corpProfileFields	The “corpProfileFields” consist of the account information including the Unique Business Identifier (UBI) (previously known as Business Registration Number (BRN)), English Company Name, Chinese Company Name (must have 1 available) and Company Address. “corpProfileFields” are solely used for the purpose of corporate identity verification, such as remote account opening, login, etc.
eCorpFields	In addition to the account information, CorpID user can voluntarily maintain a “e-Corp profile” in which additional information of the corporate can be stored and retrieved for the purpose of online form pre-filling.
nonHKResidentFields	

The details of each components of the CorpID Profiles are as below:

corpProfile Fields	Sub-Field	Description
ubi		Unique Business Identifier
did		Decentralised identifier
crn		Company Registration Number
duns		DUNS Number
lei		Legal Entity Identifier
type		Corporation type code
status	statusCode	Corporation status code
	engStatusPlaceholder	The english placeholder of the status description if any
	chiStatusPlaceholder	The chinese placeholder of the status description if any
engName		English Name
chiName		Chinese Name
engAddress		English Registered Address
chiAddress		Chinese Registered Address

commencementDate		Commencement date In YYYY-MM-DD format
cessationDate		Cessation date of Place of Business in Hong Kong In YYYY-MM-DD format
annualReturnsDate		Submission date of annual returns In YYYY-MM-DD format
brcExpiryDate		Expiry Date of Business Registration Certificate In YYYY-MM-DD format
crLstMatchTs		The last matching time between the CorpID Platform and the CR, expressed in number of milliseconds since January 1, 1970 00:00:00 GMT.
irdLstMatchTs		The last matching time between the CorpID Platform and the IRD, expressed in number of milliseconds since January 1, 1970 00:00:00 GMT.
openDataLstMatchTs		The last matching time between the CorpID Platform and the open data, expressed in number of milliseconds since January 1, 1970 00:00:00 GMT.
rcaLstMatchTs		The last matching time between the CorpID Platform and the RCA, expressed in number of milliseconds since January 1, 1970 00:00:00 GMT.

eCorpFields Field	Sub-Field	Description
eCorpAddr		Corporate address
eCorpEmailAddr		Corporate email address
eCorpTelNo	countryCode	Country code of telephone number
	nationalDestinationCode	National destination code of telephone number

	subscriberNumber	Subscriber number of telephone number
	extensionNumber	Extension number of telephone number
eCorpFaxNo	countryCode	Country code of FAX number
	nationalDestinationCode	National destination code of FAX number
	subscriberNumber	Subscriber number of FAX number
eCorpWebsite		Corporate website URL

“profileFields” and “eMEFields” of the associated “iAM Smart” user (if any) will also be returned through the integrated profile APIs. For details, please refer to “iAM Smart” API Specifications document separately.

1.1.3 Authorisation Scope and Access Token

The CorpID Platform utilises the OAuth 2.0 authentication framework to enable an e-Service to gain access to the CorpID APIs, with CorpID user’s authorisation facilitated through the “iAM Smart” testing mobile app and CorpID mock-up mini-program.

1.1.3.1 Determine Authorisation Scope

To access the CorpID APIs, the e-Service should first identify the appropriate authorisation scope(s) required for the specific CorpID APIs to be invoked for its business needs. The table below provides the mapping of authorisation scopes:

Authorisation Scope	Value
Authentication	corpidapi_auth
Token Exchange to switching corporation	corpidapi_auth
Form Pre-filling with Service Login (aka Profiles)	corpidapi_profiles
Form Pre-filling without Service Login (Anonymous Form Pre-filling)	corpidapi_formfilling
Digital Signing with Service Login	corpidapi_sign
Digital Signing without Service Login (Anonymous Digital Signing)	corpidapi_sign
Document Wallet	corpidapi_docwallet

e-Service should combine all authorisation scope(s) required into a single request to get the authorisation from the CorpID user through the CorpID Platform when the CorpID user requests login to an e-Service using “iAM Smart” testing mobile app and CorpID testing mini-program. For example, authorisation scope “corpidapi_auth”, “corpidapi_formfill” and “corpidapi_sign” are used for CorpID authentication, form pre-filling and digital signing respectively.

1.1.3.2 Get Access Token

e-Service should invoke “iAM Smart” API “Request QR Page” with the required authorisation scope(s) for CorpID (cScope) and “iAM Smart” (scope).

