Securing EDI and API links with port partners: a checklist

One line per point, in eight areas. Walk the list with whoever runs the EDI translator or the integration platform, whoever runs the API, and the person who signs partner agreements. For each point, write down who owns it and where the evidence is kept, and mark it as in place, partial, missing or not applicable. Start with the partner register (A1) and the per-partner credentials (A4): most of the rest depends on knowing who is connected, by which channel, with which key.

Scope. Covers the machine-to-machine links between a port actor and its partners: EDIFACT interchanges (stowage plans, container pre-advice and release, gate and vessel movement reports) carried over AS2 or SFTP, and REST APIs used by carriers, forwarders, hauliers and their software. It covers onboarding and offboarding of partners, the channels, keys and tokens, message integrity, replay, rate limits, logs and the response when a partner is compromised. It does not replace the port facility security plan, the contracts with your partners or legal advice on your own jurisdiction.

Status

• in place · the evidence exists, is dated and someone owns it

• partial · the practice exists but the evidence is missing, out of date or covers only some partners

• missing · nothing yet

• not applicable · write down why

Summary sheet · organisation: _____ · date: _____

Point	Area	Status	Owner
A1 · A register of every connected partner	Partners and onboarding		
A2 · A new partner is confirmed out of band	Partners and onboarding		
A3 · Test first, production credentials separate	Partners and onboarding		
A4 · Each partner has its own credentials	Partners and onboarding		
A5 · A partner that leaves is removed the same day	Partners and onboarding		
B1 · No clear-text channel	Channels: AS2 and SFTP		
B2 · AS2 messages signed, encrypted and acknowledged	Channels: AS2 and SFTP		
B3 · Certificates confirmed, expiry dates owned	Channels: AS2 and SFTP		
B4 · SFTP by key, one account per partner, host key checked	Channels: AS2 and SFTP		
B5 · Address allowlists are a second layer only	Channels: AS2 and SFTP		
B6 · Inbound files are checked before they are processed	Channels: AS2 and SFTP		
C1 · One credential per integration, limited to what it needs	API keys and OAuth		
C2 · Keys are kept in a vault, never in mail or code	API keys and OAuth		
C3 · Keys rotate and can be revoked at once	API keys and OAuth		
C4 · OAuth with strong client authentication	API keys and OAuth		
C5 · Short-lived, restricted access tokens	API keys and OAuth		
C6 · Each partner sees only its own containers	API keys and OAuth		
C7 · People in the developer console use MFA	API keys and OAuth		
D1 · Messages are validated before processing	Message integrity		
D2 · The sender may say what it says	Message integrity		
D3 · Release references are treated as secrets	Message integrity		
D4 · End-to-end signature where a hub sits in the middle	Message integrity		
D5 · Proof of what was received is kept	Message integrity		
E1 · An interchange is processed once	Replay and duplicates		
E2 · Signed requests carry a time and a nonce	Replay and duplicates		
E3 · Writes are idempotent	Replay and duplicates		
E4 · Acknowledgements are matched	Replay and duplicates		
F1 · Quotas per key and per partner	Rate limiting		
F2 · Sensitive flows have their own limits	Rate limiting		
F3 · One partner cannot block the others	Rate limiting		
G1 · Every interchange is logged	Logging and detection		
G2 · Every API call is logged, without secrets	Logging and detection		
G3 · Logs are protected and kept	Logging and detection		
G4 · Alerts have an owner	Logging and detection		
H1 · A security contact per partner, and a switch	Incidents and changes		
H2 · No change on the strength of an e-mail	Incidents and changes		
H3 · The register is reviewed at a written interval	Incidents and changes		

A · Partners and onboarding

Every connected partner is listed, checked out of band, tested before production, given its own credentials and removed on the day it leaves.

A1 · A register of every connected partner

Check: One register lists every partner connected by EDI or API: the organisation, the messages or endpoints it uses, the channel, the credentials issued (certificate, SFTP account, API client), its technical and security contacts, and the date of the last review.

