



DTCC REST API Authentication Modernization

CLIENT FAQ: OAUTH JWT-BASED CLIENT CREDENTIALS MIGRATION

VERSION 1.0

JULY 22, 2026

DOCUMENT INFORMATION

Audience	DTCC API Clients
Prepared For	Enterprise Client Operations (ECO) client communication
Version	1.0
Date	July 22, 2026
Classification	DTCC Internal (Green)

Revision History

Version	Date	Description
1.0	July 22, 2026	Initial client FAQs for OAuth JWT-based Client Credentials migration.

TABLE OF CONTENTS

Overview 4

Q1. Why is DTCC requiring this migration? 4

Q2. Which DTCC APIs are impacted? 4

Q3. Will API endpoints or business payloads change? 4

Technical FAQ..... 4

Q4. What is OAuth Client Credentials with JWT authentication?..... 4

Q5. Do we need to host our own Authorization Server? 4

Q6. What is the difference between Static Key and Dynamic Key options? 5

Q7. What information must clients provide to DTCC?..... 5

Q8. What changes are DTCC clients required to make? 5

Q9. Will clients need new credentials? 6

Q10. What cryptographic algorithms will be supported? 6

Q11. What if our organization currently uses Ping Identity or similar identity products?..... 6

Q12. Will DTCC provide sample code or implementation examples on JWT generation? 6

Q13. How do clients test the new authentication method?..... 6

Operations FAQ 7

Q14. Will current OAuth ROPC authentication continue to work during migration? 7

Q15. What happens if a client does not migrate before retirement?..... 7

Q16. Will there be service interruption during migration?..... 7

Q17. How often will keys need to rotate? 7

Q18. Will DTCC provide a self-service onboarding portal? 7

Q19. Do clients need to change how APIs are called after receiving an access token?..... 7

Q20. What benefits does this migration provide? 7

Q21. Who should clients contact for support? 7

Recommended Client Action..... 8

FREQUENTLY ASKED QUESTIONS

Overview

This FAQ is intended to help DTCC API clients understand the migration from legacy username/password-based (ROPC) API authentication methods to OAuth JWT-based Client Credentials authentication for machine-to-machine REST API integrations.

Q1. Why is DTCC requiring this migration?

DTCC is improving API security by replacing legacy authentication methods that rely on usernames and passwords. The new OAuth JWT-based Client Credentials flow strengthens machine-to-machine authentication by using standards-based asymmetric cryptography.

Q2. Which DTCC APIs are impacted?

This migration is intended for the consumers of DTCC REST APIs that currently use OAuth ROPC Authentication for machine-to-machine integrations. DTCC will provide additional onboarding communication for impacted APIs and clients.

Q3. Will API endpoints or business payloads change?

The migration is focused on authentication. Clients should expect to change how access tokens are obtained. Access token endpoint and business API endpoint URLs, request payloads, and response payloads are not expected to change solely because of this authentication migration.

Technical FAQ

Q4. What is OAuth Client Credentials with JWT authentication?

The client creates a JWT, signs it with the client private key, and submits the signed JWT to DTCC Access Token API endpoint as a client assertion. DTCC validates the JWT using the client public key and issues an OAuth access token.

Q5. Do we need to host our own Authorization Server?

Not necessarily. Clients using the Static Key model only need the ability to generate and sign JWTs and provide the corresponding public key to DTCC.

A client-hosted public key endpoint typically hosted by client authorization server is only needed for the Dynamic Key model.

Q6. What is the difference between Static Key and Dynamic Key options?

Comparison Item	Static Key Option	Dynamic Key Option
Key registration with DTCC	Required. The client provides the public key to DTCC during onboarding or key rotation.	Not required. DTCC retrieves the public key from the client-hosted endpoint during API request processing time.
Client provides public key API (JWKS endpoint)	Not required. DTCC validates JWTs using the public key persisted with DTCC.	Required. The client must host an accessible public key retrieval endpoint (JWKS endpoint) for DTCC to dynamically obtain the current public key.
Key rotation update at DTCC needed	Required. When the key changes, the client must provide the updated public key to DTCC through CRS key management functions.	Not required. No manual DTCC update is needed.
Primary consideration	Simpler implementation. Requires client to register and update public key when the key is rotated.	More flexible for key rotation. Requires the client to operate and maintain a highly available public key endpoint.

Q7. What information must clients provide to DTCC?

For Static Key model, clients must provide the client's roboID and public key to DTCC via Client Registration System (CRS).

For Dynamic Key model, clients must provide a client's roboID and public key retrieval endpoint.

