Port identity and SSO readiness self-check

The “PCA Passport” is a concept, not a product: nothing described on the page is available to buy or connect to. This self-check measures where your own estate stands today.

Fifteen questions in five areas, for the person who owns identity and access across your port operation: the CISO or IT lead, and whoever runs the portals your drivers, planners and partners log into. For each point, write down the answer you can evidence today, who owns it, and whether it is in place, partial, missing or not applicable. Start with the portal register (A1): you cannot reduce account sprawl you have not counted. This worksheet measures where you stand today; it does not sell or require any identity product.

Scope. Covers the logins your own people and partners use across port portals: terminal and gate systems, vessel and berth planning, carrier and line portals, forwarder and customs portals, and the APIs behind them. It measures account sprawl, shared and orphaned accounts, multi-factor and phishing-resistant authentication, the joiner-mover-leaver flow, and the handling of sensitive items such as container release codes and API keys. It does not replace your port facility security plan, your contracts with partners, or legal advice on your own jurisdiction, and it is not a specification of any identity service.

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• partial · the practice exists but the evidence is missing, out of date or covers only some portals

• missing · nothing yet

• not applicable · write down why

Summary sheet · organisation: _____ · date: _____

Question	Area	Status	Owner
A1 · A register of every portal your people log into	Account sprawl		
A2 · How many accounts each person carries	Account sprawl		
A3 · Which portals can federate, which only hold local accounts	Account sprawl		
B1 · One account per person, no shared logins	Shared and orphaned accounts		
B2 · Orphaned accounts are found and removed	Shared and orphaned accounts		
B3 · Non-human accounts inventoried and owned	Shared and orphaned accounts		
C1 · Multi-factor on every portal that supports it	Multi-factor and phishing resistance		
C2 · Phishing-resistant methods on the most sensitive portals	Multi-factor and phishing resistance		
C3 · Step-up for sensitive actions, not only at login	Multi-factor and phishing resistance		
D1 · A joiner's access comes from a request, not a copy	Joiners, movers and leavers		
D2 · A mover loses the access the old role had	Joiners, movers and leavers		
D3 · A leaver is removed from every portal the same day	Joiners, movers and leavers		
E1 · Container release references are need-to-know and logged	Sensitive actions and secrets		
E2 · API keys are per-integration, vaulted and revocable	Sensitive actions and secrets		
E3 · Access can be cut across portals, or only portal by portal	Sensitive actions and secrets		

A · Account sprawl

Every portal your people log into is listed, the number of accounts per person is known, and you know which portals can federate and which only hold local accounts.

A1 · A register of every portal your people log into

Check: One list names every portal and system your staff and partners sign into: terminal and gate systems, vessel and berth planning, carrier and shipping-line portals, forwarder, haulier and customs portals, and the back-office tools. For each, note how an account is created and removed, and who owns the relationship.

Why: You cannot reduce sprawl, enforce multi-factor or remove a leaver on portals you have not listed. OWASP names improper inventory of interfaces and of the parties they serve among the top API risks (API9:2023); NIS2 lists asset and access management among the minimum measures.

Evidence to hold: [ ] The portal and account register, with an owner per portal · [ ] The date of the last review and who did it

Sources: OWASP API Security Top 10 (2023); Directive (14 December 2022)

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

A2 · How many accounts each person carries

Check: Count, for a typical driver, planner or partner contact, how many separate logins they hold across those portals, and record the worst case. Note where the same person has more than one account on the same portal.

Why: Account sprawl is what pushes people to reuse passwords and share logins, and it is the problem a shared identity would address. Measuring it first tells you whether the concept would help you at all.

Evidence to hold: [ ] The average and worst-case number of logins per person, with the date measured

Sources: plain practice

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

A3 · Which portals can federate, which only hold local accounts

Check: For each portal, record whether it supports single sign-on through an open standard (OpenID Connect or SAML 2.0) or whether it only holds its own local username and password.

Why: A shared identity is only possible where the portal can accept one; knowing the split tells you how much of your estate could federate today and how much could not. OpenID Connect and SAML 2.0 are the two open standards most portals implement.

Evidence to hold: [ ] The portal register with a single-sign-on column (OIDC, SAML, or local only)

Sources: OpenID Connect Core 1.0 (15 December 2023); OASIS, Assertions and Protocols for SAML V2.0 (15 March 2005)

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

B · Shared and orphaned accounts

No shared logins, non-human accounts inventoried and owned, and a review that actually removes the accounts of people and partners who have left.