Why: A link that is not listed is neither monitored nor removed. OWASP names improper inventory of APIs and of the parties they serve as a top API risk (API9:2023); NIS2 lists supply chain security, including the relationship with direct suppliers and service providers, among the minimum measures.

Evidence to hold: [ ] The partner register, with one line per partner and per channel · [ ] The date of the last review and who did it

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05); Directive (2022-12-14); IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A2 · A new partner is confirmed out of band

Check: A request to connect, and the endpoints, certificates or keys that come with it, are confirmed with a known contact of the partner through a channel other than the one that carried the request (a call to a number already on file, for example), and the certificate fingerprint is read back.

Why: A fake partner, or a real partner's endpoint swapped by someone else, is the cheapest way into a terminal's message flows. This point is plain practice; NIS2 asks for supply chain security and the IMO guidelines ask for the risks of third parties to be assessed.

Evidence to hold: [ ] The onboarding procedure with the out-of-band check · [ ] For each recent partner, who confirmed what, and when

Sources: Directive (2022-12-14); IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A3 · Test first, production credentials separate

Check: A new partner connects first to a test endpoint with test credentials; production credentials are issued only after its messages pass validation, and they are different from the test ones.

Why: Test credentials are shared more widely and kept less carefully. OWASP lists exposed non-production versions among the API inventory risks (API9:2023).

Evidence to hold: [ ] The onboarding steps, with the validation gate between test and production · [ ] The list of credentials per partner, test and production apart

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A4 · Each partner has its own credentials

Check: No AS2 certificate, SFTP account, API key or OAuth client is shared between two partners, or between a partner and the EDI service provider that carries its messages. Each credential belongs to one partner and one channel.

Why: A shared credential cannot be removed for one partner without breaking the others, and nothing in the logs says who used it. The US Coast Guard rule asks for separate credentials for critical systems.

Evidence to hold: [ ] The credential list, showing one partner per credential

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A5 · A partner that leaves is removed the same day

Check: When a contract ends, or a partner changes its EDI provider or software, its certificates, SFTP accounts, API keys and OAuth clients are revoked on the day, and its network allowlist entries are removed.

Why: Credentials of a former partner are invisible until someone uses them. Removing the credentials of those who leave is a requirement of the US Coast Guard rule.

Evidence to hold: [ ] The offboarding checklist · [ ] The list of credentials revoked at the last offboarding, with the date

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B · Channels: AS2 and SFTP

No clear-text channel; AS2 signed, encrypted and acknowledged; SFTP by key, one account per partner; certificates and host keys confirmed out of band.

B1 · No clear-text channel

Check: No EDI or API traffic travels over plain FTP, plain HTTP or unencrypted e-mail. TLS 1.2 is the minimum and TLS 1.3 is supported where the partner can use it.

Why: A message in clear text can be read and changed on the way. NIS2 lists policies on cryptography and encryption among the minimum measures; NIST SP 800-52 Rev. 2 requires TLS 1.2 and asks for TLS 1.3 support.

Evidence to hold: [ ] The protocol and TLS settings of each inbound and outbound endpoint · [ ] A scan showing that no plain FTP or HTTP endpoint answers

Sources: Directive (2022-12-14); NIST SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (2019-08)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B2 · AS2 messages signed, encrypted and acknowledged

Check: AS2 partners sign and encrypt their messages and ask for a signed receipt (MDN); the terminal refuses unsigned or unencrypted messages and checks the receipts it gets back.

Why: AS2 (RFC 4130, July 2005) was designed for exactly this: S/MIME signature and encryption, and a signed receipt that carries a check value of the message received, so both sides can prove what was sent and received.

