

| **singpass**

Engagement Session with Public Sector

31 March 2026



Summary of key benefits/changes

Building a secure, flexible and user-first Singpass ecosystem

Area	What's changing?	What does it mean for partners?
1. Modern Security Standards	Adoption of FAPI 2.0 and OIDC best practices. - Pushed Authorization Requests (PAR) - Encrypted ID Token (JWE) - Demonstration of Proof-of-Possession (DPoP)	Aligns Singpass integrations with global financial-grade standards , providing stronger security and compliance readiness.
2. Granular Authentication Control	Introduction of Singpass specific fields like <code>acr_values</code> , <code>authentication_context_message</code> , <code>authentication_context_type</code>	Enables dynamic control over authentication context and assurance level, supporting adaptive security policies and risk-based authentication flows.
3. Enhanced User Experience	Enables context-aware and progressive logins , allowing authentication flows to adapt seamlessly based on transaction type or user risk profile.	Provides a smoother , more transparent user journey with clear purpose messaging and fewer unnecessary step-ups — improving both conversion and user trust.

Singpass FAPI 2.0



Changes applicable to all versions of Myinfo (and Login)

2

CHANGE 2

Update custom scheme URLs

4

CHANGE 4

Parse the ID Token

1

CHANGE 1

DPoP and PKCE are mandatory now

3

CHANGE 3

Use pushed authorization request (PAR)

5

CHANGE 5

Handle the new format of
the userinfo response

DPoP and PKCE are mandatory now

- Demonstrating Proof-of-Possession (DPoP) is a requirement.
- You must provide a DPoP proof in the **PAR, Token and Userinfo request**.
- This binds the Authorization Code and Access Token to your application's cryptographic key, rendering them useless if stolen by an unauthorized party.
- Each DPoP proof must be **freshly generated** and **unique per request**: DPoP proofs must not be reused. DPoP keypair must also be freshly generated for each authentication transaction.
- The DPoP key must be a separate key pair from the one used for client assertion: do not use the same key for both.
- Proof Key for Code Exchange (PKCE) is now mandatory for all clients to protect against **code injection attacks**.



Update custom scheme URLs

- The new API no longer supports custom scheme URLs (i.e., not starting with `https://`) for `redirect_uri` or `app_launch_url`.
- Mobile apps (Android/iOS) must switch to app-claimed HTTPS URLs for redirection back to the app.
 - Android: You must **implement Android App Links**.
 - iOS: You must **implement Universal Links**.
 - You can refer to official Android/iOS documentation for implementation.
- Singpass Developer Portal Updates:
 - You must **update your app configuration** in the Singpass Developer Portal **to add your new app-claimed HTTPS URLs**.
 - Once backend changes are deployed and working, **remove the old custom scheme URLs**.
- Backend Integration Changes:
 - You must **change the values for `redirect_uri` and `app_launch_url`** in the authorization request to use the new HTTPS URLs.
 - You must **include the `redirect_uri_https_type` parameter** with the value `app_claimed_https` in the authorization request.

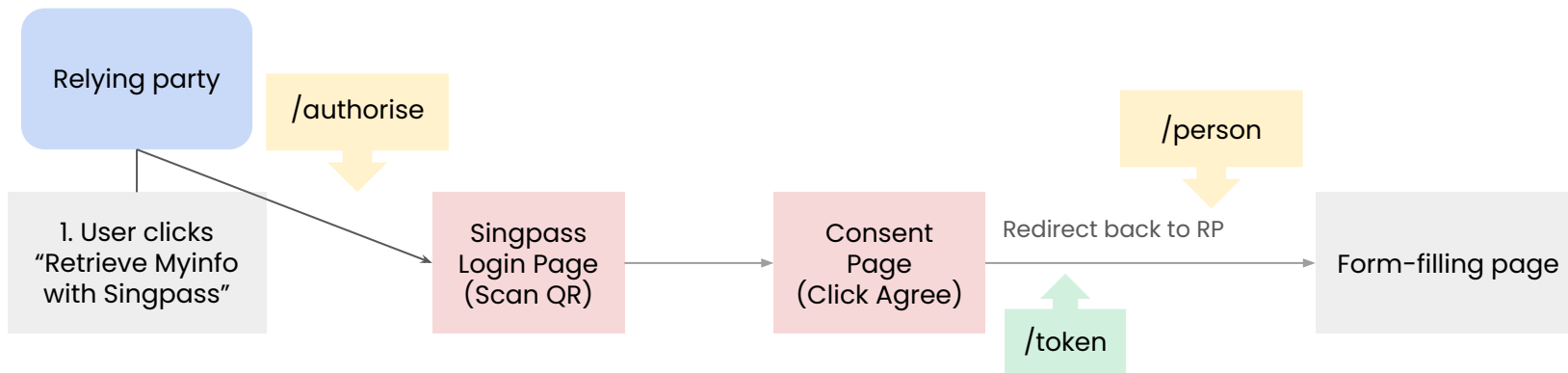


Use pushed authorization request (PAR)