B1 · One account per person, no shared logins

Check: No portal is accessed through a login shared by a team, a shift or a company. Each person has their own account; where a portal forces a single company login, it is written down as a gap with an owner.

Why: An action taken through a shared account cannot be attributed to a person, so it cannot be investigated or disputed. Accountable, attributable access underpins the logging that USCG facility rules and NIS2 expect.

Evidence to hold: [ ] A list of any shared logins still in use, with the plan to replace them

Sources: 33 CFR 101.650, Security measures for access control (eCFR, checked 11 November 2026); Directive (14 December 2022)

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

B2 · Orphaned accounts are found and removed

Check: A review, at a written interval, compares the accounts on each portal against the people and partners who should still have them, and removes the rest. Accounts of former staff and ended partners are gone.

Why: Accounts that outlive the person or the contract are a quiet way in, and nobody is watching them. USCG facility security rules require access to be withdrawn when it is no longer needed; NIS2 asks for access control across the supply chain.

Evidence to hold: [ ] The last review, what it removed, and the date

Sources: 33 CFR 101.650, Security measures for access control (eCFR, checked 11 November 2026); Directive (14 December 2022)

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

B3 · Non-human accounts inventoried and owned

Check: Service accounts, robot accounts and the API clients that move messages between systems are listed, each with a named owner, the systems it reaches and the date of its last review.

Why: Non-human accounts are created once and forgotten, often with broad rights and a password that never changes. CISA's logging guidance treats them as accounts to inventory and monitor like any other.

Evidence to hold: [ ] The inventory of service and API-client accounts, with an owner each

Sources: ASD ACSC, CISA and partners, Best practices for event logging and threat detection (21 August 2024)

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

C · Multi-factor and phishing resistance

Multi-factor authentication on every portal that supports it, phishing-resistant methods on the most sensitive ones, and step-up for sensitive actions, not only at login.

C1 · Multi-factor on every portal that supports it

Check: Multi-factor authentication is switched on for every portal that offers it, for staff and for partner contacts, and the portals that offer none are written down as a gap.

Why: A password alone is phished, guessed or reused; a second factor stops most account takeovers. NIST's digital identity guidance and CISA both treat multi-factor as the baseline, not an option.

Evidence to hold: [ ] The portal register with a multi-factor column, and the list of portals that cannot do it

Sources: NIST SP 800-63B, Authentication and Lifecycle Management (June 2017, updated 2 March 2020); CISA, Implementing Phishing-Resistant MFA (October 2022)

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

C2 · Phishing-resistant methods on the most sensitive portals

Check: For the portals that can change what happens to a container or release cargo, the second factor resists phishing: a hardware or platform passkey (FIDO2 / WebAuthn), not a one-time code read out over the phone or copied from a text message.

Why: One-time codes and push prompts can be phished or fatigued; bound credentials such as WebAuthn passkeys cannot be replayed against a look-alike site. CISA recommends phishing-resistant multi-factor for the highest-value access.

Evidence to hold: [ ] Which sensitive portals use phishing-resistant authentication, and which do not yet

Sources: W3C Web Authentication (8 April 2021); CISA, Implementing Phishing-Resistant MFA (October 2022); NIST SP 800-63B, Authentication and Lifecycle Management (June 2017, updated 2 March 2020)

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

C3 · Step-up for sensitive actions, not only at login

Check: A sensitive action — releasing a container, changing a bank or contact detail, granting access — asks for authentication again at the moment it is done, rather than trusting a session opened hours earlier.

Why: A session can be hijacked or left open after login; re-authenticating at the point of a sensitive action narrows the window. This is plain practice, in line with the risk-based levels of NIST's identity guidance.

Evidence to hold: [ ] The list of actions that trigger a re-authentication, per portal

Sources: NIST SP 800-63-3, Digital Identity Guidelines (June 2017, updated 2 March 2020)

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

D · Joiners, movers and leavers

Access is granted from a request rather than copied, reduced when a role changes, and removed from every portal the day a person leaves, tracked to completion.

D1 · A joiner's access comes from a request, not a copy

Check: A new person's portal accounts are created from a written request that states the role and the access it needs, not cloned from a colleague's account.

Why: Copied access carries whatever the colleague had accumulated, including rights they should no longer hold, and it spreads silently. Granting from a defined role keeps access to what is needed.

Evidence to hold: [ ] The joiner request form or ticket, with the role and the access granted

Sources: plain practice

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

D2 · A mover loses the access the old role had

Check: When a person changes role, the access the previous role carried is reviewed and the parts no longer needed are removed, not simply added to.