Evidence to hold: [ ] The AS2 profile of each partner (signing, encryption, signed MDN required) · [ ] A refused unsigned test message

Sources: IETF RFC 4130, MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (2005-07)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B3 · Certificates confirmed, expiry dates owned

Check: Each partner's certificate is installed only after its fingerprint is confirmed out of band; every certificate's expiry date is in a calendar with an owner, and a renewal overlaps the old and the new certificate.

Why: An expired certificate stops the flow; a certificate swapped without a check lets someone else sign as the partner. This point is plain practice built on the certificate exchange that AS2 relies on.

Evidence to hold: [ ] The certificate inventory with fingerprints, expiry dates and owners · [ ] The record of the last renewal

Sources: IETF RFC 4130, MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (2005-07)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B4 · SFTP by key, one account per partner, host key checked

Check: SFTP partners log in with a key, not a password; each has its own account limited to its own directories, with no shell; the server's host key fingerprint is given to partners, who check it at the first connection.

Why: The SSH transport protocol (RFC 4253, January 2006) relies on the client checking the server's host key: without that check, a man in the middle can pose as the server. A password shared by e-mail is a weaker secret than a key.

Evidence to hold: [ ] The SFTP account list with authentication method and directory per partner · [ ] The host key fingerprint as published to partners

Sources: IETF RFC 4253, The Secure Shell (2006-01); US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B5 · Address allowlists are a second layer only

Check: Where a partner's source addresses are stable, they are allowlisted; the allowlist never replaces the certificate, key or token, and it is reviewed with the partner register.

Why: Addresses change and are often shared by the partner's provider with its other clients. This point is plain practice: an allowlist narrows the door, it does not say who is at it.

Evidence to hold: [ ] The allowlist, with one owner partner per entry and the date of the last review

Sources: Directive (2022-12-14)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B6 · Inbound files are checked before they are processed

Check: Files received by SFTP or AS2 land in an inbound area where their size, type and syntax are checked (and scanned where the platform allows) before the translator or the terminal operating system reads them.

Why: Data from a partner is input like any other. OWASP lists unsafe consumption of APIs, trusting data from third parties more than user input, among the top API risks (API10:2023).

Evidence to hold: [ ] The inbound processing steps and the rules for a rejected file

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C · API keys and OAuth

One scoped credential per integration, kept in a vault, rotated and revocable; OAuth with strong client authentication and short, restricted tokens; each partner sees only its own data.

C1 · One credential per integration, limited to what it needs

Check: Each integration has its own API key or OAuth client, scoped to the operations it needs (reading container status is not submitting a release) and to its own organisation's data.

Why: A broad key turns a leak into a terminal-wide incident. OWASP lists broken function level authorization (API5:2023); NIST SP 800-228 asks for both the calling service and the user of every request to be authenticated and authorised.

Evidence to hold: [ ] The list of keys and clients with their scopes

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05); NIST SP 800-228 upd1, Guidelines for API Protection for Cloud-Native Systems (2026-03-13)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C2 · Keys are kept in a vault, never in mail or code

Check: API keys, client secrets and private keys are stored in a secret store or a password manager, never sent in an e-mail, a ticket or a spreadsheet, and never committed to source code; repositories are scanned for secrets.

Why: A key in a mailbox or a repository is readable by anyone who reaches that mailbox or repository. This point is plain practice; NIS2 asks for policies on cryptography, and the keys are where those policies hold or fail.

Evidence to hold: [ ] Where each production key is stored · [ ] The result of the last secret scan of the integration code

Sources: Directive (2022-12-14)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C3 · Keys rotate and can be revoked at once

Check: Keys and client secrets are rotated at a written interval and at once after a leak or the departure of someone who handled them; two keys can be valid during a rotation; revoking a key takes effect immediately and has been tested.

Why: A key that cannot be rotated without an outage is never rotated. The US Coast Guard rule asks for the credentials of those who leave to be removed.

Evidence to hold: [ ] The rotation procedure and the date of the last rotation per partner · [ ] The record of a revocation test

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C4 · OAuth with strong client authentication

Check: Machine-to-machine access uses the OAuth 2.0 client credentials grant, with asymmetric client authentication (mutual TLS or a signed JWT) rather than a shared secret where the partner can support it; the resource owner password grant is not used.