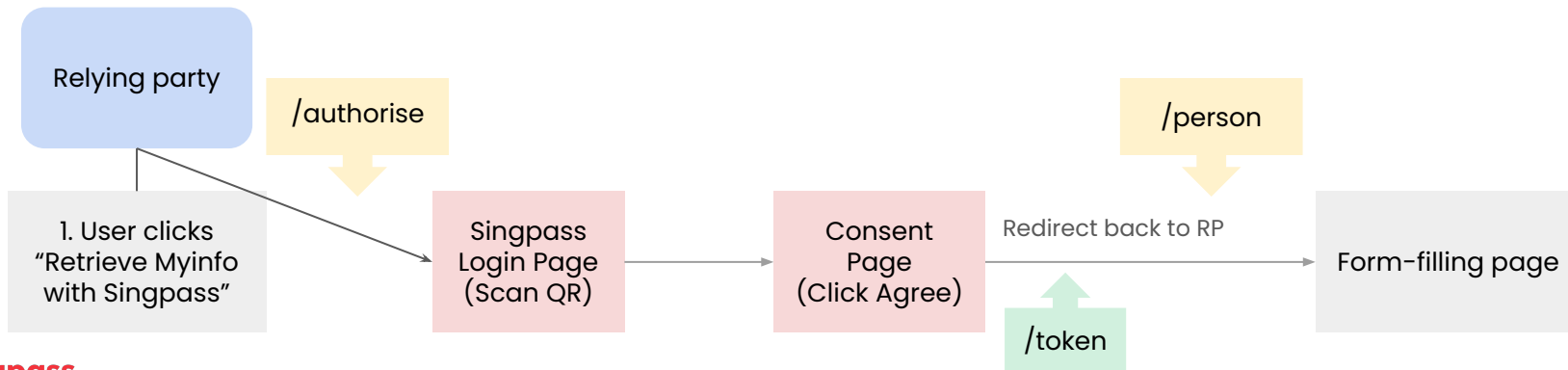
- Old Flow (Direct Redirect):
 - Sent authorization request by redirecting user to the authorization endpoint.
 - All authorization parameters were included directly as query parameters in the URL.
- New Flow (PAR):
 - First Step: Push Request
 - You must **send authorization request parameters** via a Pushed Authorization Request (PAR) endpoint.
 - Server Response
 - Receive a short-lived `request_uri` in the response from the server.
 - Final Step: Redirect
 - You must **redirect the user to the authorization endpoint**.
 - You must **only include the** `request_uri` **and your** `client_id` as query parameters in the redirect URL.