With successful authorisation of the CorpID user, CorpID System will return a CorpID Authorisation Code (“cCode”) and “iAM Smart” Authorisation Code (“code”) for HKIC Holder, with the required authorisation scopes (i.e., access rights for CorpID APIs and “iAM Smart” APIs) through “iAM Smart” System to e-Service via the e-Service client terminal (e.g., browser).

e-Service then exchanges the cCode with CorpID System for the CorpID Access Token (“cAccessToken”) and code with “iAM Smart” System for the “iAM Smart” Access Token (“accessToken”), the Tokenised ID of CorpID and “iAM Smart”, and other metadata of the CorpID user. The cAccessToken and accessToken are bound to the authorisation scope(s) and e-Service must present the cAccessToken and accessToken and relevant parameters to access the CorpID APIs or “iAM Smart” APIs. e-Service should retain the cAccessToken and accessToken for access to CorpID APIs or “iAM Smart” APIs within their validity periods and destroy the cAccessToken and accessToken when they expired, become invalid or the CorpID user left the e-Service (e.g., logout).

The process to get cAccessToken and accessToken by e-Service will be described in Authentication Workflow in later section.

1.1.3.3 User Role and User Permission

CorpID System’s User role of the corporation “userRole” will be returned in the response of get access token or switch corporation. e-Service may utilize them if needed.

- RP - Representative Person
- ADM – Administrator
- AR – Authorised Representative
- USR – User

Privileges of CorpID user at e-Service will also be returned in the response of get access token or switch corporation. e-Service may utilize them to prompt proper message or control the workflow if needed.

The value of the parameter is expressed as a list of space-delimited, case-sensitive strings

- user_access
- user_submit
- user_companychop
- user_formfilling

1.1.3.4 Switch Corporation

During authentication, the number of Corporation a user has “corpCount” will be returned in the response of get access token. If the number of Corporation is more than 1, the e-Service should call the Get Corporation List to get the list of corporation of the user, display and request the user to select, and update the corporation with Request Token Exchange for Switching Corporation API.

1.1.4 Authentication for e-Service Login and Authorisation for Anonymous CorpID APIs

Authentication for e-Service Login

To complete the “Get Access Token” process as stipulated in Section 1.1.3, CorpID user has to authenticate his/her identity using 2FA (i.e., the mobile device bound with his/her CorpID account and a local biometric authentication with the CorpID Mini-program) to log in CorpID System to give authorisation. As such, successful completion of this “Get Access Token” process resulting in return of accessToken, cAccessToken and Tokenised ID to e-Service should be accepted as successful authentication of the CorpID user to the e-Service.

Details of authentication can be found in Section 3.4.

Authorisation for Anonymous CorpID APIs

For e-Service to access CorpID APIs for anonymous form pre-filling and anonymous digital signing using CorpID, unlike the above e-Service Login process, the successful completion of “Get Access Token” process means that CorpID user has authorised a one-time access to the relevant CorpID API. The relevant accessToken and cAccessToken should be valid for only one usage. e-Service must go through the same “Get Access Token” process for every access to the same or different anonymous CorpID APIs.

Details of authorisation for anonymous CorpID API can be found in Section 3.6 and 3.8.

1.1.5 Callback API and Transient Input Data

Due to the possible unexpected delay (e.g., network latency) and/or action time of the CorpID user to perform authorisation in the CorpID Mini-program (e.g., to determine which data items in “e-ME profile” are allowed for retrieval by e-Service), e-Service may experience timeout if an instant API response design is used. Therefore, asynchronous API response is adopted in CorpID

APIs. e-Service is required to implement its own callback APIs to support the return of asynchronous API response from the CorpID System after invoking the relevant CorpID APIs. e-Service should also manage CorpID user's transient input data before invoking any CorpID APIs.

1.1.6 Data Protection for CorpID API

All CorpID and e-Service callback APIs are protected by HTTPS protocol during transmission. Additional API data encryption on API POST request and response body is implemented with encryption key being generated and renewed in CorpID System using a dedicated CorpID API “Request/Revoke Symmetric Content Encryption Key”. The data encryption key has its validity and registered e-Service must request/renew the key by itself and make use the key to protect the data when invoking the relevant CorpID APIs.

1.1.7 Identification Code and Result Notification for Digital Signing

For CorpID user to digitally sign a document in e-Service, e-Service should first generate the hash from the document (or document digest for a PDF document) to be signed (“Document Hash”). The Document Hash will be sent to CorpID System for digital signing using the private key of CorpID user's CorpID e-Cert. A signature bundle including the digital signature, CorpID e-Cert, etc., will be returned to e-Service for further computing of the signed document. When CorpID user has logged in the e-Service, both e-Service and CorpID System will compute and display a 4-digit identification code using the Document Hash and the hash of Tokenised ID of the CorpID user. For anonymous digital signing, the 4-digit identification code will be computed using the Document Hash, the hash of HKIC number and the hash of client ID of e-Service. CorpID User should be requested to verify the two identification codes are the same before authorising the digital signing request. After receiving and verifying the signature bundle using the CorpID e-Cert, e-Service should notify the digital signing result to CorpID System by calling the “e-Service Acknowledges Digital Signing Result” CorpID API.