Why: The OAuth 2.0 Security Best Current Practice (RFC 9700, January 2025) says the password grant must not be used and recommends asymmetric client authentication such as mutual TLS (RFC 8705) or signed JWTs.

Evidence to hold: [ ] The grant types and client authentication methods enabled on the authorisation server

Sources: IETF RFC 9700 (2025-01); IETF RFC 8705, OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens (2020-02)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C5 · Short-lived, restricted access tokens

Check: Access tokens expire after a short period, are restricted to the API they are meant for (audience), and are bound to the client (mutual TLS or an equivalent) where the platform allows.

Why: A stolen token is worth only what it can reach and for as long as it lives. RFC 9700 recommends restricting access tokens to a resource server and sender-constraining them.

Evidence to hold: [ ] The token lifetime, audience and binding settings

Sources: IETF RFC 9700 (2025-01); IETF RFC 8705, OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens (2020-02)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C6 · Each partner sees only its own containers

Check: Every API call that names a container, booking, bill of lading or vessel call checks that the caller is entitled to it; this is tested with two test partners trying to read each other's data.

Why: Broken object level authorization is the first risk of OWASP's API Top 10 (API1:2023): change an identifier in the request and read someone else's record. In a port, that record says where a container is and when it can leave.

Evidence to hold: [ ] The authorisation rule per endpoint · [ ] The result of the two-partner test

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C7 · People in the developer console use MFA

Check: The people who manage API keys and partner settings, on the terminal's side and on the partners' side, log in to the developer console or partner portal with multi-factor authentication.

Why: Whoever logs in to the console can create keys. NIS2 Article 21(2)(j) and 33 CFR 101.650(a)(4) both name multi-factor authentication.

Evidence to hold: [ ] The MFA setting of the console and the list of accounts without it, with a reason

Sources: Directive (2022-12-14); US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D · Message integrity

Messages are validated before processing, the sender is checked against what it may say about each container, release references are treated as secrets, and integrity can be proven later.

D1 · Messages are validated before processing

Check: Every EDIFACT interchange is checked against the syntax and the message implementation guide agreed with the partner, and every API payload against its schema, before anything is processed; a failing message is rejected whole with an error report, never half processed.

Why: The user group of shipping lines and terminals publishes message implementation guides so both sides agree on the content; validation enforces that agreement and stops malformed data before it reaches the terminal operating system (OWASP API10:2023).

Evidence to hold: [ ] The validation rules per partner and message type · [ ] The error report sent for a rejected message

Sources: SMDG, EDIFACT message implementation guides (2016-06); OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D2 · The sender may say what it says

Check: Each message is checked against what its sender is entitled to say about each container: a pre-advice or a release only from the party that holds the booking, a stowage plan only from the vessel's operator or its agent. A message about a container outside the sender's usual set goes to a person.

Why: A valid message from a valid partner can still be about someone else's container. In the message set the shipping lines' and terminals' user group recommends, COPARN carries the carrier's pre-advice and empty release to the terminal; release is the step organised crime targets.

Evidence to hold: [ ] The entitlement rules per message type · [ ] The queue of held messages and who reviews it

Sources: SMDG (2020-02-20); Europol and the security steering committees of three EU ports, Criminal networks in EU ports: risks and challenges for law enforcement (2023-04-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D3 · Release references are treated as secrets

Check: Container release references (PIN codes) are sent only to the party that needs them, through an authenticated channel, are valid for a limited time and a single pick-up, and every access to them is logged.

Why: Europol's joint report with port security committees (5 April 2023) describes criminal networks obtaining container reference codes to collect containers, and names need-to-know access to the codes, logging and traceability among the measures.