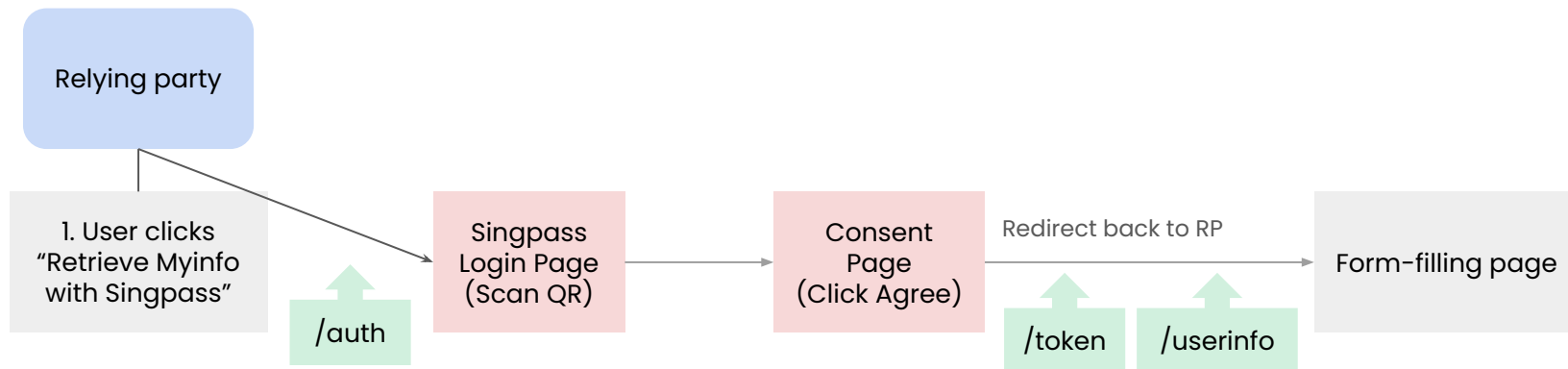
Myinfo v3



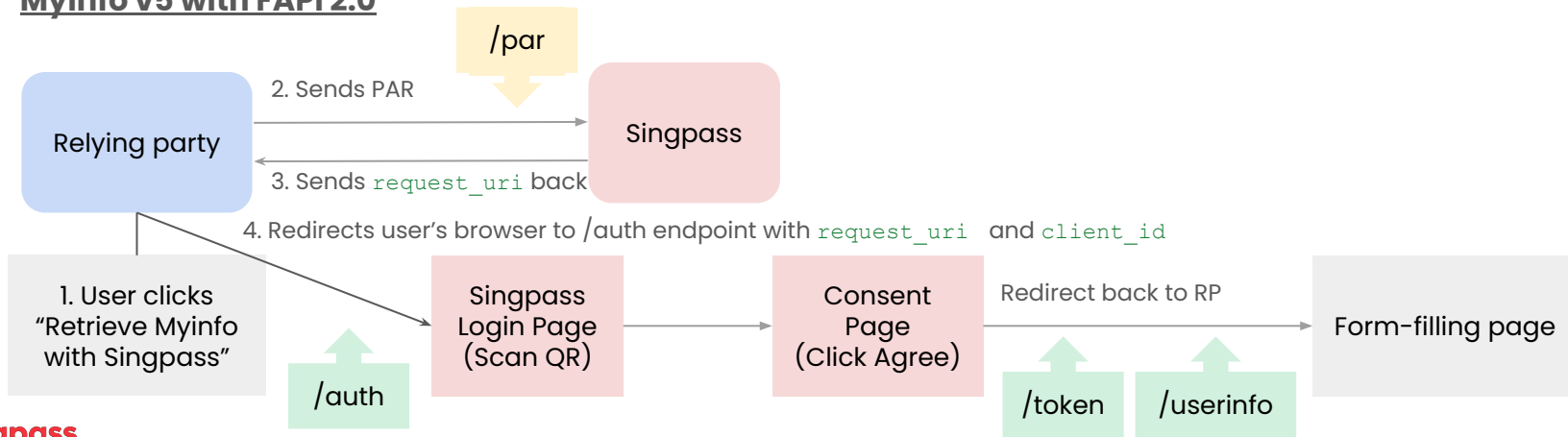
Myinfo v4



Myinfo v5



Myinfo v5 with FAPI 2.0



Parse the ID Token

1. All ID tokens are now encrypted
 - a. You must **implement ID token decryption logic** if you were previously receiving unencrypted ID tokens (e.g., if your app profile type is "UUID Only").
 - b. You must **add an encryption key** to your JSON Web Key Set (JWKS) if you don't have one already.
 - c. Note: No change is required if you are already decrypting the ID token.
2. The `sub` claim is now simplified and contains only the user's UUID.
 - a. Previous: `sub` contained comma-separated key-value pairs (e.g., `s=S8829314B,u=1c0cee38-`).
 - b. New: `sub` contains only the UUID (e.g., `1c0cee38-`).
 - c. You must **remove any custom parsing logic previously used to extract individual fields** from the `sub` claim.



Parse the ID Token

3. Retrieve the new sub_attributes claim
 - a. Information previously extracted from the sub claim (NRIC/FIN and Foreign ID/Country of Issuance) has been moved to the new sub_attributes claim.
 - b. To receive this claim, request the user.identity, name, email, or mobileno scope(s) for your app via the Singpass Developer Portal. If none of these scopes are relevant to your app, no changes are needed and you are not required to read the sub_attributes claim.
 - c. Once approved, read the sub_attributes claim from the ID token to retrieve this information.

Singapore Citizen, Permanent Resident, or FIN holder

```
"sub_attributes": {  
  "account_type": "standard",  
  "identity_number": "S1234567G",  
  "identity_coi": "SG",  
  "name": "John Doe",  
  "email": "johndoe@gmail.com",  
  "mobilenno": "91231234",  
}
```

Singpass Foreign Account holder

```
"sub_attributes": {  
  "account_type": "foreign",  
  "identity_number": "K28394589",  
  "identity_coi": "TK",  
  "name": "Larry Doe",  
  "email": "larrydoe@gmail.com",  
}
```



Handle the new format of the userinfo response

- The data returned in the UserInfo response now has a slightly different format.
 - The actual user data remains exactly the same.
 - The user's information is now nested inside a new top-level field called `person_info`.
- You must **update your parsing logic** to extract user data from the `person_info` field, rather than from the root of the response.



Handle the new format of the userinfo response

Old

```
{
  "uinfo": {
    "lastupdated": "2024-09-26",
    "source": "T",
    "classification": "C",
    "value": "S9000001B"
  },
  "name": {
    "lastupdated": "2024-09-26",
    "source": "T",
    "classification": "C",
    "value": "SOH HAO FENG"
  },
  "iss": "https://stg-id.singpass.gov.sg",
  "sub": "s=S9000001B,u=d45d8f21-6178-4713-b962-8635ed2a945a",
  "aud": "tWT3rfimn9hCezLr0MlnRUVq40fCNL4",
  "iat": 1746678089
}
```

New

```
{
  "person_info": {
    "uinfo": {
      "lastupdated": "2024-09-26",
      "source": "T",
      "classification": "C",
      "value": "S9000001B"
    },
    "name": {
      "lastupdated": "2024-09-26",
      "source": "T",
      "classification": "C",
      "value": "SOH HAO FENG"
    },
  }
  "iss": "https://stg-id.singpass.gov.sg",
  "sub": "d45d8f21-6178-4713-b962-8635ed2a945a",
  "aud": "tWT3rfimn9hCezLr0MlnRUVq40fCNL4",
  "iat": 1746678089
}
```



1 Migration guide (Myinfo v3 apps)

● Changes applicable to all versions of Myinfo

	Add/Update	Remove
General	● Implement Demonstration of Proof of Possession (DPoP) ● Update custom scheme URLs	
Authorization Request	● Use pushed authorization request ● Update existing parameters (e.g. <code>appLaunchURL</code> to <code>app_launch_url</code>) ● Add parameters for Proof Key for Code Exchange (PKCE) ● Add <code>nonce</code> parameter	● Remove parameters that are no longer used (e.g. <code>authmode</code>, <code>purpose</code>, <code>login_type</code>)
Token Exchange	● Parse the ID token ● Add parameters for Proof of Key Code Exchange (PKCE) ● Authenticate using client assertion instead of PKI Signature	● Remove the <code>state</code> parameter from request body
Userinfo Request	● Handle the new format of the userinfo response ● Update access token prefix from <code>Bearer</code> to <code>DPoP</code>	● Remove PKI Signature: authentication done via DPoP and access token ● Remove <code>sub</code> from the path: no need to perform parsing of access token ● Remove all query parameters: no longer required

Note: Myinfo (v5) apps should only have a single purpose.

