```
# Pseudocode: Token-based API Authentication

function requestAccessToken(client_id, client_secret, grant_type, scope):
    payload = {
        "client_id": client_id,
        "client_secret": client_secret,
        "grant_type": grant_type,
        "scope": scope
    }
    response = HTTP.post("https://auth.example.com/token", json=payload)
    if response.status_code != 200:
        logError(response.body)
        raise AuthError("Failed token issuance")
    token_data = parseJSON(response.body)
    return token_data["access_token"], token_data["expires_in"]

# Edge cases
- When grant_type="refresh_token", payload needs "refresh_token" field, not
client_secret.
- If JSON has BOM or non-UTF8, parseJSON will throw; wrap in try/catch.
- Rate limit: if 429 returned, backoff exponentially: base_delay=1s, max_delay=32s.

# Notes:
• Some servers ignore unknown JSON fields; others reject outright.
• Clock skew: tokens issued at T■ may be invalid until T■ + ∆; clock sync required.
```