Details of the computation algorithm of the 4-digit identification code can be found in the Appendix.

1.1.7.1 Service Catalogue and Direct Login

CorpID Platform provides a Single Portal for e-Services to enable users to access e-Service directly with one single login through CorpID. e-Service Catalogue within CorpID Mini-program offers a list of e-Services which have adopted the features of CorpID. With Direct Login function, CorpID users can choose the desired e-Service to launch its web application for logging into the e-Service directly (i.e., without the need of providing further login credentials from user). Authentication is performed at the background with minimal user intervention for better user experience.

Direct Login

To provide a better user experience to CorpID user, CorpID provides a simplified Direct Login process, allowing user to initiate the login request from CorpID service catalogue (i.e., Direct Login v2). The implementation details can be found in Section 3.10.1 of this developer guide.

Direct Access

Similar to Direct Login workflow, CorpID users can choose the desired Website or App from Service Catalogue to launch its web application with external browser if their business process does not involve “Authentication”. Special approval is required to use Direct Access, and e-Service using the Direct Access function needs to provide sound justification to the Support Team.

1.1.8 Streamline Workflow

The Streamline Workflow is one of the important enhancement to realise “single portal for online government services (一網通辦)”, aiming to provide the simplified and seamless CorpID workflow with a view to enhancing user experience without extra switching back and forth between CorpID Mini-program and e-Services.

CorpID provides below two new APIs to simplify the authentication and form pre-filling workflow.

Direct Login v2

The streamlined authentication workflow (i.e., Direct Login v2) allows CorpID user to login to e-Service from Service Catalogue in a simple and swift manner.

Form pre-filling with Service Login (aka Profiles)

The streamlined form pre-filling workflow (i.e., Profiles) allows e-Service to obtain corpProfileFields , eCorpFields , nonHKResidentFields, profileFields and eMEFields for the purpose of identity verification and form pre-filling respectively in one go after the “Authentication” process, without CorpID user to give further explicit consent for data passing.

1.2 ASSUMPTIONS AND CONSTRAINTS

1. CorpID System adopts HTTPS to protect the data in transmission. Additional API data encryption is adopted for API POST request and response body.
2. Application data in the API POST request and response is in JSON format. e-Service Applications are responsible for processing of the returned data and reflecting the result to end users if required.
3. List of browsers supported by CorpID System is shown in Appendix of the CorpID API Specification. e-Service should detect the browser’s user agent value and pass respective source value in the list to CorpID System when necessary.

4. Reference Applications and sample source codes are provided for reference by e-Service to demonstrate the interaction between CorpID System (core system and Mini-program) and e-Service (including PC and mobile browser, Mobile Apps for Android and iOS, and backend service).
5. The Reference Applications and sample source codes are provided in the form of a Springboot application written in Java JDK 17.
6. CorpID Mini-program runs within the “iAM Smart” mobile app. The minimum Android and iOS version follows that of iAM Smart.
7. For adoption of the Reference Applications and sample source codes in other development platforms, SDKs and/or application environments, e-Service is responsible to check the compatibility and performs corresponding modification.
8. For e-Service not using the Reference Applications, e-Service should follow HTTPS standard protocols, CorpID API Specification and CorpID Developer Guide to develop the interfaces with CorpID System.
9. Please also refer to CorpID API Specifications and other technical documents for other assumptions and possible constraints.

1.3 E-SERVICE REGISTRATION TO “CORPID” SYSTEM

e-Service Providers are required to register their e-Services in CorpID System for accessing CorpID APIs. Registration information including application name, digital certificate for encipherment, redirect URL, etc., are required to be submitted by e-Services for the registration. A client ID (“clientID”) and a secret key (“clientSecret”) will be generated by CorpID System to the e-Service for accessing CorpID APIs upon the completion of the registration.

e-Service Provider is also required to provide Universal Link (iOS) / App Link (Android) and Package Name (Android) that offer better user experience and greater security for CorpID Mini-program to launch e-Service App from Service Catalogue. Custom URL scheme is not accepted unless sound justification can be provided.

1.4 POTENTIAL BUSINESS CASES USING “CORPID”

Potential business cases using CorpID are listed in the following sections for reference. For each case, possible high-level steps and the corresponding CorpID APIs and callback APIs to be used and/or implemented are provided (depending on the interface of e-Service and CorpID Mini-program as stipulated in Section 3.2.1).

While the involved CorpID APIs and callback APIs are listed below, details of the CorpID APIs and callback APIs can be found in the CorpID API Specification.