If your current Myinfo (v3) app has multiple purposes, you will need to create a new Myinfo (v5) app for each purpose.

2 Migration guide (Myinfo v4 apps)

● Changes applicable to all versions of Myinfo

	Add/Update	Remove
General	● Update custom scheme URLs	
Authorization Request	● Use pushed authorization request ● Ensure <code>app_launch_url</code> is pre-registered in the Singpass Developer Portal ● Add <code>nonce</code> and <code>state</code> parameter	● Remove parameters that are no longer used (e.g. <code>subentity_id</code> <code>purpose_id</code>)
Token Exchange	● Parse the ID token ● Update your client assertion implementation (no more <code>cnf.jkt</code>)	
Userinfo Request	● Handle the new format of the userinfo response	● Remove <code>sub</code> from the path ● Remove all query parameters

Note: Myinfo (v5) apps should only have a single purpose.

If your current Myinfo (v4) app has multiple purposes, you will need to create a new Myinfo (v5) app for each purpose.



Migration Wizard

(«) Working with live data in Production ▾

Configuration

 Edit

① **Duplicate your existing app to speed up integration for FAPI 2.0**

Your existing app details will be duplicated. You only need to provide the new required parameters to proceed with the new integration.

Important note

- This app will stop working after 30 Sep 2026.
- The duplicated app retains the same scope as your existing app and does not require approval.
- Refer to the [migration guide](#) for technical details.

Duplicate app

(«) Working with live data in Production ▾

Myinfo

Provide information of your app for Myinfo integration.
All fields marked with an asterisk (*) are mandatory.

Step 1 App details

Step 2 Technical details

Step 3 Review scopes

① Your app details have been pre-filled

Review the fields and duplicate the app when ready.

Preview of Myinfo consent page your users will see – based on your inputs below.

Note: This sample Myinfo consent page is for pre-reading purposes.

singpass

Singpass retrieves personal data from relevant government agencies to pre-fill the relevant fields, making digital transactions faster and more convenient.

This digital service, **RedeemSG**, by Singpass Internal Entity for SDP, is requesting the following information from Singpass, for the purpose of **CDC Voucher Redemption**:

 <https://developer.singpass.gov.sg>

Back Next

3 Migration guide (Login / Myinfo v5 apps)

● Changes applicable to all versions of Myinfo

	Add/Update	Remove
General	● Implement Demonstration of Proof of Possession (DPoP) ● Update custom scheme URLs	
Authorization Request	● Use pushed authorization request ● Add parameters for Proof Key for Code Exchange (PKCE) ● (Only for Login apps) Add <code>authentication_context_type</code> to the authentication request	
Token Exchange	● Parse the ID token	
Userinfo Request	● Handle the new format of the userinfo response ● Update Authorization header prefix to be <code>DPoP</code> instead of <code>Bearer</code>	



Singpass Specific Fields (Login only)

`authentication_context_type`

This field communicates to Singpass the type or purpose of authentication being requested. It uses predefined “enum” values (e.g., `BANK_LOGIN_NEW_DEVICE` , `BANK_UPDATE_USER_INFORMATION`).

How it's used:

- Partners send this value to Singpass when initiating login.
- Singpass uses it to understand the authentication intent, enabling increased visibility for tracking user behaviour.
- It also helps Singpass categorise and optimise different authentication flows in the future (e.g., login vs. high-risk transaction).

Why it matters:

- Provides clarity of purpose for each authentication request.
- Enables future analytics and security tuning — for example, Singpass can track if certain authentication types are more prone to step-ups or re-authentications.



Singpass Specific Fields (Login only)

authentication_context_type

- > CPF transactions
- > Banking
- > Other Financial Institutions
- > Telcos
- > Others

Event	Enum Value
General authentication	APP_AUTHENTICATION_DEFAULT
Making a payment	APP_PAYMENT_DEFAULT
Password Change	APP_ACCOUNT_PASSWORD_CHANGE_DEFAULT
Password Reset	APP_ACCOUNT_PASSWORD_RESET_DEFAULT
Account Details Change	APP_ACCOUNT_DETAILS_CHANGE_DEFAULT

