Runbook: BankID Failure

Runbook: BankID Integration Failure

Service: BankID OAuth Authentication **Severity:** CRITICAL (blocks all logins) **MTTR Target:** <15 minutes **Owner:** John (AI Director)

Symptoms

Users report they cannot log in. Symptoms include:

- Login button doesn't redirect to BankID
- BankID redirect returns error page
- OAuth callback fails with 401/403
- Error message: "Authentication service unavailable"

Diagnosis

1. Check BankID Service Status

External status page:

```
# Check BankID status (no official status page, monitor Twitter)
open https://twitter.com/search?q=BankID%20Norge

# Or check community forums
open https://www.reddit.com/r/Norge/search?q=BankID
```

Quick test:

```
# Try BankID login from another service (e.g., tax portal)
open https://www.skatteetaten.no/person/
# If BankID works there but not in Drop → problem is our integration
```

2. Check Drop Logs

```
# CloudWatch Logs (production)
aws logs filter-log-events \
  --log-group-name /aws/apprunner/drop-production \
  --filter-pattern "bankid" \
  --start-time $(date -u -d '10 minutes ago' +%s)000 \
  --region eu-west-1

# Look for:
# - "BankID OAuth error: invalid_client"
# - "BankID callback failed: invalid_state"
# - "BankID API timeout"
```

3. Check Environment Variables

```
# Verify BankID credentials are set
aws apprunner describe-service \
  --service-arn <ARN> \
  --region eu-west-1 \
  | jq
'.Service.SourceConfiguration.ImageRepository.ImageConfiguration.RuntimeEnvironmentVariables'
\
  | grep BANKID

# Expected:
# BANKID_CLIENT_ID: <client-id>
# BANKID_CLIENT_SECRET: <exists> (value hidden)
# BANKID_CALLBACK_URL: https://getdrop.no/api/auth/bankid/callback
```

4. Check OAuth Flow

Test OAuth initiation:

```
# Start OAuth flow
curl -X POST https://getdrop.no/api/auth/bankid/initiate \
  -H "Content-Type: application/json" \
  -d '{"redirectUrl": "/dashboard"}' \
  -v

# Expected: HTTP 302 redirect to BankID with state parameter
# If 500: Check BANKID_CLIENT_ID and BANKID_CALLBACK_URL
```

Test OAuth callback:

```
# Simulate callback (replace <code> and <state> with real values from BankID redirect)
curl -X GET "https://getdrop.no/api/auth/bankid/callback?code=<code>&state=<state>" \
  -v

# Expected: HTTP 302 redirect to /dashboard with auth cookie
# If 401: Check BANKID_CLIENT_SECRET
# If 400: Check state validation logic
```

Common Causes & Solutions

Cause 1: BankID Service Outage (External)

Probability: 5% (BankID is highly reliable)

Symptoms:

- All BankID logins fail across all services
- BankID status page reports incident
- Social media mentions BankID outage

Solution:

1. **Communicate:** Post status update to users

   ```
   Subject: Login temporarily unavailable
   Body: BankID authentication is experiencing issues.
         We're monitoring the situation and will restore service
         as soon as BankID is back online. Estimated: <X> minutes.
   ```

2. **Monitor:** Watch BankID Twitter/status for updates
3. **Fallback (if available):** If demo mode exists, consider temporary activation:

```
# Enable demo mode (ONLY in emergency, requires Alem approval)
aws apprunner update-service --service-arn <ARN> \
  --source-configuration "ImageRepository={...}" \
  --instance-configuration "EnvironmentVariables={NEXT_PUBLIC_SERVICE_MODE=demo}"
```

4. **Post-incident:** Document outage duration, user impact

ETA: Depends on BankID (typically <2 hours)

Cause 2: Invalid OAuth Credentials

Probability: 20% (after credential rotation or environment change)

Symptoms:

- Logs show: "invalid_client" or "unauthorized_client"
- OAuth flow fails immediately (no redirect to BankID)

