PRD C — Pre-Signed URL Portal (Ultra-Simple Delivery)

1 Purpose & Scope

Deliver each **accepted EPCIS 1.2 ZIP** to trading partners via a secure, expiring HTTPS link—no AS2, no SFTP. Partners authenticate with username & password, open a minimal portal, and click **Download**.

2 Design Principles

1. **Zero install** – works in any modern browser.
2. **Link life-cycle** – every link has an expiry & audit trail.
3. **Shared infra** – re-use S3 object from Core Receiver; no duplicate storage.
4. **Future-proof** – can coexist with SFTP / AS2 later.

3 Personas

- **Partner Clerk (PC)** – receives e-mail, logs in, downloads file.
- **Internal Ops Clerk (IOC)** – monitors delivery status.
- **Compliance Lead (CL)** – exports logs for auditors.

4 User Stories

ID	As a…	I want to…	Acceptance Criteria
US-P 1	PC	receive an e-mail with a link that takes me directly to the file list after first-time password setup	E-mail received <1 min after file accepted; link valid 24 h
US-P 2	PC	click **Download** and get the ZIP	Browser downloads <3 s for ≤50 MB file
US-P 3	PC	see remaining time before the link expires	Countdown badge visible (HH:MM:SS)
US-P 4	IOC	confirm that Partner X has downloaded file Y	Dashboard shows status *Downloaded* and timestamp

US-P 5	CL	export CSV of all link issuances & downloads between two dates	CSV matches DB counts; ISO-8601 timestamps

5 Functional Requirements

5.1 Link Generation & Notification

ID	Requirement	Acceptance Criteria
R-LG-01	On FileAccepted event, generate presigned URL with TTL configurable (default 48 h)	URL string length ≤2048 chars; HTTPS only
R-LG-02	Compose e-mail using SES/SMTP template with partner name, file meta, expiry time	Template variables resolved; no PII leak
R-LG-03	Store **Link record** (UUID, file_id, partner_id, url_hash, expires_at, first_clicked_at)	DB row created before e-mail send
R-LG-04	Enforce **One-time use** flag (config per partner)	Second click after first download → 410 Gone

5.2 Portal Web App

ID	Requirement	Acceptance Criteria
R-UI-P1	Login via username/password (bcrypt) + optional MFA (TOTP)	Lockout after 5 failed attempts
R-UI-P2	List of active files: file name, size, expires_in countdown, **Download** button	Table loads ≤1 s for 500 rows
R-UI-P3	Download button triggers GET to presigned URL	File download begins; status row turns to *Downloaded*
R-UI-P4	Past Files tab shows history (Downloaded / Expired)	Pagination (50/page)

5.3 Security

ID	Requirement	Acceptance Criteria
R-SEC-P 1	Presigned URL TTL min 24 h, max 168 h (7 days)	Admin edit in Settings

R-SEC-P 2	Option to restrict URL by partner's IP CIDR list	If mismatch → 403 Forbidden
R-SEC-P 3	All logs immutable (CloudTrail/Kinesis-Firehose to S3)	Retention ≥6 yrs

5.4 Non-Functional

Category	Requirement
Availability	≥99.5 % (portal is stateless behind ALB)
Performance	Generate URL ≤300 ms; download start ≤3 s
Accessibility	WCAG 2.1 AA, keyboard nav

5.5 Milestones

Phase	Deliverable	Target
Design	Wireframe & e-mail templates	20 May 2025
Sprint 1	Link generator Lambda + SES email	10 Jun 2025
Sprint 2	Portal UI (React) + auth & MFA	30 Jun 2025
Sprint 3	One-time link & IP allow-list	15 Jul 2025
Pilot	1 partner live; <5 support tickets	31 Jul 2025

6   Success Metrics

- **Download completion rate** ≥98 % within 48 h of notification
- **Average user task time** (login → download) ≤30 s
- **Portal support tickets** <0.5 per 100 files

7   Risks & Mitigations

Risk	Impact	Mitigation
Partner forwards link externally	Possible data leak	One-time link + MFA + optional IP allow-list

Partner spam filter blocks e-mail	Delivery delay	Expose alternate portal login where files appear automatically
Large file (>100 MB) times out	Incomplete download	Allow optional chunked multipart download via S3 byte-ranges