Event	Enum Value
CASA opening	BANK_CASA_OPENING
CASA Initial usage	BANK_CASA_INITIAL_USAGE
Debit/Credit Card application	BANK_CARD_APPLICATION
Debit/Credit Card initial usage	BANK_CARD_INITIAL_USAGE
Loan Application	BANK_LOAN_APPLICATION
Successful additional of local recipient	BANK_ADD_LOCAL_RECIPIENT
Successful additional of overseas recipient	BANK_ADD_OVERSEAS_RECIPIENT
Increase transfer limit	BANK_INCREASE_TRANSFER_LIMIT
Report Fraud or suspicious activity	BANK_REPORT_FRAUD_SUSPICIOUS_ACTIVITY
Funds transfer	BANK_FUNDS_TRANSFER_LOCAL
Remit money overseas	BANK_REMIT_MONEY_OVERSEAS
Report lost cards	BANK_REPORT_LOST_CARD
Change of notification method	BANK_CHANGE_NOTIFICATION_METHOD
Increase credit card limit	BANK_INCREASE_CREDIT_CARD_LIMIT
Cash advance	BANK_REQUEST_CASH_ADVANCE
Increased inflow and outflow of funds transfer	BANK_INCREASE_INFLOW_OUTFLOW
Activation of a dormant account	BANK_ACTIVATE_DORMANT_ACCOUNT
Login using a new device	BANK_LOGIN_NEW_DEVICE
Login from an unfamiliar IP	BANK_LOGIN_UNFAMILIAR_IP
User Information Update	BANK_UPDATE_USER_INFORMATION
New device registration	BANK_NEW_DEVICE_REGISTRATION
Unlock money lock	BANK_UNLOCK_MONEY_LOCK
Google Pay / Apple Pay card onboarding	BANK_GOOGLE_PAY_APPLE_PAY_CARD_ONBOARDING



Singpass Specific Fields (Login only)

Authentication_context_message

This message is displayed to users on the Singpass Mobile app during authentication. It helps users understand why they are being asked to log in or verify their identity.

Example scenario:

When a user logs in to your platform via Singpass, the message might say:

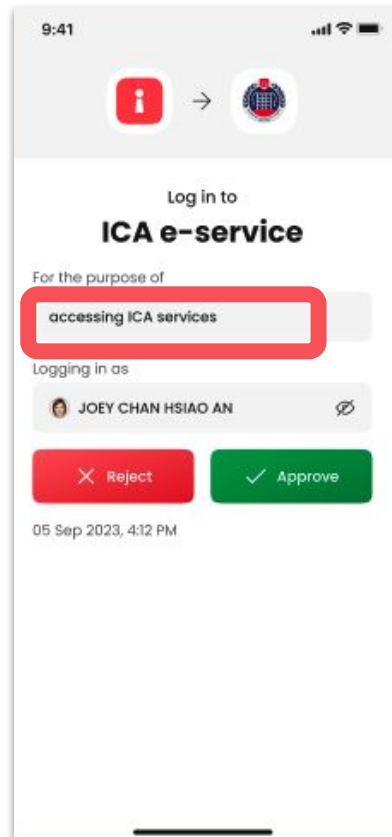
“Logging in to ABC Bank Internet Banking”

or

“Authorising access to change credit limit”

Why it matters:

- Enhances user trust and transparency by clearly stating what the login is for.
- Reduces user confusion, especially when users have multiple ongoing Singpass interactions.
- Partners can customise this message to match their service or brand context.



Singpass App Mockup Preview



Singpass Specific Fields (Login only)

Authentication_context_message

What makes a good message:

- Keep it under 70 characters for best display (hard limit is 100)
- Must be URL encoded
- Free-text, customisable per transaction to match the user's current journey

Useful guiding questions:

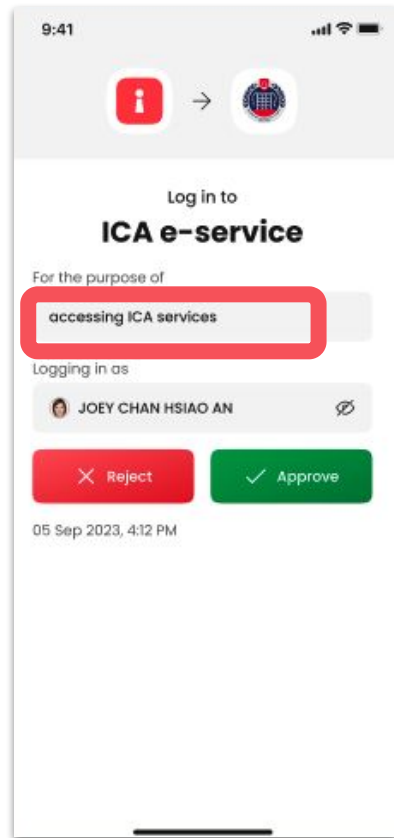
- What services are available after login?
- What action is the user trying to complete?
- What is the intended outcome?

✓ Good examples:

- "Complete the set up of your mobile banking token"
- "Manage and update your CPF nomination"
- "Apply and submit documents for your student loan"

✗ Avoid vague messages like:

- "Proceed" / "Log in to the portal" / "Continue with the application"



Singpass App Mockup Preview



Singpass Specific Fields (Login/Myinfo)

`acr_values` (Authentication Context Class Reference)

Defines the assurance level or authentication strength required for the transaction, controlling when Singpass should "step up" authentication. This gives partners granular control over authentication strength per transaction or user segment, and improves risk management. For instance, dynamically adjusting based on internal fraud-risk scoring.