Evidence to hold: [ ] How a release reference is created, sent, used and expired · [ ] The access log of release references

Sources: Europol and the security steering committees of three EU ports, Criminal networks in EU ports: risks and challenges for law enforcement (2023-04-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D4 · End-to-end signature where a hub sits in the middle

Check: When messages pass through a service provider or a hub, so that the channel signature ends there, the message itself is signed: EDIFACT security segments or an AUTACK message, HTTP message signatures for APIs, or a signed webhook.

Why: A channel signature proves who sent the last hop, not who wrote the message. ISO 9735-5 (2002) defines security for batch EDIFACT (authenticity, integrity, non-repudiation of origin) and RFC 9421 (February 2024) does the same for HTTP messages.

Evidence to hold: [ ] The list of flows that pass through a third party, and how each is signed

Sources: ISO 9735-5:2002, EDIFACT application level syntax rules, Part 5: Security rules for batch EDI (2002-07-01); IETF RFC 9421, HTTP Message Signatures (2024-02)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D5 · Proof of what was received is kept

Check: A hash of each interchange or API request is stored with its record, together with the signed receipt where there is one, so a disputed message can be shown as received.

Why: When a container leaves on a contested release, the question is what message arrived, from whom and when. The AS2 signed receipt carries a check value of the message received (RFC 4130).

Evidence to hold: [ ] The record of a sample interchange with its hash and receipt

Sources: IETF RFC 4130, MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (2005-07); ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

E · Replay and duplicates

The same interchange or request cannot be processed twice: control references, timestamps and nonces, idempotent writes and matched acknowledgements.

E1 · An interchange is processed once

Check: Each sender's interchange control reference is recorded; an interchange that repeats a reference already processed is held for review, not processed a second time.

Why: A replayed release or a duplicated gate report changes the state of a container as surely as a forged one. EDIFACT security headers include a sequence number and a time stamp for this reason (ISO 9735-5).

Evidence to hold: [ ] The duplicate check of the translator and a held duplicate

Sources: ISO 9735-5:2002, EDIFACT application level syntax rules, Part 5: Security rules for batch EDI (2002-07-01)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

E2 · Signed requests carry a time and a nonce

Check: Signed API requests and webhooks include their creation time and a nonce; the receiver refuses those outside a short window it has written down, or whose nonce it has already seen.

Why: A signature alone does not stop a captured request from being sent again. RFC 9421 defines the created and nonce parameters for this purpose.

Evidence to hold: [ ] The window and the nonce store of each signed endpoint

Sources: IETF RFC 9421, HTTP Message Signatures (2024-02)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

E3 · Writes are idempotent

Check: A call that creates or changes something (a booking, a release, a pre-advice) carries an identifier chosen by the client; a retry with the same identifier returns the first result instead of acting twice.

Why: Integrations retry on time-outs, and a retry must not become a second release. HTTP (RFC 9110, June 2022) treats only some methods as idempotent and safe to retry automatically; a POST that creates something is not one of them, so the API has to make it so.

Evidence to hold: [ ] The idempotency rule of each write endpoint

Sources: IETF RFC 9110, HTTP Semantics (2022-06)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

E4 · Acknowledgements are matched

Check: Every message sent expects an acknowledgement (an MDN, a syntax report, an API response); a missing one raises an alert, and a resend keeps the original reference so the receiver can spot it.

Why: A message that silently did not arrive is as harmful as a forged one, and a resend under a new reference looks like a new message. AS2 builds receipts into the protocol (RFC 4130).

Evidence to hold: [ ] The list of messages awaiting acknowledgement and the alert rule

Sources: IETF RFC 4130, MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (2005-07)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

F · Rate limiting

Quotas per key and per partner, lower limits on sensitive flows, and one partner's flood cannot stop the others.

F1 · Quotas per key and per partner

Check: Every API key and every partner has a limit on calls, messages and payload size per period; above it, the API answers 429 Too Many Requests with a Retry-After header, and the EDI gateway holds the excess.

