FRD-104: Upload KYC Documents to Storage (S3)

1. Functionality Summary

The system must allow customers to upload KYC documents and securely store them in an S3 bucket. The documents include Aadhaar images, PAN image, photograph, and signature. The system must validate file type, size, clarity, and ensure encrypted transport. Upload metadata must be stored in the KYC table.

2. Detailed Functional Description

2.1 Input Fields

Field	Type	Mandatory	Rules
aadhaarFront	File	Yes	PNG/JPG/PDF, ≤ 5MB
aadhaarBack	File	Yes	PNG/JPG/PDF, ≤ 5MB
panImage	File	Yes	PNG/JPG/PDF, ≤ 5MB
photo	File	Yes	PNG/JPG, Clear face
signature	File	Yes	PNG/JPG, Clear scan

2.2 Upload Flow

```
# ENDPOINT
POST /kyc/upload

# HEADERS
Content-Type: multipart/form-data

# REQUEST (FORM DATA)
aadhaarFront: <FILE>
aadhaarBack: <FILE>
panImage: <FILE>
photo: <FILE>
signature: <FILE>

# SERVER PROCESSING
1. Validate file type and size
2. Generate objectKey for S3:
■kyc/{customerId}/{documentType}/{timestamp}.png
3. Upload to S3 using PUT operation
4. Store metadata in DB:
■{s3Url, objectKey, mimeType, size}

# RESPONSE (SUCCESS)
{
■"status": "SUCCESS",
■"uploaded": [
■■"aadhaarFront",
```

```
■■"aadhaarBack",
■■"panImage",
■■"photo",
■■"signature"
■]
}

# RESPONSE (FAILURE)
{
■"status": "FAILURE",
■"errorCode": "ERR-1044",
■"message": "Failed to upload to S3"
}
```

2.3 System Behavior

On valid files:
• Upload each file to S3
• Store metadata in DB

On invalid file type/size:
• Reject request and throw validation error

On S3 failure:
• Retry upload up to 2 times
• If still failing → SYSTEM ERROR

3. Error Codes

Error Code	Description	When Triggered
ERR-1040	Invalid file type	Wrong MIME type
ERR-1041	File too large	> 5MB
ERR-1042	Unreadable image	Blurry or corrupted image
ERR-1043	S3 unreachable	Timeout / network failure
ERR-1044	S3 upload failure	PUT operation failed
ERR-1045	Metadata save failure	DB insert fails

4. Preconditions

• PAN & Aadhaar validation completed successfully (FRD-101 & FRD-102).
• CustomerId is available.
• S3 bucket credentials configured and reachable.

5. Postconditions

• KYC documents uploaded to S3.
• Metadata stored in KYC_DOCUMENTS table.

• System ready for automated/manual KYC review.

6. Acceptance Criteria

AC ID	Acceptance Criteria
AC-401	System validates file type and size before upload.
AC-402	All valid files must be uploaded to S3.
AC-403	Invalid file type triggers ERR-1040.
AC-404	Upload failure triggers retries then ERR-1044.
AC-405	Metadata must be saved in DB for each file.
AC-406	Uploaded file URLs must be masked in logs.

7. Data Storage Impact

Table: KYC_DOCUMENTS
• customer_id
• document_type
• s3_url (Encrypted)
• object_key
• file_size
• mime_type
• uploaded_at

8. Non-Functional Requirements

• Upload time < 4 seconds per file.
• S3 URLs must be pre-signed for read-only access.
• Support 50 concurrent uploads.
• All operations must be logged securely.