Example usage:

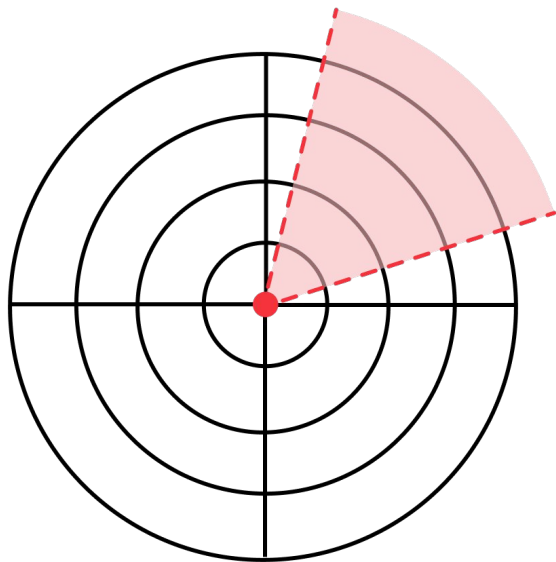
- Normal login may use `acr_values="urn:singpass:authentication:loa: 2"`.
- For high-risk or high-value transactions (e.g., large fund transfers or sensitive data access), partners can set `acr_values="urn:singpass:authentication:loa: 3"`, prompting Singpass to enforce a stronger authentication (e.g., biometric verification).

Important notes:

- `acr_values` is not applicable to all use cases. It is intended for high-risk transactions and is subject to approval on a case-by-case basis.
- Partners who require this capability should submit a support ticket request to the Singpass team for evaluation.



Call to Action



If you still have Myinfo v3/v4 apps,



Please migrate them to Myinfo v5 using Migration Wizard before 30 Sep 2026.

If you already have migrated to Myinfo v5 apps or only have Login apps,



Please ensure that your apps are FAPI 2.0 compliant by 31 Dec 2026.

Singpass FAPI 2.0 has been released for both staging & production environments

OpenID Connect Discovery endpoints	Myinfo v5	Myinfo v5 (FAPI 2.0-compliant)
Staging environment	https://stg-id.singpass.gov.sg/.well-known/openid-configuration	https://stg-id.singpass.gov.sg/fapi/.well-known/openid-configuration
Production environment	https://id.singpass.gov.sg/.well-known/openid-configuration	https://id.singpass.gov.sg/fapi/.well-known/openid-configuration

Note: All new apps created on the SDP from **11 February 2026 onwards** (including the apps created via Migration Wizard) must be FAPI 2.0 compliant.



Call for pilot partners

Exclusive FAPI 2.0 Pilot Program

We are inviting a select group of private/public sector organizations to join our Exclusive Pilot Program, which requires a commitment to go-live with FAPI 2.0-compliant app by end Q2 2026.

Selected partners of the program will receive white-glove technical and operational support up till the end of Q2 2026, including dedicated weekly technical support calls on their integration. This ensures a low-risk, accelerated deployment.

If you are interested to be a pilot partner for FAPI 2.0, please scan the following QR code to express your interest (limited slots only):

You will only be informed if you are selected as a pilot partner.



<https://go.gov.sg/pilotfapi>

Corppass FAPI 2.0

1 Migration guide (Corppass FAPI 2.0)

	Add/Update	Remove
General	● Implement Demonstration of Proof of Possession (DPoP) ● Implement Proof Key for Code Exchange (PKCE)	
Authorization Request	● Use pushed authorization request (PAR) ● Add <code>authentication_context_type</code>(mandatory) and <code>authentication_context_message</code>(optional) parameters ● Handle stricter client assertion requirements (to be covered below) ● Handle error redirect from Corppass when authorization request fails	
Token Exchange	● Handle new ID token structure (changes to sub claim, new act claim and sub_attributes claim) ● Handle stricter TTL & client assertion requirements	
Userinfo Request	● Call the renamed Userinfo endpoint instead of Authorization Info Endpoint ● Handle new structure of the userinfo response payload	



Handle new ID token structure

- Changes to sub claim, new act claim and sub_attributes claim

Old

```
{
  "iat": 1623162109,
  "iss": "https://stg-id.corppass.gov.sg",
  "at_hash": "6J4VIBBQpbAyyINL4NBW-Q",
  "sub":
  "s=SI234567P,uuid=0f14a2fc-09c2-4780-95f0-8c28347f2780,u=CP102,c=SG",
  "exp": 1623165709,
  "aud": "vOIJjWVrGyBMK6f31QYq",
  "amr": ["pwd", "sms"],
  "nonce": "ZEF+97zc3YZP7huv6nzKspfabDv0wRtce/aVNud23vU=",
  "userInfo": {
    "CPAcctType": "User",
    "CPUID_FullName": "John Grisham",
    "ISSPHOLDER": "YES"
  },
  "entityInfo": {
    "CPEntID": "T09LL0001B",
    "CPEnt_TYPE": "UEN",
    "CPEnt_Status": "Registered",
    "CPNonUEN_Country": "",
    "CPNonUEN_RegNo": "",
    "CPNonUEN_Name": ""
  }
}
```