Why: OWASP lists unrestricted resource consumption as a top API risk (API4:2023); NIST SP 800-228 asks for rate limits keyed on the caller; RFC 6585 (April 2012) defines the 429 status and its Retry-After header.

Evidence to hold: [ ] The quota per key and per partner · [ ] A 429 answer from a test

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05); NIST SP 800-228 upd1, Guidelines for API Protection for Cloud-Native Systems (2026-03-13); IETF RFC 6585, Additional HTTP Status Codes (2012-04)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

F2 · Sensitive flows have their own limits

Check: Bulk queries of container status, changes of release, and searches across many containers have lower limits than ordinary calls, and an alert when a partner approaches them.

Why: OWASP calls this unrestricted access to sensitive business flows (API6:2023): each call is allowed, the volume is the attack.

Evidence to hold: [ ] The list of sensitive flows with their limits

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

F3 · One partner cannot block the others

Check: Inbound EDI and API traffic is queued and limited per partner, so that a flood or a broken loop from one partner does not delay the messages of the others.

Why: A misbehaving integration is the most common flood, and it is rarely malicious. This point is plain practice following OWASP API4:2023.

Evidence to hold: [ ] The queue and limit layout per partner

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G · Logging and detection

Every interchange and every API call is logged without secrets, the logs are protected, and alerts have an owner.

G1 · Every interchange is logged

Check: For each EDI interchange: the partner, channel, message type, control reference, hash, size, time and result (accepted, rejected, held).

Why: The joint guide of ASD's ACSC, CISA and partners (21 August 2024) asks for logs that let an organisation detect and investigate; for EDI, the interchange is the unit of evidence.

Evidence to hold: [ ] A sample of the interchange log

Sources: ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G2 · Every API call is logged, without secrets

Check: For each API call: the key or client, the endpoint, the objects named, the result and the source address; never the key, the token or the full payload of personal data.

Why: A log that holds the token becomes a store of valid credentials. The logging guide asks for useful content and for protection of the logs themselves.

Evidence to hold: [ ] A sample of the API log, checked for secrets

Sources: ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21); OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G3 · Logs are protected and kept

Check: The logs are stored where the people and systems they record cannot change them, and kept for a written period.

Why: 33 CFR 101.650(c)(1) asks for logs to be securely captured, stored and protected so that only privileged users can reach them.

Evidence to hold: [ ] Where the logs are stored, who can reach them, and the retention period

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G4 · Alerts have an owner

Check: Alerts fire on bursts of failed authentication, a partner connecting from a new address, a certificate or key change, volumes far from the partner's pattern, and messages about containers outside its usual set; each alert has someone who reads it.

Why: An alert no one reads is a log. The joint logging guide and the IMO guidelines both ask for detection, not only collection.

Evidence to hold: [ ] The alert list with owners · [ ] The last alert and what was done

Sources: ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21); IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

H · Incidents and changes

A security contact per partner, a fast way to suspend one partner, and no change of endpoint or certificate on the strength of an e-mail.

H1 · A security contact per partner, and a switch

Check: Each partner has a security contact in the register, and the terminal can suspend one partner's access (every channel, every key) quickly without stopping the others; this has been rehearsed.

Why: When a partner is compromised, its valid credentials become the attacker's. The IMO guidelines ask for response and recovery plans; NIS2 asks for incident handling and supply chain security.

Evidence to hold: [ ] The suspension procedure and the record of a rehearsal

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28); Directive (2022-12-14)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

H2 · No change on the strength of an e-mail

Check: A request to change a partner's endpoint, certificate, SFTP key or contact is confirmed with a known contact through another channel before it is applied.

Why: Changing where messages go, or which certificate is trusted, is the quiet version of a compromise. This point is plain practice, the same rule as A2.

Evidence to hold: [ ] The change procedure and the log of recent changes with their confirmation

Sources: Directive (2022-12-14)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

H3 · The register is reviewed at a written interval

Check: At an interval the terminal writes down, the partner register, credentials, scopes, allowlists and certificates are reviewed against the contracts in force, and what is no longer needed is removed.