Why: Access that only ever grows ends with a handful of people who can reach almost everything — the accounts an attacker wants most. A review at each move keeps rights matched to the job.

Evidence to hold: [ ] The last few role changes, with what access was removed

Sources: plain practice

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

D3 · A leaver is removed from every portal the same day

Check: When a person or a partner contact leaves, their accounts are disabled on every portal the same day, and the removal is tracked to completion across all of them, including the portals a third party runs for you.

Why: The day of departure is when access is most dangerous and least watched. USCG facility rules require access to be withdrawn when it is no longer needed; NIS2 asks the same across suppliers and service providers.

Evidence to hold: [ ] The last few leavers, the portals closed, and the date each was confirmed

Sources: 33 CFR 101.650, Security measures for access control (eCFR, checked 11 November 2026); Directive (14 December 2022)

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

E · Sensitive actions and secrets

Container release references are need-to-know and logged, API keys are per-integration and revocable, and you know whether access can be cut across portals at once or only portal by portal.

E1 · Container release references are need-to-know and logged

Check: The reference codes that let a container be collected are shared only with the people who need them, through an authenticated channel, with a limited validity, and every access to them is logged.

Why: Europol's joint report describes criminal networks obtaining container reference codes to collect containers, and asks for need-to-know access and traceability. A shared or leaked code is a stolen box.

Evidence to hold: [ ] Who can see release references on each portal, and the access log

Sources: Europol and partners, Criminal networks in EU ports (5 April 2023)

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

E2 · API keys are per-integration, vaulted and revocable

Check: Each integration has its own API key or client, scoped to what it needs, kept in a secret store rather than in e-mail or a spreadsheet, rotated at a written interval and revocable at once.

Why: A key shared between integrations, or left in a mailbox, cannot be rotated or revoked without breaking everyone, and each copy is a leak waiting to happen. OWASP treats poor credential handling as a top API risk.

Evidence to hold: [ ] The list of API keys and clients, where each is stored, and the last rotation

Sources: OWASP API Security Top 10 (2023); RFC 9700, Best Current Practice for OAuth 2.0 Security (January 2025)

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

E3 · Access can be cut across portals, or only portal by portal

Check: Record honestly whether, when a device is lost or a person is dismissed, you can revoke their access across every portal at once, or whether it has to be done portal by portal, by hand, with the risk of missing one.

Why: Revoking in one place is the main thing a shared identity would give you; measuring the gap today tells you what portal-by-portal offboarding is costing you and whether the concept would be worth it.

Evidence to hold: [ ] Whether a single revocation exists today, and the list of portals it does not reach

Sources: plain practice

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

Sources (public, dated)

OWASP API Security Top 10 (2023 edition), 2023. https://owasp.org/API-Security/editions/2023/en/0x00-header/

OpenID Connect Core 1.0 (incorporating errata set 2), 15 December 2023. https://openid.net/specs/openid-connect-core-1_0.html

OASIS, Assertions and Protocols for SAML V2.0 (OASIS Standard), 15 March 2005. https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

RFC 9700, Best Current Practice for OAuth 2.0 Security, January 2025. https://www.rfc-editor.org/rfc/rfc9700

W3C Web Authentication (WebAuthn) Level 2, Recommendation, 8 April 2021. https://www.w3.org/TR/webauthn-2/

NIST SP 800-63-3, Digital Identity Guidelines, June 2017, updated 2 March 2020. https://pages.nist.gov/800-63-3/sp800-63-3.html

NIST SP 800-63B, Authentication and Lifecycle Management, June 2017, updated 2 March 2020. https://pages.nist.gov/800-63-3/sp800-63b.html

CISA, Implementing Phishing-Resistant MFA (fact sheet), October 2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

Europol and partners, Criminal networks in EU ports, 5 April 2023. https://www.europol.europa.eu/publications-events/publications/criminal-networks-in-eu-ports-risks-and-challenges-for-law-enforcement

33 CFR 101.650, Security measures for access control (eCFR), eCFR, checked 11 November 2026. https://www.ecfr.gov/current/title-33/part-101

Directive (EU) 2022/2555 (NIS2), Article 21, 14 December 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

ASD ACSC, CISA and partners, Best practices for event logging and threat detection, 21 August 2024. https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection

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 self-check, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/api-developers/pca-passport-sso/ . Generic: no terminal, port, client or vendor is named and no figure is invented. This self-check 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.