New

```
{
  "iss": "https://stg-id.corppass.gov.sg",
  "aud": "vOIJjWVrGyBMK6f31QYq",
  "iat": 1623162109,
  "exp": 1623165709,
  "nonce": "ZEF+97zc3YZP7huv6nzKspfabDv0wRtce/aVNud23vU=",
  "amr": ["pwd", "sms"],
  "at_hash": "6J4VIBBQpbAyyINL4NBW-Q",
  "sub": "T09LL0001B",
  "sub_type": "entity",
  "sub_attributes": {
    "entity_type": "UEN",
    "entity_reg_number": "T09LL0001B",
    "entity_coi": "SG",
    "entity_name": "My Example Company",
    "entity_uen_status": "Registered"
  },
  "act": {
    "sub": "1c0cee38-3a8f-4f8a-83bc-7a0e4c59d6a9",
    "sub_type": "user",
    "sub_attributes": {
      "account_type": "standard",
      "identity_number": "SI234567P",
      "identity_coi": "SG",
      "name": "John Grisham"
    }
  }
}
```



ID Token: revised sub claim

- Revised sub claim:
 - Old:
 - s : Identity ID (e.g. NRIC/FIN/Foreign ID)
 - uuid : User's globally unique identifier (e.g. 0f14a2fc-09c2-4780-95f0-8c28347f2780)
 - u : System-defined ID (e.g. CP1234)
 - c : Two-character country code, conforming to ISO 3166-1 Alpha-2 (e.g. SG)
 - New: It will be the entity's UEN (if it is of UEN type) or the Corppass Entity ID (if not UEN type).

Old

```
"sub": "s=S1234567P,  
uuid=0f14a2fc-09c2-4780-95f0-8c28347f2780,  
u=CP192,  
c=SG",
```

New

```
"sub": "T09LL0001B",
```

In Corppass Authorization API V1, you might be familiar with
1. "CPentID": "T09LL0001B",



ID Token: new sub_attributes claim

- New `sub_attributes` claim may appear in two places:
 - When present at the top level, it carries information about the Subject (Entity) identified by sub;
 - When nested under act, it carries information about the Subject (User) identified by act.sub

```
"sub": "T09LL0001B",
"sub_type": "entity",
"sub_attributes": {
  "entity_type": "UEN",
  "entity_reg_number": "T09LL0001B",
  "entity_coi": "SG",
  "entity_name": "My Example Company",
  "entity_uen_status": "Registered"
},
"act": {
  "sub": "1c0cee38-3a8f-4f8a-83bc-7a0e4c59d6a9",
  "sub_type": "user",
  "sub_attributes": {
    "account_type": "standard",
    "identity_number": "S1234567P",
    "identity_coi": "SG",
    "name": "John Grisham"
  }
}
```



New sub_attributes claim for Entity Account

- Claims under entityInfo is now subsumed under `sub_attributes` in entity account
- You can now request for 3 new entity scopes: `entity.identity`, `entity.basic_profile.name` and/or `entity.basic_profile.uen_status`
- For `sub_attributes` claim for entity account, the `entity_type` value will either be UEN, NON-UEN or GSTN (provided `entity.identity` scope is requested)

Singapore-registered entity

```
{
  ...
  "sub": "T09LL0001B",
  "sub_type": "entity",
  "sub_attributes": {
    "entity_type": "UEN",
    "entity_reg_number": "T09LL0001B",
    "entity_coi": "SG",
    "entity_name": "My Example Company",
    "entity_uen_status": "Registered"
  }
}
```

Note:

`entity_uen_status` is returned only if the represented entity is of type UEN.

In Corppass Authorization API V1, you might be familiar with

1. "CPEnt_Type": "UEN",
2. "CPEnt_Status": "Registered",

Foreign entity

```
{
  ...
  "sub": "C19001125A",
  "sub_type": "entity",
  "sub_attributes": {
    "entity_type": "NON-UEN",
    "entity_reg_number": "202219428Z",
    "entity_coi": "MY",
    "entity_name": "My Example Malaysian Company"
  }
}
```

In Corppass Authorization API V1, you might be familiar with

1. "CPNonUEN_Country": "Malaysia",
2. "CPNonUEN_RegNo": "202219428Z",
3. "CPNonUEN_Name": ""



New sub_attributes claim for User Account

- Claims under userInfo is now subsumed under `sub_attributes` in user account
- You can now request for 3 new user scopes: `user.identity`, `user.name` and/or `user.corppass.email`
- For `sub_attributes` claim for user account, the `account_type` value will either be `standard` or `foreign`

Singapore Citizen, Permanent Resident or FIN holder

```
{
  ...
  "act": {
    "sub": "1c0cee38-3a8f-4f8a-83bc-7a0e4c59d6a9",
    "sub_type": "user",
    "sub_attributes": {
      "account_type": "standard",
      "identity_number": "S1234567P", // NRIC / FIN
      "identity_coi": "SG",
      "name": "John Grisham"
    }
  }
}
```

Singpass Foreign Account holder

```
{
  ...
  "act": {
    "sub": "1c0cee38-3a8f-4f8a-83bc-7a0e4c59d6a9",
    "sub_type": "user",
    "sub_attributes": {
      "account_type": "foreign",
      "identity_number": "K28394589", // Foreign ID
      "identity_coi": "MY",
      "name": "John Grisham"
    }
  },
}
```



ID Token: new sub_attributes claim

- With regards to the entity and user scopes:
 - For existing e-services, these scopes are added by default. You are only required to include these scopes in your PAR if you intend to test for Corppass FAPI 2.0
 - For new e-services, these scopes are **NOT** added by default. You are required to request them in the Corppass Developer Portal, and also include these scopes in your PAR if you intend to test for Corppass FAPI 2.0



Handle stricter TTL & client assertion requirements

- Authorization code expiry is reduced from 10 min to 1 min
- Maximum allowed lifespan for client assertion tokens is now 2 mins **(for both PAR and Token endpoint)**
- Client assertions can no longer be reused. All client assertions must include `jti` claim to prevent client assertion replay attacks.