Why: Links accumulate; reviews remove them. OWASP API9:2023 and the US Coast Guard rule's account management both assume an inventory that is kept current.

Evidence to hold: [ ] The date and the output of the last review

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05); US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Sources (public, dated)

SMDG (user group for shipping lines and container terminals), Recommendation #06, Recommended standard messages between terminal and carrier (CODECO, COARRI, BAPLIE, VERMAS, COPRAR, COPARN, MOVINS), 2020-02-20. https://smdg.org/wp-content/uploads/Recommendations/Recommendation-06-SMDG-Recommended-Messages-v1-20200220.pdf

SMDG, EDIFACT message implementation guides (MIGs), incl. BAPLIE 3.1.1 on directory D.13B, 2016-06. https://smdg.org/documents/edifact-migs-message-implementation-guidelines/ship-planning/

ISO 9735-5:2002, EDIFACT application level syntax rules, Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin); Part 6 defines the AUTACK message, 2002-07-01. https://www.isotc154.org/standards/iso-9735-52002/

IETF RFC 4130, MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2), 2005-07. https://www.rfc-editor.org/rfc/rfc4130

IETF RFC 4253, The Secure Shell (SSH) Transport Layer Protocol (server host key verification), 2006-01. https://www.rfc-editor.org/rfc/rfc4253

NIST SP 800-52 Rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, 2019-08. https://csrc.nist.gov/pubs/sp/800/52/r2/final

IETF RFC 9700 (BCP 240), Best Current Practice for OAuth 2.0 Security, 2025-01. https://www.rfc-editor.org/rfc/rfc9700

IETF RFC 8705, OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens, 2020-02. https://www.rfc-editor.org/rfc/rfc8705

IETF RFC 9421, HTTP Message Signatures (created and nonce parameters), 2024-02. https://www.rfc-editor.org/rfc/rfc9421

IETF RFC 6585, Additional HTTP Status Codes (429 Too Many Requests, Retry-After), 2012-04. https://www.rfc-editor.org/rfc/rfc6585

OWASP API Security Top 10, 2023 edition (API1 object level authorization, API4 resource consumption, API5 function level authorization, API6 sensitive business flows, API9 inventory, API10 unsafe consumption of APIs), 2023-06-05. https://api-security.owasp.org/editions/2023/en/0x11-t10/

NIST SP 800-228 upd1, Guidelines for API Protection for Cloud-Native Systems (first published June 2025; 2.7.1 identity-based segmentation, REC-API-16 rate limits per caller), 2026-03-13. https://csrc.nist.gov/pubs/sp/800/228/upd1/final

IETF RFC 9110, HTTP Semantics (9.2.2 idempotent methods), 2022-06. https://www.rfc-editor.org/rfc/rfc9110

Directive (EU) 2022/2555 (NIS2), Article 21(2): incident handling (b), supply chain security (d), cryptography and encryption (h), access control (i), multi-factor authentication (j), 2022-12-14. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (account security: MFA, least privilege, separate credentials, removal of leavers' credentials; protected logs), in force since 16 July 2025, 2025-01-17. https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F

ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection, 2024-08-21. https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection

IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4, 2026-05-28. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

Europol and the security steering committees of three EU ports, Criminal networks in EU ports: risks and challenges for law enforcement (joint report, public version), 2023-04-05. https://www.europol.europa.eu/publications-events/publications/criminal-networks-in-eu-ports-risks-and-challenges-for-law-enforcement

Licence

Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . You may copy, adapt and share this checklist, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/api-developers/edi-api-integration-security/ . Generic: no terminal, port, client or vendor is named and no figure is invented. This checklist is not legal advice and does not replace your port facility security plan, your partner agreements or advice on the law of your jurisdiction; Port Cyber Alliance does not certify or audit terminals or integrations.