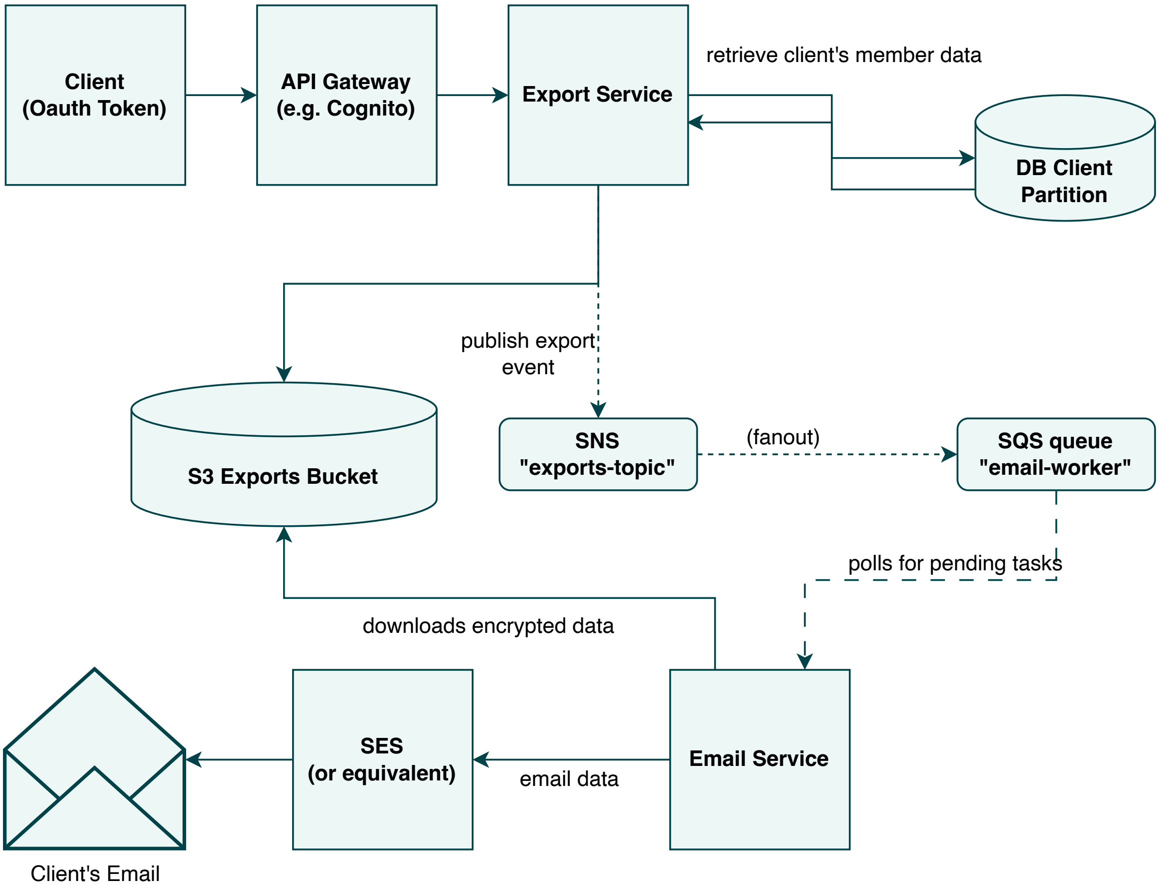
eversports

Export memberships (CSV) via email



Basic flow:

1. Client requests export (e.g. POST /exports/users) using OAuth2 client credentials -> API Gateway -> Export Service.
2. Export Service validates token, loads client metadata from database where this is stored (hereafter "DB").
3. Export Service streams user records -> produces CSV stream.
4. Export Service calls KMS GenerateDataKey to obtain a plaintext data key (e.g. AES-256-GCM).
5. Export Service encrypts CSV with data key.
6. Export Service encrypts data key (the small symmetric key) with client's public PGP key -> dataKey.asc (armored).
7. Encrypted CSV + metadata uploaded to S3. dataKey.asc stored in message payload or small S3 object. Export status saved to DB.
8. Export Service publishes message to SNS topic (or directly SQS). Message contains clientId, s3Key, encryptedDataKey (base64/armored), iv, tag, algorithm, requestId, allowed recipient(s).
9. SNS -> SQS (email queue). Email Service polls SQS.
10. Email Service downloads encrypted object (or creates short presigned link), fetches encryptedDataKey and metadata, composes MIME email (attach .enc and .key.asc or attach link + .key.asc), and sends via SES to client email(s).
11. Email Service updates DB export status to sent (via SQS -> Export Service, or directly if it has IAM rights).
12. S3 lifecycle removes object after retention window; DLQ handles failed deliveries.