Solution:

1. **Verify credentials in Vaultwarden:**

```
bw get item "BankID OAuth" --session $BW_SESSION
```

2. **Update App Runner environment variables:**

```
aws apprunner update-service --service-arn <ARN> \
  --source-configuration "ImageRepository={...}" \
  --instance-configuration "EnvironmentVariables={
    BANKID_CLIENT_ID=<correct-client-id>,
    BANKID_CLIENT_SECRET=<correct-secret>
  }"
```

3. **Trigger deployment:**

```
aws apprunner start-deployment --service-arn <ARN> --region eu-west-1
```

4. **Test:** Attempt login after deployment completes (3-5 minutes)

ETA: 10 minutes

Cause 3: Callback URL Mismatch

Probability: 15% (after domain change or deployment error)

Symptoms:

- Logs show: "redirect_uri_mismatch"
- BankID redirects to wrong URL (404 or CORS error)

Solution:

1. **Check registered callback URL in BankID portal:**
   - Login to BankID integration portal
   - Navigate to OAuth settings
   - Verify callback URL: `https://getdrop.no/api/auth/bankid/callback`
2. **If mismatch, update BankID portal:**
   - Change redirect URI to match current domain
   - Save changes (may require approval, 1-2 hours)
3. **Update App Runner env var:**

   ```
   aws apprunner update-service --service-arn <ARN> \
     --source-configuration "ImageRepository={...}" \
     --instance-configuration "EnvironmentVariables={
       BANKID_CALLBACK_URL=https://getdrop.no/api/auth/bankid/callback
     }"
   ```

4. **Test:** Login flow should work after both changes

ETA: 15 minutes (if no BankID approval required), 2 hours (if approval needed)

Cause 4: State Parameter Validation Failure

Probability: 10% (race condition or session timeout)

Symptoms:

- Logs show: "Invalid state parameter"
- User completes BankID flow but callback rejects

Solution:

1. **Check session storage:**
   - BankID state is stored in server session
   - If session expires before callback (>10 min), state is lost

2. **Increase session timeout (if needed):**

```
// src/lib/auth.ts
const SESSION_TIMEOUT = 15 * 60 * 1000; // 15 minutes (was 10)
```

3. **Clear stale sessions:**

```
# If using Redis for sessions
redis-cli FLUSHDB

# If using database sessions
sqlite3 drop.db "DELETE FROM sessions WHERE expires_at < datetime('now');"
```

4. **Ask user to retry:** State timeout is usually one-time issue

ETA: 5 minutes

Cause 5: BankID API Rate Limiting

Probability: 5% (during high-traffic events)

Symptoms:

- Logs show: "rate_limit_exceeded" or HTTP 429
- Intermittent failures (some users succeed, others fail)

Solution:

1. **Check rate limit headers in logs:**

```
X-RateLimit-Limit: 100
X-RateLimit-Remaining: 0
X-RateLimit-Reset: 1640000000
```

2. **Wait for rate limit reset:** Typically resets every 60 seconds
3. **Implement exponential backoff (if not present):**

```
// src/lib/bankid-client.ts
async function callBankIDAPI(retries = 3) {
  try {
    return await fetch(url);
  } catch (error) {
    if (error.status === 429 && retries > 0) {
      await sleep(1000 * (4 - retries)); // 1s, 2s, 3s
```

```
      return callBankIDAPI(retries - 1);
    }
    throw error;
  }
}
```

4. **Contact BankID support:** If rate limits are too low for production traffic

ETA: 5 minutes (automatic), 1-2 days (if support ticket needed)

Cause 6: Network/Firewall Issues

Probability: 5% (AWS security group misconfiguration)

Symptoms:

- Logs show: "Connection timeout" or "ECONNREFUSED"
- BankID API requests never reach destination

Solution:

1. **Check outbound rules (App Runner → BankID):**

```
# App Runner egress is unrestricted by default
# Check VPC connector security group (if using VPC)
aws ec2 describe-security-groups --group-ids <vpc-connector-sg> --region eu-west-1
```

2. **Test connectivity from container:**

```
# Exec into running container (if possible)
curl -v https://oidc.bankid.no/.well-known/openid-configuration

# Expected: HTTP 200 with JSON response
# If timeout: Network/firewall issue
```

3. **Check DNS resolution:**

```
nslookup oidc.bankid.no
# Should resolve to BankID IP addresses
```

4. **Whitelist BankID IPs (if using strict firewall):**
   - Contact BankID for IP ranges
   - Add to AWS security group outbound rules

ETA: 15 minutes (if quick fix), 1 hour (if requires networking changes)

Emergency Workarounds

Option 1: Fallback to Demo Mode (Temporary)

Use case: BankID outage affects all users, estimated >1 hour downtime

Steps:

1. Enable demo mode:

```
aws apprunner update-service --service-arn <ARN> \
  --instance-configuration "EnvironmentVariables={NEXT_PUBLIC_SERVICE_MODE=demo}"
```

2. Communicate to users:

```
Subject: Temporary login method available
Body: Due to BankID outage, we've enabled demo login.
      Use email/password to access your account.
      BankID will be restored as soon as possible.
```

3. Monitor BankID status
4. **Revert to BankID when available:**

```
aws apprunner update-service --service-arn <ARN> \
  --instance-configuration "EnvironmentVariables={NEXT_PUBLIC_SERVICE_MODE=live}"
```

Risk: Demo mode may bypass KYC checks. Only use with Alem approval.

Option 2: Redirect to Status Page

Use case: BankID outage, no ETA, no fallback available

Steps:

1. Deploy maintenance page:

```
# Update health endpoint to return 503
# This triggers BetterStack alert + status page update
```

2. Show user-friendly message:

```
<h1>Login Temporarily Unavailable</h1>
<p>Our authentication provider (BankID) is experiencing issues.</p>
<p>We expect service to resume within <strong>X minutes</strong>.</p>
<p>Status updates: <a href="https://status.drop.no">status.drop.no</a></p>
```

3. Monitor and communicate updates every 30 minutes

Post-Incident Actions

1. **Document incident:**

```
# Create incident report
touch ~/ALAI/products/Drop/comms/incidents/$(date +%Y-%m-%d)-bankid-failure.md
```

2. **Root cause analysis:**
   - What triggered the failure?
   - Why didn't monitoring detect it sooner?
   - What prevented faster recovery?
3. **Update monitoring:**
   - Add synthetic BankID login test (every 5 min)
   - Alert on OAuth callback failures >5/min
4. **Update runbook:**
   - Add new failure mode if discovered
   - Improve diagnosis steps based on what worked
5. **Team debrief (if >30 min outage):**
   - Review timeline
   - Identify improvements
   - Update on-call procedures

Escalation

Time	Action
0 min	John starts diagnosis
5 min	If not resolved, alert Alem via Slack + SMS
15 min	If BankID outage confirmed, enable fallback (Alem approval)
30 min	If still unresolved, schedule team call

Time	Action
1 hour	If major outage, public communication via email/social media

---

Contacts

- **BankID Support:** support@bankid.no
- **BankID Phone:** +47 XXXX XXXX (24/7 for critical issues)
- **Internal:** Alem (CEO, final decision on fallback modes)

Related Documentation

- `docs/architecture/authentication.md` — BankID OAuth flow
- `src/app/api/auth/bankid/route.ts` — BankID integration code
- `docs/dr-runbook.md` — Infrastructure disaster recovery
- Vaultwarden item: "BankID OAuth" — Credentials

Last Updated: 2026-02-22 **Next Review:** Before Phase 2 (Banking Integration)

Revision #6
Created 2026-02-23 11:29:20 UTC by John
Updated 2026-05-25 07:27:37 UTC by John