1 Migration guide (Corppass FAPI 2.0)

	Add/Update	Remove
General	● Implement Demonstration of Proof of Possession (DPoP) ● Implement Proof Key for Code Exchange (PKCE)	
Authorization Request	● Use pushed authorization request (PAR) ● Add <code>authentication_context_type</code>(mandatory) and <code>authentication_context_message</code>(optional) parameters ● Handle stricter client assertion requirements (to be covered below) ● Handle error redirect from Corppass when authorization request fails	
Token Exchange	● Handle new ID token structure (changes to sub claim, new act claim and sub_attributes claim) ● Handle stricter TTL & client assertion requirements	
Userinfo Request	● Call the renamed Userinfo endpoint instead of Authorization Info Endpoint ● Handle new structure of the userinfo response payload	



Handle new userinfo response payload structure

- The only structural change is that the AuthInfo and TPAuthInfo claims have been converted from PascalCase to snake_case (auth_info and tp_auth_info), while the actual data within those claims remains the same.

Old

```
{
  ... // truncated for brevity
  "AuthInfo": {
    ... // truncated for brevity
  },
  "TPAuthInfo": {
    ... // truncated for brevity
  }
}
```

New

```
{
  ... // truncated for brevity
  "auth_info": {
    ... // truncated for brevity
  },
  "tp_auth_info": {
    ... // truncated for brevity
  },
}
```



Handle new userinfo response payload structure

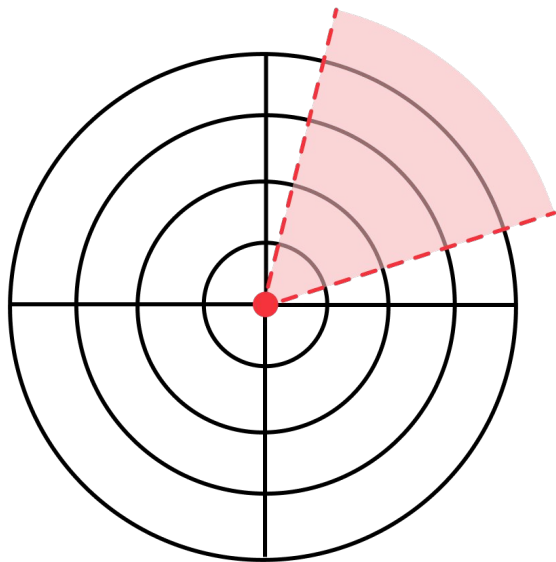
- In addition, the response format has been enhanced such that Userinfo Endpoint response is returned as JWE (JSON Web Encryption), while Authorization Info Endpoint remains as JWS (JSON Web Signature).
- Partners are therefore required to decrypt the JWE payload using their registered private key before processing the claims.

1 Migration guide (Corppass FAPI 2.0)

	Add/Update	Remove
General	● Implement Demonstration of Proof of Possession (DPoP) ● Implement Proof Key for Code Exchange (PKCE)	
Authorization Request	● Use pushed authorization request (PAR) ● Add <code>authentication_context_type</code>(mandatory) and <code>authentication_context_message</code>(optional) parameters ● Handle stricter client assertion requirements (to be covered below) ● Handle error redirect from Corppass when authorization request fails	
Token Exchange	● Handle new ID token structure (changes to sub claim, new act claim and sub_attributes claim) ● Handle stricter TTL & client assertion requirements	
Userinfo Request	● Call the renamed Userinfo endpoint instead of Authorization Info Endpoint ● Handle new structure of the userinfo response payload	



Call to Action



If your e-service is on Corppass Authorization API (Legacy),



Please ensure that your apps are FAPI 2.0 compliant by 31 March 2027.

Corppass FAPI 2.0 has been released for both staging & production environments

OpenID Connect Discovery endpoints	Corppass FAPI 2.0
Staging environment	https://stg-id.corppass.gov.sg/.well-known/openid-configuration
Production environment	https://id.corppass.gov.sg/.well-known/openid-configuration

Note: All new e-services created on the Corppass Developer Portal from **23 March 2026 onwards** must be FAPI 2.0 compliant.



Upcoming Timeline

Year	Date	Event	Note
2026	Mar	Engagement sessions with private and public sector on FAPI 2.0	
	30 Sep	Myinfo v3/v4 Decommission	Existing Myinfo v3/v4 apps will be deactivated except for Myinfo v3 Person-Basic apps
	31 Dec	Singpass FAPI 2.0 compliance deadline	Partners to ensure all Singpass apps are FAPI 2.0 compliant
2027	31 Mar	Corppass FAPI 2.0 compliance deadline	Partners to ensure all Corppass e-services are FAPI 2.0 compliant

Thank you

Support and resources



FAPI 2.0 Technical documentation	Singpass partner helpdesk	GitHub Community
https://go.gov.sg/spfapi2	https://partnersupport.singpass.gov.sg	https://github.com/singpass/demo-app