Q8. What changes are DTCC clients required to make?

Clients should plan to:

1. **Update applications** that obtain DTCC access tokens to replace OAuth ROPC username and password credentials with signed JWT client assertions.
2. **Select** a public-key management model and **register** either the client's public key for the Static Key model or its public-key retrieval endpoint for the Dynamic Key model.
If selecting the Dynamic Key model, **deploy** and operate a secure, reliable public-key retrieval endpoint accessible to DTCC.
3. **Test** the new token-acquisition and API-invocation flow in DTCC's **PSE** environment **before production migration**.

Q9. Will clients need new credentials?

- New clients starting to consume DTCC APIs will need to request a client ID (Machine ID or roboID)
- Existing clients migrating from ROPC to JWT-based client credentials will continue to use their existing client ID
- Both new clients and existing clients need to register either their public key or their public key API endpoint (JWKS URL).

Q10. What cryptographic algorithms will be supported?

DTCC will initially support **RS256**, which uses RSA with SHA-256, for signing JWT client assertions. Clients should use an **RSA key pair with a minimum key size of 2048 bits**.

Note:

The client must retain and protect the private key and make the corresponding public key available to DTCC through either the Static Key or Dynamic Key model.

Q11. What if our organization currently uses Ping Identity or similar identity products?

Clients using identity products that support JWT-based OAuth client authentication may be able to implement the migration through product configuration and key management rather than custom application code.

Q12. Will DTCC provide sample code or implementation examples on JWT generation?

Yes. DTCC will provide migration instruction, technical guidance, FAQs, and onboarding assistance. DTCC will also provide a sample JWT generator java program to illustrate JWT generation and signing at [API Marketplace](#).

Q13. How do clients test the new authentication method?

Clients should register test credentials, generate a signed JWT client assertion, request an access token in DTCC's PSE (test) environment, and then invoke the target DTCC API using the issued access token.

Operations FAQ

Q14. Will current OAuth ROPC authentication continue to work during migration?

DTCC expects to support a phased migration period to allow clients to transition. However, OAuth ROPC will be retired after migration completion.

Q15. What happens if a client does not migrate before retirement?

After DTCC retires the ROPC authentication methods, clients still using those methods will no longer be able to access impacted APIs. Clients should complete migration before published retirement deadlines.

Q16. Will there be service interruption during migration?

No. During migration period, both ROPC and JWT client credentials flows will be supported.

Q17. How often will keys need to rotate?

As a recommended best practice, clients are to rotate their signing keys at least once every 12 months and immediately upon suspected compromise that could impact key integrity.

For clients using the **Static Key** model, key rotation requires registering the new public key with DTCC before the new key is used for JWT signing.

For clients using the **Dynamic Key** model, key rotation can be performed through the client's JWKS endpoint without requiring DTCC to update.

Q18. Will DTCC provide a self-service onboarding portal?

Yes. DTCC will support self-service credential management through CRS, including client ID registration, public key or key retrieval JWKS endpoint registration, and key rotation.

Q19. Do clients need to change how APIs are called after receiving an access token?

No. Clients will continue to call APIs using OAuth bearer access tokens. The change is in how the access token is obtained.

Q20. What benefits does this migration provide?

The migration substantially improves API authentication security posture. In addition, dynamic keys eliminate manual rotation requirements.

Q21. Who should clients contact for support?

DTCC will provide support channels through Enterprise Client Operations and client migration materials. For questions related to this communication, please contact technicalchangeenablement@dtcc.com.

Recommended Client Action

Start planning now

Clients should:

- identify applications using OAuth ROPC,
- determine technical ownership,
- implement JWT support in their technology stack, and
- prepare for PSE testing.

© 2026 DTCC. All rights reserved. DTCC and DTCC (Stylized) and Financial Markets. Forward. are registered and unregistered trademarks of The Depository Trust & Clearing Corporation DTCC. The services described herein are provided under the “DTCC” brand name by certain affiliates of The Depository Trust & Clearing Corporation (“DTCC”). DTCC itself does not provide such services. Each of these affiliates is a separate legal entity, subject to the laws and regulations of the particular country or countries in which such entity operates. Please see www.dtcc.com for more information on DTCC, its affiliates and the services they offer.

Doc Date: July 22, 2026

Publication Code: CP_2034

Service: DTCC REST API Authentication Modernization

Title: Client FAQ: OAuth JWT-Based Client Credentials Migration

For More Information

DTCC Client Center: www.dtcc.com/client-center

DTCC Learning Center: www.dtccllearning.com