Danske Bank

PSD2 Onboarding *(https://psd2-api.danskebank.com/psd2/v1.0/thirdparty/register)*

This document describes the payload json accepted by the Danske Bank PSD2 registration endpoint.

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], 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 in below table
id_token_signed_response_alg	Algorithm which the TPP expects to sign the id_token, if an id_token is returned.	[RFC7519]	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.	[RFC7519]	NO	Should be one among request_object_signing_alg_values_supported in Danske Bank's Well Known Endpoint
tls_client_auth_dn	This value must be set iff token_endpoint_auth_method is set to tls_client_auth		Conditional	The tls_client_auth_dn claim MUST contain the DN of the certificate that the TPP will present to the ASPSP token endpoint.