



PSD2 Onboarding

This document describes the payload JSON accepted by the Danske Bank PSD2 registration endpoint (<https://psd2-api.danskebank.com/psd2/v1.0/thirdparty/register>)

To register as a TPP client at Danske Bank, the TPP should send an HTTP POST to the bank's registration endpoint.

1 Request Claims

The client registration request **MUST** contain the following claims unless designated as Optional.

The TPP **MAY** add additional claims to the payload. Danske Bank **MAY** ignore claims not in the chart below.

If a claim name matches a specified claim in any of [RFC7519], [RFC7591], [OIDC DCR] or [FAPI], the usage must also match the specification

Claim	Description	Source Spec	Optional	Comments
token_endpoint_auth_method	Specifies which token endpoint authentication method the TPP wants to use	[RFC7591]	NO	Should be one among token_endpoint_auth_methods_supported in Danske Bank's Well Known Endpoint
grant_types	A JSON array specifying what the TPP can request to be supplied to the token endpoint as exchange for an access token	[RFC7591]	NO	Should be one among grant_types_supported in Danske Bank's Well Known Endpoint
software_statement	Software statement is a JSON Web Token (JWT) that asserts metadata values about the client software as a bundle	[RFC7591]	NO	Software Statement signed by client's QSEAL Details of the Software Statement claims are detailed below (Section 2)
id_token_signed_response_alg	Algorithm which the TPP expects to sign the id_token, if an id_token is returned.	[OIDC DCR]	NO	Should be one among id_token_signing_alg_values_supported in Danske Bank's Well Known Endpoint
request_object_signing_alg	Algorithm which the TPP expects to sign the request object if a request object will be part of the authorization request sent to the ASPSP.	[OIDC DCR]	NO	Should be one among request_object_signing_alg_values_supported in Danske Bank's Well Known Endpoint
tls_client_auth_subject_dn	This value must be set if token_endpoint_auth_method is set to tls_client_auth		NO	The tls_client_auth_subject_dn claim MUST contain the DN of the certificate that the TPP will present to the ASPSP token endpoint.

2 Software Statement

Header

Claim	Description	Source Spec	Optional	Comments
alg		[RFC7519]	NO	Must be PS256.
kid		[RFC7519]	NO	KID in client's JWKS Endpoint corresponding to the key used to sign the Software Statement
typ		[RFC7519]	NO	Must be JWT

Pay Load

Claim	Description	Source Spec	Optional	Comments
iss	Request Issuer	[RFC7519]	NO	Should be GURN (Global Unique Reference Number): Combination of Country, Competent Authority Name and URN that is unique across Europe.
iat	Time of issuance of request	[RFC7519]	NO	Time elapsed since Unix Epoch in seconds
exp	Request expiration time	[RFC7519]	NO	- Time elapsed since Unix Epoch in seconds - Should be greater than iat. - Must be short lived i.e.10 minutes from iat.
aud	Request audience (The ASPSP aud) as advertised on the well-known openid connect endpoint	[RFC7519]	NO	Should match the issuer of Danske Bank's well-known Url.
jti	JWT ID	[RFC7519]	NO	Should be GUID in UUID v4 format.
software_id	A unique identifier string assigned by the client used by registration endpoints to identify the client software to be dynamically registered.	[RFC7591]	NO	Should be GUID in UUID v4 format if generated by client's and not by Trust Anchor.
software_client_name	Legal Entity Identifier or other known organization name	[RFC7591]	NO	

Claim	Description	Source Spec	Optional	Comments
software_version	The version number of the software should a TPP choose to register and / or maintain it	[RFC7591]	NO	
scope	JSON array of objects containing a Member State and PSD2 Role	[RFC7591]	NO	
software_contacts	JSON array of objects containing a triplet of name, email, and phone number	[RFC7591]	NO	
software_redirect_uris	JSON array of Registered URIs the TPP will use to interact with the ASPSP	[RFC7591]	NO	
software_client_uri	The website or resource root uri	[RFC7591]	NO	
software_logo_uri	Link to the TPP logo. Note, ASPSPs are not obliged to display images hosted by third parties	[RFC7591]	NO	
software_tos_uri	A link to the software's terms of service page	[RFC7591]	NO	
software_policy_uri	A link to the software's policy page	[RFC7591]	NO	
software_jwks_endpoint	Contains all active signing certificates	[RFC7591]	NO	• Must contain x5c of the signing certificate • Must contain full chain
software_jwks_revoked_endpoint	Contains all revoked signing certificates	[RFC7591]	NO	
software_type	web or mobile		YES	MUST be web if specified.