CorpID APIs:

#	CorpID API	Type
1	Request Symmetric Content Encryption Key	Data encryption / decryption

2	Revoke Symmetric Content Encryption Key	Data encryption / decryption
3	Request QR Page	Authentication
4	Request accessToken & Tokenised ID (openID)	Authentication
5	Request cAccessToken & Tokenised ID (cOpenID)	Authentication
6	Open “iAM Smart” Mobile App for Authentication	Authentication
7	Open CorpID Mini-program for Authentication	Authentication
8	Open CorpID Mini-program for Getting Context	Interface with CorpID Mini-program for business operation
9	Request Corp Profile	User Registration/Update
10	Request Form Pre-Filling	Business operation
11	Request Digital Signing	Business operation
12	Request PDF Digital Signing	Business operation
13	E-Service Acknowledges Digital Signing Result	Business operation
14	Request Document Sharing	Business operation
15	Request Anonymous Form Pre-Filling	Business operation
16	Obtain Anonymous Form Pre-Filling Result	Business operation
17	Request Anonymous Digital Signing	Business operation
18	Obtain Anonymous Digital Signing Result	Business operation
19	Request Anonymous PDF Digital Signing	Business operation
20	Obtain Anonymous PDF Digital Signing Result	Business operation
21	Request Anonymous Document Sharing	Business operation
22	Obtain Anonymous Document Sharing Result	Business operation
23	Obtain Identification Code	Business operation
24	Obtain User Profiles information	Business operation
25	Obtain Corp Profiles information	Business operation
26	Request VC Operations	Business operation
27	Obtain VC Operations Results	Business operation

Callback APIs implemented by e-Services:

#	Callback API (Implemented by e-Service)	Type
1	Callback with cAuthCode to e-Service App	Authentication
2	Callback with cAuthCode to e-Service Server	Authentication
3	Callback to Receive CorpID Profile	Business operation
4	Callback to Receive Form pre-filling Information	Business operation
5	Callback to Receive Digital Signing Result	Business operation
6	Callback to Receive PDF Digital Signing Result	Business operation
7	Callback to Receive Document Sharing Result	Business operation

8	Callback with cAuthCode to e-Service Server (Direct Login V2)	Authentication
---	---	----------------

1.4.1 e-Service Onboarding

1.4.1.1 Onboarding Journey

- e-Service shall prepare the following information before submitting the application form.
 - The public key certificate that is issued by Hong Kong Recognised Certification Authorities (Encipherment Cert);
 - Internet-facing server endpoint for CorpID callback with HTTPS enabled (depends on API used);
 - Prepare Tester's Apple ID and Google Play Account for Testing App;
 - Setup Universal Link (iOS e-Service App); and
 - Provide Android package name, activity class name (Android e-Service App).
- Upon application approval, the Support Team will create the CorpID Client ID and issue an email for the e-Service administrator in the self-service portal. The support team will provide a testing account for Testing App.
- e-Service administrator, creator and approver shall complete the following tasks in the CorpID self-service portal and "iAM Smart" self-service portal accordingly:
 - Setup Creator and Approver accounts;
 - Setup KEK certificate (Encipherment Cert) from HKRCA¹;
 - Check the Client's Secret;
 - Setup callback/ redirectURI / Direct Login v2 whitelist;
 - Setup Android Package Name and SHA-256 APP fingerprint for Android e-Service App; and
 - Setup iOS Universal Link for iOS e-Service App

1.4.1.2 Testing Environment

Domain Name	(TBC)
URL Scheme of "iAM Smart" mobile app (iOS and Android)	hk.gov.iamsmart.testapp://

¹ Recognized Certification Authorities in Hong Kong

https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/legal_framework/regulation/eto/ordinance/ca_in_hk/

“iAM Smart” App Installation	By invitation with AppStore and PlayStore with the tester list.
CorpID Self-Service Portal URL	(TBC)
KEK Certificate (Encipherment Cert)	Trial Cert from Hong Kong RCA is allowed
HTTPS Callback Endpoint	Https with production cert

1.4.1.3 Production Environment

(TBC)

1.4.1.4 Self-Service Portal

e-Service has to set up a KEK certificate (Encipherment Cert) and callback whitelist in the portal.

1.4.2 User Authentication

For CorpID user who has linked his/her CorpID account (i.e., Tokenised ID) to e-Service user repository, e-Service can authenticate the CorpID user with the following steps:

Step	Description	“iAM Smart” API	Callback API
1a	e-Service provides a link for login by CorpID in the application.		
1b	Alternatively, CorpID user can login the e-Service via CorpID service catalogue		
2a	e-Service requests for cAuthCode with required authorisation scopes (e.g., CorpID authentication, form pre-filling authorisation, etc.).	3, 5	A, B
2b	Alternatively, if CorpID user login the e-Service via CorpID service catalogue, e-Service would receive the cAuthCode accordingly.		H
3	e-Service gets cAccessToken and Tokenised ID (cOpenID) of CorpID and checks if it has linked with any account in the e-Service.	4	